

ClearPass Guest 6.6



User Guide

Copyright Information

© Copyright 2017 Hewlett Packard Enterprise Development LP.

Open Source Code

This product includes code licensed under the GNU General Public License, the GNU Lesser General Public License, and/or certain other open source licenses. A complete machine-readable copy of the source code corresponding to such code is available upon request. This offer is valid to anyone in receipt of this information and shall expire three years following the date of the final distribution of this product version by Hewlett Packard Enterprise Company. To obtain such source code, send a check or money order in the amount of US \$10.00 to:

Hewlett Packard Enterprise Company
Attn: General Counsel
3000 Hanover Street
Palo Alto, CA 94304
USA

About this Guide	17
Audience	17
Related Documents	17
Conventions	17
Contacting Support	18
ClearPass Guest Overview	19
About ClearPass Guest	19
Visitor Access Scenarios	20
Reference Network Diagram	21
Key Interactions	22
AAA Framework	23
Key Features	24
Visitor Management Terminology	25
ClearPass Guest Deployment Process	26
Operational Concerns	26
Network Provisioning	26
Site Preparation Checklist	27
Security Policy Considerations	28
AirGroup Deployment Process	28
Documentation and User Assistance	29
User Guide and Online Help	29
Context-Sensitive Help	29
Field Help	30
Quick Help	30
If You Need More Assistance	30
Use of Cookies	30
Guest Manager	33
Accessing Guest Manager	33
About Guest Management Processes	34
Sponsored Guest Access	34
Self Provisioned Guest Access	35
Active Sessions Management	35
Session States	37

RFC 3576 Dynamic Authorization	37
Filtering the List of Active Sessions	38
Disconnecting Multiple Active Sessions	39
Sending Multiple SMS Alerts	39
About SMS Guest Account Receipts	40
Using Standard Guest Management Features	41
Creating a Guest Account	41
Changing a Guest Account Role	44
Creating a Guest Account Receipt	44
Creating a Device	45
Creating Devices Manually in ClearPass Guest	45
Creating Devices During Self-Registration - MAC Only	48
Creating Devices During Self-Registration - Paired Accounts	49
Creating Multiple Guest Accounts	50
Creating Multiple Guest Account Receipts	52
Creating a Single Password for Multiple Accounts	54
Exporting Guest Account Information	58
About CSV and TSV Exports	59
About XML Exports	59
Importing Guest Accounts	60
Managing Single Guest Accounts	64
Changing a Guest Account Role	69
Managing Devices	69
Changing a Device's Expiration Date	70
Disabling and Deleting Devices	72
Activating a Device	72
Editing a Device	73
Viewing Current Sessions for a Device	75
Printing Device Details	75
Viewing Device Details	76
Managing Multiple Guest Accounts	76
Changing a Guest Account Role	78
AirGroup Device Registration	78
Registering Groups of Devices or Services	79
Registering Personal Devices	82
AirGroup Time-Based Sharing Syntax Examples	85
Time-Based Syntax Reference	88
About AirGroup Time-Based Sharing	89

Basics of Time-Based Sharing Setup	90
MAC Authentication in ClearPass Guest	91
MAC Address Formats	91
Automatically Registering MAC Devices in ClearPass	92
Importing MAC Devices	93
Advanced MAC Features	93
User Detection on Landing Pages	93
Click-Through Login Pages	94
Onboard	95
Accessing Onboard	95
About ClearPass Onboard	96
Onboard Deployment Checklist	97
Onboard Feature List	99
Supported Platforms	100
Public Key Infrastructure for Onboard	101
Certificate Hierarchy	101
Certificate Configuration in a Cluster	102
Revoking Unique Device Credentials	102
Revoking Credentials to Prevent Network Access	102
Re-Provisioning a Device	103
Network Requirements for Onboard	103
Using Same SSID for Provisioning and Provisioned Networks	104
Using Different SSID for Provisioning and Provisioned Networks	104
Configuring Online Certificate Status Protocol	104
Configuring Certificate Revocation List (CRL)	104
Providing MAC Addresses for Android 6 Devices	105
Network Architecture for Onboard	105
Network Architecture for Onboard when Using ClearPass Guest	106
The ClearPass Onboard Process	107
Devices Supporting Over-the-Air Provisioning	108
Devices Supporting Onboard Provisioning	110
Configuring the User Interface for Device Provisioning	113
Using the {nwa_mdps_config} Template Function	113
Onboard Troubleshooting	114
iOS Device Provisioning Failures	114
Hostname-to-Certificate Match Failures	115
Onboard Interface Not Displayed	116

Certificate Renewal through OS X Mavericks	116
Certificate Authorities	116
Creating a New Certificate Authority	117
Editing Certificate Authority Settings	122
Requesting a Certificate for the Certificate Authority	128
Installing a Certificate Authority's Certificate	128
The Trust Chain and Uploading Certificates for the CA	130
Considerations for iOS Devices	133
Using Microsoft Active Directory Certificate Services	133
Management and Control	136
Device Management (View by Device)	136
Device Management (View by Username)	141
Certificate Management (View by Certificate)	144
Searching for Certificates in the List	146
Working with Certificates in the List	147
Working with Certificate Signing Requests	149
Importing a Code-Signing Certificate	153
Importing a Trusted Certificate	154
Creating a Certificate	155
Requesting a Certificate	159
Onboard Usage	162
Onboard Configuration	163
Network Settings	163
Configuring Basic Network Access Settings	164
Configuring Enterprise Protocol Settings	167
Configuring Device Authentication Settings	170
Configuring Certificate Trust Settings	171
Configuring Windows-Specific Network Settings	174
Configuring Proxy Settings	175
iOS Settings	177
Configuring ActiveSync Settings	178
Configuring AirPlay Settings	181
Configuring AirPrint Settings	183
Configuring APN Settings	184
Configuring Calendar (CalDAV) Settings	185
Configuring Contacts (CardDAV) Settings	187
Configuring Device Restrictions Settings	189
Configuring Email Settings	197

Configuring an iOS Device Passcode Policy	200
Configuring Calendar Subscription Settings	203
Configuring an iOS Device VPN Connection	204
Configuring Web Clips	213
Windows Applications	214
Configuring App Sets	215
Deployment and Provisioning	216
Configuration Profiles	216
Creating and Editing Configuration Profiles	217
Provisioning Settings	220
About Configuring Provisioning Settings	221
Configuring General Provisioning Settings	222
Configuring Provisioning Settings for Supported Devices	227
Configuring Provisioning Settings for the Web Login Page	229
Configuring Provisioning Settings for Instructions and Messages	238
Configuring Provisioning Settings for iOS and OS X Profiles	259
Configuring Options for Onboard Client Devices	261
Configuring Provisioning Settings for Sponsorship Confirmation	265
About the Self-Service Portal	268
Configuration	271
Accessing Configuration	271
Configuring ClearPass Guest Authentication	273
Content Manager	273
Managing Content: Private Files and Public Files	274
Uploading Content	275
Downloading Content	276
Creating a New Content Directory	276
Configuring Guest Manager	277
Default Settings for Account Creation	277
About Fields, Forms, and Views	284
Business Logic for Account Creation	284
Verification Properties	285
Basic User Properties	285
Visitor Account Activation Properties	286
Visitor Account Expiration Properties	287
Other Properties	287
Standard Fields	287

Standard Forms and Views	288
Configuring Access Code Logins	289
Customize Random Username and Passwords	289
Create the Print Template	289
Customize the Guest Accounts Form	291
Create the Access Code Guest Accounts	291
Pages	294
Customizing Fields	294
Creating a Custom Field	295
Customizing AirGroup Registration Forms	302
Customizing Forms and Views	305
Editing Forms and Views	306
Editing Forms	308
Form Field Editor	309
Form Display Properties	310
Form Validation Properties	326
Examples of Form field Validation	328
Advanced Form Field Properties	331
Creating a Single Password for Multiple Accounts	332
Form Field Validation Processing Sequence	333
Editing Views	337
View Field Editor	339
Customizing Guest Self-Registration	341
Accessing the Guest Self-Registration Customization Forms	342
Self-Registration Sequence Diagram	346
Editing Self-Registration Pages	347
Creating a Self-Registration Page	348
Configuring Basic Properties for Self-Registration	350
Editing Registration Page Properties	353
Editing the Default Self-Registration Form Settings	355
Editing Guest Receipt Page Properties	357
Editing Receipt Actions	358
Editing Sponsor Confirmation	365
Editing Login Page Properties	373
Editing Social Logins Properties	379
Enabling and Editing NAS Login Properties	384
Self-Service Portal Properties	386
Resetting Passwords with the Self-Service Portal	394

Managing Web Logins	396
Creating and Editing Web Login Pages	397
About Multi-Factor Authentication	412
Managing Web Pages	414
The Web Page Templates	415
Creating and Editing Simple Web Pages	417
Receipts	419
Digital Passes	420
About Digital Passes	420
Viewing Digital Pass Certificates	424
Installing Digital Pass Certificates	425
Managing Digital Passes	426
Creating and Editing a Digital Pass Template	427
Example Template Code Variables	433
Images in Digital Passes	434
Email Receipts and SMTP Services	435
About Email Receipts	435
Configuring Email Receipts	438
Email Receipt Options	438
About Customizing SMTP Email Receipt Fields	440
Customizing SMS Receipt	442
SMS Receipt Fields	443
Customizing Print Templates	444
Creating New Print Templates	445
Print Template Wizard	448
Modifying Wizard-Generated Templates	451
Setting Print Template Permissions	451
SMS Services	453
Viewing SMS Gateways	454
Creating or Editing an SMS Gateway	454
Sending an SMS	460
About SMS Credits	460
About SMS Guest Account Receipts	461
About SMS Receipt Options	462
Working with the Mobile Carriers List	462
About Translations	465
Translation Packs	466
Creating and Editing Translation Packs	467

Translation Assistant	468
Customizing Translated User Interface Text	469
Advertising Services	473
About Advertising Services	473
Materials	473
Promotions	473
Campaigns	474
Spaces	474
Pages	474
Advertising Services Process Overview	474
About the Tutorial	474
Navigating the Tutorial	475
Advertising Pages	476
Editing Advertising Pages	477
The nwa_adspace Smarty Template Tag	481
Advertising Spaces	484
Creating and Editing Advertising Spaces	486
"Other Location" Example	488
"Maximum Height" Example	490
"Maximum Width" Example	491
Advertising Campaigns	492
Creating and Editing Advertising Campaigns	493
Campaign Rank and Weight	496
Advertising Promotions	496
Creating and Editing Advertising Promotions	497
Using Labels in Advertising Services	501
Advertising Materials	502
Creating and Editing Advertising Materials	503
Hotspot Manager	507
Accessing Hotspot Manager	507
About Hotspot Management	508
Managing the Hotspot Sign-up Interface	508
Captive Portal Integration	511
Managing Hotspot Plans	511
Editing or Creating a Hotspot Plan	512
Managing Transaction Processors	516
Occupied Room List	518

Re-Synchronizing Rooms	519
Creating a New Transaction Processor	520
Managing Customer Information	524
Managing Hotspot Invoices	524
Customizing the User Interface	526
Customizing Visitor Sign-Up Page One	526
Customizing Visitor Sign-Up Page Two	529
Customizing Visitor Sign-Up Page Three	533
Viewing the Hotspot User Interface	534
Administration	537
Accessing Administration	537
AirGroup Services	538
AirGroup Controllers	538
Creating and Editing AirGroup Controllers	540
Configuring AirGroup Services	542
AirGroup Diagnostics	543
Creating AirGroup Administrators	545
Creating AirGroup Operators	545
Authenticating AirGroup Users via LDAP	545
Configuring LDAP User Search for AirGroup	545
LDAP User Search Architecture for AirGroup	546
User Search Workflow for AirGroup	546
Configuration Summary for AirGroup	546
Basic LDAP Server Settings for AirGroup	546
User Search Settings for AirGroup	548
Configuring the AirGroup Shared User Field	549
Select2 Options Details	551
Select2 Hook Details	552
MACTrac Services	553
Creating MACTrac Operators	554
Managing MACTrac Devices	555
Registering MACTrac Devices	557
About MAC Addresses	558
Automatically Supplying the MACTrac Device Address	559
API Services	560
API Clients	560
Creating and Editing API Clients	561

API Explorer	564
Setting API Privileges in Operator Profiles	565
About OAuth	566
OAuth Basics	566
OAuth2 Client or App for OAuth	567
Client ID and Secret for OAuth	567
Redirect URI	567
Authorization Grant Types for OAuth	568
Application Service Accounts for OAuth	569
SOAP Web Services and API	570
Viewing Available Web Services	570
SOAP API Introduction	572
Audience	572
API Documentation Overview	572
Disclaimer	572
About the SOAP API	572
Using the SOAP API	575
Integration Example	577
API Documentation	582
The XML-RPC Interface and API	597
About the XML-RPC API	597
Accessing the API	600
Invoking the API	603
Method Summary	604
API Documentation	604
Data Retention	622
3.9 Configuration Import	622
Creating a Customized Configuration Backup	623
Uploading the 3.9 Backup File	623
Restoring Configuration Items	625
Viewing Imported Item Details	627
Import Information for Specific Import Items	629
Import Information: AirGroup Services	629
Import Information: Cisco IP Phones	629
Import Information: Guest Manager	629
Import Information: High Availability (HA)	630
Import Information: Hotspot Manager	631
Import Information: Onboard	631

Import Information: Operator Logins	631
Import Information: Palo Alto Network Services	631
Import Information: RADIUS Services	631
Import Information: Reporting Manager Definitions	633
Import Information: Server Configuration	633
Import Information: SMS Services	634
Import Information: SMTP Services	634
Plugin Manager	635
Viewing Available Plugins	635
Configuring Plugins	636
Configuring AirGroup Services	638
Configuring the API Framework Plugin	639
Configuring the Aruba ClearPass Skin Plugin	641
Configuring the Guest Manager Plugin	644
Configuring the IP Phone Services Plugin	650
Configuring the Kernel Plugin	651
Configuring the MAC Authentication Plugin	653
Configuring the Platform Services Plugin	654
Configuring the SMS Services Plugin	654
Configuring the SMTP Services Plugin	657
Configuring the Translations Plugin	659
Configuring the Web Analytics Plugin	660
Configuring the SOAP Web Services Plugin	661
Support	662
Viewing the Application Log	663
Exporting the Application Log	665
Contacting Support	665
Viewing Documentation	666
Operator Logins	667
Accessing Operator Logins	667
About Operator Logins	667
Role-Based Access Control for Multiple Operator Profiles	668
Operator Logins Configuration	668
Operator Login UI Area	668
Advanced Options Area	670
Operator Profiles	671
Creating an Operator Profile	673

Operators Supported in Filters	676
Configuring the User Interface	676
Operator Profile Privileges	679
Configuring AirGroup Operator Device Limit	679
Local Operator Authentication	680
Creating a New Operator	680
External Operator Authentication	680
Managing LDAP Operator Authentication Servers	681
Viewing the LDAP Server List	681
Creating an LDAP Server	683
Advanced LDAP URL Syntax	686
LDAP Operator Server Troubleshooting	687
Testing Connectivity	687
Testing Operator Login Authentication	687
Looking Up Sponsor Names	688
Troubleshooting Error Messages	688
LDAP Translation Rules	689
Configuring LDAP Translation Rules	690
Custom LDAP Translation Processing	693
Reference	697
Basic HTML Syntax	697
Standard HTML Styles	698
Smarty Template Syntax	700
Basic Template Syntax	700
Text Substitution	700
Template File Inclusion	700
Comments	700
Variable Assignment	700
Conditional Text Blocks	701
Script Blocks	701
Repeated Text Blocks	701
Foreach Text Blocks	701
Modifiers	702
Predefined Template Functions	703
dump	703
nwa_commandlink	703
nwa_iconlink	704

nwa_icontext	704
nwa_quotejs	705
nwa_radius_query	705
Advanced Developer Reference	712
nwa_assign	712
nwa_bling	712
nwa_makeid	712
nwa_nav	713
nwa_plugin	714
nwa_privilege	715
nwa_replace	715
nwa_text	715
nwa_userpref	715
nwa_youtube	716
Date/Time Format Syntax	716
nwdateformat Modifier	716
nwatimeformat Modifier	717
Date/Time Format String Reference	718
Programmer's Reference	719
NwaAlnumPassword	719
NwaBoolFormat	719
NwaByteFormat	720
NwaByteFormatBase10	720
NwaComplexPassword	720
NwaCsvCache	720
NwaDigitsPassword(\$len)	720
NwaDynamicLoad	720
NwaGeneratePictureString	721
NwaGenerateRandomPasswordMix	721
NwaLettersDigitsPassword	721
NwaLettersPassword	721
NwaMoneyFormat	721
NwaParseCsv	722
NwaParseXml	722
NwaPasswordByComplexity	723
NwaSmsIsValidPhoneNumber	723
NwaStrongPassword	723
NwaVLookup	723

NwaWordsPassword	724
Field, Form, and View Reference	724
GuestManager Standard Fields	725
Hotspot Standard Fields	733
SMS Services Standard Fields	734
SMTP Services Standard Fields	734
Format Picture String Symbols	736
Form Field Validation Functions	737
Form Field Conversion Functions	744
Form Field Display Formatting Functions	745
View Display Expression Technical Reference	747
LDAP Standard Attributes for User Class	748
Regular Expressions	749
Chromebook in Onboard	751
About Chromebook in Onboard	751
Caveats and Recommendations	752
Google Admin Chromebook License is Required	752
Managed Chromebook Deployment is Required	752
Chrome Extension is Required	752
Chromebook Release 37 or Later is Required	752
Chromebook Supports Only “Created by Device” Certificates	753
A Separate Provisioning SSID is Required	753
Directory-Based Authentication Source is Recommended	754
Onboard Configuration for Chromebook	754
Enable Chromebook Provisioning	754
Configure Instructions and Messages	755
Google Admin Configuration for Chromebook	755
Configuring the Chrome extension	755
Configuring Network Settings	757
Glossary	761
Index	779

ClearPass Guest 6.6 provides a simple and personalized user interface through which operational staff can quickly and securely manager visitor network access. An [HTML version](#) of this User Guide is also available.

Audience

This User Guide is intended for system administrators and people who are installing and configuring ClearPass Guest 6.6 as their visitor management solution. It describes the installation and configuration process.

Related Documents

The following documents are part of the complete documentation set for the ClearPass platform:

- *ClearPass Guest 6.6 User Guide*
- *ClearPass Policy Manager 6.6 User Guide*
- *ClearPass Deployment Guide*
- *ClearPass 6.6.x Release Notes*
- *ClearPass Insight 6.6 User Guide*
- *ClearPass Policy Manager 6.6 Getting Started Guide*
- *ClearPass Policy Manager Configuration API Guide*
- *ClearPass Policy Model: An Introduction*
- *Tech Note: Installing or Upgrading ClearPass 6.6 on a Virtual Machine*
- *Tech Note: Upgrading to ClearPass 6.6*

Conventions

The following conventions are used throughout this guide to emphasize important concepts:

Table 1: *Typographical Conventions*

Type Style	Description
<i>Italics</i>	This style is used to emphasize important terms and to mark the titles of books.
<code>System items</code>	This fixed-width font depicts the following: <ul style="list-style-type: none"> • Sample screen output • System prompts • Filenames, software devices, and specific commands when mentioned in the text
Commands	In the command examples, this bold font depicts text that you must type exactly as shown.
<code><Arguments></code>	In the command examples, italicized text within angle brackets represents items that you should replace with information appropriate to your specific situation. For example:

Type Style	Description
	# send <text message> In this example, you would type “send” at the system prompt exactly as shown, followed by the text of the message you wish to send. Do not type the angle brackets.
[Optional]	Command examples enclosed in brackets are optional. Do not type the brackets.
{Item A Item B}	In the command examples, items within curled braces and separated by a vertical bar represent the available choices. Enter only one choice. Do not type the braces or bars.

The following informational icons are used throughout this guide:



Indicates helpful suggestions, pertinent information, and important things to remember.



Indicates a risk of damage to your hardware or loss of data.



Indicates a risk of personal injury or death.

Contacting Support

Main Site	arubanetworks.com
Support Site	support.arubanetworks.com
Airheads Social Forums and Knowledge Base	community.arubanetworks.com
North American Telephones	1-800-943-4526 (Toll Free) 1-408-754-1200
International Telephones	arubanetworks.com/support-services/contact-support/
Software Licensing Site	licensing.arubanetworks.com
End-of-life Information	arubanetworks.com/support-services/end-of-life/
Security Incident Response Team (SIRT)	arubanetworks.com/support-services/security-bulletins/

This chapter explains the terms, concepts, processes, and equipment involved in managing visitor access to a network, and helps you understand how ClearPass Guest 6.6 can be successfully integrated into your network infrastructure. It is intended for network architects, IT administrators, and security consultants who are planning to deploy visitor access, or who are in the early stages of deploying a visitor access solution.

This chapter includes the following sections:

- "About ClearPass Guest" on page 19
- "Visitor Access Scenarios" on page 20
- "Reference Network Diagram" on page 21
- "Key Interactions" on page 22
- "AAA Framework" on page 23
- "Key Features" on page 24
- "Visitor Management Terminology" on page 25
- "ClearPass Guest Deployment Process" on page 26
- "AirGroup Deployment Process" on page 28
- "Documentation and User Assistance" on page 29
- "Use of Cookies" on page 30

About ClearPass Guest

ClearPass Guest 6.6 provides a simple and personalized user interface through which operational staff can quickly and securely manage visitor network access. It gives your non-technical staff controlled access to a dedicated visitor management user database. Through a customizable Web portal, your staff can easily create an account, reset a password, or set an expiry time for visitors. Access permissions to ClearPass Guest functions are controlled through an operator profile that can be integrated with an LDAP server or Active Directory login.

Visitors can be registered at reception and provisioned with an individual guest account that defines their visitor profile and the duration of their visit. The visitor can be given a printed customized receipt with account details, or the receipt can be delivered wirelessly using the integrated SMS services. Companies are also able to pre-generate custom scratch cards, each with a defined network access time, which can then be handed out in a corporate environment or sold in public access scenarios.

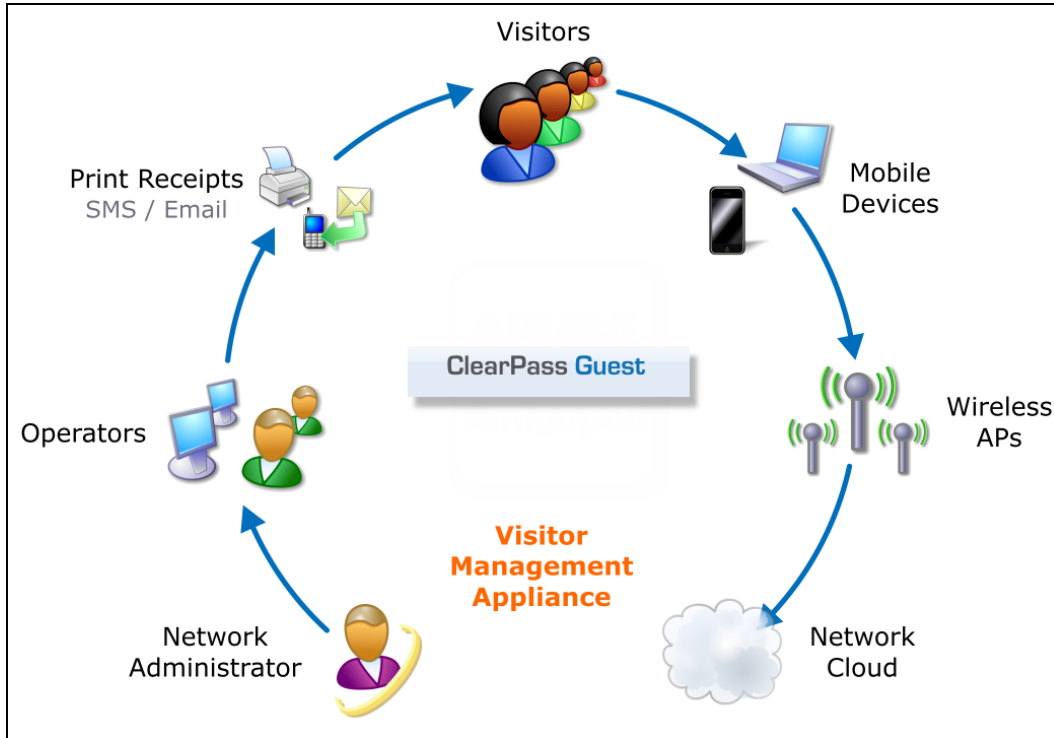
You can use the customization features to define settings that allow your visitors to self-provision their own guest accounts. Visitors register through a branded and customized Web portal, ensuring a streamlined and professional experience. Surveys can also be presented during the self-registration process and the data stored for later analysis and reporting, providing additional insight to your visitors and their network usage.

ClearPass Guest integrates with all leading wireless and NAC solutions through a flexible definition point, ClearPass Policy Manager. This ensures that IT administrators have a standard integration with the network security framework, but gives operational staff the user interface they require.

Visitor Access Scenarios

The following figure shows a high-level representation of a typical visitor access scenario.

Figure 1 Visitor Access Using ClearPass Guest



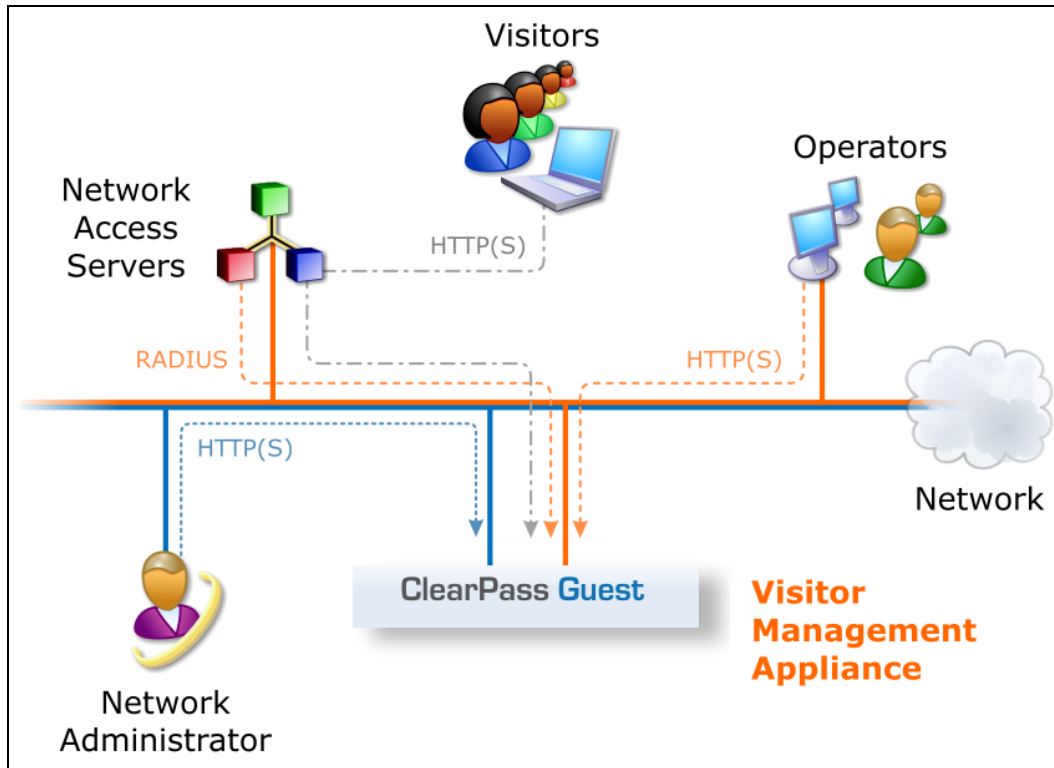
In this scenario, visitors are using their own mobile devices to access a corporate wireless network. Because access to the network is restricted, visitors must first obtain a username and password. A guest account may be provisioned by a corporate operator such as a receptionist, who can then give the visitor a print receipt that shows their username and password for the network.

When visitors use self-registration, as might be the case for a network offering public access, the process is broadly similar but does not require a corporate operator to create the guest account. The username and password for a self-provisioned guest account may be delivered directly to the visitor's Web browser, or sent via SMS or email.

Reference Network Diagram

The following figure shows the network connections and protocols used by ClearPass Guest.

Figure 2 Reference Network Diagram for Visitor Access

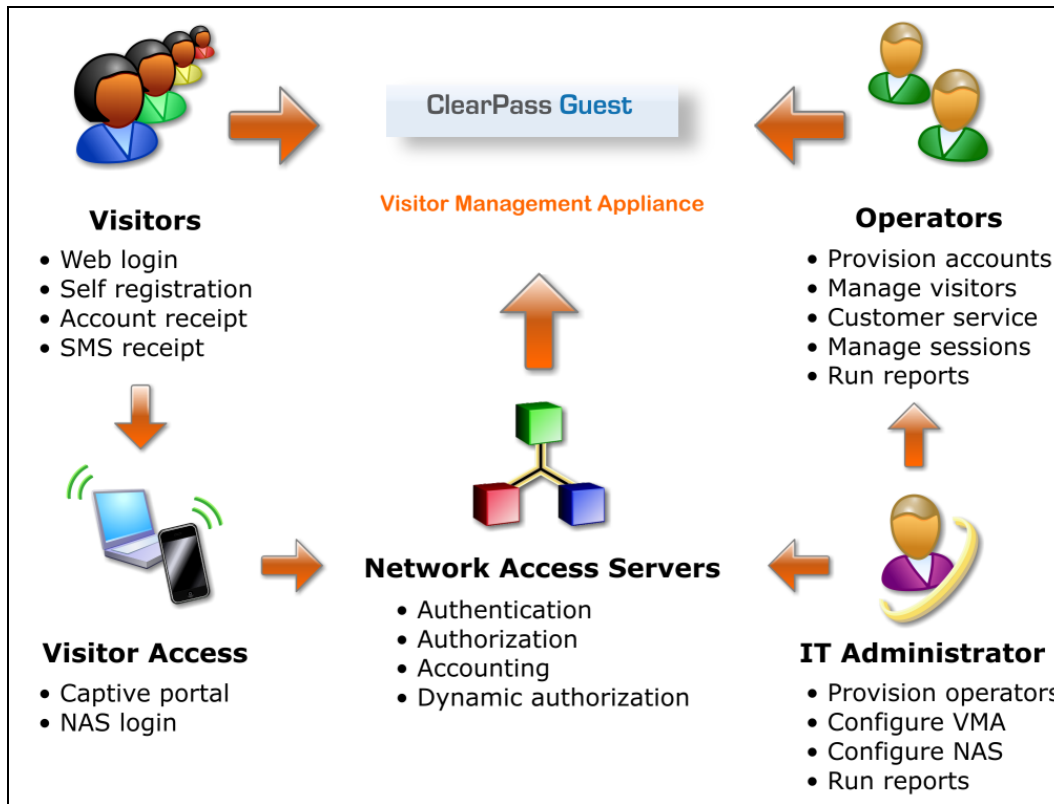


The network administrator, operators, and visitors may use different network interfaces to access the visitor management features. The exact topology of the network and the connections made to it will depend on the type of network access offered to visitors and the geographical layout of the access points.

Key Interactions

The following figure shows the key interactions between ClearPass Guest and the people and other components involved in providing guest access.

Figure 3 *Interactions Involved in Guest Access*



ClearPass Guest is part of your network's core infrastructure and manages guest access to the network.

NAS devices, such as wireless access points and wired switches on the edge of the network, use the RADIUS protocol to ask ClearPass Policy Manager to authenticate the username and password provided by a guest logging in to the network. If authentication is successful, the guest is then authorized to access the network.

Roles are assigned to a guest as part of the context ClearPass Policy Manager uses to apply its policies. RADIUS attributes that define a role's access permissions are contained within Policy Manager's Enforcement Profile. Additional features such as role mapping for ClearPass Guest can be performed in ClearPass Policy Manager.

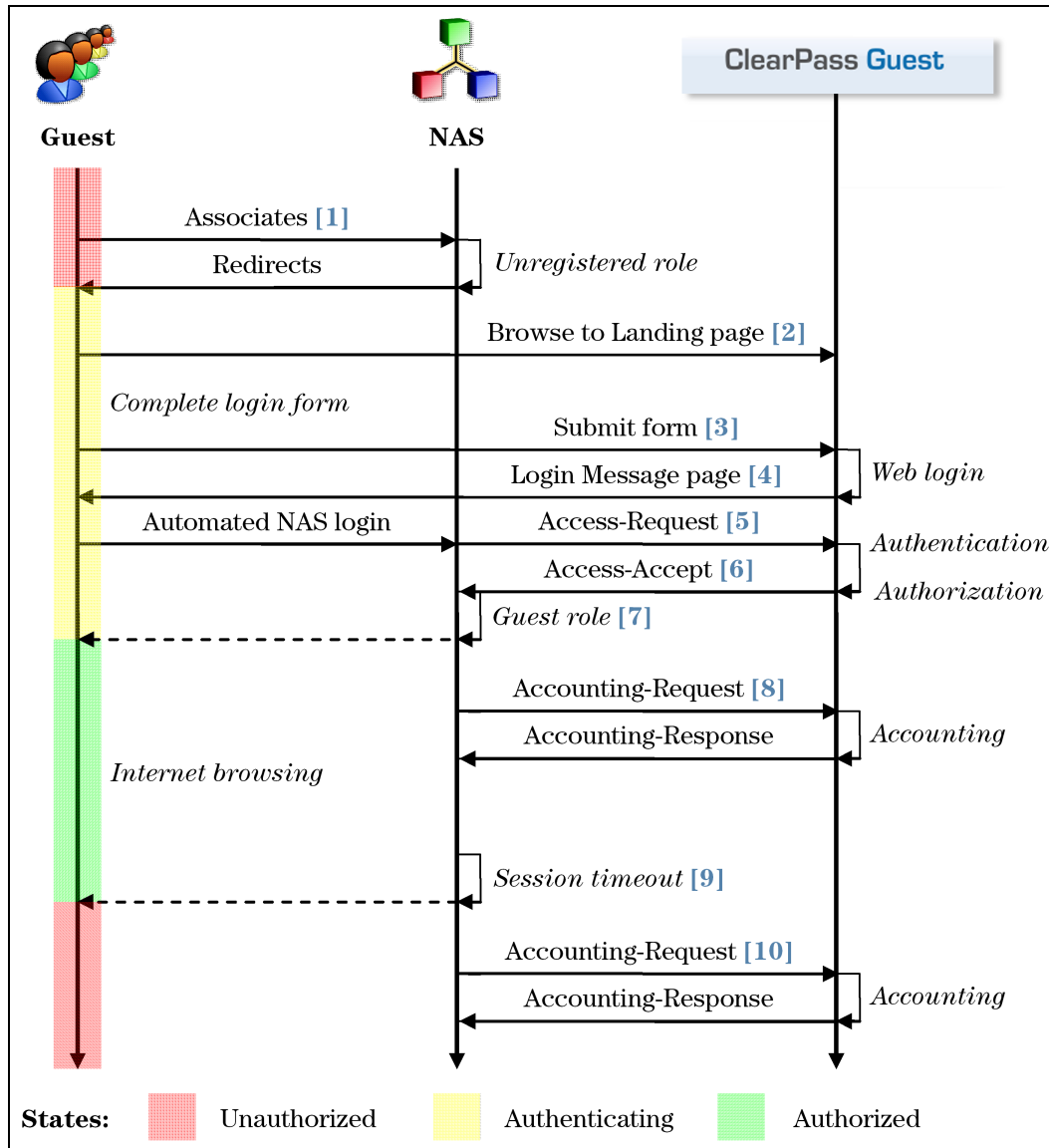
The network usage of authorized guests is monitored by the NAS and reported in summary form to ClearPass Policy Manager using RADIUS accounting, which allows administrators to generate network reports in ClearPass Insight.

AAA Framework

ClearPass Guest is built on the industry standard AAA framework, which consists of authentication, authorization, and accounting components.

The following figure shows how the different components of this framework are employed in a guest access scenario.

Figure 4 Sequence Diagram for Network Access Using AAA



In the standard AAA framework, network access is provided to a user according to the following process:

- The user connects to the network by associating with a local access point [1].
- A landing page is displayed to the user [2] which allows them to log in to the NAS [3], [4] using the login name and password of their guest account.
- The NAS authenticates the user with the RADIUS protocol [5].
- ClearPass Policy Manager determines whether the user is authorized, and, if so, returns vendor-specific attributes [6] that are used to configure the NAS based on the user's role and other policies [7].

- If the user's access is granted, the NAS permits the guest access to the network based on the settings provided by the ClearPass Policy Manager server.
- The NAS reports details about the user's session to the ClearPass Policy Manager server using RADIUS accounting messages [8].
- After the user's session times out [9], the NAS will return the user to an unauthorized state and finalize the details of the user's session with an accounting update [10].

Key Features

Refer to the table below for a list of key features and a cross-reference to the relevant section of this User Guide.

Table 2: *List of Key Features*

Feature	Reference
Visitor Access	
Web server providing content delivery for guests	"Managing Content: Private Files and Public Files" on page 274
Guest self-registration	"Customizing Guest Self-Registration" on page 341
Visitor Management	
Create and manage visitor accounts, individually or in groups	"Using Standard Guest Management Features" on page 41
Manage active RADIUS sessions using RFC 3576 Dynamic Authorization support	"Active Sessions Management" on page 35
Import and export visitor accounts	"Importing Guest Accounts" on page 60
Create guest self-registration forms	"Creating a Self-Registration Page" on page 348
Configure a self-service portal for guests	"Self-Service Portal Properties" on page 386
Local printer, SMS or email delivery of account receipts	"Editing Guest Receipt Page Properties" on page 357
Visitor Account Features	
Independent activation time, expiration time, and maximum usage time	"Business Logic for Account Creation" on page 284
Define unlimited custom fields	"Customizing Fields" on page 294
Username up to 64 characters	"GuestManager Standard Fields" on page 725

Feature	Reference
Customization Features	
Create new fields and forms for visitor management	"Customizing Forms and Views" on page 305
Use built-in data validation to implement visitor survey forms	"Form Validation Properties" on page 326
Create print templates for visitor account receipts	"Editing Guest Receipt Page Properties" on page 357
Administrative Management Features	
Operators defined and authenticated locally	"Local Operator Authentication" on page 680
Operators authenticated via LDAP	"External Operator Authentication" on page 680
Role based access control for operators	"Operator Profiles" on page 671
Plugin-based application features, automatically updated by ClearPass Policy Manager	"Plugin Manager" on page 635
User Interface Features	
Context-sensitive help with searchable online documentation	"Documentation and User Assistance" on page 29

Visitor Management Terminology

The following table describes the common terms used in ClearPass Guest and this guide.

Table 3: *Common Terms*

Term	Explanation
Accounting	Process of recording summary information about network access by users and devices.
Authentication	Verification of a user's credentials; typically a username and password.
Authorization	Controls the type of access that an authenticated user is permitted to have.
Captive Portal	Implemented by a Network Access Server to restrict network access to authorized users only.
Field	In a user interface or database, a single item of information about a user account.
Form	In a user interface, a collection of editable fields displayed to an operator.
Network Access Server	Device that provides network access to users, such as a wireless access point, network switch, or dial-in terminal server. When a user connects to the NAS device, a RADIUS access request is generated by the NAS.

Term	Explanation
Operator Profile	Characteristics assigned to a class of operators, such as the permissions granted to those operators.
Operator/Operator Login	User of ClearPass Guest to create guest accounts or perform system configuration.
Print Template	Formatted template used to generate guest account receipts.
Role	Type of access being granted to visitors. You can define multiple roles. Such roles could include employee, guest, team member, or press.
Sponsor	Operator
User Database	Database listing the guest accounts in ClearPass Guest.
View	In a user interface, a table displaying data, such as visitor account information, to operators.
Visitor/Guest	Someone who is permitted to access the Internet through your Network Access Server.
Visitor Account	Settings for a visitor stored in the user database, including username, password and other fields.
Web Login/NAS Login	Login page displayed to a guest user.

ClearPass Guest Deployment Process

As part of your preparations for deploying a visitor management solution, you should consider the following areas:

- Management decisions about security policy
- Decisions about the day-to-day operation of visitor management
- Technical decisions related to network provisioning

Operational Concerns

When deploying a visitor management solution, you should consider these operational concerns:

- Who is going to be responsible for managing guest accounts? What privileges will the guest account manager have? Will this person only create guest accounts or will this person also be permitted access to reports?
- Do you want guests to be able to self-provision their own network access? What settings should be applied to self-provisioned visitor accounts?
- How will operator logins be provisioned? Should operators be authenticated against an LDAP server?
- Who will manage reporting of guest access? What are the reports of interest? Are any custom reports needed?

Network Provisioning

ClearPass Guest requires provisioning the following:

- Physical location – rack space, power and cooling requirements; or deployment using virtualization

- Network connectivity – VLAN selection, IP address, and hostname
- Security infrastructure – SSL certificate

Site Preparation Checklist

The following is a checklist of the items that should be considered when setting up ClearPass Guest.

Table 4: *Site Preparation Checklist*

✓	Policy Decision
Security Policy	
	Segregated guest accounts?
	Type of network access?
	Time of day access?
	Bandwidth allocation to guests?
	Prioritization of traffic?
	Different guest roles?
	IP address ranges for operators?
	Enforce access via HTTPS?
Operational Concerns	
	Who will manage guest accounts?
	Guest account self provisioning?
	What privileges will the guest managers have?
	Who will be responsible for printing reports?
Network Management Policy	
	Password format for guest accounts?
	Shared secret format?
	Operator provisioning?
Network Provisioning	
	Physical location?
	Network connectivity?
	Security infrastructure?

Security Policy Considerations

To ensure that your network remains secure, decisions have to be made regarding guest access:

- Do you wish to segregate guest access? Do you want a different VLAN, or different physical network infrastructure to be used by your guests?
- What resources are you going to make available to guests (for example, type of network access; permitted times of day; bandwidth allocation)?
- Will guest access be separated into different roles? If so, what roles are needed?
- How will you prioritize traffic on the network to differentiate quality of service for guest accounts and non-guest accounts?
- What will be the password format for guest accounts? Will you be changing this format on a regular basis?
- What requirements will you place on the shared secret, between NAS and the RADIUS server to ensure network security is not compromised?
- What IP address ranges will operators be using to access the server?
- Should HTTPS be required in order to access the visitor management server?

AirGroup Deployment Process

AirGroup allows users to register their personal mobile devices on the local network and define a group of friends or associates who are allowed to share them. You use ClearPass Guest to define AirGroup administrators and operators. AirGroup administrators can then use ClearPass Guest to register and manage an organization's shared devices and configure access according to username, role, location, or time. AirGroup operators (end users) can use ClearPass Guest to register their personal devices and define the group who can share them.

[Table 5](#) summarizes the steps for configuring Aruba AirGroup functionality in ClearPass Guest. Details for these steps are provided in the relevant sections of this Guide. This table does not include the configuration steps performed in ClearPass Policy Manager or the ArubaOS controller. For complete AirGroup deployment information, refer to the AirGroup sections in the *ArubaOS User Guide* and the ClearPass Policy Manager documentation.

Table 5: Summary of AirGroup Configuration Steps in ClearPass Guest

Step	Section in this Guide
Create AirGroup administrators	"Creating a New Operator" on page 680
Create AirGroup operators	
Configure an operator's device limit	"Configuring AirGroup Operator Device Limit" on page 679
Configure an AirGroup controller	"AirGroup Controllers" on page 538
Enable support for dynamic notifications	"Configuring AirGroup Services" on page 638
To authenticate AirGroup users via LDAP: Define the LDAP server Define appropriate translation rules	"External Operator Authentication" on page 680 "LDAP Translation Rules" on page 689

Step	Section in this Guide
AirGroup administrator: Register devices or groups of devices	"AirGroup Device Registration" on page 78
AirGroup operator: Register personal devices	
(Optional) Configure device registration form with drop-down lists for existing locations and roles	"Customizing AirGroup Registration Forms" on page 302
Set up time-based sharing	"About AirGroup Time-Based Sharing" on page 89

Documentation and User Assistance

This section describes the variety of user assistance available for ClearPass Guest.

User Guide and Online Help

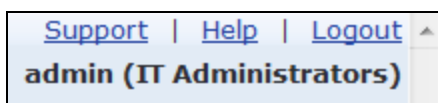
This User Guide provides complete information for all ClearPass Guest features. The following quick links may be useful in getting started.

Table 6: Quick Links

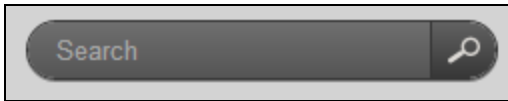
For information about...	Refer to...
What visitor management is and how it works	"About ClearPass Guest" on page 19
Using the guest management features	"Using Standard Guest Management Features" on page 41
Role-based access control for operators	"Operator Profiles" on page 671
Setting up LDAP authentication for operators	"External Operator Authentication" on page 680
Guest self-provisioning features	"Self Provisioned Guest Access" on page 35
Dynamic Authorization extensions	"RFC 3576 Dynamic Authorization" on page 37
SMS receipts for guest accounts	"SMS Services" on page 453
Email receipts for guest accounts	"Email Receipts and SMTP Services" on page 435
Network administration of the appliance	"Administration" on page 537

Context-Sensitive Help

For more detailed information about the area of the application you are using, click the context-sensitive **Help** link displayed at the top right of the page. This opens a new browser tab showing the relevant section of this User Guide.



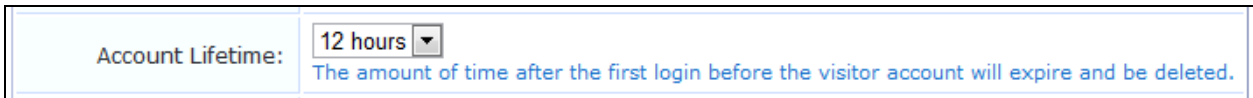
The User Guide may be searched using the **Search** box in the top right corner.




Type in keywords related to your search and click the **Search** button to display a list of matches. The most relevant matches will be displayed first. Words may be excluded from the search by typing a minus sign directly before the word to exclude (for example-exclude). Exact phrase matches may also be searched for by enclosing the phrase in double quotes (for example, "word phrase").

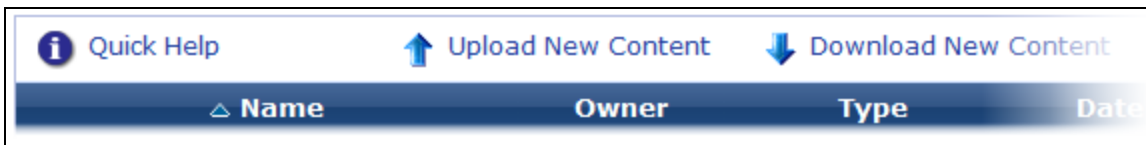
Field Help

The ClearPass Guest user interface has field help built into every form. The field help provides a short summary of the purpose of the field at the point you need it most. In many cases this is sufficient to use the application without further assistance or training.



Quick Help

In list views, click the  **Quick Help** tab located at the top left of the list to display additional information about the list you are viewing and the actions that are available within the list.



On some forms and views, the Quick Help icon may also be used to provide additional detail about a field.

2012-10-09 14:05:57	192.0.2.12	admin	 info	Issued new certificate for 192.0.2.12
2012-10-09 14:05:57	192.0.2.21	admin	 info	Onboard: Signed certificate 13: 192.0.2.21
2012-10-09 13:46:20	192.0.2.09	admin	 info	Operator login: admin

If You Need More Assistance

If you encounter a problem using ClearPass Guest, your first step should be to consult the appropriate section in this User Guide.

If you cannot find an answer here, the next step is to contact your reseller. The reseller can usually provide you with the answer or obtain a solution to your problem.

If you still need information, you can refer to the **Contact Support** command available under **Support** in the user interface, or see "[Contacting Support](#)" on page 18.

Use of Cookies

Cookies are small text files that are placed on a user's computer by Web sites the user visits. They are widely used in order to make Web sites work, or work more efficiently, as well as to provide information to the owners

of a site. Session cookies are temporary cookies that last only for the duration of one user session.

When a user registers or logs in via an Aruba captive portal, Aruba uses session cookies solely to remember between clicks who a guest or operator is. Aruba uses this information in a way that does not identify any user-specific information, and does not make any attempt to find out the identities of those using its ClearPass products. Aruba does not associate any data gathered by the cookie with any personally identifiable information (PII) from any source. Aruba uses session cookies only during the user's active session and does not store any permanent cookies on a user's computer. Session cookies are deleted when the user closes his/her Web browser.



The ability to easily create and manage guest accounts is the primary function of ClearPass Guest. The Guest Manager module provides complete control over the user account creation process.

Guest Manager features for managing guest accounts let you:

- View and manage active sessions
- Create single or multiple guest accounts and receipts
- Create new MAC devices
- Bulk edit accounts
- Export a list of accounts
- Import new accounts from a text file
- View guest accounts and edit individual or multiple guest accounts
- View MAC devices and edit individual or multiple devices

Many features can also be customized. For information on customizing Guest Manager settings, forms and views, guest self-registration, and print templates, see "[Configuration](#)" on page 271.

Accessing Guest Manager

To access ClearPass Guest's guest management features, click the **Guest** link in the left navigation.



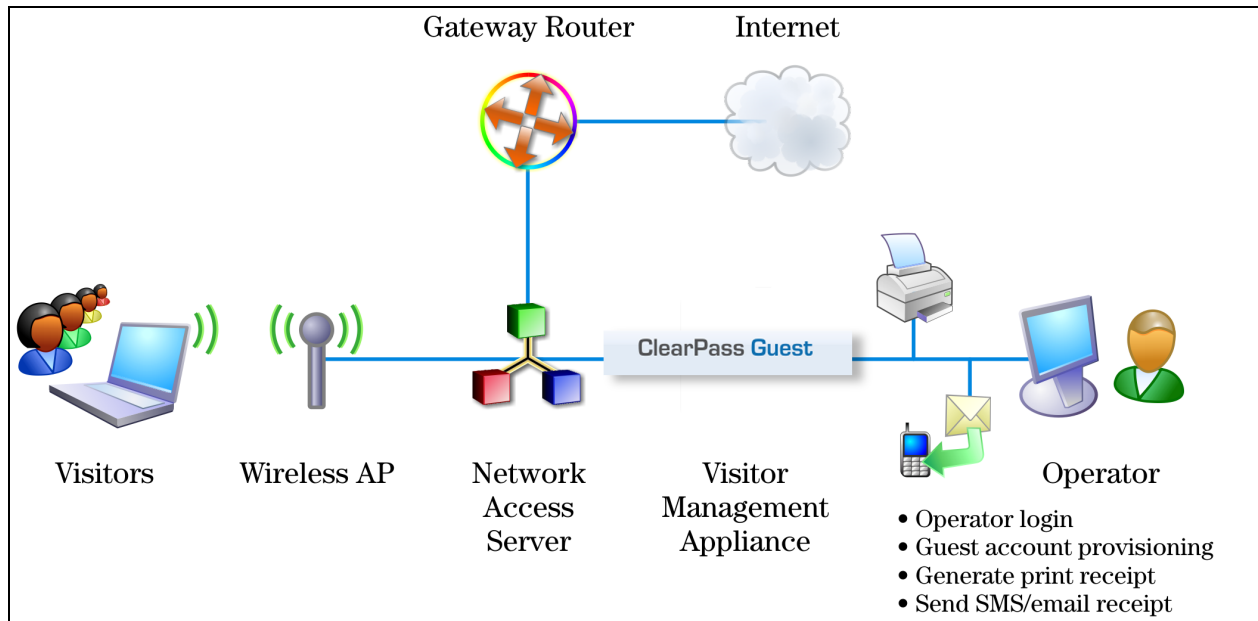
About Guest Management Processes

There are two major ways to manage guest access – either by your operators provisioning guest accounts, or by the guests self-provisioning their own accounts. Both of these processes are described in this chapter.

Sponsored Guest Access

The following figure shows the process of sponsored guest access.

Figure 5 *Sponsored Guest Access with Guest Created by Operator*



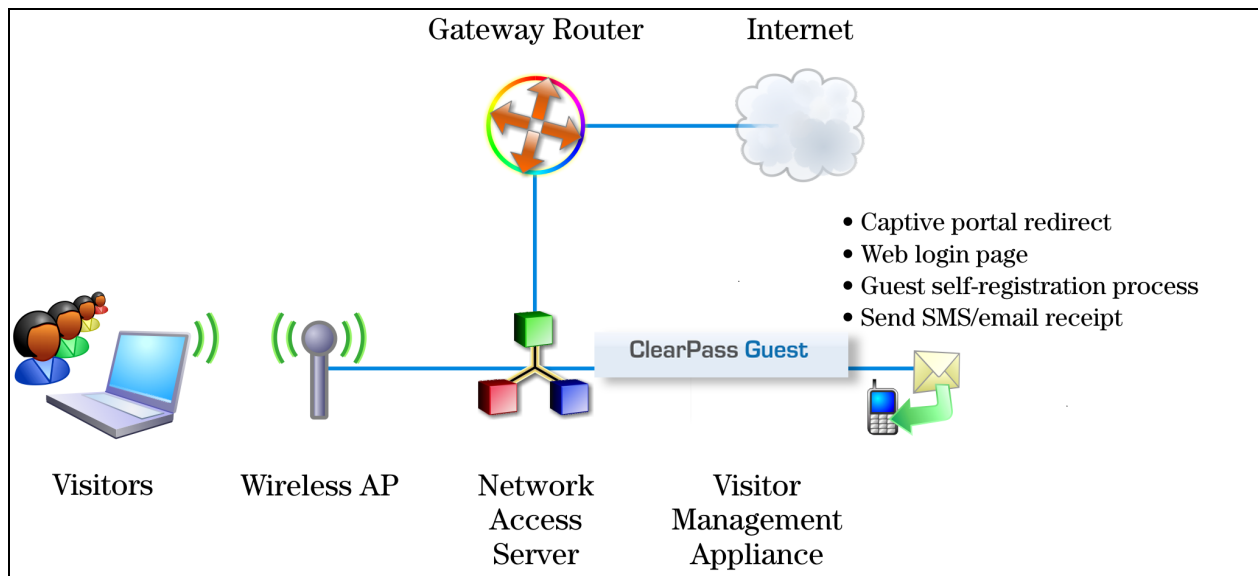
The operator creates the guest accounts and generates a receipt for the account.

The guest logs on to the Network Access Server (NAS) using the credentials provided on her receipt. The NAS authenticates and authorizes the guest's login in ClearPass Guest. After authorization, the guest is able to access the network.

Self Provisioned Guest Access

Self-provisioned access is similar to sponsored guest access, but there is no need for an operator to create the account or to print the receipt. The following figure shows the process of self-provisioned guest access.

Figure 6 Guest Access When Guest is Self-Provisioned



The guest logs on to the Network Access Server (NAS), which captures the guest and redirects them to a captive portal login page. From the login page, guests without an account can browse to the guest self-registration page, where the guest creates a new account. At the conclusion of the registration process, the guest is automatically redirected to the NAS to log in.

The guest can print or download a receipt, or have the receipt information delivered by SMS or email.

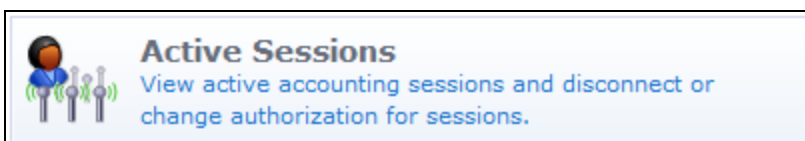
The NAS performs authentication and authorization for the guest in ClearPass Guest. After authorization, the guest is able to access the network.

See "[Customizing Guest Self-Registration](#)" on page 341 for details on creating and managing self-registration pages.

Active Sessions Management



The RADIUS server maintains a list of active visitor sessions. If your NAS equipment has RFC 3576 support, the RADIUS Dynamic Authorization extensions allow you to disconnect or modify an active session. For more information, see "[RFC 3576 Dynamic Authorization](#)" on page 37.



To view and manage active sessions for the RADIUS server, go to **Guest > Active Sessions**. The Active Sessions list opens. Click a session's row in the list for more options. You can use this list to modify, disconnect

or reauthorize, or send SMS notifications for active visitor sessions; manage multiple sessions; or customize the list to include additional fields.

Figure 7 *The Active Sessions List View*

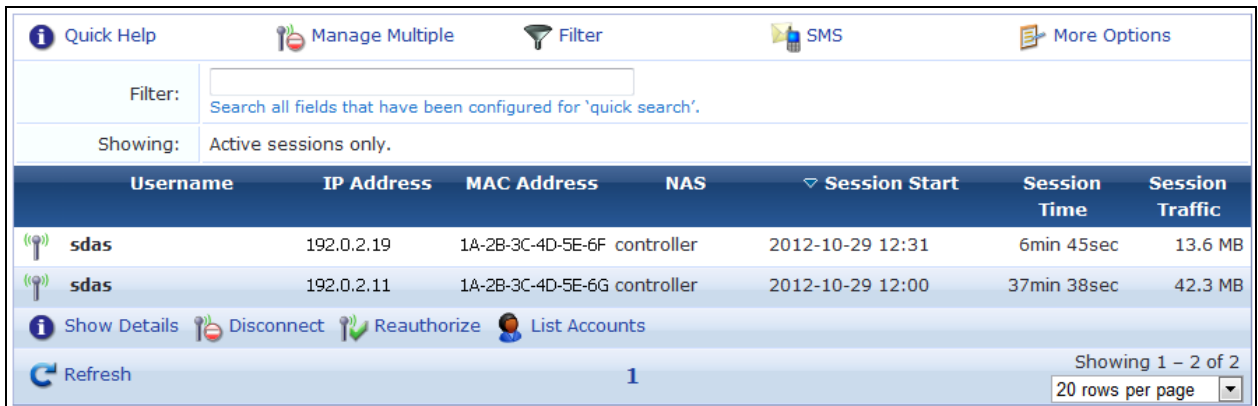




Table 7: *Active Sessions List View*


Field	Description																												
Show Details	Lets you view details for an active session. <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th colspan="2" style="background-color: #003366; color: white; text-align: center;">Session Details</th> </tr> </thead> <tbody> <tr><td style="text-align: right;">Username:</td><td>test</td></tr> <tr><td style="text-align: right;">IP Address:</td><td>192.0.2.11</td></tr> <tr><td style="text-align: right;">NAS:</td><td>controller</td></tr> <tr><td style="text-align: right;">NAS IP Address:</td><td>192.0.2.3</td></tr> <tr><td style="text-align: right;">NAS Port Type:</td><td>Wireless-802.11</td></tr> <tr><td style="text-align: right;">Calling Station ID:</td><td>70DEE2C723B6</td></tr> <tr><td style="text-align: right;">Called Station ID:</td><td>000B866D1F58</td></tr> <tr><td style="text-align: right;">Service Type:</td><td>Onboard Service</td></tr> <tr><td style="text-align: right;">Session ID:</td><td>R0000017f-01-508ef9f4</td></tr> <tr><td style="text-align: right;">Session Upload:</td><td>707,722 bytes</td></tr> <tr><td style="text-align: right;">Session Download:</td><td>45,361,239 bytes</td></tr> <tr><td style="text-align: right;">Session End:</td><td>2012-10-29 14:51</td></tr> <tr><td style="text-align: right;">Termination Cause:</td><td>Lost-Service</td></tr> </tbody> </table> </div>	Session Details		Username:	test	IP Address:	192.0.2.11	NAS:	controller	NAS IP Address:	192.0.2.3	NAS Port Type:	Wireless-802.11	Calling Station ID:	70DEE2C723B6	Called Station ID:	000B866D1F58	Service Type:	Onboard Service	Session ID:	R0000017f-01-508ef9f4	Session Upload:	707,722 bytes	Session Download:	45,361,239 bytes	Session End:	2012-10-29 14:51	Termination Cause:	Lost-Service
Session Details																													
Username:	test																												
IP Address:	192.0.2.11																												
NAS:	controller																												
NAS IP Address:	192.0.2.3																												
NAS Port Type:	Wireless-802.11																												
Calling Station ID:	70DEE2C723B6																												
Called Station ID:	000B866D1F58																												
Service Type:	Onboard Service																												
Session ID:	R0000017f-01-508ef9f4																												
Session Upload:	707,722 bytes																												
Session Download:	45,361,239 bytes																												
Session End:	2012-10-29 14:51																												
Termination Cause:	Lost-Service																												
Disconnect	Disconnects an active session. A message is displayed to show that the disconnect is in progress and to acknowledge when it is complete.																												
Reauthorize	Reauthorizes a session that was disconnected. The Reauthorize Session form opens. Click the Reauthorize Session button on the form.																												
Manage	To disconnect multiple sessions, click the tab. The form expands to include the Manage Multiple																												

Table 7: Active Sessions List View(Continued)



Field	Description
Multiple	Sessions form. For more information, see " Disconnecting Multiple Active Sessions " on page 39.
List Accounts	To view and work with the guest accounts associated with a session, click the session's row in the list, then click its link. The Guest Manager Accounts view opens. See " Managing Single Guest Accounts " on page 64 for more information.
Filter	To display only sessions that meet certain criteria, click the tab. For more information, see " Filtering the List of Active Sessions " on page 38.
SMS	To send SMS notifications to visitors, click the tab. For more information, see " Sending Multiple SMS Alerts " on page 39.
More Options	To include additional fields in the Active Sessions list, or delete fields from it, click the  tab. The Customize View Fields page opens. For more information, see " Editing Forms " on page 308.
Paging Control	You can use the paging control at the bottom of the list to jump forwards or backwards by one page, or to the first or last page of the list. You can also click an individual page number to jump directly to that page. 

Session States

A session may be in one of three possible states:

-  **Active**—An active session is one for which the RADIUS server has received an accounting start message and has not received a stop message, which indicates that service is being provided by a NAS on behalf of an authorized client.


While a session is in progress, the NAS sends interim accounting update messages to the RADIUS server. This maintains up-to-date traffic statistics and keeps the session active. The frequency of the accounting update messages is configurable in the RADIUS server.


-  **Stale**—If an accounting stop message is never sent for a session—for example, if the visitor does not log out—that session will remain open. After 24 hours without an accounting update indicating session traffic, the session is considered 'stale' and is not counted towards the active sessions limit for a visitor account. To ensure that accounting statistics are correct, you should check the list for stale sessions and close them.
-  **Closed**—A session ends when the visitor logs out or if the session is disconnected. When a session is explicitly ended in either of these ways, the NAS sends an accounting stop message to the RADIUS server. This closes the session. No further accounting updates are possible for a closed session.

RFC 3576 Dynamic Authorization

Dynamic Authorization describes the ability to make changes to a visitor account's session while it is in progress. This includes disconnecting a session, or updating some aspect of the authorization for the session.

The Active Sessions page provides two Dynamic Authorization capabilities that apply to currently active sessions:

-  **Disconnect** causes a Disconnect-Request message to be sent to the NAS for an active session, requesting that the NAS terminate the session immediately. The NAS should respond with a Disconnect-ACK message if the session was terminated or Disconnect-NAK if the session was not terminated.

-  **Reauthorize** causes a Disconnect-Request message to be sent to the NAS for an active session. This message will contain a Service-Type attribute with the value 'Authorize Only'. The NAS should respond with a Disconnect-NAK message, and should then reauthorize the session by sending an Access-Request message to the RADIUS server. The RADIUS server's response will contain the current authorization details for the visitor account, which will then update the corresponding properties in the NAS session.

If the NAS does not support RFC 3576, attempts to perform Dynamic Authorization will time out and result in a 'No response from NAS' error message.

Refer to [RFC 3576](#) for more details about Dynamic Authorization extensions to the RADIUS protocol.

Filtering the List of Active Sessions


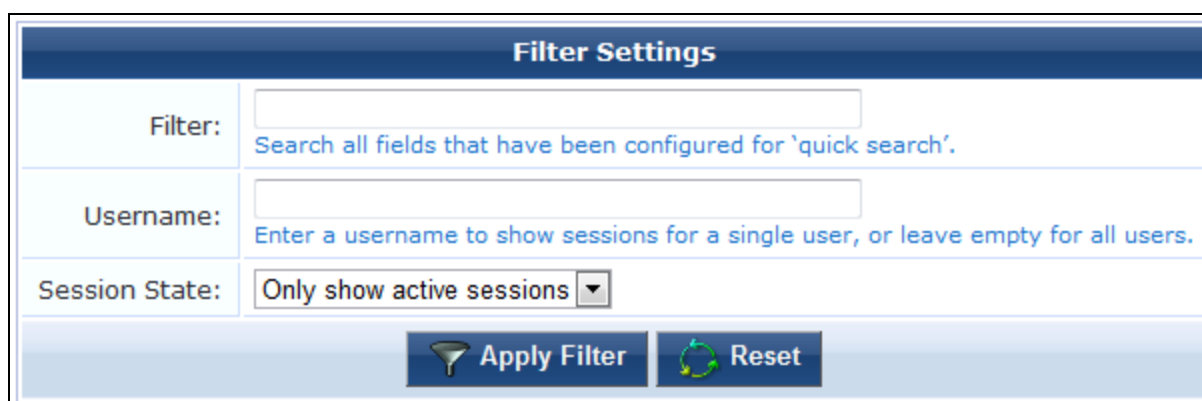

On the **Guest > Active Sessions** list, you can use the  **Filter** tab to narrow the search parameters and quickly find all matching sessions.

Figure 8 The Filter Settings Form for Active Sessions






Enter a username or IP address in the **Filter** field. Additional fields can be included in the search if the "Include values when performing a quick search" option was selected for the field within the view. To control this option, use the **Choose Columns** command link on the  **More Options** tab.

You may enter a simple substring to match a portion of the username or any other fields that are configured for search, and you can include the following operators:

Table 8: Operators Supported in Filters

Operator	Meaning	Additional Information
=	is equal to	<p>You may search for multiple values when using the equality (=) or inequality (!=) operators. To specify multiple values, list them separated by the pipe character ().</p> <p>For example, specifying the filter "role_id=2 3, custom_field=Value" restricts the accounts displayed to those with role IDs 2 and 3 (Guest and Employee), and with the field named "custom_field" set to "Value".</p>
!=	is not equal to	
>	is greater than	
>=	is greater than or equal to	
<	is less than	
<=	is less than or equal to	
~	matches the regular expression	
!~	does not match the regular expression	

To restore the default view, click the  **Clear Filter** link.

Click the  **Apply Filter** button to save your changes and update the view, or click the  **Reset** button to remove the filter and return to the default view.

Disconnecting Multiple Active Sessions

To disconnect multiple sessions:


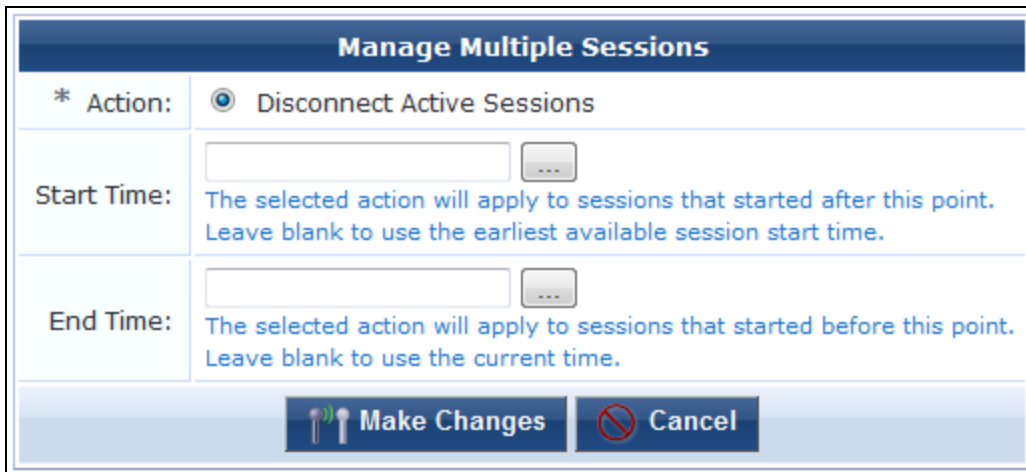


1. On the **Guest > Active Sessions** list view, click the  **Manage Multiple Sessions** tab. The **Manage Multiple Sessions** form opens.

Figure 9 *The Manage Multiple Sessions Form*



Manage Multiple Sessions	
* Action:	<input checked="" type="radio"/> Disconnect Active Sessions
Start Time:	<input type="text"/>  The selected action will apply to sessions that started after this point. Leave blank to use the earliest available session start time.
End Time:	<input type="text"/>  The selected action will apply to sessions that started before this point. Leave blank to use the current time.
<input type="button" value="Make Changes"/> <input type="button" value="Cancel"/>	

2. To close all active sessions, leave the **Start Time** and **End Time** fields empty and click **Make Changes**. All active sessions are closed and are removed from the **Active Sessions** list.

To disconnect sessions in a specified time range:

1. To close all sessions that started after a particular time, click the button in the **Start Time** row. The calendar picker opens. Use the calendar to specify the year, month, and day, and click the numbers in the **Time** fields to increment the hours and minutes. All sessions that started after the specified date and time will be disconnected.
2. To close all sessions that started before a particular time, click the button in the **End Time** row. The calendar picker opens. Use the calendar to specify the year, month, and day, and click the numbers in the **Time** fields to increment the hours and minutes. All sessions that started before the specified date and time will be disconnected.
3. Click **Make Changes**. The specified sessions are closed and are removed from the Active Sessions list.

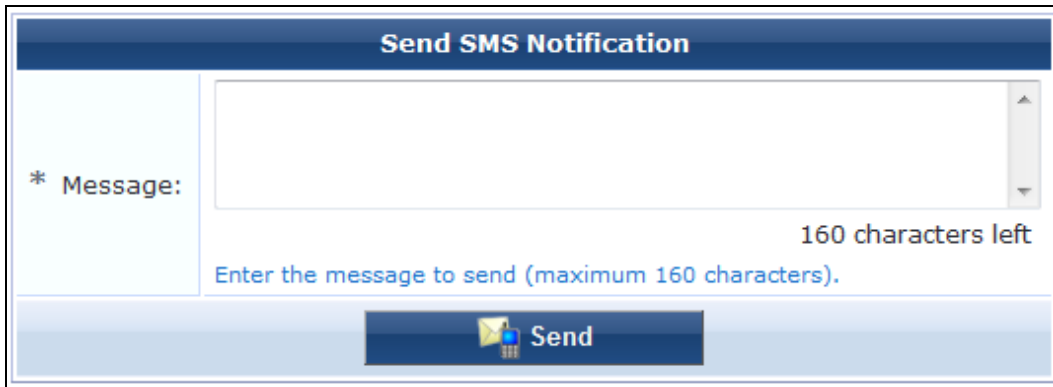
Sending Multiple SMS Alerts

The SMS tab on the Active Sessions page lets you send an SMS alert message to all active sessions that have a valid phone number. An SMS alert during an active session can be used to send a group of visitors information you might want them to have immediately—for example, a special offer that will only be available for an hour, a change in a meeting's schedule or location, or a public safety announcement.

To create an SMS message:

1. Click the **SMS** tab on the Active Sessions page. The Send SMS Notification form opens.

Figure 10 *The Send SMS Notification Form*



2. Use the filter to specify the group of addresses that should receive the message. See "[Filtering the List of Active Sessions](#)" on page 38. Only accounts with valid phone numbers can be sent SMS alerts.
3. Enter the message in the **Message** text box. Messages may contain up to 160 characters.
4. Click **Send**.

About SMS Guest Account Receipts



You can send SMS receipts for guest accounts that are created using either sponsored guest access or self-provisioned guest access. This is convenient in situations where the visitor may not be physically present to receive a printed receipt.

ClearPass Guest may be configured to automatically send SMS receipts to visitors, or to send receipts only on demand.

To manually send an SMS receipt:

1. Go to the **Guest > Manage Accounts** and click to expand the row of the guest to whom you want to send a receipt.
2. Click **Print** to display the **Updated Account Details** view, and then click the **Send SMS receipt** link. The **SMS Receipt** form opens.
3. Use the fields on the **SMS Receipt** form to enter the service to use, the recipient's mobile phone number, and the message text.

Figure 11 *The SMS Receipt Form*

SMS Receipt

* Service:
Select the service to use when sending the message.

Recipient:
Enter the mobile telephone number of the recipient in international format.

Message:
Visitor Access
Username: SHA@SH
Password:
--
Powered by Aruba
96 characters left
This is the message that will be sent.

When using guest self-registration, SMS Delivery options are available for the receipt page actions. See "Editing Receipt Actions" on page 358 for full details. For more information on SMS services, see "SMS Services" on page 453.

Using Standard Guest Management Features


This section describes:

- "Creating a Guest Account " on page 41
- "Creating a Guest Account Receipt " on page 44
- "Creating a Device" on page 45
- "Creating Multiple Guest Accounts" on page 50
- "Creating Multiple Guest Account Receipts" on page 52
- "Creating a Single Password for Multiple Accounts " on page 54
- "Managing Single Guest Accounts " on page 64
- "Managing Multiple Guest Accounts " on page 76
- "Exporting Guest Account Information " on page 58
- "Importing Guest Accounts" on page 60
- "Managing Single Guest Accounts " on page 64
- "Managing Devices " on page 69
- "Managing Multiple Guest Accounts " on page 76

To customize guest self-registration, please see [Configuration on page 271](#).

Creating a Guest Account

To create a new account, go to **Guest > Create Account**, or click the **Create New Guest Account** command link on the **Guest > Start Here** page. The **Create New Guest Account** form opens.



Create New Guest Account

Set up a new account for guest access to your network.



The Create New Guest Account form (create_user) can be customized by adding new fields, or modifying or removing the existing fields. See "Customizing Guest Self-Registration" on page 341 for details about the customization process. The default settings for this form are described below.

Figure 12 The Create New Guest Account Form

Create New Guest Account	
* Guest's Name:	<input style="width: 90%;" type="text"/> <small>Name of the guest.</small>
* Company Name:	<input style="width: 90%;" type="text"/> <small>Company name of the guest.</small>
* Email Address:	<input style="width: 90%;" type="text"/> <small>The guest's email address. This will become their username to log into the network.</small>
Account Activation:	<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">Now ▼</div> <small>Select an option for changing the activation time of this account.</small>
Account Expiration:	<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">1 day from now ▼</div> <small>Select an option for changing the expiration time of this account.</small>
* Account Role:	<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">[Guest] ▼</div> <small>Role to assign to this account.</small>
Password:	911420
Notes:	<div style="border: 1px solid #ccc; height: 40px; width: 100%;"></div>
* Terms of Use:	<input type="checkbox"/> I am the sponsor of this account and accept the terms of use
<div style="background-color: #005596; color: white; padding: 5px 20px; display: inline-block; border-radius: 5px;"> Create </div>	

Table 9: The Create New Guest Account Form

Field	Description
Guest's Name	(Required) Name of the guest user for this account.
Company Name	(Required) Name of the organization the guest user belongs to.
Email Address	(Required) The guest user's email address. This email address will be the guest's username.
Account Activation	Specifies the activation time for the account. The guest's account cannot be used before the activation time. Options include:

Field	Description
	<ul style="list-style-type: none"> ● Now ● Disable account ● Tomorrow ● Next Monday ● 1 hour from now ● 1 day from now ● 1 week from now ● Activate at specified time...
Activation Time	Specifies the date and time to activate the account. Click the button to open the calendar picker. In the calendar, use the arrows to select the year and month, click the numbers in the Time fields to increment the hours and minutes, and then click a day to select the date. If no selection is made, the account will be enabled immediately.
Account Expiration	Lets you change the expiration setting. The guest's account cannot be used after the expiration time. Options include: <ul style="list-style-type: none"> ● Account will not expire ● Now ● Tonight ● Friday night ● 1 hour from now ● 1 day from now ● 1 week from now ● 30 days from now ● 90 days from now ● 180 days from now ● 1 year from now ● Account expires after... ● Account expires at specified time...
Expires After	Specifies the amount of time after which the account will expire. Options include increments of one to twenty hours and one to fourteen days.
Expiration Time	Specifies the date and time when the account will expire. Click the button to open the calendar picker. In the calendar, use the arrows to select the year and month, click the numbers in the Time fields to increment the hours and minutes, and then click a day to select the date. If no selection is made, the account will not expire.
Account Role	(Required) Specify the type of account the guest should have. Options include: <ul style="list-style-type: none"> ● Contractor ● Employee ● Guest If you are editing an account's role, see "Changing a Guest Account Role" on page 44 .
Password	Displays the random password created for each visitor account. The password also available on the guest account receipt.
Notes	You may enter notes about this guest account.
Terms of Use	(Required) You must select the check box in this field in order to create the account.
Create	Creates the guest's account.

Changing a Guest Account Role

If you are changing a guest account's role, you must also configure change of authorization (CoA) requests to handle the change correctly. This ensures that the appropriate CoA requests are triggered for active sessions. The following steps are performed in ClearPass Policy Manager:


1. Go to **Policy Manager > Configuration > Enforcement > Profiles > Add**.
2. On the **Profile** tab, open the the **Template** drop-down list and select **RADIUS Change of Authorization (CoA)**.
3. In the **Name** field, the name you enter for the profile must include the exact role name in square brackets. For example, for the role "[Guest]", the profile name might be "My Company [Guest] CoA".
4. On the **Attributes** tab, open the **Select RADIUS CoA Template** drop-down list and select **Aruba - Change-User-Role**.
5. Click a row and add an attribute with the **Type** as **Radius:IETF**. For the **Value** enter the role name, but without the square brackets this time.


Creating a Guest Account Receipt

After you click the **Create** button on the **Create New Guest Account** form, the details for that account are displayed.


Figure 13 *The Account Details View*

Account Details	
Guest username:	aliddel@wonderland.org
Guest password:	95539400
Account status:	Active
Account activation:	Monday, 29 October 2012, 01:27 PM
Account expiration:	Account will expire at Tuesday, 30 October 2012, 01:27 PM
Account role:	[Contractor]
Sponsor name:	Wonderland

To print a receipt for the guest, select an appropriate template from the  **Open print window using template...** list. A new Web browser window opens and the browser's Print dialog box is displayed.

Click the  **Send SMS receipt** link to send a guest account receipt via text message. Use the **SMS Receipt** form to enter the mobile telephone number to which the receipt should be sent.

Sending SMS receipts requires the SMS Services plugin. If the administrator has enabled automatic SMS, and the visitor's phone number was typed into the **Create New Guest Account** form, an SMS message will be sent automatically. A message is displayed on the account receipt page after an SMS message has been sent.

Click the  **Send email receipt** link to send an email copy of the guest account receipt. Use the **Email Receipt** form to enter the email address to which the receipt should be sent. You can also specify the subject line for the email message. If the administrator has enabled automatic email for guest account receipts, and the visitor's email address was typed into the **Create New Guest Account** form, an email receipt will be sent automatically. A message is displayed on the account receipt page after an email has been sent.

Creating a Device

Device accounts may be created in three ways:

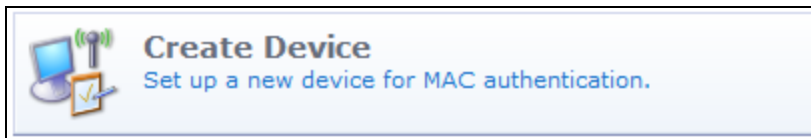
- Manually in ClearPass Guest using the **Create New Device** form
- During guest self-registration by a MAC parameter passed in the redirect URL, if the process is configured to create a MAC device account
- During guest self-registration by a MAC parameter passed in the redirect URL, creating a parallel account paired with the guest account

This section includes:

- ["Creating Devices Manually in ClearPass Guest" on page 45](#)
- ["Creating Devices During Self-Registration - MAC Only" on page 48](#)
- ["Creating Devices During Self-Registration - Paired Accounts" on page 49](#)

Creating Devices Manually in ClearPass Guest

If you have the MAC address, you can create a new device manually. To create a new device, go to **Guest > Create Device**, or go to **Guest > Manage Devices** and then click the **Create** link.



The **Create New Device** form opens.

Figure 14 *The New Device Form*



New Device	
* MAC Address:	<input type="text"/> MAC address of the device.
* Device Name:	<input type="text"/> Name of the device.
AirGroup:	<input checked="" type="checkbox"/> Enable AirGroup AirGroup uses device ownership and location information to limit the printers and Apple TVs available to network users.
Ownership:	<input type="radio"/> Personal <input checked="" type="radio"/> Shared A personal device is automatically shared with other devices owned by the same user. A shared device has no owner, but more sharing options are available.
Shared With:	<input type="text"/> Enter the usernames that will be able to use this device. Use a comma-separated list, e.g. user1,user2,user3, or blank for all users.
Shared Locations:	<input type="text"/> Select the locations where this device will be shared.
Shared Roles:	<input type="text"/> Select the user roles that will be able to use this device.
Shared Groups:	<input type="text"/> Select the user groups that will be able to use this device. This feature requires AOS 6.4 or later.
Time Sharing:	<input type="text"/>  Syntax Specify time-based sharing rules for this device.
Account Activation:	Now <input type="text"/> Select an option for changing the activation time of this account.
Account Expiration:	1 year from now <input type="text"/> Select an option for changing the expiration time of this account.
* Account Role:	[Guest] <input type="text"/> Role to assign to this account.
Notes:	<input type="text"/>
* Terms of Use:	<input checked="" type="checkbox"/> I am the sponsor of this account and accept the terms of use
	

Table 10: *New Device*

Field	Description
MAC Address	(Required) Enter the device's MAC address.
Device Name	(Required) Enter the name for the device. If you need to modify the configuration for expected separator format or case, go to Administration > Plugin Manager > Manage Plugins and click the Configuration link for the MAC Authentication Plugin .
AirGroup	Enables AirGroup for the device. Configuration options are added to the form.
Ownership	Specifies whether device ownership should be personal or shared. Personal devices are automatically shared with the owner's other devices.
Shared With	Usernames of people who can share this device. Enter usernames as a comma-separated list. To make the device available to all users, leave this field blank. Each username may not exceed 64 characters. A maximum of 100 usernames may be entered. The maximum character limit for the list is 1000 characters (including comma

Field	Description
	separators).
Shared Locations	<p>Locations where the device can be shared. When you type a location name in the Shared Locations field and press the Enter key, the location appears as a "tag" and is created in the system when the form is saved.</p> <p>Each location name may not exceed 64 characters. A maximum of 100 location names may be entered. The maximum character limit for the list is 1000 characters (including comma separators).</p>
Shared Roles	<p>User roles that can share this device. When you type a role name in the Shared Roles field and press the Enter key, the role appears as a "tag" and is created in the system when the form is saved.</p> <p>Each role name may not exceed 64 characters. A maximum of 100 role names may be entered. The maximum character limit for the list is 1000 characters (including comma separators).</p>
Shared Groups	<p>User groups that can share this device. These will be available in the Shared Groups field for users to choose from when they share a device.</p> <p>When you type a name for the group in the Group Names field and press the Enter key, the group appears as a "tag" and is created in the system when the form is saved.</p> <p>Each group name may not exceed 64 characters. A maximum of 32 group names may be entered. The maximum character limit for the list is 320 characters (including comma separators).</p> <p>This feature requires AOS 6.4 or later.</p>
Time Sharing	Time-based sharing rules for this device. For more information, see "About AirGroup Time-Based Sharing" on page 89 .
Syntax	Opens the help topic "AirGroup Time-Based Sharing Syntax Examples" on page 85
Account Activation	<p>Specifies when the account will be activated. Options include: Activate the account immediately, at a preset interval of hours or days, at a specified time, or leave the account disabled.</p> <p>If you choose Activate at a specified time, the ActivationTime row is added to the form. Click the button to open the calendar picker. In the calendar, use the arrows to select the year and month, click the numbers in the Time fields to increment the hours and minutes, then click a day to select the date.</p>
Account Expiration	<p>Specifies when the account will expire. Options include: Never expire, expire at a preset interval of hours or days, or expire at a specified time.</p> <ul style="list-style-type: none"> • If you choose any time in the future, the Expire Action row is added to the form. Indicate the expiration action for the account—either delete, delete and log out, disable, or disable and log out. The action will be applied at the time set in the Account Expiration row. • If you choose Account expires after, the ExpiresAfter row is added to the form. Choose an interval of hours, days, or weeks. The maximum is two weeks. • If you choose Account Expires at a specified time, the ExpirationTime row is added to the form. In the calendar picker, use the arrows to select the year and month, click the numbers in the Time fields to increment the hours and minutes, then click a day to select the date.

Field	Description
Account Role	Assigns the visitor's role.
Terms of Use	Click the terms of use link and read the agreement, and then mark the check box to agree to the terms.
Create Device	Commits your changes and creates the device. The Account Details and print options are displayed. For more information, see " Printing Device Details " on page 75.

Creating Devices During Self-Registration - MAC Only

This section describes how to configure a guest self-registration so that it creates a MAC device account. After the guest is registered, future authentication can take place without the need for the guest to enter their credentials. A registration can be converted to create a MAC device instead of standard guest credentials.

This requires a vendor to pass a **MAC** parameter in the redirect URL. ClearPass Guest does not support querying the controller or DHCP servers for the client's MAC based on IP.

To edit the registration form fields:

1. Go to **Configuration > Pages > Forms and Views**.
2. In the **guest_register** row, click the **Edit Fields** link. The **Customize Form Fields** page opens.
3. If you do not see **mac** or **mac_auth** in the list, click the **Customize fields** link above the list.
4. Click the **Edit** link in the field's row. In the **Edit Field** form, edit the following registration form fields:
 - Add or enable **mac**
 - UI: **Hidden field**
 - Field Required: checked
 - Validator: **IsValidMacAddress**
 - Add or enable **mac_auth**
 - UI: **Hidden field**
 - Any other expiration options, role choice, surveys, and so on can be entered as usual.

Figure 15 *Modify fields*

Rank	Field	Type	Label	Description
30	visitor_company	text	Company Name:	Please enter your company name.
40	email	text	Email Address:	Please enter your email address. This will become your username to log into the network.
45	mac	text	MAC Address:	MAC address of the device.
47	mac_auth	hidden		
50	start_time	datetime	Activation Time:	Scheduled date and time at which to enable the visitor account. If blank, the account will be enabled immediately.
60	expire_after	hidden	Expires After:	Amount of time before this visitor account will expire.
65	expire_time	datetime	Expiration Time:	Optional date and time at which the visitor accounts will expire and be deleted. If blank, the account will not expire.

5. Edit the following receipt form fields:
 - Edit **username** to be a **Hidden field**
 - Edit **password** to be a **Hidden field**
6. Adjust any headers or footers as needed.

When the visitor registers, they should be able to still log in via the **Log In** button. The MAC will be passed as their username and password via standard captive portal means.

The account will only be visible on the **List Devices** page.

If the guest logs out and reconnects, they should be immediately logged in without being redirected to the captive portal page.

Creating Devices During Self-Registration - Paired Accounts

Paired accounts is a means to create a standard visitor account with credentials, but to have a MAC account created in parallel that is directly tied to the visitor account. These accounts share the same role, expiration and other properties.

This requires a vendor passing a **mac** parameter in the redirect URL. ClearPass Guest does not support querying the controller or DHCP servers for the client's MAC based on IP.

To edit the registration form fields:

1. Go to **Configuration > Pages > Forms and Views**.
2. In the **guest_register** row, click the **Edit Fields** link. The **Customize Form Fields** page opens.
3. If you do not see **mac** or **mac_auth_pair** in the list, click the **Customize fields** link above the list.
4. Click the **Edit** link in the field's row. In the **Define Custom Field** form, edit the following registration form fields:
 - Add or enable **mac**
 - UI: **Hidden field**
 - Field Required: optional

- Validator: **IsValidMacAddress**
- Add or enable **mac_auth_pair**
 - UI: **Hidden field**
 - Initial Value: **-1**
- Any other expiration options, role choice, surveys and so on can be entered as usual.

You will see an entry under both **List Accounts** and **List Devices**. Each should have a **View Pair** action that cross-links the two.

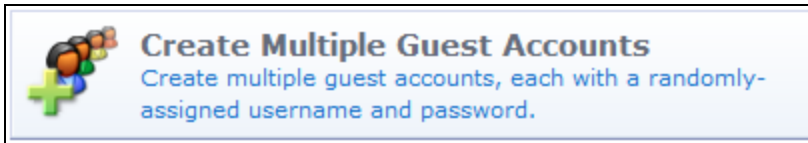


If you delete the base account, all of its pairings will also be deleted. If RFC-3576 has been configured, all pairs will be logged out.

Creating Multiple Guest Accounts

The **Create Multiple Guest Accounts** form is used to create a group of visitor accounts.

To create multiple accounts, go to **Guest > Create Multiple**, or click the **Create Multiple Guest Accounts** command link on the **Guest > Start Here** page. The **Create Multiple Guest Accounts** form opens.



The **Create Multiple Guest Accounts** form (create_multi) can be customized by adding new fields, or modifying or removing the existing fields. See "[Customizing Guest Self-Registration](#)" on page 341 for details about the customization process. The default settings for this form are described below.

Figure 16 *The Create Multiple Guest Accounts Form*

Create Multiple Guest Accounts	
* Number of Accounts:	<input type="text" value="1"/> <small>Number of guest accounts to create.</small>
Account Activation:	<input type="text" value="Now"/> <small>Select an option for changing the activation time of this account.</small>
Account Expiration:	<input type="text" value="1 day from now"/> <small>Select an option for changing the expiration time of this account.</small>
* Expire Action:	<input type="text" value="Disable at specified time"/> <small>Select an option for controlling the expiration of this account. Note that a logout can only occur if the NAS is RFC-3576 compliant.</small>
Account Lifetime:	<input type="text" value="N/A"/> <small>The amount of time after the first login before the account will expire and be deleted.</small>
* Account Role:	<input type="text" value="[Guest]"/> <small>Role to assign to this account.</small>
Notes:	<input type="text"/>

Table 11: The Create New Guest Account Form

Field	Description
Number of Accounts	(Required) Enter the number of accounts to create.
Account Activation	<p>Activation time for the accounts. The guests' accounts cannot be used before the activation time. Options include:</p> <ul style="list-style-type: none"> ● Now ● Disable account ● Tomorrow ● Next Monday ● 1 hour from now ● 1 day from now ● 1 week from now ● Activate at specified time...
Activation Time	<p>Specifies the date and time to activate the accounts. Click the button to open the calendar picker. In the calendar, use the arrows to select the year and month, click the numbers in the Time fields to increment the hours and minutes, then click a day to select the date. If no selection is made, the accounts will be enabled immediately.</p>
Account Expiration	<p>Specifies the expiration time for the accounts. The guests' accounts cannot be used after the expiration time. Options include:</p> <ul style="list-style-type: none"> ● Account will not expire ● Now ● Tonight ● Friday night ● 1 hour from now ● 1 day from now ● 1 week from now ● 30 days from now ● 90 days from now ● 180 days from now ● 1 year from now ● Account expires after... ● Account expires at specified time...
Expires After	<p>Specifies an amount of time after which the accounts will expire. Options include intervals of hours, days, or weeks.</p>
Expiration Time	<p>Specifies the date and time the accounts will expire. Click the button to open the calendar picker. In the calendar, use the arrows to select the year and month, click the numbers in the Time fields to increment the hours and minutes, then click a day to select the date. If no selection is made, the accounts will not expire.</p>
Expire Action	<p>(Required) Specify the behavior of the expiration. Options include:</p> <ul style="list-style-type: none"> ● Delete and log out at specified time ● Delete at specified time ● Disable and log out at specified time ● Disable at specified time <p>Be aware that a logout can only occur if the NAS is RFC-3576 compliant.</p>

Field	Description
Account Role	(Required) Specify the type of account the guest should have. Options include: <ul style="list-style-type: none"> ● Contractor ● Employee ● Guest
Notes	You may enter notes about these guest accounts.
Terms of Use	(Required) You must select the check box in this field in order to create the accounts.
Create Accounts	When your entries on the form are complete, click this button to create the accounts.

A random username and password will be created for each visitor account. This is not displayed on this form, but will be available on the guest account receipt. The default password length is six characters.

Creating Multiple Guest Account Receipts


After a group of guest accounts has been created, the details for the accounts are displayed.

Figure 17 Account Details Displayed for Multiple Accounts

Account Details		
	Username	91972747
	Password	20626907
	Role	[Contractor]
	Current State	Active
	Account Activation	Friday, 26 October 2012, 03:50 PM
	Account Expiration	Saturday, 27 October 2012, 03:50 PM

Account Details		
	Username	09609879
	Password	97625198
	Role	[Contractor]
	Current State	Active
	Account Activation	Friday, 26 October 2012, 03:50 PM
	Account Expiration	Saturday, 27 October 2012, 03:50 PM

Account Details		
	Username	41915905
	Password	97695485
	Role	[Contractor]
	Current State	Active
	Account Activation	Friday, 26 October 2012, 03:50 PM
	Account Expiration	Saturday, 27 October 2012, 03:50 PM

To print the receipts, select an appropriate template from the  **Open print window using template...** drop-down list. A new browser window opens with the **Print** dialog displayed.


To download a copy of the receipt information in CSV format, click the  **Save list for scratch cards (CSV file)** link. You will be prompted to either open or save the spreadsheet (CSV) file. The fields available in the CSV file are shown in [Table 12](#).

Table 12: *Fields in the CSV Spreadsheet File*

Field	Description
Number	Sequential number of the visitor account, starting at one.
Username	Username for the visitor account.
Password	Password for the visitor account. The default password length is six characters. The maximum password length is 128 characters.
Role	The visitor account's role.
Activation Time	Date and time at which the account will be activated, or N/A if there is no activation time.
Expiration Time	Date and time at which the account will expire, or N/A if there is no activation time.
Lifetime	Account lifetime in minutes, or N/A if the account does not have a lifetime specified.
Successful	"Yes" if the account was created successfully, or "No" if there was an error creating the account.

Creating a Single Password for Multiple Accounts

You can create multiple accounts that have the same password. In order to do this, you first customize the **Create Multiple Guest Accounts** form to include the **Password** field.

To include the **Password** field on the **Create Multiple Guest Accounts** form:

1. Go to **Configuration > Pages > Forms & Views**.
2. Click the **create_multi** row, then click its **Edit Fields** link. The **Customize Form Fields** view opens, showing a list of the fields included in the **Create Multiple Guest Accounts** form and their descriptions.
At this point, the **Password** field is not listed because the **Create Multiple Guest Accounts** form (create_multi) has not yet been customized to include it. You will create it for the form in the next step.
3. Click on any field in the list to expand a row, and then click the **Insert After** link (you can modify this placement later). The **Form Field Editor** form opens.
4. In the **Field Name** row, choose **password** from the drop-down list. The form displays configuration options for the **Password** field.

Figure 18 Password Field in Form Field Editor

Form Field Editor

* Field Name: Select the field definition to attach to the form.

Form Display Properties
These properties control the user interface displayed for this field.

Field: Enable this field
When checked, the field will be included as part of the form.

* Rank:
Number indicating the relative ordering of user interface fields, which are displayed in order of increasing rank.

* User Interface:
The kind of user interface element to use when entering or editing this field.

Label:
Label for this field to display on the form.

Table 13: The Form Field Editor for the Password Field

Field	Description
Field	If selected, the password field will be included in the form.
Rank	Lets you change the rank number to adjust the relative placement of the password field on the Create Multiple Guest Accounts form. Fields are displayed in order of increasing rank.
User Interface	Choose Password text field from the drop-down list.
Label	(Optional) You may change the label that is displayed on the form.
Field Required	If selected, the password field cannot be left blank.
Validator	Select IsValidPassword in the drop-down list.
Save Changes	Saves your changes. The Customize Form Fields view opens again, and the password field is now included and can be edited.

To create multiple accounts that all use the same password:

1. Go to **Guest > Create Multiple**. The **Create Multiple Guest Accounts** form opens, and includes the **Guest Password** field.

Figure 19 *The Create Guest Accounts Form with Guest Password Field Included*

Table 14: *The Create Guest Accounts Form*

Field	Description
Number of Accounts	(Required) Enter the number of accounts you wish to create.
Guest Password	(Required) Enter the password that is to be used by all the accounts. The minimum password length is six characters. The maximum password length is 128 characters.
Account Activation	Specify the activation time for the account. Options include: <ul style="list-style-type: none"> ● Now ● Disable account ● Tomorrow ● Next Monday ● 1 hour from now ● 1 day from now ● 1 week from now ● Activate at specified time...
Activation Time	Specifies a date and time when the account will be activated. Click the button to open the calendar picker. In the calendar, use the arrows to select the year and month, click the numbers in the Time fields to increment the hours and minutes, and then click a day to select the date.
Account Expiration	Specify the expiration time for the account. Options include: <ul style="list-style-type: none"> ● Account will not expire ● Now ● Tonight ● Friday night ● 1 hour from now ● 1 day from now ● 1 week from now ● 30 days from now ● 90 days from now

Field	Description
	<ul style="list-style-type: none"> ● 180 days from now ● 1 year from now ● Account expires after... ● Account expires at specified time...
Expires After	Specifies the amount of time after which the account will expire. Options include increments of one to twenty hours and one to fourteen days.
Expiration Time	Specifies a date and time when the account will expire. Click the button to open the calendar picker. In the calendar, use the arrows to select the year and month, click the numbers in the Time fields to increment the hours and minutes, and then click a day to select the date.
Expire Action	(Required) Specify the action to take when the account expires. Options include: <ul style="list-style-type: none"> ● Delete and log out at specified time ● Delete at specified time ● Disable and log out at specified time ● Disable at specified time
Account Lifetime	Specifies the amount of time after the first login when the account will expire and be deleted. Options include increments of days or weeks, up to one week.
Account Role	(Required) Specify the role to assign to the account. Options include: <ul style="list-style-type: none"> ● Contractor ● Employee ● Guest
Notes	You may enter additional information.
Create Accounts	Saves your changes and creates the accounts. The Finished Creating Guest Accounts view opens. The password and other account details are displayed for each account.

Figure 20 Account Details Displayed for Multiple Accounts with Single Password

Account Details		
	Username	57744937
	Password	1PW4all
	Role	[Contractor]
	Current State	Active
	Account Activation	Friday, 26 October 2012, 04:18 PM
	Account Expiration	Saturday, 27 October 2012, 04:18 PM

Account Details		
	Username	09641588
	Password	1PW4all
	Role	[Contractor]
	Current State	Active
	Account Activation	Friday, 26 October 2012, 04:18 PM
	Account Expiration	Saturday, 27 October 2012, 04:18 PM

Account Details		
	Username	60600985
	Password	1PW4all
	Role	[Contractor]
	Current State	Active
	Account Activation	Friday, 26 October 2012, 04:18 PM
	Account Expiration	Saturday, 27 October 2012, 04:18 PM

Exporting Guest Account Information

Guest account information may be exported to a file in one of several different formats.

To export a file with the current list of guest accounts, go to **Guest > Export Accounts**, or go to **Guest > Start Here** and click the **Export Guest Accounts** command link. The **Export Accounts** page opens with three options displayed. Click the appropriate command link to save a list of all guest accounts in comma-separated values (CSV), tab-separated values (TSV), or XML format.



The **Export Accounts** view (guest_export) may be customized by adding new fields, or by modifying or removing the existing fields. See "[Customizing Guest Self-Registration](#)" on page 341 for details about this customization process.

About CSV and TSV Exports

In CSV and TSV format, the following default fields are included in the export:

- **Number** – Sequential number of the guest account in the exported data
- **User ID** – Numeric user ID of the guest account
- **Username** – Username for the guest account
- **Role** – Role for the guest account
- **Activation** – Date and time at which the guest account will be activated, or "N/A" if there is no activation time
- **Expiration** – Date and time at which the guest account will expire, or "N/A" if there is no expiration time
- **Lifetime** – The guest account's lifetime in minutes after login, or 0 if the account lifetime is not set
- **Expire Action** – Number specifying the action to take when the guest account expires (0 through 4)

About XML Exports

The default XML format consists of a **<GuestUsers>** element containing a **<GuestUser>** element for each exported guest account. The numeric ID of the guest account is provided as the "id" attribute of the **<GuestUser>** element. This format is compatible with the ClearPass Policy Manager XML format for guest users.

The values for both standard and custom fields for guest accounts are exported as the contents of an XML tag, where the tag has the same name as the guest account field.

An example XML export is given below:

```
<?xml version="1.0" encoding="UTF-8" standalone="true"?>
<MyContents xmlns="http://www.example.com/myapiDefs/1.0">
  <MyHeader version="6.0" exportTime="Sun, 16 Dec 2012 16:36:03 PST"/>
  <GuestUsers>
    <GuestUser guestType="USER" enabled="true" sponsorName="55480025"
      expiryTime="2012-12-04 13:39:25" startTime="1969-12-31 16:00:00"
      password="08654361" name="55480025">
      <GuestUserTags tagValue="Hotspot Services self-provisioned guest account
        Source IP: 10.11.10.254 MAC: unknown Plan: Free Access x 1 Transaction
        Amount: $0.00 Invoice Number: P-15 Transaction ID: " tagName="notes"/>
      <GuestUserTags tagValue="2" tagName="[Role ID]"/>
      <GuestUserTags tagValue="1" tagName="do_expire"/>
    </GuestUser>
  </GuestUsers>
</MyContents>
```

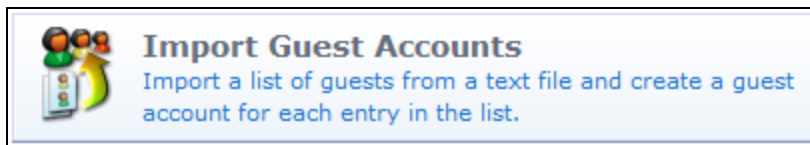
```

<GuestUserTags tagValue="1" tagName="simultaneous_use"/>
<GuestUserTags tagValue="ff" tagName="Company Name"/>
<GuestUserTags tagValue="2012-12-04 12:39:14" tagName="Create Time"/>
<GuestUserTags tagValue="fff@df" tagName="Email"/>
<GuestUserTags tagValue="ff" tagName="first_name"/>
<GuestUserTags tagValue="plan0" tagName="hotspot_plan_id"/>
<GuestUserTags tagValue="Free Access" tagName="hotspot_plan_name"/>
<GuestUserTags tagValue="ff" tagName="last_name"/>
<GuestUserTags tagValue="ff ff" tagName="Visitor Name"/>
<GuestUserTags tagValue="ff" tagName="zip"/>
</GuestUser>

```

Importing Guest Accounts

Guest accounts may be created from an existing list by uploading the list to ClearPass Guest.




To import a file with the current list of guest accounts, go to **Guest > Import Accounts**, or go to **Guest > Start Here** and click the **Import Guest Accounts** command link. The **Import Accounts** page opens with the first part of the form displayed, **Upload User List**.

The **Upload User List** form provides you with different options for importing guest account data. To complete the form, you must either specify a file containing account information, or type or paste in the account information.

Figure 21 *The Upload User List Form for Importing Guest Accounts*

Upload User List	
Size Limit:	Maximum file upload size: 5.0 MB. A maximum of 1000 records can be imported at one time.
Accounts File:	<input type="text"/> <input type="button" value="Browse..."/> Upload a file containing a list of user accounts. This field may be left blank if you provide the list in the field below.
Accounts Text:	<div style="border: 1px solid #ccc; height: 40px;"></div> Type in or paste the list of user accounts. This field may be left blank if you upload a file.
Advanced:	<input checked="" type="checkbox"/> Show additional import options
* Character Set:	UTF-8 <input type="button" value="v"/> Select the character set encoding of the file.
Import Format:	Automatically detect format <input type="button" value="v"/> Select the file format of the file.
Header:	<input type="checkbox"/> Force first row as header row
<input type="button" value="Next Step"/>	

Table 15: The Import Accounts Form, Step 1: Upload User List

Field	Description
Accounts File	Lets you specify a file that contains a list of user accounts. Click the Choose File button in this row to browse to the file and select it.
Accounts Text	Lets you enter the account information directly. Type or paste the information in the text box in this row.
Advanced	To display the advanced options, select the Show additional import options check box in this row.
Character Set	Specifies the character set encoding of the file. ClearPass Guest uses the UTF-8 character set encoding internally to store visitor account information. If your accounts file is not encoded in UTF-8, the import might fail or produce unexpected results if non-ASCII characters are used. To avoid this, you should specify what character set encoding you are using.
Import Format	Specifies the file format of the file. Options include: <ul style="list-style-type: none"> • Automatically detect format (This default option recognizes guest accounts exported from ClearPass Policy Manager in XML format) • XML • Comma separated values • Tab separated values • Pipe () separated values • Semicolon (;) separated values • Colon (:) separated values <p>The format of the accounts file is automatically detected. You may specify a different encoding type if automatic detection is not suitable for your data.</p>
Header	If your data contains a header row that specifies the field names, select the Force first row as header row check box in this row. This option is only required if the header row is not automatically detected.
	The header row must contain the mac_auth and mac columns. The mac_auth value should be set to 1, and the mac value should be the MAC address. Any other fields may also be included.
Next Step	Uploads the account data and proceeds to the next step.

In step 2 of 3, ClearPass Guest determines the format of the uploaded account data and matches the appropriate fields to the data. The first few records in the data are displayed, together with any automatically detected field names.

In this example, the following data was used:

```
username,visitor_name,password,expire_time
demo005,Demo five,secret005,2011-06-10 09:00
demo006,Demo six,secret006,2011-06-11 10:00
demo007,Demo seven,secret007,2011-06-12 11:00
demo008,Demo eight,secret008,2011-06-13 12:00
demo009,Demo nine,secret009,2011-06-13 12:00
demo010,Demo ten,secret010,2011-06-13 12:00
demo011,Demo eleven,secret011,2011-06-13 12:00
```

Because this data includes a header row that contains field names, the corresponding fields were automatically detected in the data:

Figure 22 *Data File with Fields Detected from Header Row*

Record	Username	Full Name	Password	Expiration
1	username	visitor_name	password	expire_time
2	demo005	Demo five	secret005	2011-06-10 09:00
3	demo006	Demo six	secret006	2011-06-11 10:00
4	demo007	Demo seven	secret007	2011-06-12 11:00
5	demo008	Demo eight	secret008	2011-06-13 12:00
6	demo009	Demo nine	secret009	2011-06-13 12:00
7	demo010	Demo ten	secret010	2011-06-13 12:00
8	demo011	Demo eleven	secret011	2011-06-13 12:00

Use the **Match Fields** form to identify which guest account fields are present in the imported data. You can also specify the values to be used for fields that are not present in the data.

Figure 23 *The Match Fields Form*

Match Fields	
* Username:	Username <input type="text"/> <small>The username of the created guest accounts.</small>
* Password:	Password <input type="text"/> <small>The password for the created guest accounts.</small>
* Role:	Assign role: [Contractor] <input type="text"/> <small>The role to assign to each of the created guest accounts.</small>
* Activation Time:	None (Activate immediately) <input type="text"/> <small>The date and time at which to enable the guest accounts.</small>
* Expiration Time:	Expiration <input type="text"/> <small>The date and time at which a guest account will expire and be deleted.</small>
* Account Lifetime:	None (No lifetime) <input type="text"/> <small>The amount of time after the first login before the visitor account will expire and be deleted.</small>
Expire Action:	Delete and logout at specified time <input type="text"/> <small>Select an option for controlling the expiration of this account. Note that a logout can only occur if the NAS is RFC-3576 compliant.</small>
* Notes:	None <input type="text"/> <small>A note stored with each of the guest accounts.</small>
Auto-Detected Fields:	<input checked="" type="checkbox"/> Full Name <small>The above fields were auto-detected in your file. Check the ones you wish to import.</small>
* Header Rows:	1 <input type="text"/> <small>The number of rows shown in the imported data that do not correspond to user accounts.</small>
<input type="button" value="Next Step"/>	

To complete the **Match Fields** form, make a selection from each of the drop-down lists. Choose a column name to use the values from that column when importing guest accounts, or select one of the other available options to use a fixed value for each imported guest account.

Click the **Next Step** button to preview the final result. Import Step 3 of 3, the **Import Accounts** form, opens and shows a preview of the import operation. The values of each guest account field are determined, and any conflicts with existing user accounts are shown.

Figure 24 *The Import Accounts Form*

Import Accounts					
Select:	This Page (7) • All (7) • None • New (7) • Existing (0)				
Total number of records currently selected: 7					
Username	Password	Role	Expiration	Expire Action	Full Name
<input checked="" type="checkbox"/> demo005	secret005	[Contractor]	2011-06-10 09:00	4	Demo five
<input checked="" type="checkbox"/> demo006	secret006	[Contractor]	2011-06-11 10:00	4	Demo six
<input checked="" type="checkbox"/> demo007	secret007	[Contractor]	2011-06-12 11:00	4	Demo seven
<input checked="" type="checkbox"/> demo008	secret008	[Contractor]	2011-06-13 12:00	4	Demo eight
<input checked="" type="checkbox"/> demo009	secret009	[Contractor]	2011-06-13 12:00	4	Demo nine
<input checked="" type="checkbox"/> demo010	secret010	[Contractor]	2011-06-13 12:00	4	Demo ten
<input checked="" type="checkbox"/> demo011	secret011	[Contractor]	2011-06-13 12:00	4	Demo eleven

Accounts: 1 Showing 1 - 7 of 7 10 rows per page

Select the accounts to import.

The icon displayed for each user account indicates whether it is a new entry () or if an existing user account will be updated ()

By default, this form shows ten entries per page. To view additional entries, click the arrow button at the bottom of the form to display the next page, or click the **10 rows per page** drop-down list at the bottom of the form and select the number of entries that should appear on each page.

Click the check box by the account entries you want to create, or click one of the links in the **Select** field at the top of the form to select the desired accounts. These options links are described in [Table 16](#).

Table 16: *The Import Accounts Form, Options Links*






Field	Description
This Page	Selects all entries on the current page.
All	Selects all entries on all pages.
None	Deselects all entries.
New	Selects all new entries.
Existing	Selects all existing user accounts in the list.
Create Guest Accounts	Click the button to finish the import process. The selected items will be created or updated. You can then print new guest account receipts or download a list of the guest accounts. See " Creating Multiple Guest Account Receipts " on page 52 in this chapter for more information.

Managing Single Guest Accounts

Use the **Manage Guest Accounts** list view to work with individual guest accounts. To open the **Manage Guest Accounts** list, go to **Guest > Manage Accounts**.






The **Manage Guest Accounts** list view opens. This view (guest_users) may be customized by adding new fields or modifying or removing the existing fields. See "[Customizing Fields](#)" on page 294 for details about this customization process. The default settings for this view are described below.

Figure 25 *The Manage Guest Accounts List View*

△ Username	Role	State	Activation	Expiration
 09609879	[Contractor]	Active	40 minutes ago	2012-10-27 15:50
 09641588	[Contractor]	Active	12 minutes ago	2012-10-27 16:18
 41915905	[Contractor]	Active	40 minutes ago	2012-10-27 15:50
 57744937	[Contractor]	Active	12 minutes ago	2012-10-27 16:18
 60600985	[Contractor]	Active	12 minutes ago	2012-10-27 16:18
 91972747	[Contractor]	Active	40 minutes ago	2012-10-27 15:50
 ipod	[Contractor]	Expired	1.1 days ago	Expired
 sham@a	[Contractor]	Expired	1.2 days ago	Expired
 tom@a	[Guest]	Expired	N/A	Expired

Refresh Showing 1 – 9 of 9
20 rows per page


The **Username**, **Role**, **State**, **Activation**, and **Expiration** columns display information about the visitor accounts that have been created:

- The value in the **Expiration** column is **colored red** if the account will expire within the next 24 hours. The expiration time is additionally highlighted in **boldface** if the account will expire within the next hour.
- In addition, icons in the **Username** column indicate the account's activation status:
 - —Visitor account is active
 - —Visitor account was created but is not activated yet
 - —Visitor account was disabled by Administrator
 - —Visitor account has expired
 - —Visitor account was deleted
- If you are editing an account's role, see "[Changing a Guest Account Role](#)" on page 78.

You can use the **Filter** field to narrow the search parameters. You may enter a simple substring to match a portion of the username or any other fields that are configured for search, and you can include the following operators:

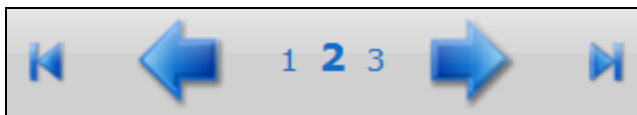
Table 17: Operators supported in filters

Operator	Meaning	Additional Information
=	is equal to	<p>You may search for multiple values when using the equality (=) or inequality (!=) operators. To specify multiple values, list them separated by the pipe character ().</p> <p>For example, specifying the filter "role_id=2 3, custom_field=Value" restricts the accounts displayed to those with role IDs 2 and 3 (Guest and Employee), and with the field named "custom_field" set to "Value".</p>
!=	is not equal to	
>	is greater than	
>=	is greater than or equal to	
<	is less than	
<=	is less than or equal to	
~	matches the regular expression	
!~	does not match the regular expression	


To restore the default view, click the  **Clear Filter** link.


You can use the paging controls at the bottom of the list to jump forwards or backwards by one page or to jump directly to an individual page number, or to change the number of rows that are displayed on one page.

Figure 26 *The Paging Control*



When the list contains numerous user accounts, consider using the Filter field to speed up finding a specific user account.

Use the  **Create** tab to create new visitor accounts using the **Create New Guest Account** form. See "[Creating a Guest Account](#)" on page 41 for details about this form.

Use the  **More Options** tab for additional functions, including import and export of guest accounts and the ability to customize the view.

Click a user account's row to select it. You can then select from one of these actions:




-  **Reset password** – Changes the password for a guest account. A new randomly generated password is displayed on the **Reset Password** form. The default password length is six characters. The maximum password length is 128 characters.



Figure 27 *The Reset Password Form*

Reset Password	
Username:	41915905
* New password:	77876546 This is the new password that will be assigned to this guest account.
	

Click  **Update Account** to reset the guest account's password. A new account receipt is displayed, allowing you to print a receipt showing the updated account details.

-  **Change expiration** – Lets you change the expiration time for a guest account.


Figure 28 *The Change Expiration Form*

Change Expiration	
Username:	41915905
Account Activation:	Friday, 26 October 2012, 03:50 PM
Account Expiration:	Account will expire at Saturday, 27 October 2012, 03:50 PM
Account Expiration:	(No changes: 2012-10-27 15:50:44)  Select an option for changing the expiration time of this account.
	



This form (change_expiration) can be customized by adding new fields, or modifying or removing the existing fields. See "Customizing Forms and Views" on page 305 for details about this customization process.

Select an option from the drop-down list to change the expiration time of the guest account.

Click  **Update Account** to set the new expiration time for the guest account. A new account receipt is displayed, allowing you to print a receipt showing the updated account details.


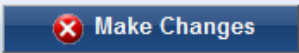
-  **Remove** – Disables or deletes a guest account.

Figure 29 *The Remove Account Form*

Remove Account	
Username:	57744937
Account Expiration:	Account will expire at Saturday, 27 October 2012, 04:18 PM
* Action:	<input checked="" type="radio"/> Disable account <input type="radio"/> Delete account Caution: Deleting a guest account cannot be undone! Use this option with care.
	

Select the appropriate **Action** radio button, and click  **Make Changes** to disable or delete the account.

If you wish to have automatic disconnect messages sent when the enabled value changes, you can specify this in the Configuration module. See "[Configuring ClearPass Guest Authentication](#) " on page 273.

- **✓ Activate** – Re-enables a disabled guest account, or specifies an activation time for the guest account.

Figure 30 *The Enable Guest Account Form*

Enable Guest Account	
Username:	60600985
Account Expiration:	Account will expire at Saturday, 27 October 2012, 04:18 PM
Account Activation:	Friday, 26 October 2012, 04:18 PM
Activate Account:	Now <input type="button" value="v"/> <small>Select an option for changing the activation time of this account.</small>
<input type="button" value="✓ Enable Account"/>	

Select an option from the drop-down list to change the activation time of the guest account. To re-enable an account that has been disabled, choose **Now**. Click **✓ Enable Account** to set the new activation time for the guest account. A new account receipt is displayed, allowing you to print a receipt showing the updated account details.


-  **Edit** – Lets you change the properties of a guest account. The account’s row expands to include the Edit Account form. This form is similar to the Create Account form, and all fields can be edited. If you are editing the account’s role, see "[Managing Single Guest Accounts](#) " on page 64.

Figure 31 *The Edit Account Form*

Edit Account	
* Visitor’s Name:	Alice Liddel <input type="text"/> <small>Name of the visitor.</small>
* Username:	aliddel@fireside.org <input type="text"/> <small>Name of the visitor account.</small>
Account Activation:	(No changes: Account is active) <input type="button" value="v"/> <small>Select an option for changing the activation time of this account.</small>
Account Expiration:	(No changes: 2012-10-27 16:18:47) <input type="button" value="v"/> <small>Select an option for changing the expiration time of this account.</small>
Total Allowed Usage:	(No changes) <input type="button" value="v"/> <small>Select an option for changing the allowed usage time of this account.</small>
Account Role:	(No changes: [Contractor]) <input type="button" value="v"/> <small>Role to assign to this visitor account.</small>
* Password:	(No changes) <input type="button" value="v"/> <small>Select an option for editing the visitor account’s password.</small>
Session Limit:	1 <input type="text"/> <small>The number of simultaneous sessions allowed for this visitor account. Type 0 for unlimited use.</small>
<input type="button" value="✎ Update Account"/>	



This form can be customized by adding new fields, or modifying or removing the existing fields. See "[Customizing](#)

Click  **Update Account** to update the properties of the guest account. A new account receipt is displayed, allowing you to print a receipt showing the updated account details.




-  **Sessions** – Displays the active sessions for a guest account. See "Active Sessions Management" on page 35 in this chapter for details about managing active sessions.
-  **Print** – Displays the guest account’s receipt and the delivery options for the receipt. For security reasons, the guest’s password is not displayed on this receipt. To recover a forgotten or lost guest account password, use the  **Reset password** link.
- **Show Details**—The row expands to display all the properties of the guest's account in a table, including endpoint details. This option is only available to users whose operator profile includes the Show Details privilege.

Figure 32 *The Show Details View*

Username	Role	State	Activation	Expiration
 test	[Guest]	Active	2.2 days ago	No expiry
 Reset password  Change expiration  Remove  Edit  Sessions  Print  Show Details				
Field	Label	Value	Display	
id		3001	3001	
username	Username:	test	test	
create_time	Created:	1405359304	2014-07-14 10:35:04	
current_state	Current State:	active	Active	
do_expire	Expire Action:	0	0	
email	Email Address:	test@a	test@a	
enabled	Account Status:	1	Enabled	
expired_notify_status	Expired Notification Status:	1	1	
expire_postlogin	Account Lifetime:	0		
expire_time	Expiration Time:	0		
notes	Notes:			
remote_addr	Create Address:	10.11.9.215	10.11.9.215	
role_id	Account Role:	2	2	
role_name	Account Role:	[Guest]	[Guest]	
simultaneous_use	Session Limit:	1	1	
source	Create Source:	create_user	create_user	
sponsor_name	Sponsor's Name:	admin	admin	
sponsor_profile		1	1	
sponsor_profile_name	Sponsor's Profile:	Super Administrator	Super Administrator	
start_time	Activation Time:	1405359315	2014-07-14 10:35	
visitor_carrier	Mobile Carrier:			
visitor_company	Company Name:	c	c	
visitor_name	Guest's Name:	test	test	

Changing a Guest Account Role

If you are changing a guest account's role, you must also configure change of authorization (CoA) requests to handle the change correctly. This ensures that the appropriate CoA requests are triggered for active sessions. The following steps are performed in ClearPass Policy Manager:

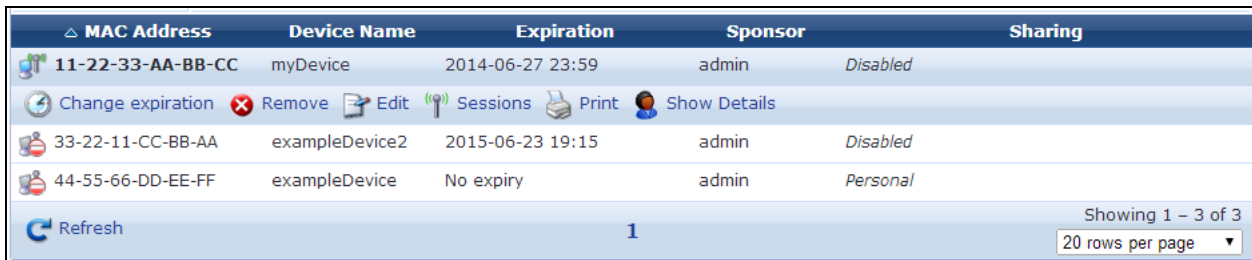
1. Go to **Policy Manager > Configuration > Enforcement > Profiles > Add**.
2. On the **Profile** tab, open the the **Template** drop-down list and select **RADIUS Change of Authorization (CoA)**.
3. In the **Name** field, the name you enter for the profile must include the exact role name in square brackets. For example, for the role "[Guest]", the profile name might be "My Company [Guest] CoA".
4. On the **Attributes** tab, open the **Select RADIUS CoA Template** drop-down list and select **Aruba - Change-User-Role**.
5. Click a row and add an attribute with the **Type** as **Radius:IETF**. For the **Value** enter the role name, but without the square brackets this time.




Managing Devices

To view the list of current MAC devices, go to **Guest > Manage Devices**.

The **Manage Devices** list view opens.






Figure 33 *The Manage Devices List View*



MAC Address	Device Name	Expiration	Sponsor	Sharing
 11-22-33-AA-BB-CC	myDevice	2014-06-27 23:59	admin	Disabled
 33-22-11-CC-BB-AA	exampleDevice2	2015-06-23 19:15	admin	Disabled
 44-55-66-DD-EE-FF	exampleDevice	No expiry	admin	Personal

All devices created by one of methods described in the section "[Creating a Device](#)" on page 45 are listed. Options let you change a device's account expiration time; activate, remove, or edit the device; view active sessions or details for the device; or print details, receipts, confirmations, or other information.


The **MAC Address**, **Device Name**, **Expiration**, **Sponsor**, and **Sharing** columns display information about the device accounts that have been created:

- The value in the **Expiration** column is **colored red** if the device account will expire within the next 24 hours. The expiration time is additionally highlighted in **boldface** if the device account will expire within the next hour.
- In addition, icons in the **MAC Address** column indicate the device account's activation status:
 -  —Device account is active
 -  —Device account was created but is not activated yet
 -  —Device account was disabled by Administrator
 -  —Device account has expired
 -  —Device account was deleted

You can use the **Filter** field to narrow the search parameters. You may enter a simple substring to match a portion of any fields that are configured for search, and you can include the following operators:

Table 18: Operators supported in filters

Operator	Meaning	Additional Information
=	is equal to	<p>You may search for multiple values when using the equality (=) or inequality (!=) operators. To specify multiple values, list them separated by the pipe character ().</p> <p>For example, specifying the filter "role_id=2 3, custom_field=Value" restricts the accounts displayed to those with role IDs 2 and 3 (Guest and Employee), and with the field named "custom_field" set to "Value".</p>
!=	is not equal to	
>	is greater than	
>=	is greater than or equal to	
<	is less than	
<=	is less than or equal to	
~	matches the regular expression	
!~	does not match the regular expression	

To restore the default view, click the  **Clear Filter** link.

You can use the paging controls at the bottom of the list to jump forwards or backwards by one page or to jump directly to an individual page number, or to change the number of rows that are displayed on one page.

Figure 34 The Paging Control



To select a device, click the device you want to work with.

Changing a Device's Expiration Date

To change a device's expiration date, click the device's row in the **Guest Manager Devices** list, and then click its **Change expiration** link. The row expands to include the **Change Expiration** form.

Figure 35 *The Change Expiration Form*

Table 19: *The Change Expiration Form*

Field	Description
Username	The device's MAC address.
Account Expiration	The first Account Expiration row displays the expiration setting that is currently configured.
Account Expiration	Lets you change the expiration setting. Options include: <ul style="list-style-type: none"> • No changes: Account will not expire • Now • Tonight • Friday night • 1 hour from now • 1 day from now • 1 week from now • 30 days from now • 90 days from now • 180 days from now • 1 year from now • Account expires after... • Account expires at a specified time
Expire Action	Specifies the action to take at expiration. Options include: <ul style="list-style-type: none"> • Delete and log out at specified time • Delete at specified time • Disable and log out at specified time • Disable at specified time

Field	Description
Expires After	Specifies an amount of time after which the account will expire. Options include intervals of hours, days, or weeks.
Expiration Time	Specifies a date and time when the account will expire. Click the button to open the calendar picker. In the calendar, use the arrows to select the year and month, click the numbers in the Time fields to increment the hours and minutes, and then click a day to select the date.
Update Account	Commits your changes.

Disabling and Deleting Devices

To remove a device's account by disabling or deleting it, click the device's row in the **Guest Manager Devices** list, then click its **Remove** link. The row expands to include the **Remove Account** form.

Figure 36 *The Remove Account Form*

You may choose to either disable or delete the account. If you disable it, it remains in the device list and you may activate it again later. If you delete the account, it is removed from the list permanently.

Activating a Device

To activate a disabled device's account, click the device's row in the **Guest Manager Devices** list, then click its **Activate** link. The row expands to include the **Enable Guest Account** form.

Figure 37 *The Enable Guest Account Form*

Table 20: *The Enable Guest Account Form*

Field	Description
Username	The MAC address of the device.
Account Expiration	The expiration setting that is currently configured.
Activate Account	Specifies when to activate the account. You may choose an interval, or you may choose to specify a time.
Activation Time	Specifies the date and time to activate the account. Click the button to open the calendar picker. In the calendar, use the arrows to select the year and month, click the numbers in the Time fields to increment the hours and minutes, and then click a day to select the date.
Enable Account	Commits your changes.

Editing a Device

To edit a device's account, click the device's row in the **Guest Manager Devices** list, then click its **Edit** link. The row expands to include the **Edit Device** form. You can edit any of the device's properties.

Figure 38 *The Edit Device Form*

Edit Device

* MAC Address:	<input type="text" value="1A-2B-3C-4D-5E-6F"/> <small>MAC address of the device.</small>
* Device Name:	<input type="text" value="myDevice"/> <small>Name of the guest.</small>
AirGroup:	<input checked="" type="checkbox"/> Enable AirGroup <small>AirGroup uses device ownership and location information to limit the printers and Apple TVs available to network users.</small>
Ownership:	<input type="radio"/> Personal <input checked="" type="radio"/> Shared <small>A personal device is automatically shared with other devices owned by the same user. A shared device has no owner, but more sharing options are available.</small>
Shared With:	<input type="text"/> <small>Enter the usernames that will be able to use this device. Use a comma-separated list, e.g. user1,user2,user3, or blank for all users.</small>
Shared Locations:	<input type="text"/> <small>Select the locations where this device will be shared.</small>
Shared Roles:	<input type="text"/> <small>Select the user roles that will be able to use this device.</small>
Shared Groups:	<input type="text"/> <small>Select the user groups that will be able to use this device. This feature requires AOS 6.4 or later.</small>
Time Sharing:	<input type="text"/> Syntax <small>Specify time-based sharing rules for this device.</small>
Account Activation:	(No changes: Account is active) ▾ <small>Select an option for changing the activation time of this account.</small>
Account Expiration:	(No changes: 2015-01-06 15:02:42) ▾ <small>Select an option for changing the expiration time of this account.</small>
Account Role:	(No changes: [Guest]) ▾ <small>Role to assign to this account.</small>
Notes:	<input style="width: 100%; height: 40px;" type="text"/>

Table 21: *New Device*

Field	Description
MAC Address	The device's MAC address.
Device Name	The name for the device. If you need to modify the configuration for the expected separator format or case, go to Administration > Plugin Manager > Manage Plugins and click the Configuration link for the MAC Authentication Plugin .
AirGroup	Enables AirGroup for the device. Configuration options are added to the form.
Ownership	Specifies whether device ownership should be personal or shared. Personal devices are automatically shared with the owner's other devices.
Shared With	<p>Username of people who can share this device. Enter usernames as a comma-separated list. To make the device available to all users, leave this field blank.</p> <p>Each username may not exceed 64 characters. A maximum of 100 usernames may be entered. The maximum character limit for the list is 1000 characters (including comma separators).</p>
Shared Locations	<p>Locations where the device can be shared. When you type a location name in the Shared Locations field and press the Enter key, the location appears as a "tag" and is created in the system when the form is saved.</p> <p>Each location name may not exceed 64 characters. A maximum of 100 location names may be entered. The maximum character limit for the list is 1000 characters (including comma separators).</p>
Shared Roles	<p>User roles that can share this device. When you type a role name in the Shared Roles field and press the Enter key, the role appears as a "tag" and is created in the system when the form is saved.</p> <p>Each role name may not exceed 64 characters. A maximum of 100 role names may be entered. The maximum character limit for the list is 1000 characters (including comma separators).</p>
Shared Groups	<p>User groups that can share this device. These will be available in the Shared Groups field for users to choose from when they share a device.</p> <p>When you type a name for the group in the Group Names field and press the Enter key, the group appears as a "tag" and is created in the system when the form is saved.</p> <p>Each group name may not exceed 64 characters. A maximum of 32 group names may be entered. The maximum character limit for the list is 320 characters (including comma separators).</p>
Time Sharing	Time-based sharing rules for this device. For more information, see "About AirGroup Time-Based Sharing" on page 89 .
Syntax	Opens the help topic "AirGroup Time-Based Sharing Syntax Examples" on page 85 .
Account Activation	Options include: Activate the account immediately, at a preset interval of hours or days, at a specified time, or leave the account disabled.
Activation Time	Specifies the date and time to activate the account. Click the button to open the calendar picker. In the calendar, use the arrows to select the year and month, click the numbers in the Time fields to increment the hours and minutes, then click a day to select the date.
Account Expiration	<p>Lets you change the expiration setting. Options include: Never expire, expire at a preset interval of hours or days, or expire at a specified time.</p> <ul style="list-style-type: none"> If you choose any time in the future, the Expire Action row is added to the form.

Field	Description
	<p>Indicate the expiration action for the account—either delete, delete and log out, disable, or disable and log out. The action will be applied at the time set in the Account Expiration row.</p> <ul style="list-style-type: none"> If you choose Account expires after, the ExpiresAfter row is added to the form. Choose an interval of hours, days, or weeks. The maximum is two weeks. If you choose Account Expires at a specified time, the ExpirationTime row is added to the form. In the calendar picker, use the arrows to select the year and month, click the numbers in the Time fields to increment the hours and minutes, then click a day to select the date.
Account Role	Assigns the visitor's role.
Notes	Optional additional information.
Update Device	Commits your changes and updates the device. The Updated Device Details and print options are displayed.

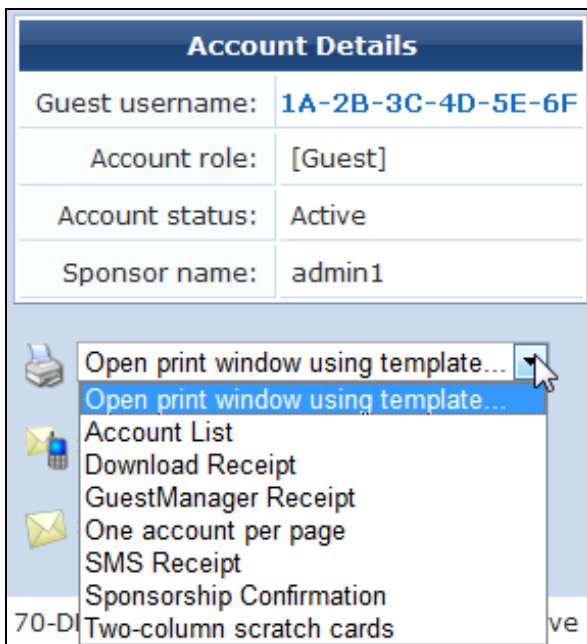
Viewing Current Sessions for a Device

To view any sessions that are currently active for a device, click the **Sessions** link in the device's row on the **Guest Manager Devices** form. The **Active Sessions** list opens. For more information, see "[Active Sessions Management](#)" on page 35.

Printing Device Details

To print details, receipts, confirmations, or other information for a device, click the device's row in the **Guest Manager Devices** list, then click its **Print** link. The row expands to include the **Account Details** view and a drop-down list of information that can be printed for the device.

Figure 39 *The Account Details and Printing Options*



Choosing an option in the **Open print window using template** drop-down list opens a print preview window and the printer dialog. Options include account details, receipts in various formats, a session expiration alert, and a sponsorship confirmation notice.

Viewing Device Details

- **Show Details**—The row expands to display all the properties of the device's account in a table. This option is only available to users whose operator profile includes the Show Details privilege.

Managing Multiple Guest Accounts

Use the **Bulk Edit Accounts** list view to work with multiple guest accounts. To open the **Bulk Edit Accounts** list, go to **Guest > Manage Multiple Accounts**.

This view (guest_multi) may be customized by adding new fields or by modifying or removing the existing fields. See "Customizing Guest Self-Registration" on page 341 for details about this customization process. The default settings for this view are described below.

Figure 40 The Bulk Edit Accounts List View

Username	Role	State	Activation	Expiration	Lifetime
11-22-33-AA-BB-CC	[Guest]	Active	10 minutes ago	2014-06-27 23:59	N/A
33-22-11-CC-BB-AA	[Guest]	Disabled	3 minutes ago	2015-06-23 19:15	N/A
44-55-66-DD-EE-FF	[Guest]	Disabled	9 minutes ago	No expiry	N/A


The **Username**, **Role**, **State**, **Activation**, **Expiration**, and **Lifetime** columns display information about the visitor accounts that have been created:

- The value in the **Expiration** column is **colored red** if the visitor account will expire within the next 24 hours. The expiration time is additionally highlighted in **boldface** if the visitor account will expire within the next hour.
- In addition, icons in the **Username** column indicate the account's activation status:
 - —Visitor account is active
 - —Visitor account was created but is not activated yet
 - —Visitor account was disabled by Administrator
 - —Visitor account has expired

You can use the **Filter** field to narrow the search parameters. You may enter a simple substring to match a portion of the username or any other fields that are configured for search, and you can include the following operators:

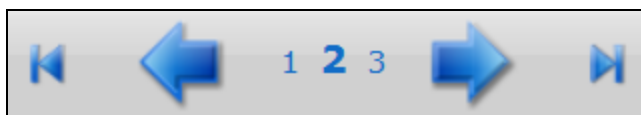
Table 22: Operators supported in filters

Operator	Meaning	Additional Information
=	is equal to	<p>You may search for multiple values when using the equality (=) or inequality (!=) operators. To specify multiple values, list them separated by the pipe character ().</p> <p>For example, specifying the filter "role_id=2 3, custom_field=Value" restricts the accounts displayed to those with role IDs 2 and 3 (Guest and Employee), and with the field named "custom_field" set to "Value".</p>
!=	is not equal to	
>	is greater than	
>=	is greater than or equal to	
<	is less than	
<=	is less than or equal to	
~	matches the regular expression	
!~	does not match the regular expression	

To restore the default view, click the  **Clear Filter** link.


You can use the paging controls at the bottom of the list to jump forwards or backwards by one page or to jump directly to an individual page number, or to change the number of rows that are displayed on one page.


Figure 41 The Paging Control



To select guest accounts, click the accounts you want to work with. You may click either the check box or the row to select a visitor account. To select or deselect all visible visitor accounts, click the check box in the header row of the table.

Use the selection row at the top of the table to work with the current set of selected accounts. The number of currently selected accounts is shown. When a filter is in effect, the "All Matching" link can be used to add all pages of the filtered result to the selection.

Use the  **Create** tab to create new visitor accounts using the **Create Multiple Guest Accounts** form. See "[Managing Multiple Guest Accounts](#)" on page 76 in this chapter for details about this form.

Use the  **Delete** tab to delete the visitor accounts that you have selected. This option is not active if there are no visitor accounts selected.




Use the  **Edit** tab to make changes to multiple visitor accounts at once. This option is not active if there are no visitor accounts selected. If you are editing an account's role, see "[Managing Multiple Guest Accounts](#)" on page 76.

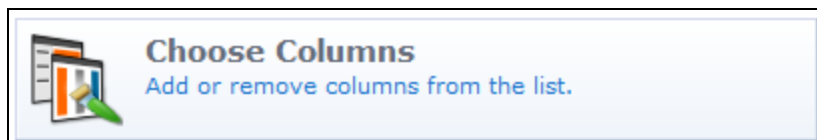
Figure 42 *The Edit Guest Accounts Form*

Edit Guest Accounts	
* Password:	(No changes) <input type="button" value="v"/> <small>Select an option for changing visitor account passwords.</small>
Account Role:	(No changes) <input type="button" value="v"/> <small>Select a new role for these visitor accounts.</small>
Account Activation:	(No changes) <input type="button" value="v"/> <small>Select an option for changing the activation time of this account.</small>
Account Expiration:	(No changes) <input type="button" value="v"/> <small>Select an option for changing the expiration time of this account.</small>
Session Limit:	<input type="text"/> <small>The number of simultaneous sessions allowed for these visitor accounts. Type 0 for unlimited use. Leave this field blank to not make any changes.</small>
<input type="button" value="Make Changes"/>	

The **Edit Guest Accounts** form may be customized by adding new fields, or modifying or removing the existing fields. See "Customizing Guest Self-Registration" on page 341 for details about this customization process. This is the **guest_multi_form** form.

The  **Results** tab will be automatically selected after you have made changes to one or more guest accounts. You can create new guest account receipts or download the updated guest account information. See "Creating Multiple Guest Account Receipts" on page 52 in this chapter for more information.

The  **More Options** tab includes the **Choose Columns** command link. You can click this link to open the Configuration module's **Customize View Fields** form, which may be used to customize the **Edit Guest Accounts** view.



Changing a Guest Account Role

If you are changing a guest account's role, you must also configure change of authorization (CoA) requests to handle the change correctly. This ensures that the appropriate CoA requests are triggered for active sessions. The following steps are performed in ClearPass Policy Manager:

1. Go to **Policy Manager > Configuration > Enforcement > Profiles > Add**.
2. On the **Profile** tab, open the the **Template** drop-down list and select **RADIUS Change of Authorization (CoA)**.
3. In the **Name** field, the name you enter for the profile must include the exact role name in square brackets. For example, for the role "[Guest]", the profile name might be "My Company [Guest] CoA".
4. On the **Attributes** tab, open the **Select RADIUS CoA Template** drop-down list and select **Aruba - Change-User-Role**.
5. Click a row and add an attribute with the **Type** as **Radius:IETF**. For the **Value** enter the role name, but without the square brackets this time.

AirGroup Device Registration

AirGroup allows users to register their personal mobile devices on the local network and define a group of friends or associates who are allowed to share them. If AirGroup Services is enabled, AirGroup administrators can provision their organization's shared devices and manage access, and AirGroup operators can register and

provision a limited number of their own personal devices for sharing. For complete AirGroup deployment information, refer to the AirGroup sections in the *ArubaOS User Guide* and the ClearPass Policy Manager documentation.

This section includes:

- "Registering Groups of Devices or Services" on page 79
- "Registering Personal Devices" on page 82
- "AirGroup Time-Based Sharing Syntax Examples" on page 85
- "About AirGroup Time-Based Sharing" on page 89

Registering Groups of Devices or Services

This functionality is only available to AirGroup administrators.

To register and manage an organization's shared devices and configure device access, log in as the AirGroup administrator and go to **Guest > Create Device**. The **Register Shared Device** form opens.

Figure 43 *The Register Shared Device Form*

Table 23: *The Register Shared Device Form*

Field	Description
Device Name	(Required) Enter the name used to identify the device.
Device Type	(Required) Specifies the device type.
MAC Address	(Required) Enter the device's MAC address.

Field	Description								
Shared Locations	<p>Lets you specify the locations where the device can be shared. To allow the device to be shared with all locations, leave this field blank.</p> <p>Each location name may not exceed 64 characters. A maximum of 100 location names may be entered. The maximum character limit for the list is 1000 characters (including comma separators). Each location is entered as a tag=value pair describing the MAC address of the access point (AP) closest to the registered device. Use commas to separate the tag=value pairs in the list. Tag=value pair formats are as follows:</p> <table border="1"> <thead> <tr> <th>AP Type</th> <th>Tag=Value Format</th> </tr> </thead> <tbody> <tr> <td>Name-based AP</td> <td>ap-name=<name></td> </tr> <tr> <td>Group-based AP</td> <td>ap-group=<group></td> </tr> <tr> <td>FQLN-based AP</td> <td>fqln=<fqln></td> </tr> </tbody> </table> <ul style="list-style-type: none"> AP FQLNs should be configured in the format <ap name>.<floor>.<building>.<campus> Floor names should be in the format floor <number> The <ap-name> should not include periods (.) <p>Example: AP105-1.Floor 1.TowerD.Mycompany</p>	AP Type	Tag=Value Format	Name-based AP	ap-name=<name>	Group-based AP	ap-group=<group>	FQLN-based AP	fqln=<fqln>
AP Type	Tag=Value Format								
Name-based AP	ap-name=<name>								
Group-based AP	ap-group=<group>								
FQLN-based AP	fqln=<fqln>								
Shared With	<p>Lets you specify the usernames of your organization's staff or students who are allowed to use the device. Use commas to separate usernames in the list.</p> <p>Each username may not exceed 64 characters. A maximum of 100 usernames may be entered. The maximum character limit for the list is 1000 characters (including comma separators).</p> <ul style="list-style-type: none"> If the Shared With field is left blank, this device can be accessed by all devices. If users are entered in the Shared With field, the device can only be accessed by the specified users. 								
Shared Roles	<p>Lets you specify the user roles that are allowed to use the device. Use commas to separate the roles in the list.</p> <p>Each role name may not exceed 64 characters. A maximum of 100 role names may be entered. The maximum character limit for the list is 1000 characters (including comma separators).</p> <ul style="list-style-type: none"> To make the device available to all roles, leave this field blank. If roles are entered in the Shared Roles field, the device can only be accessed by users with matching roles. 								
Register Shared Device	<p>Saves your changes and registers the device. The Finished Creating Guest Account page opens. This page displays Account Details and provides printer options.</p>								

Field	Description												
	<div style="border: 1px solid black; padding: 5px;"> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th colspan="2" style="background-color: #003366; color: white; text-align: center;">Account Details</th> </tr> </thead> <tbody> <tr> <td style="padding: 2px;">Guest username:</td> <td style="padding: 2px;">34-44-22-12-34-56</td> </tr> <tr> <td style="padding: 2px;">Account role:</td> <td style="padding: 2px;">[Guest]</td> </tr> <tr> <td style="padding: 2px;">Account status:</td> <td style="padding: 2px;">Active</td> </tr> <tr> <td style="padding: 2px;">Account activation:</td> <td style="padding: 2px;">Friday, 05 April 2013, 1:12 AM</td> </tr> <tr> <td style="padding: 2px;">Sponsor name:</td> <td style="padding: 2px;">AGAdmin</td> </tr> </tbody> </table> <p style="font-size: small; margin-top: 5px;">* required field</p> <div style="display: flex; align-items: center; margin-top: 5px;"> <input style="border: 1px solid gray; padding: 2px 10px;" type="text" value="Open print window using template..."/> </div> </div>	Account Details		Guest username:	34-44-22-12-34-56	Account role:	[Guest]	Account status:	Active	Account activation:	Friday, 05 April 2013, 1:12 AM	Sponsor name:	AGAdmin
Account Details													
Guest username:	34-44-22-12-34-56												
Account role:	[Guest]												
Account status:	Active												
Account activation:	Friday, 05 April 2013, 1:12 AM												
Sponsor name:	AGAdmin												

To view and edit your organization's shared AirGroup devices:

1. Go to **Guest > List Devices**, or click the **Manage my AirGroup Devices** link on the **Create AirGroup Device** page. The **AirGroup Devices** page opens. This page lists all the shared AirGroup devices for the organization. You can remove a device; edit a device's name, MAC address, shared locations, shared-user list, or shared roles; print device details; or add a new device.
2. To work with a device, click the device's row in the list. The form expands to include the **Remove**, **Edit**, and **Print** options.

Figure 44 The Edit Shared Device Form

The screenshot shows a web interface for managing shared devices. At the top, there is a 'Quick Help' link and a 'Create' button. Below this is a 'Filter' input field. A table lists shared devices with columns for Device Name, MAC Address, Created By, Created, Shared Locations, Shared With, and Shared Roles. The first device is 'SharedPrinter1' with MAC address '34-44-22-12-34-56', created by 'AGAdmin' on '2013-04-05 01:10', and shared with 'Sushant,Asano,Bill'. Below the table are 'Remove', 'Edit', and 'Print' icons. A text prompt says 'To update the properties of this shared AirGroup device, use the form below:'. The 'Edit Shared Device' form has the following fields:

- * Device Name:** Enter a name to identify the device.
- * Device Type:** Select the type of your device.
- * MAC Address:** Enter the MAC address of the device.
- Shared Locations:** Select up to 5 locations where this device will be shared.
- Shared With:** Enter up to 10 usernames that will be able to use this device. Use a comma-separated list, e.g. user1,user2,user3.
- Shared Roles:** Select up to 10 user roles that will be able to use this device.

A 'Save Changes' button is located at the bottom of the form.

3. To edit properties of a shared device, click the **Edit** link for the device. The row expands to include the **Edit Shared Device** form. You can modify the device’s name, MAC address, shared locations, group of users, and shared roles.
4. When your edits are complete, click **Save Changes**.

Registering Personal Devices

This functionality is available to AirGroup operators.

To register your personal devices and define a group who can share them:

1. Log in as the AirGroup operator and go to **Guest > Create Device**. The **Register Device** form opens.

Figure 45 *The Register Device Form*

Register Device

* Your Name:	<div style="display: flex; align-items: center;"> AGoperator1 </div> <p style="font-size: small; color: #003366;">Name of the person sponsoring this visitor account.</p>
* Device Name:	<input style="width: 80%;" type="text" value="MyBluRay"/> <p style="font-size: small; color: #003366;">Enter a name to identify your device.</p>
* Device Type:	<input style="width: 80%;" type="text" value="Blu-Ray Player"/> <p style="font-size: small; color: #003366;">Select the type of your device.</p>
* MAC Address:	<input style="width: 80%;" type="text" value="11-22-33-AA-BB-CC"/> <p style="font-size: small; color: #003366;">Enter the MAC address of the device.</p>
Shared With:	<input style="width: 80%;" type="text" value="user1,user2,user3"/> <p style="font-size: small; color: #003366;">Enter up to 10 usernames that will be able to use this device. Use a comma-separated list, e.g. user1,user2,user3.</p>

Table 24: *The Register Device Form*

Field	Description
Your Name	(Required) Enter your username for your organization.
Device Name	(Required) Enter the name used to identify the device.
Device Type	(Required) Select the device type.

Field	Description												
MAC Address	(Required) Enter the device's MAC address.												
Shared With	<p>Lets you enter the usernames of your friends or colleagues who are allowed to use the device. Use commas to separate usernames in the list. You may enter up to ten usernames.</p> <ul style="list-style-type: none"> If the Shared With field is left blank, this device can only be accessed by devices registered by the same operator or with a dot1x username that matches the operator's name. If users are entered in the Shared With field, the device can be accessed by the device owner and by the specified users. 												
Register Device	<p>Saves your changes and registers the device. The Finished Creating Guest Account page opens. This page displays account details and provides printer options.</p> <table border="1" data-bbox="370 590 1063 919"> <thead> <tr> <th colspan="2">Account Details</th> </tr> </thead> <tbody> <tr> <td>MAC Address:</td> <td>11-22-33-AA-BB-CC</td> </tr> <tr> <td>Account status:</td> <td>Active</td> </tr> <tr> <td>Account activation:</td> <td>Friday, 05 April 2013, 12:55 AM</td> </tr> <tr> <td>Account role:</td> <td>[Guest]</td> </tr> <tr> <td>Sponsor name:</td> <td>AGoperator1</td> </tr> </tbody> </table>	Account Details		MAC Address:	11-22-33-AA-BB-CC	Account status:	Active	Account activation:	Friday, 05 April 2013, 12:55 AM	Account role:	[Guest]	Sponsor name:	AGoperator1
Account Details													
MAC Address:	11-22-33-AA-BB-CC												
Account status:	Active												
Account activation:	Friday, 05 April 2013, 12:55 AM												
Account role:	[Guest]												
Sponsor name:	AGoperator1												

To view and edit your personal AirGroup devices:

- Go to **Guest > List Devices**, or click the **Manage my AirGroup Devices** link on the **Create AirGroup Device** page. The **AirGroup Devices** page opens. This page lists all your personal AirGroup devices. You can remove a device; edit a device's name, MAC address, or shared-user list; print device details; or add a new device.
- To work with a device, click the device's row in the list. The form expands to include the **Remove**, **Edit**, and **Print** options.

Figure 46 *The Edit Device Form*

The screenshot shows a web interface for managing AirGroup devices. At the top, there is a 'Quick Help' link and a 'Create' button. Below this is a 'Filter' input field. A table lists devices with columns for 'Device Name', 'MAC Address', 'Created', and 'Shared With'. The first device is 'MyBluRay' with MAC address '11-22-33-AA-BB-CC', created on '2013-04-05 00:44', and shared with 'user1,user2,user3'. Below the table are 'Remove', 'Edit', and 'Print' actions. A message states: 'To update the properties of this personal AirGroup device, use the form below:'. The 'Edit Device' form includes:

- Your Name: AGoperator1 (Name of the person sponsoring this visitor account.)
- * Device Name: MyBluRay (Enter a name to identify this device.)
- * Device Type: Blu-Ray Player (Select the type of your device.)
- * MAC Address: 11-22-33-AA-BB-CC (Enter the MAC address of the device.)
- Shared With: user1,user2,user3 (Enter up to 10 usernames that will be able to use this device. Use a comma-separated list, e.g. user1,user2,user3.)

 A 'Save Changes' button is at the bottom of the form. A legend indicates '* required field'. At the bottom of the page, there is a 'Refresh' button, a page number '1', and a 'Showing 1 - 1 of 1' indicator with a '20 rows per page' dropdown.

- To edit properties of a device, click the **Edit** link for the device. The row expands to include the **Edit Device** form. You can modify the device's name, MAC address, and group of users. When your edits are complete, click **Save Changes**.

AirGroup Time-Based Sharing Syntax Examples

This section provides examples and discussions of syntax for time-based sharing policies for AirGroup shared devices.

For information on using time-based sharing for AirGroup, see ["About AirGroup Time-Based Sharing"](#) on page 89. For supplemental time-based syntax information, see ["Time-Based Syntax Reference"](#) on page 88.

Example:

```
periodic Monday 9am to 10am shared users A, B
```

The device is shared with users A and B, from 9am to 10am every Monday (relative to the server's current time zone). Outside of this time slot, the device is **not** shared (except as otherwise controlled by AOS).

Example:

```
periodic Monday 9:00 to 10:30 shared users A, B
periodic Monday 12:00 to 13:30 shared users A, B
periodic Monday 15:00 to 16:30 shared users C, D
```

The device is shared with users A and B, from 9am to 10:30am and from noon to 1:30pm every Monday (relative to the server's current time zone). From 3pm to 4:30pm, the device is shared with users C and D. Outside of these two time slots, the device is **not** shared.

With **periodic**, times may be specified either in 24-hour format (**hh:mm**, from **0:00** to **24:00**), or in 12-hour format (**hh:mm** and **am** or **pm**).

Don't specify overlapping time ranges with **periodic** rules; this can lead to unexpected results.

The synonyms **rep**, **repeat** or **repeating** may also be used in place of **period** or **periodic**. All of these terms are treated identically.

Example:

```
default allow
periodic mon 9am to 10am shared users A, B
```

As in the first example, the device is shared with users A and B, from 9am to 10am every Monday. Outside of this time slot, the device **is shared** as specified by the other sharing state fields (shared users, locations, roles and/or groups). This is the meaning of the **default allow** statement.

If **default allow** is not specified, the normal behavior is **default deny**, which is the same as in the first example. Note that with **default deny** in effect, the AirGroup time sharing policy will override any other sharing rules that are specified, for as long as the time sharing policy is in effect.

Two and three-character shortened forms of weekdays are acceptable (e.g. "Mon" or "Mo" can be used for Monday, "Tue" or "Tu" for Tuesday, etc.) Case is not significant in the time sharing policy, so "Mon", "MON", and "mon" are all equivalent ways to specify "Monday".

Example:

```
default deny
not after 01-Feb-2014
periodic mon 9am to 10am shared users A, B
```

The device is shared with users A and B, from 9am to 10am every Monday. The **not after date** sets the end of the time sharing policy. Monday, January 27, 2014 is the last day that this time sharing policy will take effect.

After 10am on this date, the time sharing policy is no longer in effect; any other sharing rules that have been specified will then take effect.

Example:

```
default deny
not before 1/1/14
not after 01-Feb-2014
periodic mon 9am to 10am shared users A, B
```

The device is shared with users A and B, from 9am to 10am every Monday. The **not before date** sets the beginning of the time sharing policy. In this case, Monday, January 6, 2014 is the first day that this time sharing policy will take effect.

Prior to 9am 6 January 2014, the device is not shared (due to the **default deny**).

After 10am on 27 January 2014, the time sharing policy is no longer in effect; any other sharing rules that have been specified will then take effect.

Example:

```
time zone America/Los_Angeles
periodic Monday 9am to 10am shared users A, B
```

The device is shared with users A and B, from 9am to 10am every Monday (relative to the U.S. Pacific time zone). Daylight savings time rules are observed; the time period **9am to 10am** is always relative to that time zone.

Example:

```
periodic mon tue wed thu fri 9am to 10am shared users A, B
```

The device is shared with users A and B, from 9am to 10am every weekday (Monday, Tuesday, Wednesday, Thursday and Friday).

Example:

```
periodic weekdays 9am to 10am shared users A, B
```

weekday or **weekdays** can be used as a synonym for "Monday Tuesday Wednesday Thursday Friday". Similarly, **weekend** or **weekends** can be used as a synonym for "Saturday Sunday".

Example:

```
on Sep 16 9:00 to 13:00 shared location AP-Name=1341-ap01 shared group ABC shared role SomeRole shared user user02, user03, "user04", 'user05'
```

The device is shared with a single access point named **1341-ap01**, a single group named **ABC**, a single role named **SomeRole**, and 4 users named **user02**, **user03**, **user04**, and **user05**.

Note the quotes are not considered to be part of the user names **user04** and **user05**. (In this case, the quotes are redundant as there is no space or comma that requires quoting.)

No time zone is specified, so the date and time are determined relative to the server's time zone.

No year is specified, so the server's current year is used. In particular, after September 16 of any year, this rule will have no effect until the following year.

Example:

```
default allow
periodic 0:00 to 24:00 shared roles default_role
periodic mon 9am to 5pm shared roles other_role
```

The device is normally shared ("default allow") with a single role named **default_role** ("periodic 0:00 to 24:00 shared roles default_role").

On Monday from 9am to 5pm, the device is shared with a different role named **other_role**.

Note that even though the time ranges overlap, the sharing policies are completely distinct; on Mondays from 9am to 5pm, the role **default_role** will NOT have access to the device, because a different sharing rule is in effect. (The rule could instead have been written "periodic mon 9am to 5pm shared roles default_role, other_role" if this was the desired result.)

This example shows how to use an overlapping time range: place the most general time range first, with more specific time ranges later. In particular, reversing the order of the **periodic** statements will not work.

Example:

```
default deny
periodic 9:00 to 22:00 shared roles default_role
no periodic thu 9:00 to 17:00
periodic fri 9:00 to 17:00 not shared
```

This example shows how to share a device with a basic policy, and demonstrates two ways to disable sharing for a subset of the time period.

The device will be shared with a single role named **default_role**, from 9:00 to 22:00 each day. ("periodic 9:00 to 22:00 shared roles default_role").

On Thursday, the device is **not** shared between 9:00 and 17:00.

On Friday, the device is **not** shared between 9:00 and 17:00.

Example:

```
default allow
periodic 9:00 to 22:00 shared roles default_role
no periodic thu 9:00 to 17:00
periodic fri 9:00 to 17:00 not shared
```

This example is similar to the previous example; the device is not shared on Thursday and Friday between 9:00 and 17:00.

The difference is after 22:00 and before 9:00: in the previous example, the device is not shared during this time period, whereas with **default allow** the other AirGroup sharing rules will take effect (any shared users, roles, groups or locations that have been defined for the device).

Time-Based Syntax Reference

This reference describes the syntax used for time formats in time-based sharing rules. It supplements the examples for AirGroup time-based sharing by user groups discussed in ["AirGroup Time-Based Sharing Syntax Examples" on page 85](#). For more information on using time-based sharing with AirGroup, see ["About AirGroup Time-Based Sharing" on page 89](#).

The syntax for AirGroup time-based sharing policies supports all the default time-based ACL rules specified in TimeRangeACL. This ACL is a sequence of rules, one per line, according to the following syntax:

- `default allow|deny`

Specifies the default behavior for unmatched times; this is 'allow' only if no 'periodic' or 'absolute' rules are specified, otherwise it is 'deny'. Use 'default allow' if the remaining rules exclude times, otherwise use 'default deny' if the remaining rules are to include times. This rule may only be used once.

- `[time] zone default|server|...`

Specifies the time zone to use for matching times and specifying the time of day. If unset, the current time zone setting is used (note that this may vary due to operator and/or profile settings). If the value "default" or "server" is specified, the system's time zone is used. Otherwise, the named time zone is used. This rule may only be used once, and must be before any rules specifying a time interval.

- `[not] period(ic) [day-list] hh:mm to [day] hh:mm`

Specifies a periodic or daily interval. Recognized days include Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday and 3-letter abbreviations; the tokens "weekends" and "weekdays" may also be used. Without a day-list, all days of the week are matched. Time may be specified in 12 or 24 hour format, with the special time 24:00 indicating the end of the day.

Example: `periodic monday 8:00 to friday 17:00` matches between 8am and 5pm, Monday through Friday.

Example: `periodic weekdays 8:00 to 17:00` specifies the same thing as the example in the previous line.

Example: `periodic wed 11am to 11pm` matches between 11:00 and 23:00 on a Wednesday.

Example: `periodic weekend 0:00 to 24:00` matches any time on a Saturday or Sunday.

Example: `periodic saturday sunday 0:00 to 24:00` specifies the same thing as the example in the previous line.

The 'not' keyword may be specified to invert the allow/deny decision.

Example: `default allow; not period 23:00 to 6:00` (on 2 separate lines) allows access, except between 11pm and 6am.

Example: period 6:00 to 23:00 is equivalent to the example in the previous line.

- not before [date-and-time]

Specifies an absolute time before which access will always be rejected.

Example: not before 2010-07-01 09:00 matches after 9am on 1 July 2010.

- not after [date-and-time]

Specifies an absolute time after which access will always be rejected.

Example: not after 2011-01-01 00:00 matches before midnight on New Year's Day 2011.

- [not] abs(olute) [start-date-and-time] to [end-date-and-time]

Specifies a start and end interval. The date and time is a format recognized by strtotime(). Times between the start and end point are matched. The 'not' keyword may be specified to invert the allow/deny decision.

Example: absolute December 25 to December 26 matches all day on Christmas Day each year. (This does not match on December 26 as midnight on this date is the endpoint of the interval.)

A blank time ACL means "all times are allowed".

The following examples give common usage:

- 8:00 to 18:00 - allows access 8am to 6pm, every day, but not outside those times
- weekdays 9am to 5pm - allows access 9am to 5pm, Monday through Friday, but not outside those times
- weekdays 9am to 5pm
weekends 10am to 4pm - allows access 9am to 5pm, Monday through Friday, with reduced hours on Saturday and Sunday

Annual recurrences may be specified:

- weekdays 9am to 5pm
not absolute December 25 to December 26 - allows access 9am to 5pm, Monday through Friday, but not on Christmas Day

Less common cases:

- default allow
not 23:00 to 6:00 - allows access, except between 11pm and 6am daily
- 9:00 to 18:00
not before 2010-02-01 - allows daily access between 9am and 6pm, starting on February 1, 2010
- time zone Etc/GMT
9:00 to 18:00
not before 2010-02-01 - allows daily access between 9am and 6pm, starting on February 1, 2010, in the GMT time zone (useful if server is in a different time zone)

About AirGroup Time-Based Sharing

This section discusses time-based sharing policies for an AirGroup shared device.

For information on the syntax for time-based sharing policies for a AirGroup shared devices, see ["AirGroup Time-Based Sharing Syntax Examples" on page 85](#)

Time-based sharing is used in settings where an organization's shared devices are made available to groups of users according to a regular schedule, and device access is configured by group at the user level—for example:

- A university classroom or laboratory is used by a first-year physics class on Mondays, Wednesdays, and Fridays, by a group of researchers on Tuesdays and Thursdays, and for visiting speakers every other Saturday.
- A convention center has several major exhibitors who each hold an annual event, and who reserve their customary section of the convention center several years in advance.

In cases like this, you can enter rules to define the schedule on which shared devices in an area will be available to certain groups. You can also specify times when a device will not be available. This is a time-based sharing policy.

Device association is dynamic: When a shared device is available to a group, any user with that group attribute can access the device. When the user is no longer a member of the group (for example, at the end of the semester), they no longer have access, but the time-based sharing policy remains in effect and new users who are assigned the group attribute can access the shared device.

Basics of Time-Based Sharing Setup

When you create a device, enable it for AirGroup Services, and configure it as a shared device, you also have the option to specify time-based sharing (time fencing) for the device.

You first use the **Administration > AirGroup Services > Configure** form to create the groups who can share devices. When you type a name for the group in the **Group Name** field, press the **Enter** key, and click **Save**, the group is created in the system and appears as a "tag".

Figure 47 Tags Added in the Group Names Field

Sharing Options
Options for different AirGroup sharing types.

Group Names:

List the user groups that are available in the 'Shared Groups' field.
This list is automatically updated as new user group names are entered.
Note that removing a group name from this list does not remove it from any shared group lists.

On the **Guest > Create Device** or **Guest > List Devices > Edit** forms, the shared user groups you created are then available for selection when you click in the **Shared Groups** field. (This feature requires AOS 6.4 or later)

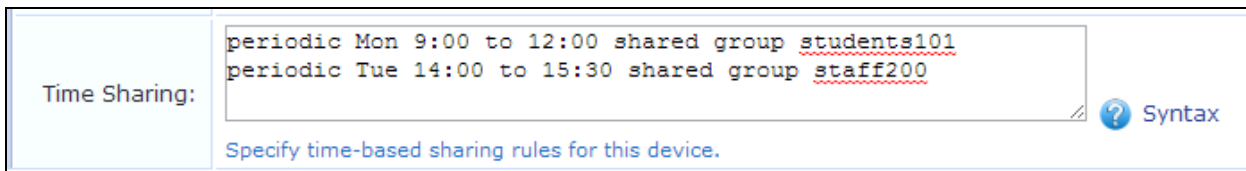
Figure 48 Groups Created as Tags Available for Selection in the Shared Groups Field

Shared With:	CityGardenShow
Shared Locations:	SaturdaySpeakerSeries
Shared Roles:	SRNTclinic
Shared Groups:	staff200
	students101

Select the user groups that will be able to use this device.

On the same screen, the next step is then to enter the rules for the time-based sharing policy, using the group names you created. For more information, see "[AirGroup Time-Based Sharing Syntax Examples](#)" on page 85

Figure 49 Entering Rules that Use the New Groups



Time Sharing:

```
periodic Mon 9:00 to 12:00 shared group students101
periodic Tue 14:00 to 15:30 shared group staff200
```

Specify time-based sharing rules for this device.

MAC Authentication in ClearPass Guest

ClearPass Guest supports a number of options for MAC Authentication and the ability to authenticate devices. The advanced features described in this section generally require a WLAN capable of MAC authentication with captive portal fallback. Please refer to the Aruba WLAN documentation for setting up the controller appropriately.

To verify that you have the most recent MAC Authentication Plugin installed and enabled before you configure these advanced features, go to **Administration > Plugin Manager**. For information on plugin management, see "Plugin Manager" on page 635.

MAC Address Formats

Different vendors format the client MAC address in different ways—for example:

- 112233AABBCC
- 11:22:33:aa:bb:cc
- 11-22-33-AA-BB-CC

ClearPass Guest supports adjusting the expected format of a MAC address. To configure formatting of separators and case in the address, as well as user detection and device filtering for views, go to **Administration > Plugin Manager** and click the **Configuration** link for the **MAC Authentication** plugin. The **MAC Authentication Configuration** page opens.

Figure 50 MAC Authentication Plugin Configuration



Configure MAC Authentication 6.0.1-22683

* MAC Detect:	<input type="checkbox"/> Allow users to be detected via their MAC address Provides access to user configuration for headers, footers, etc on login and registration pages. Please note that a passed MAC can be easily changed by the user, so personal details should not be displayed. Requires a vendor that passed the mac as part of the redirection.
Device Filter:	<input checked="" type="checkbox"/> List Accounts <input type="checkbox"/> Edit Accounts Select which views should not display devices (user accounts with the 'mac_auth' field set).



Table 25: *The Configure MAC Authentication Form*

Field	Description
MAC Detect	(Required) If selected, users can be detected by their MAC address, providing access to user configuration for headers, footers, etc. on login and registration pages. Requires a vendor that passed the MAC address as part of the redirect. Because a passed MAC address can easily be changed by the user, personal details should not be displayed.
Device Filter	Specifies which views should not display devices (user accounts with the “mac_auth” field set). Views that can be specified include: <ul style="list-style-type: none">• Manage Accounts• Manage Multiple Accounts
Save Configuration	Saves your changes.

On the controller, the fields look as follows:

Figure 51 *MAC Authentication Profile*

The screenshot shows a configuration form titled "MAC Authentication Profile > amigopod-mac". At the top right, there are three buttons: "Show Reference", "Save As", and "Reset". The form contains three fields: "Delimiter" is a dropdown menu set to "none"; "Case" is a dropdown menu set to "upper"; and "Max Authentication failures" is a text input field containing the number "0".

Automatically Registering MAC Devices in ClearPass

You can configure a guest MAC address to be automatically registered as an endpoint record in ClearPass Policy Manager when the guest uses a Web login page or a guest self-registration workflow. This customization option is available if a valid Local or RADIUS pre-authentication check was performed.

To configure auto-registration for an address through a Web login page:

1. Go to **Configuration > Pages > Web Logins**, click the row of the page you wish to configure, and then click its **Edit** link. The **Web Login Editor** form opens.
2. Scroll down to the **Post-Authentication** area.

Figure 52 The Web Login Editor Form, Post-Authentication Area

Post-Authentication	
Actions to perform after a successful pre-authentication.	
Health Check:	<input checked="" type="checkbox"/> Require a successful OnGuard health check If selected, the guest will be required to pass a health check prior to accessing the network.
Client Agents:	Native agents only Select the agent options for client scanning. Native agents are available for Microsoft Windows and Apple OS X. All other OS will fall back to Java.
Header HTML:	<input type="text"/> Insert... HTML template code displayed before the health check text.
Footer HTML:	<input type="text"/> Insert... HTML template code displayed after the health check text.
Update Endpoint:	<input checked="" type="checkbox"/> Mark the user's MAC address as a known endpoint If selected, the endpoint's attributes will also be updated with other details from the user account.
Advanced:	<input checked="" type="checkbox"/> Customize attributes stored with the endpoint
Endpoint Attributes:	username Username visitor_name Visitor Name cn Visitor Name visitor_phone Visitor Phone List of name value pairs to pass along. user_field Endpoint Attribute.
<input type="button" value="Save Changes"/> <input type="button" value="Save and Reload"/>	

3. Select the check box in the **Update Endpoint** row. This will mark the guest's MAC address as a known endpoint, and will also update the the endpoint's attributes with other details of the user account.
4. To specify custom attributes to store in the endpoint, select the check box in the **Advanced** row.
5. In the **Endpoint Attributes** field, enter a list of name-value pairs to pass as custom attributes. Follow the format "user_field | Endpoint Attribute". Examples are shown in this text box.
6. Click **Save Changes** to complete this configuration and continue with other tasks, or click **Save and Reload** to proceed to Policy Manager and apply the network settings.

Importing MAC Devices

The standard **Guest > Import Accounts** form supports importing MAC devices. At a minimum the following two columns are required: **mac** and **mac_auth**.

```
mac_auth,mac,notes
1,aa:aa:aa:aa:aa:aa,Device A
1,bb:bb:bb:bb:bb:bb,Device B
1,cc:cc:cc:cc:cc:cc,Device C
```

Any of the other standard fields can be added similar to importing regular guests.

Advanced MAC Features

This section describes some advanced features for MAC authentication.

User Detection on Landing Pages

When **mac** is passed in the redirect URL, the user is detected and a customized message displays on the landing page.

To use this feature:

1. Go to **Administration > Plugin Manager: MAC Authentication: Configuration** and enable **MAC Detect**.
2. Edit the header of your redirect landing page (login or registration) and include the following:

```
<p>{if $guest_receipt.u.visitor_name}
Welcome back to the show, { $guest_receipt.u.visitor_name|htmlspecialchars}!
{else}
Welcome to the show!
{/if}</p>
```

3. For debugging purposes, include the following to see all the fields available:

```
{dump var=$guest_receipt export=html}
```

Click-Through Login Pages

A click-through login page will present a splash or terms screen to the guest, yet still provide MAC-auth style seamless authentication. Under this scenario, you could have people create an account, with a paired MAC, yet still have them click the terms and conditions on every new connection.

To use this feature:

1. Disable MAC authentication on the controller.
2. Go to **Administration > Plugin Manager: MAC Authentication: Configuration** and enable **MAC Detect**.
3. Create a **Web Login**. Include the following settings:
 - Authentication: **Anonymous**
 - Anonymous User: **_mac** (*_mac is a special secret value*)
 - Pre-Auth Check: **Local**
 - Terms: **Require a Terms and Conditions confirmation**
4. Set the Web login as your landing page and test. Using a registered device the 'Log In' button should be enabled, otherwise it will be disabled.
5. You might also want to add a message so visitors get some direction:

```
<p>{if $guest_receipt.u.username}
{if $guest_receipt.u.visitor_name}
Welcome back, { $guest_receipt.u.visitor_name|htmlspecialchars}!
{else}
Welcome back.
{/if}
Please accept the terms before proceeding.
{else}
You need to register...
{/if}</p>
```

6. You can hide the login form by having the final line of the header be:

```
{if !$guest_receipt.u.username}<div style="display:none">{/if}
```

and the first line of the footer be:

```
{if !$guest_receipt.u.username}</div>{/if}
```



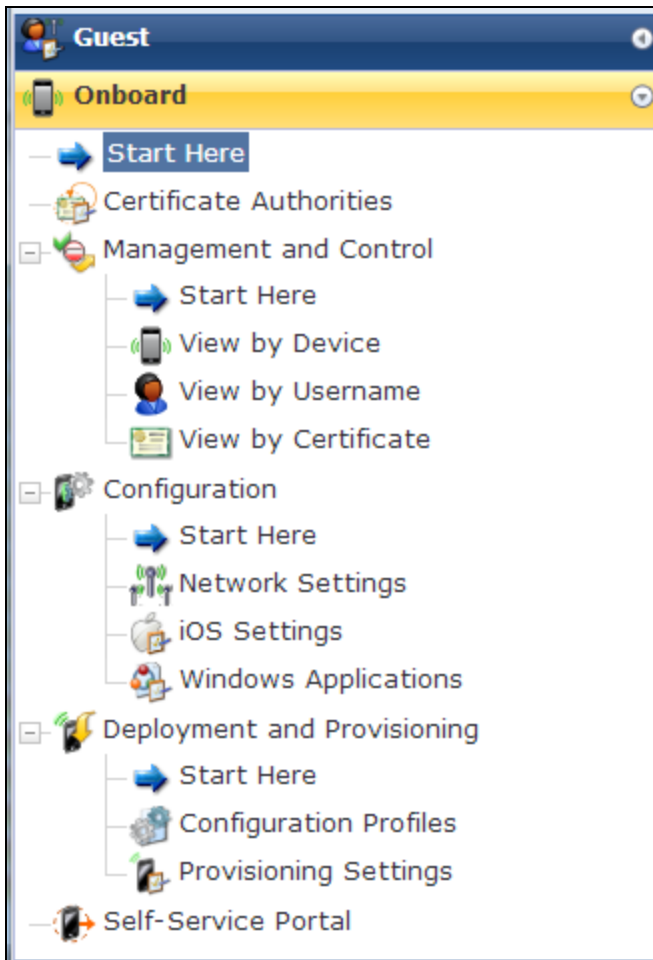
Onboarding is the process of preparing a device for use on an enterprise network by creating the appropriate access credentials and setting up the network connection parameters. ClearPass Onboard automates 802.1X configuration and provisioning for “bring your own device” (BYOD) and IT-managed devices across wired, wireless, and virtual private networks (VPNs).

ClearPass Onboard includes the following key features:

- Automatic configuration of network settings for wired and wireless endpoints
- Provisioning of unique device credentials for BYOD and IT-managed devices
- Support for Windows, Mac OS X, iOS, and Android devices
- Ability to revoke unique credentials on a specific user's device
- ClearPass Profiler for identifying device type, manufacturer, and model

Accessing Onboard

To access the device provisioning features of ClearPass Onboard, click the **Onboard** link in the left navigation.



About ClearPass Onboard

ClearPass Onboard automates 802.1X configuration and provisioning for “bring your own device” (BYOD) and IT-managed devices—Windows, Mac OS X, iOS and Android—across wired, wireless, and virtual private networks (VPNs).

ClearPass Onboard includes the following key features:

- Automatic configuration of network settings for wired and wireless endpoints.
- Provisioning of unique device credentials for BYOD and IT-managed devices.
- Support for Windows, Mac OS X, iOS, and Android devices.
- Enables the revocation of unique credentials on a specific user’s device.
- Uses ClearPass Profiler to identify device type, manufacturer, and model.

This section provides the following important information about ClearPass Onboard:

- ["Onboard Deployment Checklist " on page 97](#)
- ["Onboard Feature List " on page 99](#)
- ["Supported Platforms" on page 100](#)
- ["Public Key Infrastructure for Onboard" on page 101](#)
- ["Revoking Unique Device Credentials" on page 102](#)

- ["Network Requirements for Onboard"](#) on page 103
- ["Network Architecture for Onboard"](#) on page 105
- ["The ClearPass Onboard Process"](#) on page 107
- ["Configuring the User Interface for Device Provisioning"](#) on page 113
- ["Onboard Troubleshooting"](#) on page 114

Onboard Deployment Checklist

Table 26 lists planning, configuration, and testing procedures. Use this checklist to complete your Onboard deployment.

Onboard events are stored in the Application Log for seven days by default. After seven days, significant runtime events are listed in the Audit Viewer in ClearPass Policy Manager's Monitoring module. Onboard events that are listed include:

- Changing the CA certificate
- Issuing a new certificate
- Signing a certificate signing request
- Revoking a certificate
- Deleting a certificate
- Importing a trusted certificate
- Uploading a code-signing or other certificate

Table 26: *Onboard Deployment Checklist*

Deployment Step	Reference
Planning and Preparation	
Review the Onboard feature list to identify the major areas of interest for your deployment.	"Onboard Feature List " on page 99
Review the list of platforms supported by Onboard, and identify the platforms of interest for your deployment.	"Supported Platforms" on page 100
Review the Onboard public key infrastructure, and identify any Certificate Authorities that will be needed during the deployment.	"Public Key Infrastructure for Onboard" on page 101
Review the network requirements and the network architecture diagrams to determine how and where to deploy the Onboard solution.	Refer to the ClearPass Policy Manager documentation, and "Network Architecture for Onboard" on page 105 in this chapter
Configuration	
Configure the hostname and networking properties of the Onboard provisioning server. <ul style="list-style-type: none"> • DNS is required for SSL. • Ensure that hostname resolution will work for devices being provisioned. 	Refer to the ClearPass Policy Manager documentation
Configure SSL certificate for the Onboard provisioning server. A commercial SSL certificate is required to enable secure device	Refer to the ClearPass Policy Manager documentation

Deployment Step	Reference
provisioning for iOS devices.	
Configure the Onboard Certificate Authority. <ul style="list-style-type: none"> Decide whether to use the Root CA or Intermediate CA mode of operation. Create the certificate for the Certificate Authority.	"Certificate Authorities " on page 116
Configure device provisioning settings. <ul style="list-style-type: none"> Select certificate options for device provisioning. Select which device types should be supported.	"About Configuring Provisioning Settings " on page 221
Configure network settings for device provisioning. <ul style="list-style-type: none"> Set network properties. Upload 802.1X server certificates. Set device-specific networking settings.	"Network Settings " on page 163
Configure networking equipment for non-provisioned devices. <ul style="list-style-type: none"> Set authentication for the provisioning SSID, if required. Ensure the captive portal redirects non-provisioned devices to the device provisioning page.	"Network Requirements for Onboard" on page 103
Configure networking equipment to authenticate provisioned devices. <ul style="list-style-type: none"> Ensure 802.1X authentication methods and trust settings are configured correctly for all EAP types that are required. Configure OCSP or CRL on the authentication server to check for client certificate validity.	"Network Requirements for Onboard" on page 103
Configure the user interface for device provisioning. <ul style="list-style-type: none"> Set display options for iOS devices. Set user interface options for other Onboard devices. Setup the device provisioning Web login page.	"Configuring the User Interface for Device Provisioning" on page 113
Testing and Verification	
Test device provisioning. <ul style="list-style-type: none"> Verify that each type of device can be provisioned successfully. Verify that each type of device can join the provisioned network and is authenticated successfully.	
Test device revocation. <ul style="list-style-type: none"> Revoke a device's certificate. Verify that the device is no longer able to authenticate. Verify that re-provisioning the device fails.	

Onboard Feature List

The following features are available in ClearPass Onboard.

Table 27: *Onboard Features*

Feature	Uses
Automatic configuration of network settings for wired and wireless endpoints.	<ul style="list-style-type: none"> • Configure wired networks using 802.1X • Configure Wi-Fi networks using either 802.1X or Pre-Shared Key (PSK) • Configure trusted server certificates for 802.1X • Configure Windows-specific networking settings • Configure HTTP proxy settings for client devices (Android, OS X only)
Secure provisioning of unique device credentials for BYOD and IT-managed devices.	<ul style="list-style-type: none"> • Configure EAP-TLS and PEAP-MSCHAPv2 without user interaction • Revoke unique device credentials to prevent network access
Support for Windows, Mac OS X, iOS, and Android devices.	<ul style="list-style-type: none"> • Leverage ClearPass Profiling to identify device type, manufacturer, and model • Control the user interface displayed during device provisioning
Certificate Authority enables the creation and revocation of unique credentials on a specific user's device.	<ul style="list-style-type: none"> • Root and intermediate CA modes of operation • Supports SCEP enrollment of certificates • Supports CRL generation to list revoked certificates • Supports OCSP responder to query for certificate status • Approve certificate signing request • Reject certificate signing request • Sign certificate from uploaded certificate signing request (CSR) • Issue certificate • Revoke certificate • Display certificates • Export certificate • Renew root certificate
Provision additional settings specific to iOS devices	<ul style="list-style-type: none"> • Exchange ActiveSync • Passcode policy • VPN settings

Supported Platforms

The platforms supported by ClearPass Onboard and the version requirements for each platform are summarized in the following table.

Table 28: *Platforms Supported by ClearPass Onboard*

Platform	Example Devices	Version Required for Onboard Support	Notes
Apple iOS	iPhone iPad iPod Touch	iOS 4 and later	1, 3
Apple Mac OS X	MacBook Pro MacBook Air	Mac OS X 10.5 and later	1
		Mac OS X 10.5 and later	2
Android	Samsung Galaxy Motorola Droid Google Pixel	Android 2.2 (or higher)	2
Microsoft Windows	Laptop Desktop Tablet	Windows Vista with Service Pack 2 Windows 7.x Windows 8.x Windows 10.x	2, 4

Note 1: Uses the “Over-the-air provisioning” method.

Note 2: Uses the “Onboard provisioning” method.

Note 3: Onboard may also be used to provision VPN settings, Exchange ActiveSync settings, and passcode policy on these devices.

Note 4: Windows 10 Mobile is not currently supported in Onboard.

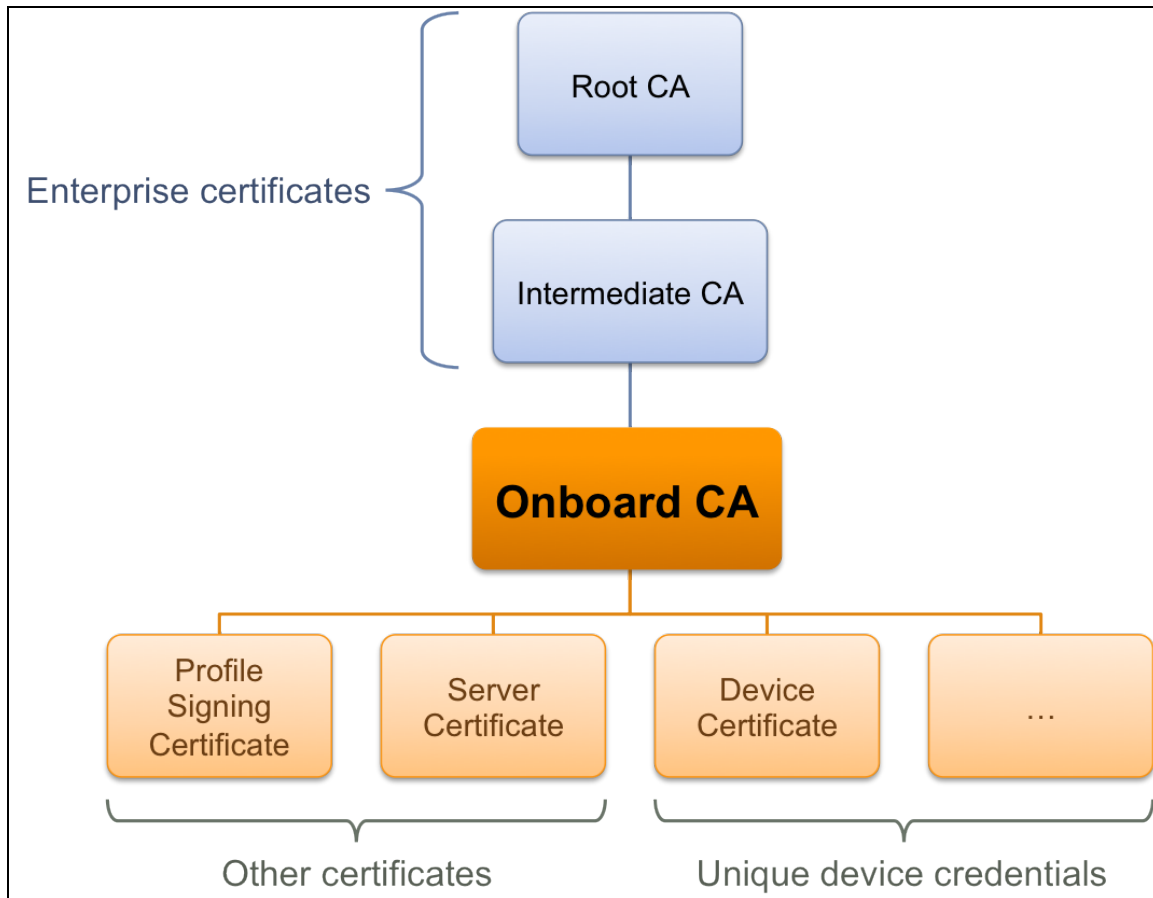
Public Key Infrastructure for Onboard

During the device provisioning process, one or more digital certificates are issued to the device. These are used as the unique credentials for a device. To issue the certificate, ClearPass Onboard must operate as a Certificate Authority (CA). The following sections explain how the Certificate Authority works, and which certificates are used in this process.

Certificate Hierarchy

In a public key infrastructure (PKI) system, certificates are related to each other in a tree-like structure.

Figure 53 Relationship of Certificates in the Onboard Public Key Infrastructure



The root Certificate Authority (CA) is typically an enterprise Certificate Authority, with one or more intermediate CAs used to issue certificates within the enterprise.

Onboard may operate as a root CA directly, or as an intermediate CA. See ["Certificate Authorities"](#) on page 116. For information on setting up certificates when using Onboard in a cluster, see ["Certificate Configuration in a Cluster"](#) on page 102.

The Onboard CA issues certificates for several purposes:

- The **Profile Signing Certificate** is used to digitally sign configuration profiles that are sent to iOS devices.
 - The identity information in the profile signing certificate is displayed during device provisioning.
- One or more **Server Certificates** may be issued for various reasons – typically, for an enterprise's authentication server.
 - The identity information in the server certificate may be displayed during network authentication.
- One or more **Device Certificates** may be issued – typically, one or two per provisioned device.

- The identity information in the device certificate uniquely identifies the device and the user that provisioned the device.

You do not need to manually create the profile signing certificate; it is created when it is needed. See ["Configuring Provisioning Settings for iOS and OS X Profiles" on page 259](#) to control the contents of this certificate.

You may revoke the profile signing certificate. It will be recreated when it is needed for the next device provisioning attempt.

Certificate Configuration in a Cluster

When you use Onboard in a cluster, you must use one common root Certificate Authority (CA) to issue all ClearPass appliance certificates for the cluster. This allows the “verified” message in iOS and lets you verify that a ClearPass appliance’s certificate is valid during EAP-PEAP or EAP-TLS authentication.

In a cluster of ClearPass appliances, devices can be onboarded through any node or authenticated through any node. Each ClearPass appliance has a different certificate, used for both SSL and RADIUS server identity. In the default configuration, these are self-signed certificates—that is, they are not issued by a root CA. This configuration of multiple self-signed certificates will not work for Onboard: Although a single self-signed certificate can be trusted, multiple self-signed certificates are not.

There are two ways to configure a common root CA to issue all the ClearPass appliance certificates for a cluster:

- Use the Onboard Certificate Authority. Create a certificate signing request on each ClearPass node, sign the certificates using Onboard, and install them in ClearPass. You can then onboard devices on any node in the cluster, and can perform secure EAP authentication from a provisioned device to any node in the cluster.
- Use a commercial Certificate Authority to issue ClearPass appliance certificates. Verify that the same root CA is at the top of the trust chain for every server certificate, and that it is the trusted root certificate for Onboard. Provisioning and authentication will then work across the entire cluster.

Revoking Unique Device Credentials

Because each provisioned device uses unique credentials to access the network, it is possible to disable network access for an individual device. This offers a greater degree of control than traditional user-based authentication — disabling a user’s account would impact all devices using those credentials.

To disable network access for a device, revoke the TLS client certificate provisioned to the device. See ["Working with Certificates in the List" on page 147](#).



Revoking access for a device is only possible when using an enterprise network. Personal (PSK) networks do not support this capability.

Revoking Credentials to Prevent Network Access



Revoking a device's certificate will cause the device to be unable to authenticate. It will not prevent it from being re-provisioned. If you wish to deny access to a device, use the **Manage Access** link in the device's row on the **Onboard > Management and Control > View by Device** form.

If the device is provisioned with an EAP-TLS client certificate, revoking the certificate will cause the Certificate Authority to update the certificate's state. When the certificate is next used for authentication, it will be recognized as a revoked certificate and the device will be denied access.



When using EAP-TLS authentication, you must configure your authentication server to use either OCSP or CRL to check the revocation status of a client certificate. OCSP is recommended as it offers a real-time status update for certificates. If the device is provisioned with PEAP unique device credentials, revoking the certificate will automatically delete the unique username and password associated with the device. When this username is next used for authentication, it will not be recognized as valid and the device will be denied access.



OCSP and CRL are not used when using PEAP unique device credentials. The ClearPass Onboard server automatically updates the status of the username when the device's client certificate is revoked.

Re-Provisioning a Device

Because “bring your own” devices are not under the complete control of the network administrator, it is possible for unexpected configuration changes to occur on a provisioned device.

For example, the user may delete the configuration profile containing the settings for the provisioned network, instruct the device to forget the provisioned network settings, or reset the device to factory defaults and destroy all the configuration on the device.

When these events occur, the user will not be able to access the provisioned network and will need to re-provision their device.

The Onboard server detects a device that is being re-provisioned and prompts the user to take a suitable action (such as connecting to the appropriate network). If this is not possible, the user may choose to restart the provisioning process and re-provision the device.

Re-provisioning a device will reuse an existing TLS client certificate or unique device credentials, if these credentials are still valid.

If the TLS client certificate has expired then the device will be issued a new certificate. This enables re-provisioning to occur on a regular basis.

A new certificate is generated when any of the following conditions occur:

- The key is set to be created by the device
- The fields in the certificate change
- The previous certificate has only 25% of its validity period remaining

Network Requirements for Onboard

To achieve complete functionality, ClearPass Onboard has certain requirements that must be met by the provisioning network and the provisioned network:

- The provisioning network must use a captive portal or other method to redirect a new device to the device provisioning page.
- The provisioning server (Onboard server) must have an SSL certificate that is trusted by devices that will be provisioned. In practice, this means a commercial SSL certificate is required.
- The provisioned network must support EAP-TLS and PEAP-MSCHAPv2 authentication methods.
- The provisioned network must support either OCSP or CRL checks to detect when a device has been revoked and deny access to the network.

Using Same SSID for Provisioning and Provisioned Networks

To configure a single SSID to support both provisioned and non-provisioned devices, use the following guidelines:

- Configure the network to use both PEAP and EAP-TLS authentication methods.
- When a user authenticates via PEAP with their domain credentials, place them into a provisioning role.
- The provisioning role should have limited network access and a captive portal that redirects users to the device provisioning page.
- When a user authenticates via PEAP with unique device credentials, place them into a provisioned role.
- When a user authenticates via EAP-TLS using an Onboard client certificate, place them into a provisioned role.

For provisioned devices, additional authorization steps can be taken after authentication has completed to determine the appropriate provisioned role.

Using Different SSID for Provisioning and Provisioned Networks

To configure dual SSIDs to support provisioned devices on one network, and non-provisioned devices on a separate network, use the following guidelines:

- Configure the provisioning SSID to use PEAP, or another suitable authentication method.
- When a user connects to the provisioning SSID, place them into a provisioning role.
 - The provisioning role should have limited network access and a captive portal that redirects users to the device provisioning page.
- When a user connects to the provisioned SSID, authenticate based on the type of credentials presented.
 - For PEAP authentication with unique device credentials, place them into a provisioned role.
 - For EAP-TLS authentication using an Onboard client certificate, place them into the provisioned role.
 - In all other cases, deny access.

As for the single-SSID case, additional authorization steps may be taken after authentication has completed to determine the appropriate provisioned role.

Configuring Online Certificate Status Protocol

Onboard supports the Online Certificate Status Protocol (OCSP) to provide a real-time check on the validity of a certificate.

To configure OCSP for your network, you will need to provide the URL of an OCSP service to your network equipment. This URL can be constructed by using the relative path `mdps_ocsp.php/1`.

For example, if the Onboard server's hostname is `onboard.example.com`, the OCSP URL to use is:
`http://onboard.example.com/guest/mdps_ocsp.php/1`.



OCSP does not require the use of HTTPS and can be configured to use HTTP.

Configuring Certificate Revocation List (CRL)

Onboard supports generating a Certificate Revocation List (CRL) that lists the serial numbers of certificates that have been revoked.

To configure a CRL, you will need to provide its URL to your network equipment. This URL can be constructed by using the relative path `mdps_crl.php?id=1`.

For example, if the Onboard server's hostname is `onboard.example.com`, the location of the CRL is: `http://onboard.example.com/guest/mdps_crl.php?id=1`.



A certificate revocation list does not require the use of HTTPS and can be configured to use HTTP.

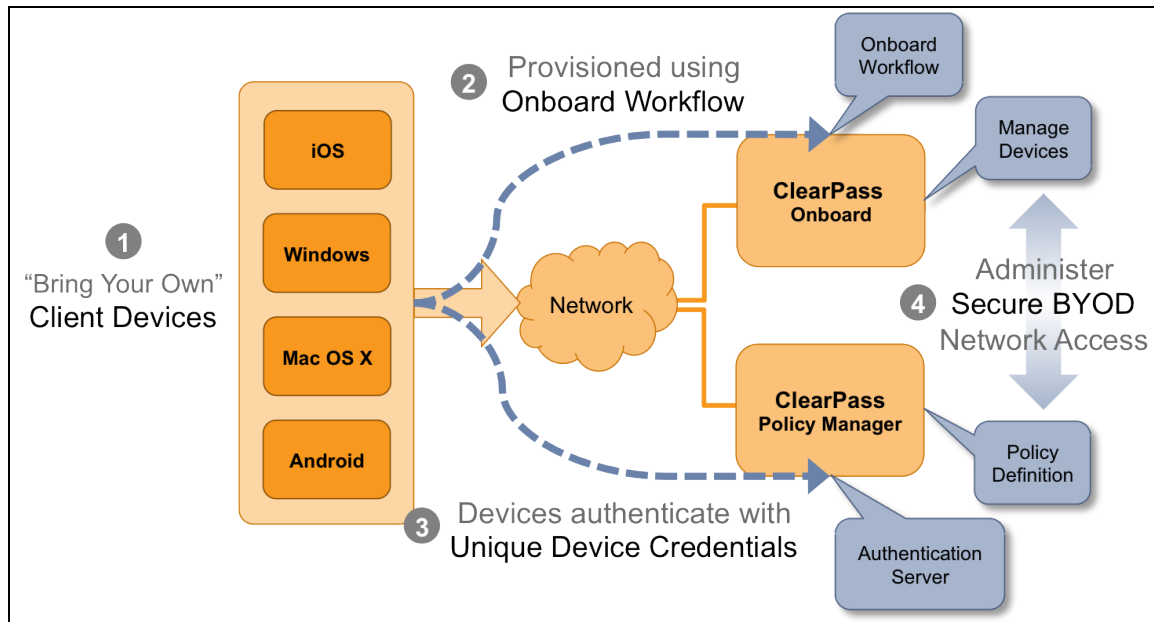
Providing MAC Addresses for Android 6 Devices

The MAC address is not provided by Android 6 and later devices. Instead, it must be provided in the captive portal redirect. When an Aruba controller is used, we strongly recommend that you enable the URL hash to prevent tampering.

Network Architecture for Onboard

The high-level network architecture for the Onboard solution is shown in the following figure.

Figure 54 *ClearPass Onboard Network Architecture*

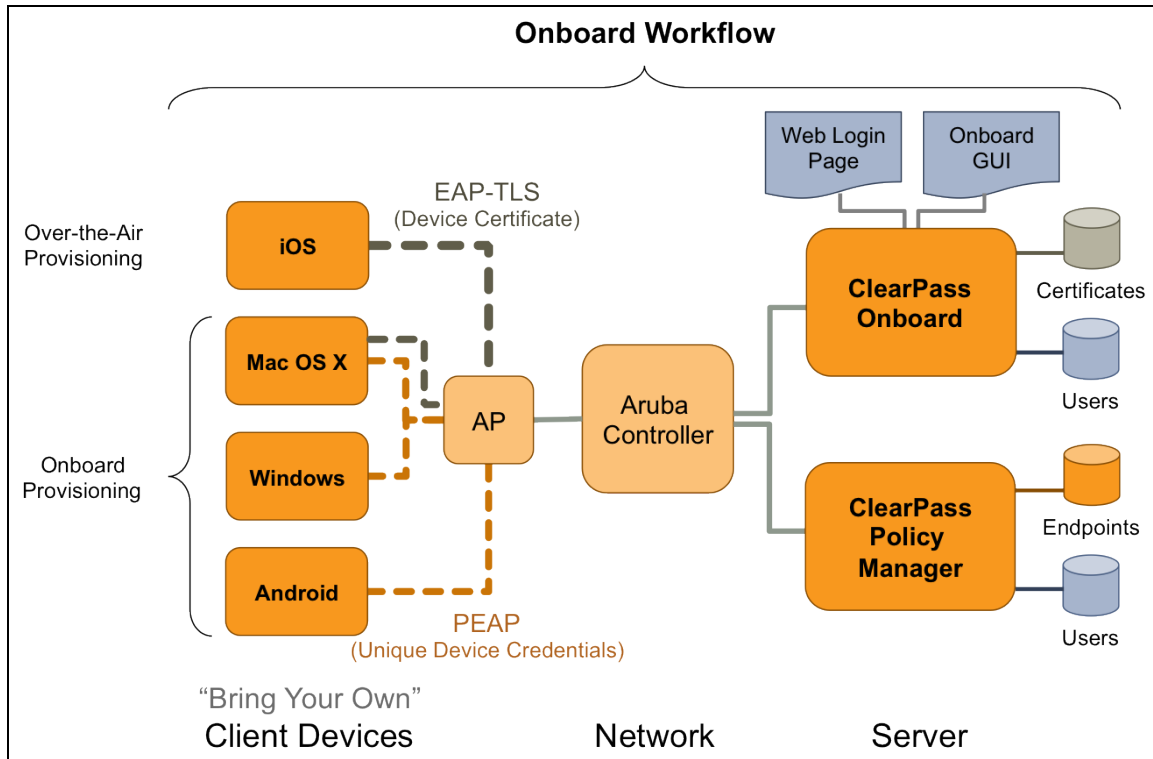


The sequence of events shown in [Figure 54](#) is:

1. Users bring their own device to the enterprise.
2. The ClearPass Onboard workflow is used to provision the user's device securely and with a minimum of user interaction.
3. After it is provisioned, the device re-authenticates to the network using a set of unique device credentials. These credentials uniquely identify the device and user and enable management of provisioned devices.
4. Administrators can configure all aspects of the provisioning workflow – including the devices that have been provisioned, policies to apply to devices and the overall user experience for BYOD.

A more detailed view of the network architecture is shown in [Figure 55](#). This diagram shows different types of client devices using the Onboard workflow to gain access to the network. Some of the components that may be configured by the network administrator are also shown.

Figure 55 Detailed View of the ClearPass Onboard Network Architecture



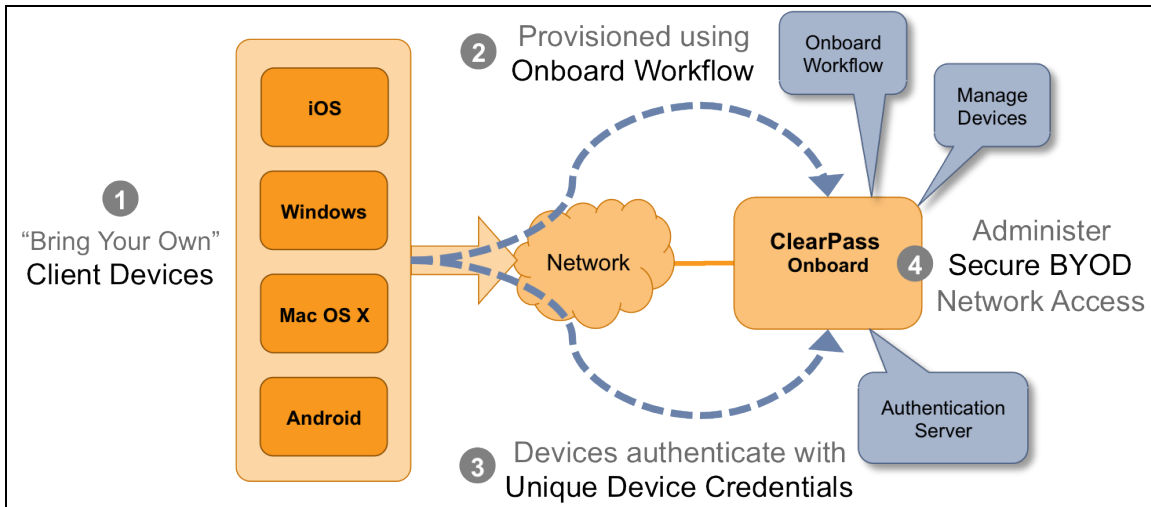
The components shown in Figure 55 are:

1. Users bring different kinds of client device with them. Onboard supports “smart devices” that use the iOS or Android operating systems, such as smartphones and personal tablets. Onboard also supports the most common versions of Windows and Mac OS X operating systems found on desktop computers, laptops and netbooks.
2. The Onboard workflow is used to provision the user’s device securely and with a minimum of user interaction. The provisioning method used depends on the type of device.
 - a. Newer versions of Mac OS X (10.7 and later) and iOS devices use the “over-the-air” provisioning method.
 - b. Other supported platforms use the “Onboard provisioning” method.
3. After it is provisioned, a client device uses a secure authentication method based on 802.1X and the capabilities best supported by the device.
 - a. The unique device credentials issued during provisioning are in the form of an EAP-TLS client certificate for iOS devices and OS X (10.7+) devices.
 - b. Other supported devices are also issued a client certificate, but will use the PEAP-MSCHAPv2 authentication method with a unique username and strong password.
4. Administrators can manage all Onboard devices using the certificate issued to that device.

Network Architecture for Onboard when Using ClearPass Guest

ClearPass Guest supports the provisioning, authentication, and management aspects of the complete Onboard solution. Figure 56 shows the high-level network architecture for the Onboard solution when using ClearPass Guest as the provisioning and authentication server.

Figure 56 ClearPass Onboard Network Architecture when Using ClearPass Guest



The user experience for device provisioning is the same in [Figure 56](#) and [Figure 54](#), however there are implementation differences between these approaches.

The ClearPass Onboard Process

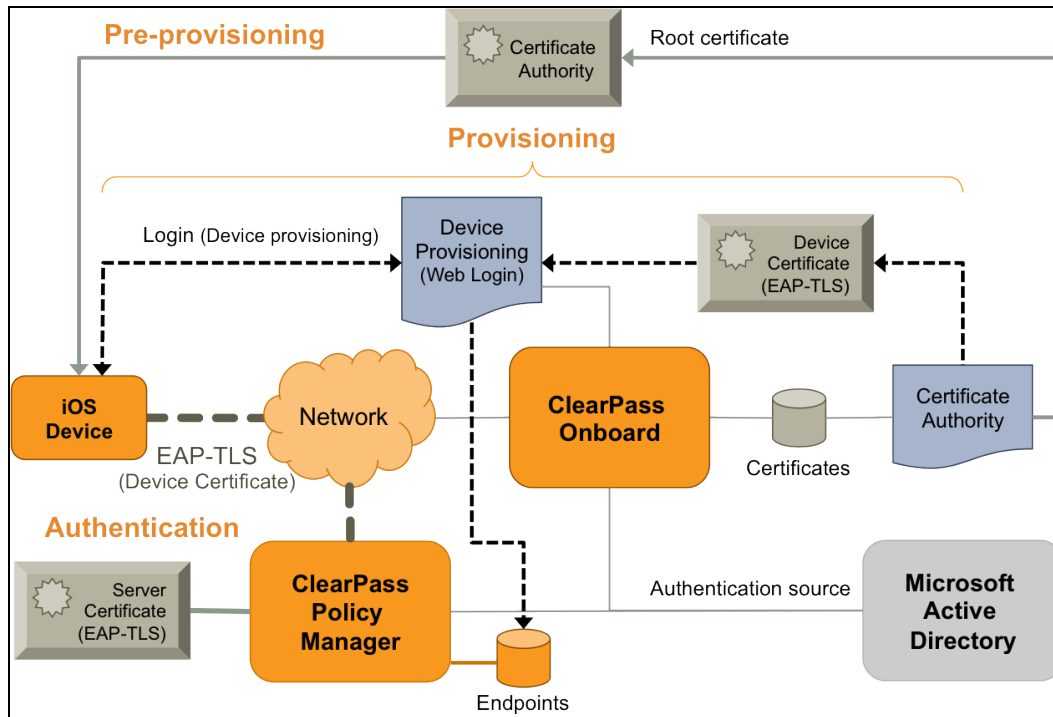
This section provides provisioning process overviews for different device types. It includes the following:

- ["Devices Supporting Over-the-Air Provisioning"](#) on page 108
- ["Devices Supporting Onboard Provisioning"](#) on page 110

Devices Supporting Over-the-Air Provisioning

ClearPass Onboard supports secure device provisioning for iOS 4, iOS 5, iOS 6, and recent versions of Mac OS X (10.7 “Lion” and later). These are collectively referred to as “iOS devices”. The Onboard process for iOS devices is shown in [Figure 57](#).

Figure 57 Onboard Process for iOS Devices

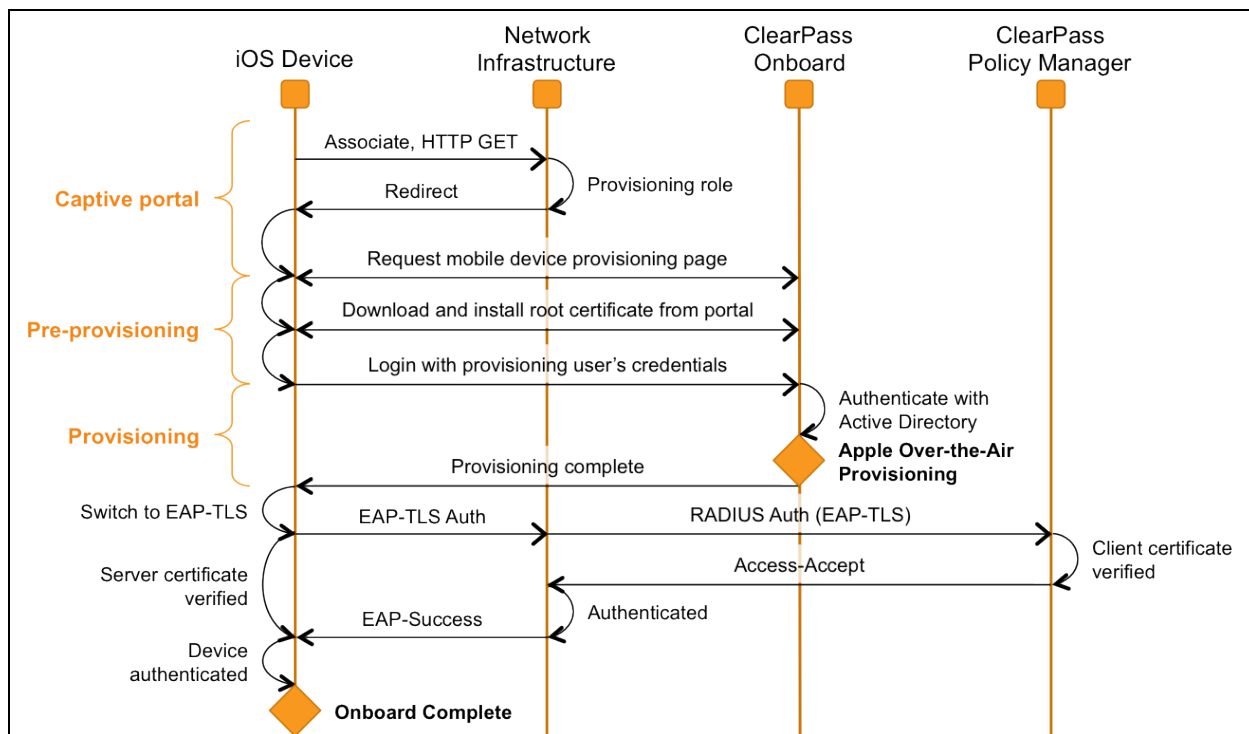


The Onboard process is divided into three stages:

1. **Pre-provisioning.** The enterprise’s root certificate is installed on the iOS device.
2. **Provisioning.** The user is authenticated at the device provisioning page and then provisions their device with the Onboard server. The device is configured with appropriate network settings and a device-specific certificate.
3. **Authentication.** After configuration is complete, the user switches to the secure network and is authenticated using an EAP-TLS client certificate.

A sequence diagram showing the interactions between each component of this workflow is shown in [Figure 58](#).

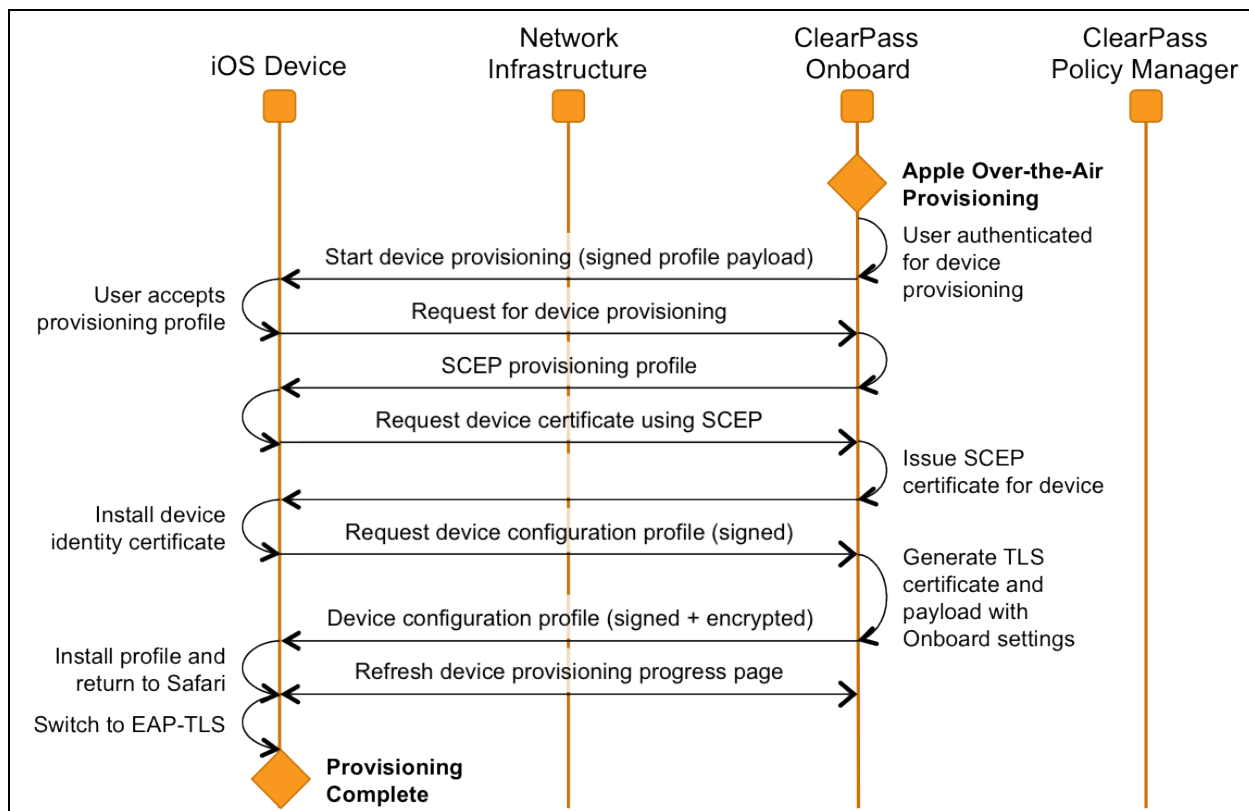
Figure 58 Sequence Diagram for the Onboard Workflow on iOS Platform



1. When a BYOD device first joins the provisioning network it does not have a set of unique device credentials. This will trigger the captive portal for that device, which brings the user to the mobile device provisioning page.
2. A link on the mobile device provisioning page prompts the user to install the enterprise's root certificate. Installing the enterprise's root certificate enables the user to establish the authenticity of the provisioning server during device provisioning.
3. The user then authenticates with their provisioning credentials – these are typically the user's enterprise credentials from Active Directory. If the user is authorized to provision a mobile device, the over-the-air provisioning workflow is then triggered (see [Figure 59](#), below).
4. After provisioning has completed, the device switches to EAP-TLS authentication using the newly provisioned client certificate. Mutual authentication is performed (the authentication server verifies the client certificate, and the client verifies the authentication server's certificate).
5. The device is now onboarded and is able to securely access the provisioned network.

Over-the-air provisioning is used to securely provision a device and configure it with network settings. [Figure 59](#) shows a sequence diagram that explains the steps involved in this workflow.

Figure 59 *Over-the-Air Provisioning Workflow for iOS Platform*

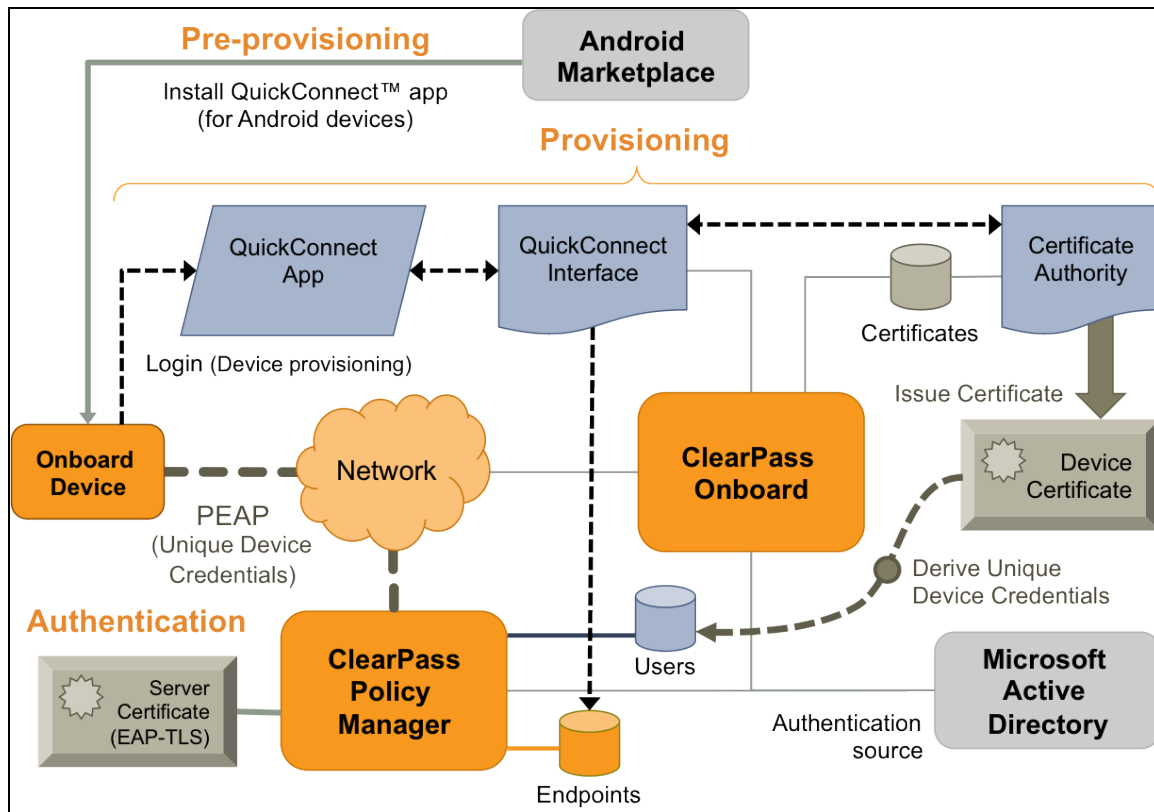


1. The only user interaction required is to accept the provisioning profile. This profile is signed by the Onboard server, so that the user can be assured of its authenticity.
2. An iOS device will have two certificates after over-the-air provisioning is complete:
 - a. A Simple Certificate Enrollment Protocol (SCEP) certificate is issued to the device during the provisioning process. This certificate identifies the device uniquely, and is used to encrypt the device configuration profile so that only this device can read its unique settings.
 - b. A Transport Layer Security (TLS) client certificate is issued to the device. This certificate identifies the device and the user that provisioned the device. It is used as the device's network identity during EAP-TLS authentication.

Devices Supporting Onboard Provisioning

ClearPass Onboard supports secure device provisioning for Microsoft Windows Vista, Microsoft Windows 7, Apple Mac OS X 10.5 and 10.6, and Android devices (smartphones and tablets). These are collectively referred to as "Onboard-capable devices". The Onboard process for these devices is shown in [Figure 60](#).

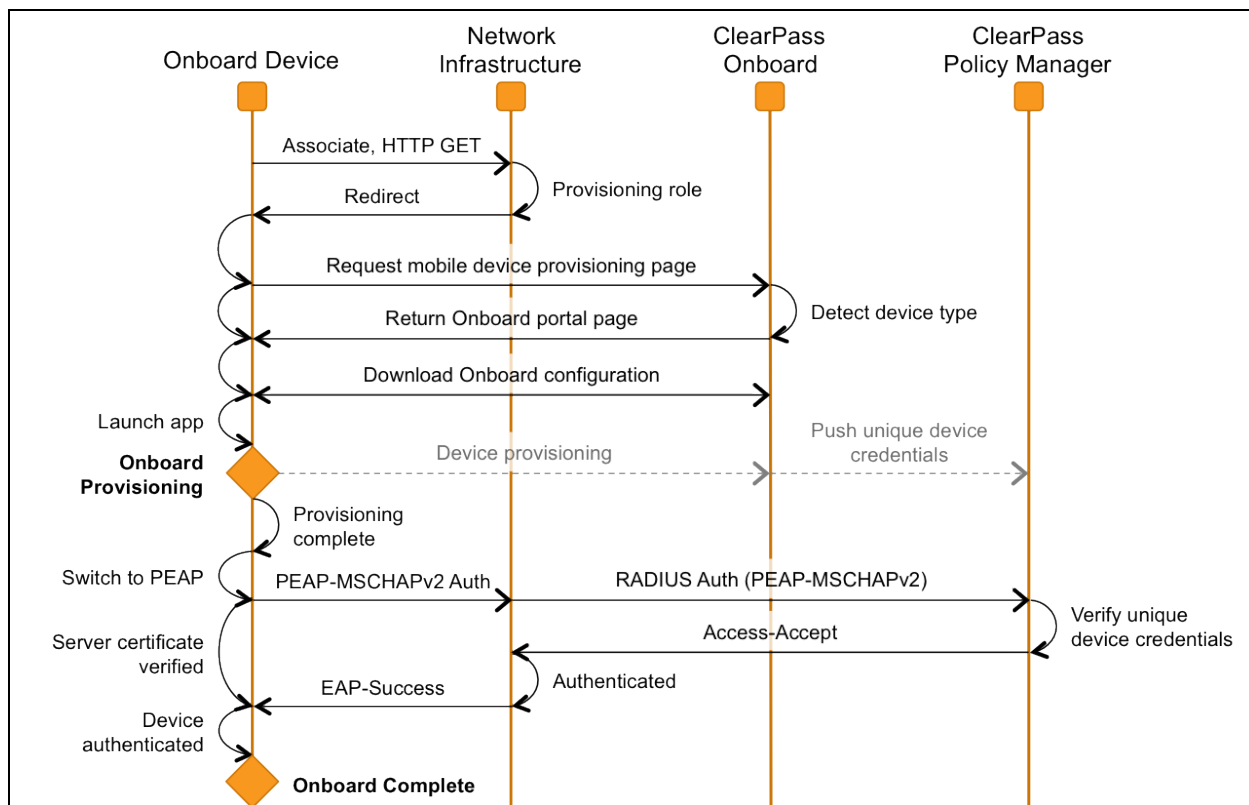
Figure 60 ClearPass Onboard Process for Onboard-Capable Devices



The Onboard process is divided into three stages:

1. **Pre-provisioning.** This step is only required for Android devices; the Aruba QuickConnect app must be installed for secure provisioning of the device.
2. **Provisioning.** The device provisioning page detects the device type and downloads or starts the QuickConnect app. The app authenticates the user and then provisions their device with the Onboard server. The device is configured with appropriate network settings and credentials that are unique to the device. See [Figure 61](#) for details.
3. **Authentication.** After configuration is complete, the user switches to the secure network and is authenticated using PEAP-MSCHAPv2 unique device credentials.

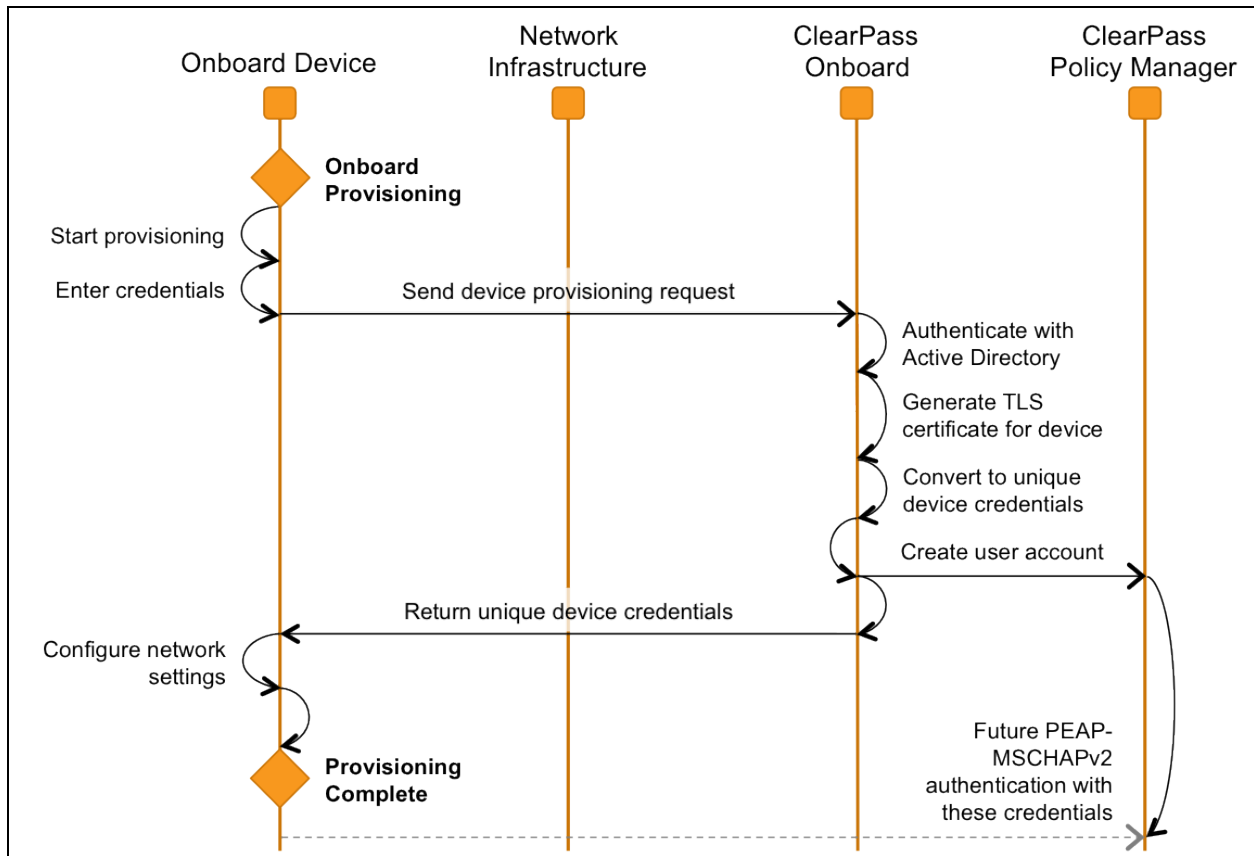
Figure 61 Sequence Diagram for the Onboard Workflow on Android Platform



1. When a BYOD device first joins the network it does not have a set of unique device credentials. This will trigger the captive portal for that device, which brings the user to the mobile device provisioning page.
2. The Onboard portal is displayed. The user's device type is detected, and a link is displayed depending on the device type:
 - a. For Android devices, the link is to a file containing the Onboard configuration settings; downloading this file will launch the QuickConnect app on the device.
 - b. For Windows and Mac, the link is to a executable file appropriate for that operating system that includes both the QuickConnect app and the Onboard configuration settings.
3. The QuickConnect app uses the Onboard provisioning workflow to authenticate the user and provision their device with the Onboard server. The device is configured with appropriate network settings and credentials that are unique to the device.
4. After provisioning has completed, the app switches the device to PEAP authentication using the newly provisioned unique device credentials. Mutual authentication is performed (the authentication server verifies the client's username and password, and the client verifies the authentication server's certificate).
5. The device is now onboarded and is able to securely access the network.

The Onboard provisioning workflow is used to securely provision a device and configure it with network settings. [Figure 62](#) shows a sequence diagram that explains the steps involved in this workflow.

Figure 62 Onboard Provisioning Workflow in the QuickConnect App



Configuring the User Interface for Device Provisioning

The user interface for device provisioning can be customized in three different ways:

- Customizing the Web login page used for device provisioning.
All devices will reach the device provisioning Web login page as the first step of the provisioning process. See ["Configuring Provisioning Settings for the Web Login Page"](#) on page 229 to make changes to the content or formatting of this page.
- Customizing the properties of the device provisioning profile for iOS and OS X devices.
After starting the provisioning process, users of iOS and OS X are prompted to accept a configuration profile. See ["Configuring Provisioning Settings for iOS and OS X Profiles"](#) on page 259 to make changes to the content of this profile.
- Customizing the user interface of the QuickConnect app for Windows, Mac OS X, and Android devices.
The provisioning process for Windows, Mac OS X, and Android devices uses a separate app, which has a customizable user interface. See ["Configuring Options for Onboard Client Devices"](#) on page 261 to make changes to the user interface.

Using the {nwa_mdps_config} Template Function

Certain properties can be extracted from the Onboard configuration and used in the device provisioning page.

To obtain these properties, use the {nwa_mdps_config} Smarty template function. The “name” parameter specifies which property should be returned, as described in [Table 29](#).

Table 29: Properties Available with the {nwa_mdps_config} Smarty Template Function

Name	Description
root_cert	URL of the Onboard Certificate Authority's root certificate. Browsing to this URL will install the root certificate on the device, which is required as part of the pre-provisioning step. Example: <code> Install Onboard root certificate</code>
wifi_ssid	Name of the wireless network. See " Configuring Basic Network Access Settings " on page 164. Example: Connect to the network named {nwa_mdps_config name=wifi_ssid}
organization_name	The organization name. See " Configuring General Provisioning Settings " on page 222. Example: <code><h2> Welcome to {nwa_mdps_config name=organization_name}</h2></code>

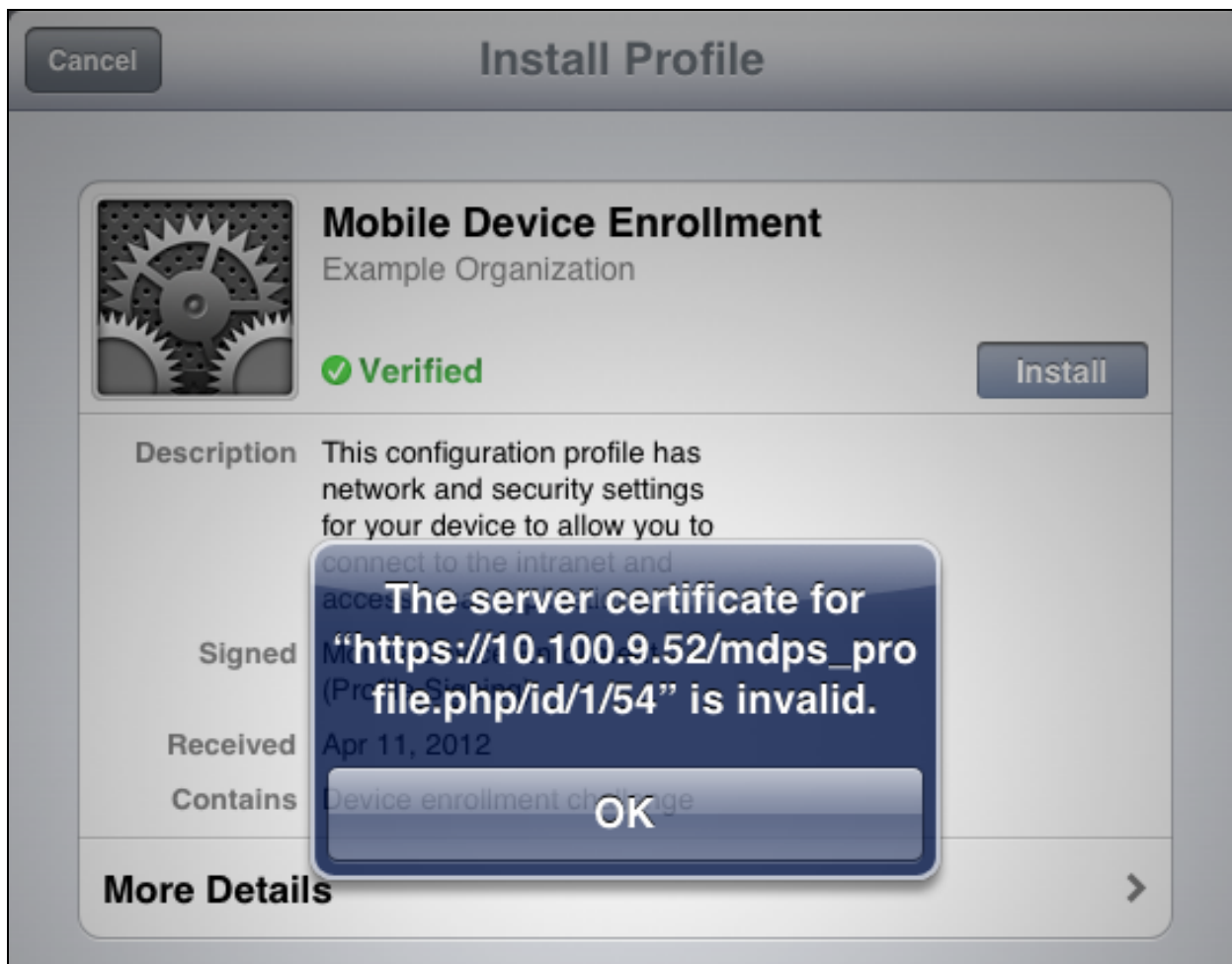
Onboard Troubleshooting

If you encounter a problem that is not listed here, refer to the "[Onboard Deployment Checklist](#)" on page 97 and check each of the configuration steps listed there.

iOS Device Provisioning Failures

Symptom: Device provisioning fails on iOS with the message “The server certificate for https://... is invalid”.

Figure 63 "Server certificate... invalid" Message on the Device Enrollment Form



Resolution: If you use HTTPS for device provisioning, you **must** obtain a commercial SSL certificate.

Self-signed SSL certificates, and SSL server certificates that have been issued by an untrusted or unknown root Certificate Authority, will cause iOS device provisioning to fail with the message "The server certificate for ... is invalid".

A workaround for this issue is to install an appropriate root certificate on the iOS device. This root certificate must be the Web server's SSL certificate (if it is a self-signed certificate), or the Certificate Authority that issued the SSL certificate. This is not recommended for production deployments as it increases the complexity of deployment for users with iOS devices.

Hostname-to-Certificate Match Failures

Symptom: Device provisioning fails with the message "Onboard provisioning cannot be performed at this address. If you were directed here, please contact a network administrator."

This occurs if the hostname used to access ClearPass does not match the hostname configured in the ClearPass appliance's certificate. These items must match or device provisioning will fail. This error is detected by Onboard and results in the above message.

Resolution: To correct the problem, ensure that the DNS is correctly configured for the server, ensure that the hostname is correctly set, and ensure that the server's certificate contains the correct hostname.

Onboard Interface Not Displayed

If Onboard is not visible in the ClearPass Guest user interface, verify whether Public Facing Enterprise (PFE) mode is set in ClearPass Policy Manager. If PFE mode is enabled, Onboard is not permitted and Onboard licenses cannot be added. The PFE mode is enabled or disabled in ClearPass on the **Mode** tab at **Administration > Server Manager > Server Configuration > Cluster-Wide Parameters**.

Certificate Renewal through OS X Mavericks

OS X Mavericks allows users to renew certificates automatically, and provides a notice and an update link in the Mavericks Profile fifteen days before a certificate expires. Onboard supports certificate renewal through OS X Mavericks. However, only local certificates can be renewed; AD CS is not supported. Also, certificates that have been revoked cannot be renewed.

Certificate Authorities



You can create and manage multiple Certificate Authorities for Onboard. To view and work with the list of Certificate Authorities and to configure new Certificate Authorities, go to **Onboard > Certificate Authorities**. The **Certificate Authorities** list view opens. All Certificate Authorities that have been set up are included in the list. Information shown for each Certificate Authority includes its name, mode, status, expiration time, and OCSP URL.

Figure 64 *The Certificate Authorities List View*

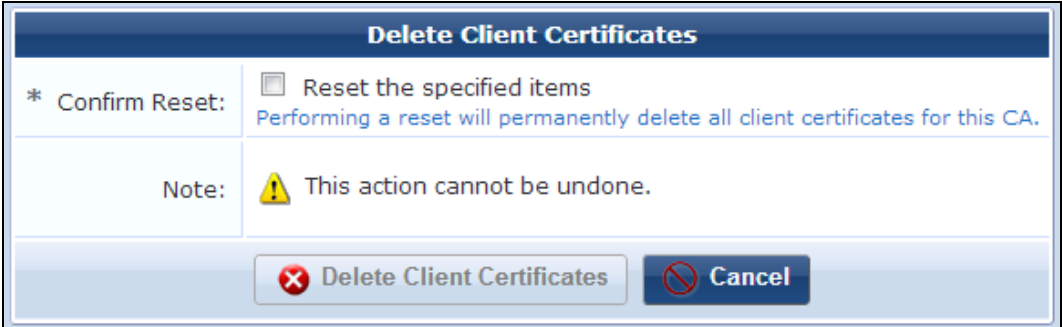
Name	Mode	Status	Expiry	OCSP URL
Intermediate CA	intermediate	Valid	2015-03-20 19:48:10+00	http://qa99.amigopod.arubanetworks.com/guest/mdps_ocsp.php/4
Show Details Edit Duplicate Delete Show Usage Trust Chain Certificates Renew Delete Client Certificates				
Local Certificate Authority <small>This is the default certificate authority.</small>	root	Valid	2023-03-21 16:41:05+00	http://qa99.amigopod.arubanetworks.com/guest/mdps_ocsp.php/1
My Root CA	root	Valid	2014-03-26 04:35:03+00	http://qa99.amigopod.arubanetworks.com/guest/mdps_ocsp.php/2
Refresh				Showing 1 - 3 of 3 20 rows per page

You can click a Certificate Authority's row in the list for additional options:

Table 30: *Options in the Certificate Authorities List View*

Option	Description
Show Details	Displays details for the Certificate Authority. The form expands to show a summary of the settings defined for it, including information for certificate issuing, retention policy, identity, private key, and self-signed certificate.
Edit	Lets you edit any of a Certificate Authority's attributes and configure certificate issuing options on the Certificate Authority Settings form. See "Editing Certificate Authority Settings" on page 122.
Duplicate	Lets you create a copy of a Certificate Authority configuration to use as a basis for a new Certificate Authority. The first page of the Certificate Authority Settings form opens with the identity, private key, and self-signed certificate attributes prepopulated and "Copy" appended to the name. You can rename the new Certificate Authority and edit any of its attributes.

Table 30: Options in the Certificate Authorities List View(Continued)

Option	Description
Delete	Deletes the Certificate Authority. You will be asked to confirm the deletion.
Show Usage	Lets you verify whether the Certificate Authority is currently used. The form expands to show a list of provisioning sets that use the Certificate Authority.
Trust Chain	Displays the trust chain for the Certificate Authority on the Certificate Authority Trust Chain page. See "The Trust Chain and Uploading Certificates for the CA " on page 130.
Certificates	Displays a list of certificates associated with the Certificate Authority on the Certificate Management page. See "Certificate Management (View by Certificate) " on page 144.
Renew	<p>Renews the Certificate Authority. If it is an intermediate Certificate Authority, the Intermediate Certificate Renewal page opens, where you can send a certificate signing request; see "Requesting a Certificate for the Certificate Authority" on page 128. If it is a root Certificate Authority, the row expands to include the Root Certificate Renewal option. Click the Renew Root Certificate button.</p>  <p>Renewing the certificate uses the same private key for the root certificate, but reissues the root CA certificate with an updated validity period. This will maintain the validity of all certificates issued by the CA. When you renew a certificate, you should distribute a new copy of the root certificate to all users of that certificate.</p>
Delete Client Certificates	<p>Deletes a Certificate Authority's client certificates. The row expands to include the Delete Client Certificates form. To confirm the deletion, you must mark the Reset the specified items check box in the Confirm Reset field, and then click the Delete Client Certificates button. Doing so will permanently delete all client certificates for the Certificate Authority. This action cannot be reversed.</p> 
Create new certificate authority	To create a new Certificate Authority, click this link in the upper right corner. The initial setup page of the Certificate Authority Settings form opens. See the next section, "Creating a New Certificate Authority" on page 117.

Creating a New Certificate Authority

The first page of the **Certificate Authority Settings** form is used to create the Onboard Certificate Authority (CA) and to configure some basic properties:

- Give it a name and description
- Specify root CA, intermediate CA, local CA, or Registration Authority (RA) mode
- Configure the identity, private key, and self-signed certificate attributes

To create an Onboard Certificate Authority, go to **Onboard > Certificate Authorities**, and then either click the **Duplicate** link for a Certificate Authority in the **Certificate Authorities** list or click the **Create new certificate authority** link. The initial setup page of the **Certificate Authority Settings** form opens.

Figure 65 Mode Options on the Certificate Authority Settings Form





Certificate Authority Settings	
* Name:	<input type="text"/> Enter a name to identify this certificate authority.
Description:	<div style="border: 1px solid #ccc; height: 60px; width: 100%;"></div> A description of the certificate authority.
* Mode:	<div style="border: 1px solid #ccc; padding: 10px;"> <div style="text-align: center; margin-bottom: 10px;">  <p>Root CA The certificate authority has a self-signed root certificate and issues client certificates locally.</p> </div> <div style="text-align: center; margin-bottom: 10px;">  <p>Intermediate CA The certificate authority has a certificate issued by another CA and issues client certificates locally.</p> </div> <div style="text-align: center; margin-bottom: 10px;">  <p>Imported CA Import an existing CA certificate to use as the certificate authority. This certificate authority will issue certificates locally.</p> </div> <div style="text-align: center;">  <p>Registration Authority The registration authority sends certificate requests to another CA and only stores client certificates locally.</p> </div> </div> <p>Select the mode of operation for the certificate authority.</p>

Table 31: Certificate Authority Settings Form, Basic and Mode Areas

Field	Description
Name	Short name that clearly identifies the Certificate Authority. Certificate Authority names can include spaces. If you are duplicating a CA, the original name has "Copy" appended to it. You may highlight the name and replace it with a new name.
Description	You may include a brief description of the CA. This description is shown in the Certificate Authorities list. The Name and Description fields are used internally to identify this Certificate Authority for the network administrator. These values are never displayed to the user during device provisioning.
Mode	Specifies the type of Certificate Authority: <ul style="list-style-type: none"> • Root CA—The Onboard Certificate Authority issues its own root certificate. The Certificate Authority issues client and server certificates using a local signing certificate, which is an intermediate CA that is subordinate to the root certificate. Use this option when you do not have an existing public-key infrastructure (PKI), or if you want to completely separate the certificates issued for Onboard devices from your existing PKI. • Intermediate CA—The Onboard Certificate Authority is issued a certificate by an external Certificate Authority. The Onboard Certificate Authority issues client and server certificates using this certificate. Use this option when you already have a public-key infrastructure (PKI), and would like to include the certificate issued for Onboard devices in that infrastructure. • Imported CA— If you choose Imported CA, the following fields are removed from the form. If you choose Root or Intermediate, complete the following fields. • Registration Authority — Onboard is used as the Registration Authority (RA). Instead of issuing certificates, Onboard will proxy a certificate request to another Certificate Authority (CA) via SCEP. Only client certificates are stored locally.

Figure 66 *The Identity Area*

Identity	
These details are used to create a Distinguished Name for the certificate authority.	
* Country:	<input type="text" value="US"/> Enter the 2-letter ISO country code of your country.
* State:	<input type="text" value="California"/> Enter the full name of your state or province.
* Locality:	<input type="text" value="Sunnyvale"/> Enter the name of your locality (town or city).
* Organization:	<input type="text" value="Aruba Networks"/> Enter the name of your organization or company.
Organizational Unit:	<input type="text"/> Enter the name of your organizational unit (e.g. section or division of the company).
* Common Name:	<input type="text" value="My Certificate Authority"/> Enter a name for the certificate authority. This is the 'common name' of the digital certificate.
* Signing Common Name:	<input type="text" value="My Certificate Authority (Signing)"/> Enter a name for the signing certificate. This is the 'common name' of the digital certificate.
* Email Address:	<input type="text" value="my-ca@example.com"/> Enter an email address.


Table 32: Certificate Authority Settings Form, Identity Area

Field	Description
Country	Two-letter ISO country code for your organization. This value forms part of the distinguished name for the certificate.
State	Full name of the state or province for your organization. This value forms part of the distinguished name for the certificate.
Locality	Name of the town or city where your organization is located. This value forms part of the distinguished name for the certificate.
Organization	Name of your organization. This value forms part of the distinguished name for the certificate.
Organizational Unit	(Optional) Name of your organizational unit (section or division of the organization). This value forms part of the distinguished name for the certificate.
Common Name	Descriptive name for the certificate. This value is used to identify the certificate as the issuer of other certificates, notably the signing certificate.
Signing Common Name	(Included for root certificates) Descriptive name for the signing certificate. This value is used to identify the signing certificate as the issuer of client and server certificates from this Certificate Authority. The other identity information in the signing certificate will be the same as for the root certificate.
Email Address	Contact email address. This email address is included in the root and signing certificates, and provides a way for users of the certificate authority to contact your organization.

Figure 67 The Private Key and Self-Signed Certificates Areas


Private Key


These options are used to create a private key for the root certificate.

* Key Type: 
Select the type of private key to create for the root certificate.

Self-Signed Certificate

These options specify the validity period of the signed certificate.

* CA Expiration:  days
The number of days before the certificate authority's root certificate will expire.

* Digest Algorithm: 
Select the algorithm used to sign the digital certificate request.


 **Create Certificate Authority**

Table 33: Certificate Authority Settings Form, Private Key and Self-Signed Certificates Areas

Field	Description
Key Type	Specify the type of private key that should be created for the certificate: <ul style="list-style-type: none"> ● 1024-bit RSA (not recommended for a root certificate) ● 2048-bit RSA (recommended for general use) ● 4096-bit RSA (higher security) ● X9.62/SECG curve over a 256-bit prime field ● NIST/SECG curve over a 384-bit prime field
CA Expiration	(Included for root certificates) Specifies the lifetime of the root certificate in days. The default value is 365 days.
Digest Algorithm	Specifies which hash algorithm should be used to sign the digital certificate request. Options include: <ul style="list-style-type: none"> ● SHA-1 (not recommended) ● SHA-224 ● SHA-256 ● SHA-384 ● SHA-512 (Default)
Create Certificate Authority	Creates the Certificate Authority: <ul style="list-style-type: none"> ● If you selected root mode, the root certificate is included in the Certificate Authorities list. ● If you selected intermediate mode, the Intermediate Certificate Request page opens with text for the certificate signing request (CSR). You can send the CSR to a Certificate Authority, who will generate a signed certificate you can install. See "Requesting a Certificate for the Certificate Authority" on page 128. ● If you selected imported mode, the Certificate Authority Certificate Import form opens, where you can upload the digital certificates and private key to the server. See "Installing a Certificate Authority's Certificate" on page 128.

Figure 68 The Registration Authority Area

Registration Authority
 These options specify the Certificate Authority this Registration Authority will use to issue certificates.

* SCEP URL:	<input style="width: 90%;" type="text"/> URL of the SCEP server that will act as the CA for this RA.
SCEP Challenge Password:	<input style="width: 90%;" type="text"/> Shared secret for SCEP CA used in generating RA certificate. Leave blank if the SCEP server does not enforce a challenge password.
Confirm SCEP Challenge Password:	<input style="width: 90%;" type="text"/> Shared secret for SCEP CA used in generating RA certificate. Leave blank if the SCEP server does not enforce a challenge password.
CRL URL:	<input style="width: 90%;" type="text"/> URL to the CRL for the CA. If supplied Onboard will sync revocation status of certificates.



Table 34: Certificate Authority Settings Form, Registration Authority Area

Field	Description
SCEP URL	URL of the SCEP server that will act as the Certificate Authority (CA) for this Registration Authority.
SCEP Challenge Password	Shared secret for the SCEP Certificate Authority, used for generating the Registration Authority certificate. If the SCEP server will not enforce a challenge password, leave this field empty.
Confirm SCEP Challenge Password	
CRL URL	URL of the Certificate Revocation List (CRL) for the Certificate Authority. If a URL is entered in this field, Onboard will synchronize the revocation status of certificates.

After you have configured the SCEP-RA certificate, you may specify the CA to use for TLS certificates independently of the CA used for enrollment by using the **SCEP-RA** option in the **TLS Certificate Authority** and **Certificate Authority** fields on the **Provisioning Settings** form. For more information, see ["Configuring General Provisioning Settings"](#) on page 222.

Editing Certificate Authority Settings

You can edit some properties of a Certificate Authority after you create it, and configure some attributes that were not included on the setup form.

To edit a Certificate Authority, go to **Onboard > Certificate Authorities**, click the certificate to expand its row, and click its **Edit** link. The **Certificate Authority Settings** form opens.

In the basic information area at the top of the form, the **Name** and **Description** fields are used internally to identify this Certificate Authority for the network administrator. These values are never displayed to the user during device provisioning.

Figure 69 The Certificate Authority Settings Form, Basic Information Area

Field	Description
Name	Short name that identifies the certificate clearly. Certificate Authority names can include spaces.
Description	Briefly describes the CA. This description is shown in the Certificate Authorities list.
Mode	Either Root CA , Intermediate CA , Imported CA , or Registration Authority . The certificate's mode cannot be edited after creation.

In the **Certificate Issuing** area:

Figure 70 *The Certificate Authority Settings Form, Certificate Issuing Area*

Certificate Issuing	
These options control how certificates are issued by this certificate authority.	
* Authority Info Access:	<input type="text" value="Do not include OCSP Responder URL"/> <small>Select the information about the certificate authority to include in the client certificate. Note that when an OCSP URL is provided, clients may need to access this URL in order to determine if the certificate is still valid.</small>
* Validity Period:	<input type="text" value="365"/> days <small>Maximum validity period for client certificates (in days).</small>
* Clock Skew Allowance:	<input type="text" value="15"/> <small>Amount to pre/post date certificate validity period (in minutes).</small>
Subject Alternative Name:	<input checked="" type="checkbox"/> Include device information in TLS client certificates <small>Store information about the device in the subjectAltName extension of the certificate. Note: Aruba OS version 6.1 or later is required to enable this feature.</small>
* Digest Algorithm:	<input type="text" value="SHA-1"/> <small>Select the algorithm used to sign issued certificates.</small>

Authority Info Access	Specify one of the following options to control automatic certificate revocation checks: <ul style="list-style-type: none"> • Do not include OCSP responder URL – The Authority Info Access extension is not included in the client certificate. Certificate revocation checking must be configured manually on the authentication server. This is the default option. • Include OCSP responder URL – The Authority Info Access extension is added to the client certificates, with the OCSP responder URL set to a predetermined value. This value is displayed as the “OCSP URL”. • Specify an OCSP responder URL – The Authority Info Access extension is added to the client certificates, with the OCSP responder URL set to a value defined by the administrator. This value may be specified in the “OCSP URL” field.
Validity Period	Specifies the maximum length of time for which a client certificate issued during device provisioning will remain valid.
Clock Skew Allowance	Adds a small amount of time to the start and end of the client certificate’s validity period. This permits a newly issued certificate to be recognized as valid in a network where not all devices are perfectly synchronized. <p>For example, if the current time is 12:00 and the clock skew allowance is set to the default value of 15 minutes, then the client certificate will be issued with a “not valid before” time of 11:45. In this case, if the authentication server that receives the client certificate has a time of 11:58, it will still recognize the certificate as valid. If the clock skew allowance was set to 0 minutes, then the authentication server would not recognize the certificate as valid until its clock has reached 12:00.</p> <p>The default of 15 minutes is reasonable. If you expect that all devices on the network will be synchronized, then the value may be reduced. A setting of 0 minutes is not recommended as this does not permit any variance in clocks between devices.</p> <p>When issuing a certificate, the certificate’s validity period is determined as follows:</p> <ul style="list-style-type: none"> • The “not valid before” time is set to the current time, less the clock skew allowance. • The “not valid after” time is first calculated as the earliest of the following: <ul style="list-style-type: none"> ■ The current time, plus the maximum validity period. ■ The expiration time of the user account for whom the device certificate is being issued. • The “not valid after” time is then increased by the clock skew allowance.

Subject Alternative Name	To include additional fields in the TLS client certificate issued for a device, mark the Include device information in TLS client certificates check box. These fields are stored in the subject alternative name (subjectAltName) of the certificate. Refer to Table 35 for a list of the fields that are stored in the certificate when this option is enabled. Storing additional device information in the client certificate allows for additional authorization checks to be performed during device authentication.
Digest Algorithm	Algorithm used to sign issued certificates.



If you are using an Aruba controller to perform EAP-TLS authentication using these client certificates, you must have ArubaOS 6.1 or later to enable the **Subject Alternative Name** option and store device information in the subject alternative name.

Table 35: *Device Information Stored in TLS Client Certificates*

Name	Description	OID
Device ICCID	Integrated Circuit Card Identifier (ICCID) number from the Subscriber Identity Module (SIM) card present in the device. This is only available for devices with GSM (cellular network) capability, where a SIM card has been installed.	mdpsDeviceIccid (.4)
Device IMEI	International Mobile Equipment Identity (IMEI) number allocated to this device. This is only available for devices with GSM (cellular network) capability.	mdpsDeviceImei (.3)
Device Serial	Serial number of the device.	mdpsDeviceSerial (.9)
Device Type	Type of device, such as "iOS", "Android", etc.	mdpsDeviceType (.1)
Device UDID	Unique device identifier (UDID) for this device. This is typically a 64-bit, 128-bit or 160-bit number represented in hexadecimal (16, 32, or 40 characters, respectively).	mdpsDeviceUdid (.2)
MAC Address	IEEE MAC address of this device. This element may be present multiple times, if a device has more than one MAC address (for example, an Ethernet port and a Wi-Fi adapter).	mdpsMacAddress (.5)
Product Name	Product string identifying the device and often including the hardware version information.	mdpsProductName (.6)
Product Version	String containing the software version number for the device.	mdpsProductVersion (.7)
User Name	String containing the username of the user who provisioned the device.	mdpsUserName (.8)

In the **Retention Policy** area:

Figure 71 The Certificate Authority Settings Form, Retention Policy Area

Retention Policy	
These options control how long to retain certificates after revocation or expiry.	
Store Certificates:	<input type="checkbox"/> Keep a copy of client certificates When checked issued certificates will be stored. When unchecked, only metadata about the certificate will be retained.
Maximum Period:	52 <input type="text"/> weeks The period after which an expired certificate (or a rejected request) will be automatically deleted. Leave blank to disable automatic deletion.


Field	Description
Maximum Period	Specify values that are appropriate for your organization's retention policy. The default data retention policy specifies a maximum period of 52 weeks.
Store Certificates	If selected, a copy of the issued certificate is stored. If this check box is not selected, only metadata about the certificate is stored.



To enable the **Delete Certificate** and **Delete Request** actions in the **Certificate Management** list view, use a blank value for **Minimum Period**. This is useful for testing and initial deployment.

In the **SCEP & EST Server** area:

Figure 72 The Certificate Authority Settings Form, SCEP & EST Server Area

SCEP & EST Server	
These options control access to the SCEP server for this CA.	
SCEP & EST Server:	<input checked="" type="checkbox"/> Enable access to the SCEP and EST servers Allows this CA to issue tls-client certificates via SCEP and EST
SCEP URL:	http://Garuda-77/guest/mdps_scep.php/1
EST URL:	http://Garuda-77/.well-known/est/ca:1
* SCEP & EST Secret:	<input type="text"/> Shared secret that SCEP and EST clients must supply.
* SCEP & EST Secret:	<input type="text"/> Shared secret that SCEP and EST clients must supply.
Allowed Access:	<input type="text"/> Enter the IP addresses and networks from which logins are permitted.
Denied Access:	<input type="text"/> Enter the IP addresses and networks that are denied login access.
Identity	
Country:	US
State:	California
Locality:	Sunnyvale
Organization:	Aruba Networks
Organizational Unit:	
Common Name:	ClearPass Onboard Local Certificate Authority
Signing Common Name:	ClearPass Onboard Local Certificate Authority (Signing)
Email Address:	10a6b768-9789-49b2-adea-39157cf8721a@example.com
Private Key	
Key Type:	2048-bit RSA
Self-Signed Certificate	
CA Expiration:	3653
Digest Algorithm:	SHA-1
	

Onboard may be used as a CA with third-party products that use Simple Certificate Enrollment Protocol (SCEP) to enroll certificates.

Field	Description
SCEP & EST Server	If selected, enables access to the SCEP and EST servers. The form expands to include SCEP and EST server configuration options.
SCEP URL	Shows the SCEP URL for this SCEP server.
EST URL	Shows the EST URL for this SCEP server.
SCEP & EST Secret	Enter the shared secret that SCEP and EST clients must supply.
Allowed Access	Enter the IP addresses and networks from which logins are permitted. (IPv4 and IPv6 are both supported)
Denied Access	Enter IP addresses and networks that are denied login access. (IPv4 and IPv6 are both

Field	Description
	supported)
Identity	The information in these fields cannot be edited after creation.
Private Key	
Self-Signed Certificate	

In the **Registration Authority** area:

Figure 73 *The Certificate Authority Settings Form, Registration Authority Area*

Registration Authority
These options specify the Certificate Authority this Registration Authority will use to issue certificates.

* SCEP URL:	<input type="text" value="http://10.100.8.82/certsrv/mscep"/> <small>URL of the SCEP server that will act as the CA for this RA.</small>
SCEP Challenge Password:	<input type="text"/> <small>Shared secret for SCEP CA used in generating RA certificate. Leave blank if the SCEP server does not enforce a challenge password.</small>
Confirm SCEP Challenge Password:	<input type="text"/> <small>Shared secret for SCEP CA used in generating RA certificate. Leave blank if the SCEP server does not enforce a challenge password.</small>
Details:	<p>Certificate: Data: Version: 3 (0x2) Serial Number: 4b:71:69:84:ba:bd:9d:87:48:ac:11:db:87:31:17:07 Signature Algorithm: sha1WithRSAEncryption</p> <pre style="font-family: monospace; font-size: 0.8em;"> 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00: f4:e7:1c:8e:81:c9:f8:4e:59:ee:de:ef:d5:c3:bd:a9:2c:e8: 37:af:6b:a9:60:34:d9:eb:a1:b1:a7:e1:95:5c:ad:0b:0b:20: 9b:03:73:82:50:88:b6:f1:2b:3a:b9:a9:ca:ea:ae:e4:f8:bb: e5:58:e0:59 </pre>
Confirm CA Certificate:	<input checked="" type="checkbox"/> The above certificate should be trusted for this CA <small>You should validate the above certificate is the correct certificate for your CA.</small>
CRL URL:	<input type="text" value="http://10.100.8.82/crl/amg-ad-DC-CA.crl"/> <small>URL to the CRL for the CA. If supplied Onboard will sync revocation status of certificates.</small>

[Edit Certificate Authority](#)

Field	Description
SCEP URL	(Required) Shows the URL of the SCEP server that will act as the Certificate Authority for this Registration Authority.
SCEP Challenge Password	Shared secret for the SCEP CA used to generate the RA certificate. If the SCEP server does not enforce a challenge password, leave this field empty.
Confirm SCEP Challenge Password	


Field	Description
Details	Displays the certificate details such as the data and signature algorithm. This field cannot be edited after creation.
Confirm CA Certificate	if selected, validates that the certificate is the trusted certificate for your Certificate Authority.
CRL URL	URL of the Certificate Revocation List for the Certificate Authority. If this is supplied here, Onboard will synchronize the revocation status of certificates.

When you are done, click **Edit Certificate Authority** to complete your changes.


Requesting a Certificate for the Certificate Authority

The **Intermediate Certificate Request** page displays the certificate signing request for the Certificate Authority's intermediate certificate.

You can copy the certificate signing request in text format using your Web browser. Use this option when you can paste the request directly into another application to obtain a certificate.

You can click the  **Download the current CSR** link to download the certificate signing request as a file. Use this option when you need to provide the certificate signing request as a file to obtain a certificate.

After you have obtained the certificate, click the  **Install a signed certificate** link to continue configuring the intermediate Certificate Authority. See "[Installing a Certificate Authority's Certificate](#)" on page 128.

You can also click the  **Change CA settings** link to return to the main **Certificate Authority Settings** form. Use this option to switch to a root CA, or to change the name or properties of the intermediate CA and reissue the certificate signing request.

Installing a Certificate Authority's Certificate

You can import a private key and certificate pair to use for the root certificate or intermediate certificate. The **CA Certificate Import** page may be used to:

- Upload a certificate that has been issued by another Certificate Authority. This process is required when configuring an intermediate Certificate Authority.
 - A private key is not required, as the Certificate Authority has already generated one and used it to create the certificate signing request.
- Upload a certificate and private key to be used as the Certificate Authority's certificate. This process may be used to configure a root Certificate Authority.
 - A private key is required, as the Certificate Authority's existing private key will be replaced.

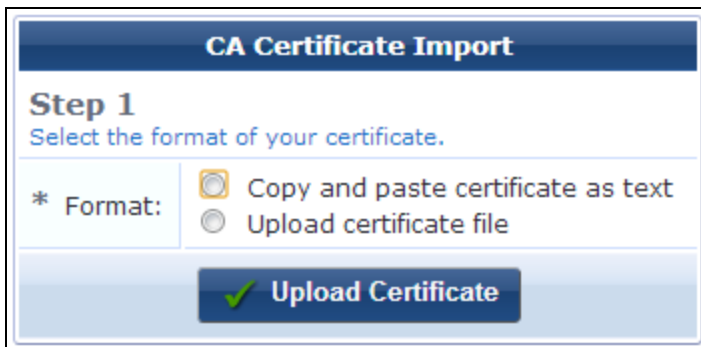


This form may be used multiple times in order to import each of the certificates in the trust chain. Check the message displayed above the form to determine which certificate or type of file must be uploaded next.

To upload a certificate:

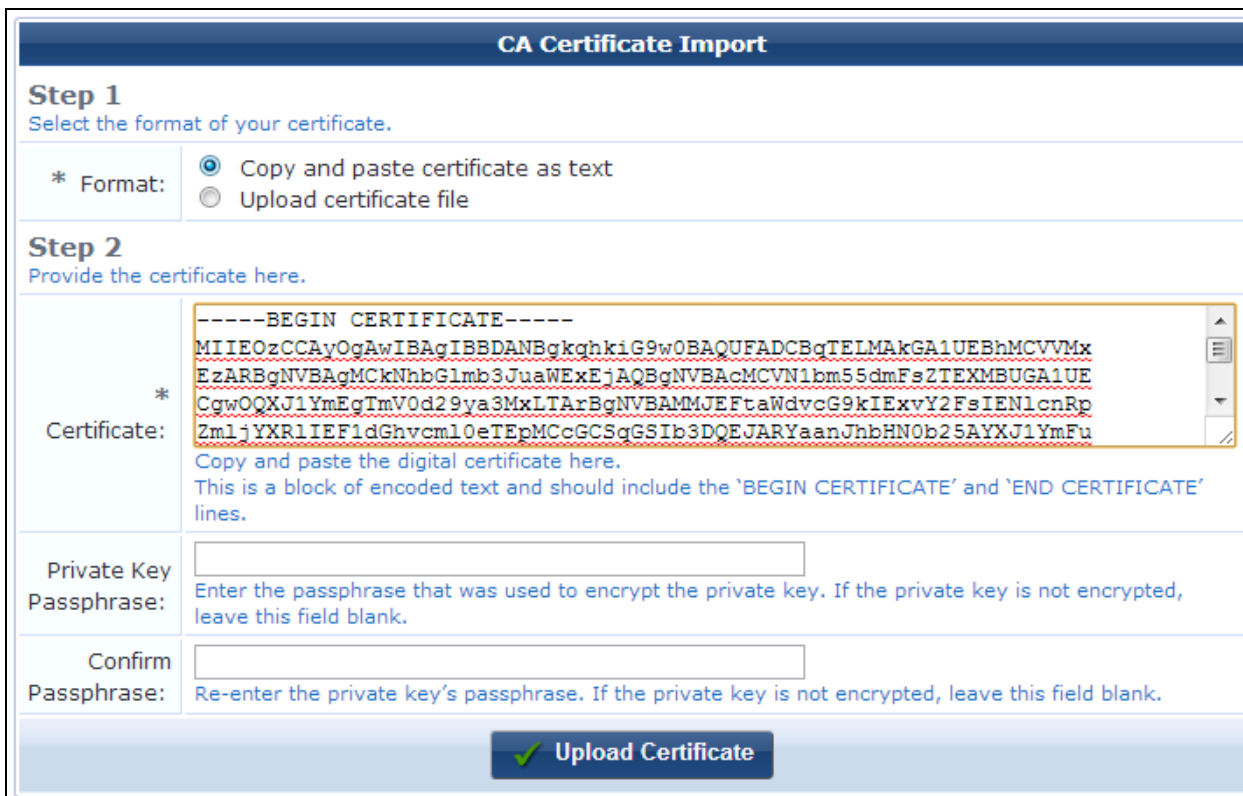
1. On either the **Certificate Management** or **Intermediate Certificate Settings** page, click the **Import Certificate** link above the form. The **Step 1** area of the **CA Certificate Import** form opens.

Figure 74 The CA Certificate Import Form, Step 1



2. Select one of the radio buttons to either copy and paste the certificate as encoded text or browse to the file to upload. The form expands to include options for that method.
3. If you selected **Copy and paste certificate as text**:
 - To upload a single certificate, copy and paste the certificate into the **Certificate** text field. The text must include the "BEGIN CERTIFICATE" and "END CERTIFICATE" lines. Leave the passphrase fields blank.
 - To upload a certificate and private key, copy and paste the certificate and private key into the **Certificate** text field. The text must include the "BEGIN CERTIFICATE" and "END CERTIFICATE" lines, as well as the "BEGIN RSA PRIVATE KEY" and "END RSA PRIVATE KEY" lines.

Figure 75 The CA Certificate Import Form, Step 2



4. If you selected **Upload certificate file**, click **Choose File** in the **Certificate** row to browse to the file and select it.
 - To upload a single certificate, choose a certificate file in PEM (base-64 encoded) or binary format (.crt or PKCS#7). Leave the passphrase fields blank.

- To upload a certificate's private key as a separate file, choose the private key file in PEM (base-64 encoded) format. If the private key has a passphrase, enter it in the **Private Key Passphrase** and **Confirm Passphrase** fields. The private key will be automatically matched to its corresponding certificate when uploaded.
- To upload a combined certificate and private key, choose a file in either PEM (base-64 encoded) or PKCS#12 format. If the private key has a passphrase, enter it in the **Private Key Passphrase** and **Confirm Passphrase** fields.

Figure 76 *The CA Certificate Import Form, Step 3*

CA Certificate Import	
Step 1 Select the format of your certificate.	
* Format:	<input type="radio"/> Copy and paste certificate as text <input checked="" type="radio"/> Upload certificate file
Step 2 Upload the certificate file here.	
* Certificate:	<input type="button" value="Choose File"/> No file chosen Choose a digital certificate to upload. This should be a PEM encoded X.509 certificate file.
Step 3 Specify the passphrase for the private key.	
Private Key Passphrase:	<input type="text"/> Enter the passphrase that was used to encrypt the private key. If the private key is not encrypted, leave this field blank.
Confirm Passphrase:	<input type="text"/> Re-enter the private key's passphrase. If the private key is not encrypted, leave this field blank.
<input type="button" value="✔ Upload Certificate"/>	

5. Click **Upload Certificate** to save your changes.

If additional certificates are required, you will remain at the same page. Check the message displayed above the form to determine which certificate or type of file must be uploaded next. When the trust chain is complete, it will be displayed. This completes the initialization of the certificate authority.

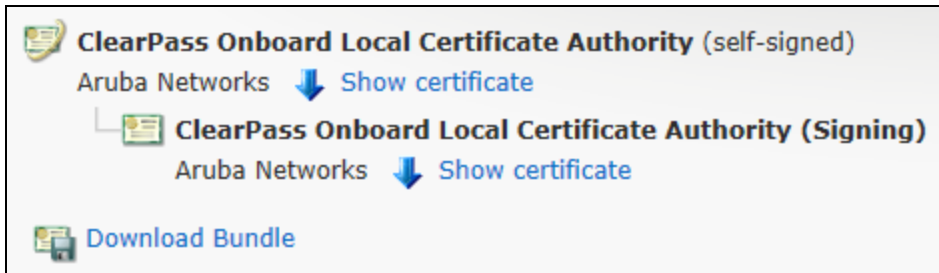
The Trust Chain and Uploading Certificates for the CA

The **Certificate Authority Trust Chain** page is used to view the Certificate Authority's current trust chain, or to upload a new certificate in the trust chain when configuring a Certificate Authority.

Viewing the Trust Chain

To view the Certificate Authority's trust chain, go to **Onboard > Certificate Authorities** and click the **Trust Chain** link for a certificate in the list. The **Certificate Authority Trust Chain** page opens. This page shows a graphical representation of the certificates that make up the trust chain.

Figure 77 *The Certificate Authority Trust Chain Page*



The first certificate listed is the root certificate. Root certificates are always self-signed and are explicitly trusted by clients.





Each additional certificate shown is an intermediate certificate. The last certificate in the list is the signing certificate that is used to issue client and server certificates.

For RADIUS certificates that are not self-signed, only the chain (root and intermediate certificates) is pushed to the user's device, and not the certificate itself. This avoids the need to reprovision when the certificate expires.

Viewing Certificate Properties

To view the properties of a certificate in the trust chain, click the [Show certificate](#) link. The **Certificate Information** view opens.

Figure 78 *The Certificate Information View*

Certificate Information	
Certificate Details Details about the certificate and its owner.	
Issued To:	 ClearPass Onboard Local Certificate Authority
Valid From:	 Monday, 22 October 2012, 02:02 PM
Valid To:	 Sunday, 23 October 2022, 02:32 PM
Subject:	Country US State California Locality Sunnyvale Organization Aruba Networks Common Name ClearPass Onboard Local Certificate Authority
Issuer Details Details about the certificate authority that issued the certificate.	
Issued By:	 ClearPass Onboard Local Certificate Authority
Issuer:	Country US State California Locality Sunnyvale Organization Aruba Networks Common Name ClearPass Onboard Local Certificate Authority
Advanced Technical information about the certificate.	
Fingerprint:	3ddc 0e03 1480 2513 3773 6b2a 0643 6b2c a8c7 6abc This is the SHA-1 "fingerprint" or "thumbprint" of the certificate.
Private Key:	2048-bit RSA The type of the private key for this certificate.
Details:	Show

Exporting the Certificate

To export a certificate:

1. Click the **Download Bundle** link on the **Certificate Authority Trust Chain** page. The **Export Certificate** form opens.

Figure 79 *The Export Certificate Form*

Export Certificate	
* Format:	PKCS#12 Certificate & Key (.p12) Select the file format for the exported item.
Trust Chain	<input checked="" type="checkbox"/> Include certificate trust chain Select this option to include the certificates for the CA and any intermediate certificate authorities in the PKCS#12 container.
* Passphrase:	<input type="text"/> Passphrase to protect the PKCS#12 file.
* Confirm Passphrase:	<input type="text"/> Re-enter the passphrase.
<input type="button" value="Export Certificate"/> <input type="button" value="Cancel"/>	

2. In the **Format** row, choose the certificate format. The form expands to include configuration options for that format.
3. Complete the fields with the appropriate information, and then click **Export Certificate**.

Considerations for iOS Devices

The server certificate is used by ClearPass to secure Web (HTTPS) and authentication (RADIUS) traffic. It can be configured in **ClearPass Policy Manager** under **Administration > Certificates > Server Certificate**.

The optimal configuration for Onboard is a server certificate issued by a trusted commercial Certificate Authority. A list of Certificate Authorities trusted by iOS devices can be found at <http://support.apple.com/kb/HT5012>.

Alternatively, if you only wish to use a single Onboard Certificate Authority, then you can use that Certificate Authority to sign the server certificate. Users will then have to install the certificate as part of the provisioning process.

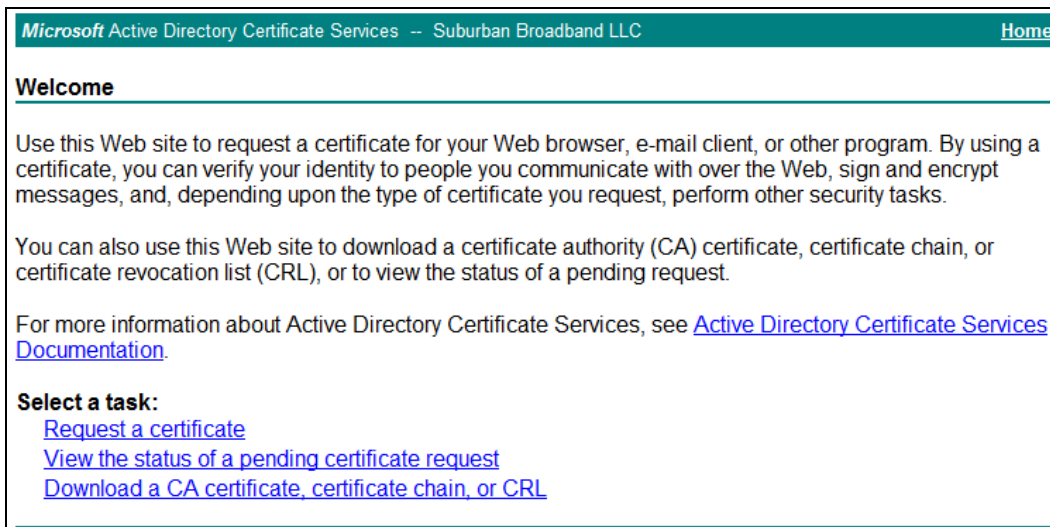
For testing purposes, you can disable the requirement for HTTPS on the **Policy Manager > Configuration > Authentication** page; however, this is an insecure configuration that should not be used in a production environment.

Using Microsoft Active Directory Certificate Services

To use Microsoft Active Directory Services:

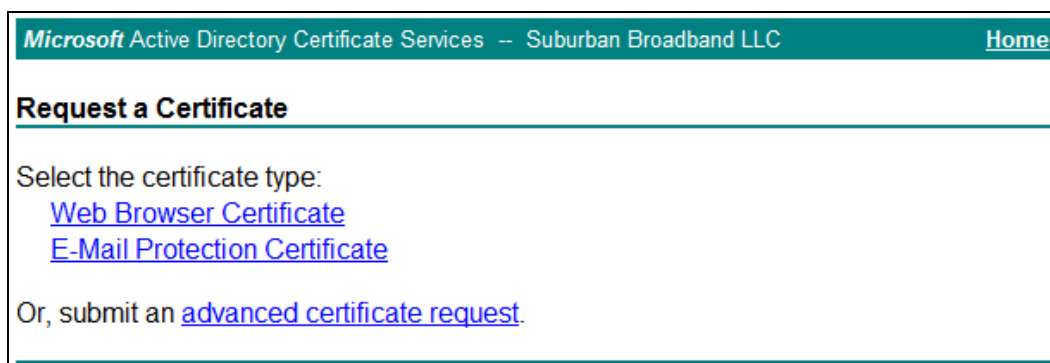
1. Go to the **Microsoft Active Directory Certificate Services** Web page. This page is typically found at <https://<yourdomain>/certsrv/>. The **Welcome** page opens.

Figure 80 *The Welcome Page*



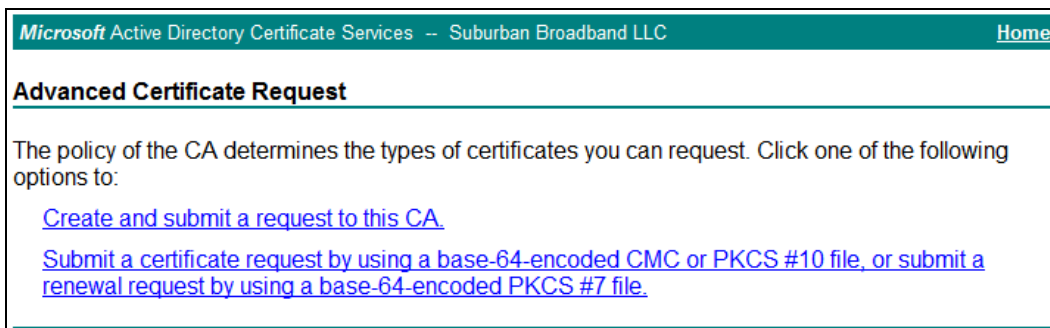
2. Click the **Request a Certificate** link on this page. The **Request a Certificate** page opens.

Figure 81 *The Request a Certificate Page*



3. Click the link to submit an **advanced certificate request**. The **Advanced Certificate Request** page opens.

Figure 82 *The Advanced Certificate Request Page*



4. Click the link to submit a request using a **base-64-encoded CMC or PKCS #10** file. The **Submit a Certificate Request or Renewal Request** page is displayed.

Figure 83 *The Submit a Certificate Request or Renewal Request Page*

Microsoft Active Directory Certificate Services -- Suburban Broadband LLC [Home](#)

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
MIIDVTCCAjOCAQAwbMxCzAIBgNVBAYTAIVTMRMw
MRIwEAYDVQHDAITdW5ueXZhbGUxFzAVBgNVBAoMn
FwYDVQQLEDBBWAxNpdG9y1FN1cnZpY2VzMSYwJAYD
ZmljYXRlIF1dGhvcml0eTEfMB0GCSqGSI1b3DQEJA
bTCCAS1wDQYJKoZIhvcNAQEBBQADggEPADCCAQoC
```

Additional Attributes:

Attributes:

5. Copy and paste the certificate signing request text into the **Saved Request** text field.
6. Because this certificate is for a Certificate Authority, select **Subordinate Certificate Authority** in the **Certificate Template** drop-down list.
7. Click the **Submit** button to issue the certificate. Either the **Certificate Pending** or the **Certificate Issued** page is displayed.

Figure 84 *The Certificate Pending Page*

Microsoft Active Directory Certificate Services -- Suburban Broadband LLC [Home](#)

Certificate Pending

Your certificate request has been received. However, you must wait for an administrator to issue the certificate you requested.

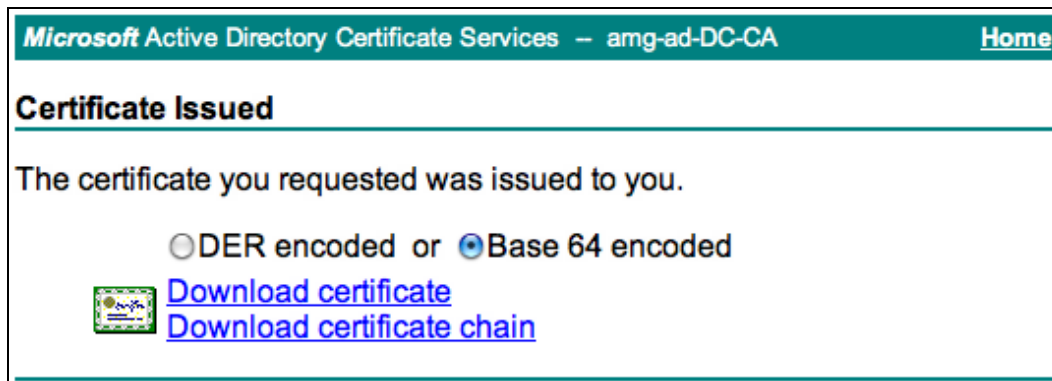
Your Request Id is 826.

Please return to this web site in a day or two to retrieve your certificate.

Note: You must return with **this** web browser within 10 days to retrieve your certificate

8. If the **Certificate Pending** page is displayed, follow the directions on the page to retrieve the certificate when it is issued.

Figure 85 The Certificate Issued Page



9. If the **Certificate Issued** page is displayed, select the **Base 64 encoded** option and then click the **Download certificate chain** link. A file containing the intermediate certificate and the issuing certificates in the trust chain will be downloaded to your system.

Refer to the instructions in "Installing a Certificate Authority's Certificate " on page 128 for information on uploading the certificate file to Onboard.

Management and Control



The Management and Control section in the Onboard navigation lets you view and manage devices and the users and certificates associated with them, as well as the asset database of corporate devices. To access the device management features, go to **Onboard > Management and Control > Start Here**.

- To view and manage your list of devices, see "Device Management (View by Device) " on page 136
- To view and manage the list of users associated with the devices, see "Device Management (View by Username)" on page 141
- To view, create, and manage digital certificates for devices, servers, and certificate authorities, see "Certificate Management (View by Certificate) " on page 144

Device Management (View by Device)



The **Device Management (View by Device)** page lists all devices and lets you manage the devices' access to the network. For each device, you can allow or deny network access.

To work with the list of device users, see "Device Management (View by Username)" on page 141.

When a device is denied access, its certificates are revoked. For a device that has had its access denied, you can grant access again, allowing it to re-enroll and obtain a new certificate.

To view the list of devices, go to **Onboard > Management and Control > View by Device**. The **Device Management (View by Device)** list view opens. This list displays all currently provisioned devices.

Table 36: *The Device Management (View by Device) List View(Continued)*

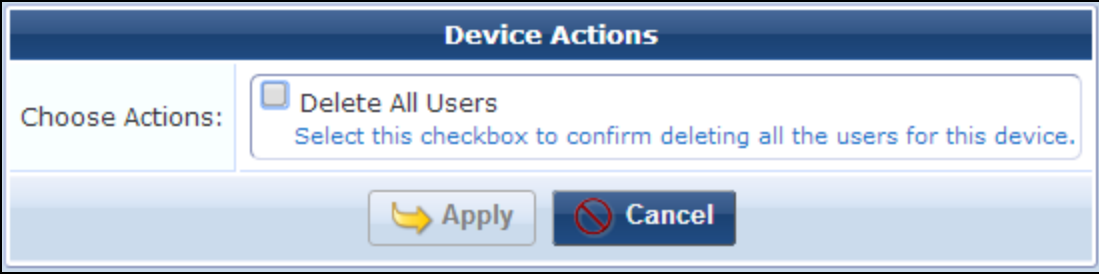

Field	Description
	
Certificates	Displays certificate details and lets you revoke or delete all client certificates for the device. The form expands to include both the Certificate Information view and the Manage Certificates form. The Certificate Information view lets you review all details of the certificate:

Table 36: The Device Management (View by Device) List View(Continued)

Field	Description												
	<div style="border: 1px solid #ccc; padding: 10px;"> <div style="background-color: #004a7c; color: white; text-align: center; padding: 2px 5px;">Certificate Information</div> <div style="padding: 5px 0;"> <p>Certificate Details <small>Details about the certificate and its owner.</small></p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 20%;">Issued To:</td> <td> sham</td> </tr> <tr> <td>Valid From:</td> <td> Tuesday, 24 June 2014, 11:25 AM</td> </tr> <tr> <td>Valid To:</td> <td> Wednesday, 24 June 2015, 11:55 AM</td> </tr> </table> <p>Subject:</p> <ul style="list-style-type: none"> Country US State California Locality Sunnyvale Organization Example Organization Common Name sham mdpsDeviceType iOS mdpsDeviceName iOS mdpsDeviceUdid 9811d8548fe8de157a4338da4d551773627effb5 mdpsMacAddress 70:DE:E2:C7:23:B6 mdpsProductName iPad2,1 mdpsProductVersion 10A523 mdpsUserName sham </div> <div style="padding: 5px 0;"> <p>Issuer Details <small>Details about the certificate authority that issued the certificate.</small></p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 20%;">Issued By:</td> <td> ClearPass Onboard Local Certificate Authority (Signing)</td> </tr> </table> <p>Issuer:</p> <ul style="list-style-type: none"> Country US State California Locality Sunnyvale Organization Aruba Networks Common Name ClearPass Onboard Local Certificate Authority (Signing) Email Address a0d4fe4d-e6df-4cb7-8f95-90b614853e5f@example.com </div> <div style="padding: 5px 0;"> <p>Advanced <small>Technical information about the certificate.</small></p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 20%;">Fingerprint:</td> <td>99dd d7f5 af57 c889 274c d8eb 558e 1d59 8eeb ea86 <small>This is the SHA-1 "fingerprint" or "thumbprint" of the certificate.</small></td> </tr> <tr> <td>Details:</td> <td> Show</td> </tr> </table> </div> </div>	Issued To:	sham	Valid From:	Tuesday, 24 June 2014, 11:25 AM	Valid To:	Wednesday, 24 June 2015, 11:55 AM	Issued By:	ClearPass Onboard Local Certificate Authority (Signing)	Fingerprint:	99dd d7f5 af57 c889 274c d8eb 558e 1d59 8eeb ea86 <small>This is the SHA-1 "fingerprint" or "thumbprint" of the certificate.</small>	Details:	Show
Issued To:	sham												
Valid From:	Tuesday, 24 June 2014, 11:25 AM												
Valid To:	Wednesday, 24 June 2015, 11:55 AM												
Issued By:	ClearPass Onboard Local Certificate Authority (Signing)												
Fingerprint:	99dd d7f5 af57 c889 274c d8eb 558e 1d59 8eeb ea86 <small>This is the SHA-1 "fingerprint" or "thumbprint" of the certificate.</small>												
Details:	Show												
	<p>The Manage Certificates form lets you revoke or delete all TLS client certificates issued to the device. Mark the appropriate radio button, and then click Manage Certificates.</p>												

Table 36: The Device Management (View by Device) List View(Continued)

Field	Description
	
Delete Device	Deletes the device. You will be asked to confirm the deletion. Deleting the device will also delete all user, certificate, and other data associated with the device. Certificates are deleted according to the Certificate Authority's retention policy. After a device is deleted, it can still access the network and be reprovisioned. To deny network access for the device, use the Manage Access link instead.

Device Management (View by Username)



The **Device Management (View by Username)** page lists all users associated with devices. For each user, you can:

- View and edit default configuration profile and provisioning settings
- View and manage all devices registered to the user
- Allow or deny network access for the user
- Delete all the user's devices
- Revoke or delete all TLS client certificates issued to the user
- Delete the user

To work with the list of devices, see "[Device Management \(View by Device\)](#) " on page 136.

To view the list of users, go to **Onboard > Management and Control > View by Username**. The **Device Management (View by Username)** list view opens. Information shown in this list for each user includes username, network access status, number of devices, and number of onboarded devices.

You can filter the list by keywords, and you can click a user's row in the list to show the available options. These include configuration details, device information, access management, device actions, certificate actions, and user deletion.

Figure 87 The Device Management (View by Username) List View

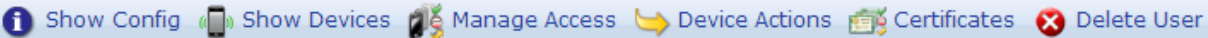

User	Status	Number of Devices	Onboarded
sham	✓ Allowed	1	1 Device(s)
			
 Refresh		1	Showing 1 - 1 of 1 10 rows per page ▼

Table 37: The Device Management (View by Username) List View

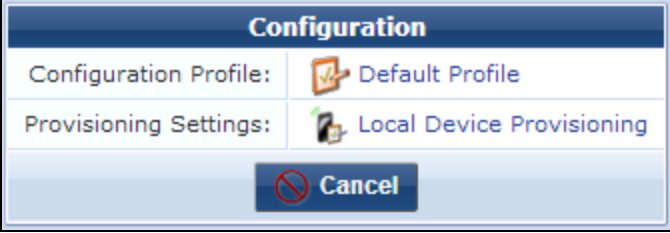
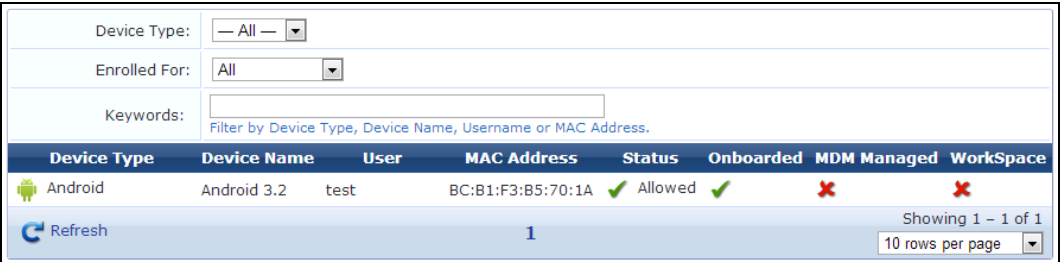

Field	Description
Keywords	Lets you filter by username.
Show Config	<p>Lets you configure the user's details. The row expands to include the Configuration form. You can click the Default Profile link to edit the user's device configuration profile, or click the Local Device Provisioning link to edit the user's local device provisioning settings.</p> 
Device Details	<p>Displays a list of the user's devices.</p> 
Certificates	<p>Displays details of certificates belonging to this user, and lets you revoke or delete all client certificates issued to the user. The form expands to include both the Certificate Information view and the Manage Certificates form.</p> <p>The Certificate Information view lets you review all details of the certificate:</p>

Table 37: The Device Management (View by Username) List View(Continued)

Field	Description						
	<div style="border: 1px solid #ccc; padding: 10px;"> <div style="background-color: #2c5e8c; color: white; text-align: center; padding: 5px; font-weight: bold;">Certificate Information</div> <div style="padding: 10px 0 0 10px;"> <h3 style="margin: 0;">Certificate Details</h3> <p style="margin: 0; font-size: small;">Details about the certificate and its owner.</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 20%; padding: 5px;">Issued To:</td> <td style="padding: 5px;"> sham</td> </tr> <tr> <td style="padding: 5px;">Valid From:</td> <td style="padding: 5px;"> Tuesday, 24 June 2014, 11:25 AM</td> </tr> <tr> <td style="padding: 5px;">Valid To:</td> <td style="padding: 5px;"> Wednesday, 24 June 2015, 11:55 AM</td> </tr> </table> <div style="margin-top: 10px;"> <p style="margin: 0;">Subject:</p> <ul style="list-style-type: none"> Country US State California Locality Sunnyvale Organization Example Organization Common Name sham mdpsDeviceType iOS mdpsDeviceName iOS mdpsDeviceUdid 9811d8548fe8de157a4338da4d551773627effb5 mdpsMacAddress 70:DE:E2:C7:23:B6 mdpsProductName iPad2,1 mdpsProductVersion 10A523 mdpsUserName sham </div> </div> </div>	Issued To:	sham	Valid From:	Tuesday, 24 June 2014, 11:25 AM	Valid To:	Wednesday, 24 June 2015, 11:55 AM
Issued To:	sham						
Valid From:	Tuesday, 24 June 2014, 11:25 AM						
Valid To:	Wednesday, 24 June 2015, 11:55 AM						
	<div style="border: 1px solid #ccc; padding: 10px;"> <div style="padding: 10px 0 0 10px;"> <h3 style="margin: 0;">Issuer Details</h3> <p style="margin: 0; font-size: small;">Details about the certificate authority that issued the certificate.</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 20%; padding: 5px;">Issued By:</td> <td style="padding: 5px;"> ClearPass Onboard Local Certificate Authority (Signing)</td> </tr> </table> <div style="margin-top: 10px;"> <p style="margin: 0;">Issuer:</p> <ul style="list-style-type: none"> Country US State California Locality Sunnyvale Organization Aruba Networks Common Name ClearPass Onboard Local Certificate Authority (Signing) Email Address a0d4fe4d-e6df-4cb7-8f95-90b614853e5f@example.com </div> </div> </div>	Issued By:	ClearPass Onboard Local Certificate Authority (Signing)				
Issued By:	ClearPass Onboard Local Certificate Authority (Signing)						
	<div style="border: 1px solid #ccc; padding: 10px;"> <div style="padding: 10px 0 0 10px;"> <h3 style="margin: 0;">Advanced</h3> <p style="margin: 0; font-size: small;">Technical information about the certificate.</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 20%; padding: 5px;">Fingerprint:</td> <td style="padding: 5px;">99dd d7f5 af57 c889 274c d8eb 558e 1d59 8eeb ea86 <small>This is the SHA-1 "fingerprint" or "thumbprint" of the certificate.</small></td> </tr> <tr> <td style="padding: 5px;">Details:</td> <td style="padding: 5px;"> Show</td> </tr> </table> </div> </div>	Fingerprint:	99dd d7f5 af57 c889 274c d8eb 558e 1d59 8eeb ea86 <small>This is the SHA-1 "fingerprint" or "thumbprint" of the certificate.</small>	Details:	Show		
Fingerprint:	99dd d7f5 af57 c889 274c d8eb 558e 1d59 8eeb ea86 <small>This is the SHA-1 "fingerprint" or "thumbprint" of the certificate.</small>						
Details:	Show						

The **Manage Certificates** form lets you revoke or delete all TLS client certificates issued to the user. Mark the appropriate radio button, and then click **Manage Certificates**.

Table 37: The Device Management (View by Username) List View(Continued)

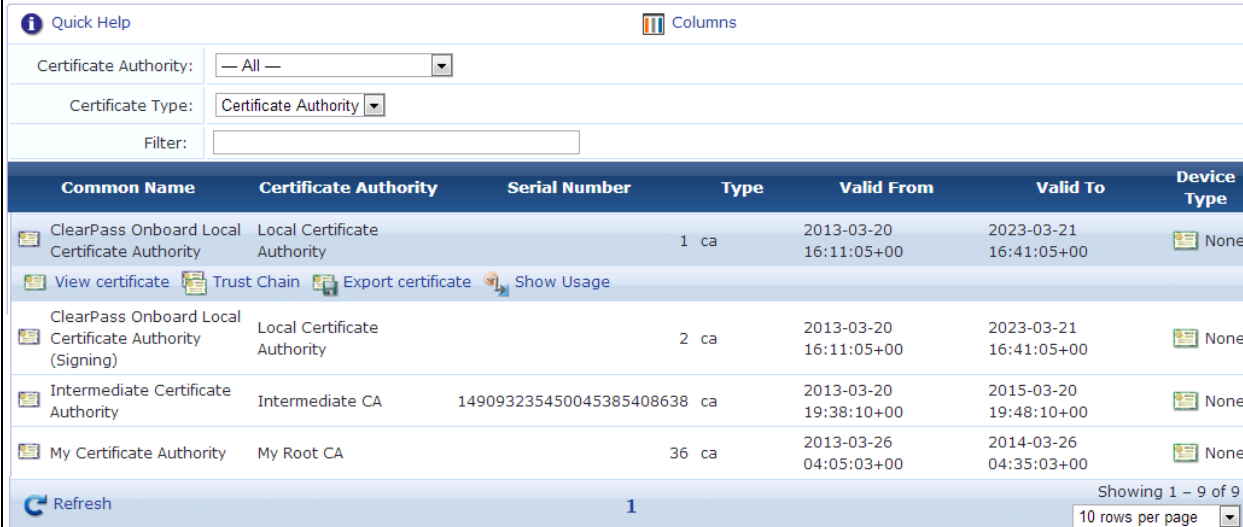
Field	Description
	
Delete User	Deletes the user. You will be asked to confirm the deletion. Deleting the user will also delete all devices, TLS client certificates, and other data associated with the user. Certificates are deleted according to the Certificate Authority's retention policy.

Certificate Management (View by Certificate)



To view the list of certificates and work with them, go to **Onboard > Management and Control > View by Certificate**. The **Certificate Management** list view opens. This list displays all of the certificates and certificate requests in the Onboard system.

Figure 88 *The Certificate Management (View by Certificate) List View*



Common Name	Certificate Authority	Serial Number	Type	Valid From	Valid To	Device Type
ClearPass Onboard Local Certificate Authority	Local Certificate Authority	1	ca	2013-03-20 16:11:05+00	2023-03-21 16:41:05+00	None
ClearPass Onboard Local Certificate Authority (Signing)	Local Certificate Authority	2	ca	2013-03-20 16:11:05+00	2023-03-21 16:41:05+00	None
Intermediate Certificate Authority	Intermediate CA	149093235450045385408638	ca	2013-03-20 19:38:10+00	2015-03-20 19:48:10+00	None
My Certificate Authority	My Root CA	36	ca	2013-03-26 04:05:03+00	2014-03-26 04:35:03+00	None







The default columns in the **Certificate Management** list provide information about the common name, certificate authority, serial number (if available), certificate type, validity date range, and device type—iOS, Android, Windows, or None (if not associated with a device type).





To display different columns, click the **Columns** link above the list view. The view expands to include the **Choose Columns** form. You can select or deselect columns to change the way the **Certificate Management** list view is displayed.

Figure 89 The Certificate Management View, Choose Columns Form

Table 38 lists the types of certificate that are displayed in the **Certificate Management** list view.

Table 38: Types of Certificate Supported by Onboard Certificate Management



	Certificate Type	"Type" Column	Notes
	Root certificate	ca	Self-signed certificate for the Certificate Authority
	Intermediate certificate	ca	Issued by the root CA or another intermediate CA
	Certificate signing request	tls-client or trusted	The type shown depends on the kind of certificate requested
	Rejected certificate signing request	tls-client or trusted	Certificate request that was rejected due to an administrator decision
	Device certificate	scep-client	Issued to iOS and OS X (10.7+) devices only
	Client certificate	tls-client	Identity certificate issued to a specific


	Certificate Type	"Type" Column	Notes
			user's device
	Server certificate	trusted	Identity certificate issued to a server
	Code-signing certificate	ca	Used for signing the Windows provisioning application and iOS/OS X profiles
	Revoked certificate	--	Certificate that has been administratively revoked and is no longer valid
	Expired certificate	--	Certificate that is outside its validity period and is no longer valid
	HTTPS		Certificate for HTTPS server certificates

- To create a new certificate, see ["Creating a Certificate " on page 155.](#)
- To search for certificates, see ["Searching for Certificates in the List " on page 146.](#)
- To work with your certificates, see ["Working with Certificates in the List" on page 147.](#)
- To work with certificate signing requests, see ["Working with Certificate Signing Requests " on page 149.](#)
- To import a code-signing certificate, see ["Importing a Code-Signing Certificate " on page 153.](#)
- To import a trusted certificate, see ["Importing a Trusted Certificate " on page 154.](#)

Searching for Certificates in the List

In the **Certificate Management** list, the **Filter** field can be used to quickly search for a matching certificate. Type a username into this field to quickly locate all certificates matching that username.

The filter is applied to all columns displayed in the list view. To search by another field, such as MAC address, device type, or device serial number, click the  **Columns** tab, select the appropriate column(s), and then click the  **Save and Reload** button. The list view will refresh to update the results of the filter.

Click the  **Clear Filter** link to restore the default view.

Use the paging control at the bottom of the list to jump forwards or backwards by one page, or to the first or last page of the list. You can also click an individual page number to jump directly to that page.





When the list contains many thousands of certificates, consider using the Filter field to speed up finding a specific certificate.

Click the column headers to sort the list view by that column. Click the column header a second time to reverse the direction of the sort.

Working with Certificates in the List

To work with a certificate in the **Certificate Management** list, go to **Onboard > Management and Control > View by Certificate** and click a certificate in the list to select it. You can then select from **View Certificate**, **Export Certificate**, **Revoke Certificate**, and **Delete Certificate** actions:

View Certificate

The  **View certificate** link displays the properties of the certificate. Information includes certificate details, issuer details, and the certificate's "fingerprint" or "thumbprint". In the **Details** row, you can click the **Show** link to display advanced details, including such things as the version, serial number, signature algorithms, and public key algorithms. SHA-512, SHA-384, SHA-256, and SHA-224 are supported as digest algorithms. Click the  **Cancel** button to close the certificate properties.

Export Certificate

 **Export certificate** – Displays the **Export Certificate** form.

Figure 90 *The Export Certificate Form*




Use the **Format** drop-down list to select the format in which the certificate should be exported. The following formats are supported:

- **PKCS#7 Certificates (.p7b)**—Exports the certificate, and optionally the other certificates forming the trust chain for the certificate, as a PKCS#7 container.
- **Base-64 Encoded (.pem)**—Exports the certificate as a base-64 encoded text file. This is also known as “PEM format”. You may optionally include the other certificates forming the trust chain for the certificate.
- **Binary Certificate (.crt)**—Exports the certificate as a binary file. This is also known as “DER format”.
- **Open SSL Text Format**—Exports the certificate as a full openssl text-format output, allowing you to view advanced details such as X509v3 extensions. It also includes the certificate in .pem format appended to the .txt file.



To protect against brute-force password attacks and ensure the security of the private key, you should use a strong passphrase – one consisting of several words, mixed upper- and lower-case letters, and punctuation or other symbol characters.





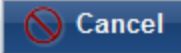
Click  **Export Certificate** to download the certificate file in the selected format.


Revoke Certificate

The  **Revoke certificate** link displays the **Revoke Certificate** form.

Figure 91 *The Revoke Certificate Form*



Revoke Certificate	
Certificate Details Details about the certificate and its owner.	
Issued To:	 Device Enrollment (Profile Signing)
Valid From:	 Monday, 22 October 2012, 02:02 PM
Valid To:	 Sunday, 23 October 2022, 02:32 PM
Subject:	Country US State California Locality Sunnyvale Organization Aruba Networks Common Name Device Enrollment (Profile Signing)
Confirm:	<input type="checkbox"/> Revoke this client certificate Select this checkbox to confirm the certificate revocation.
 	

Mark the **Revoke this client certificate** check box to confirm that the certificate should be revoked, and then click  **Revoke Certificate**.

After the certificate has been revoked, future checks of the certificate's validity using OCSP or CRL will indicate that the certificate is no longer valid.



Due to the way in which certificate revocation lists work, a certificate cannot be un-revoked. A new certificate must be issued if a certificate is revoked in error.

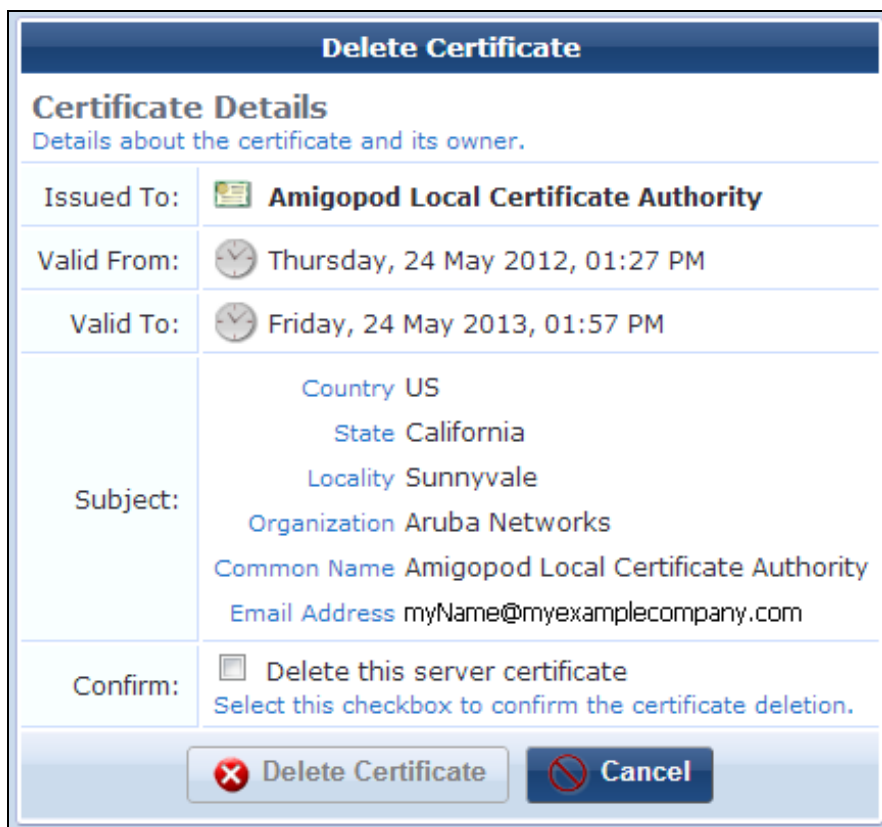






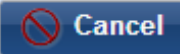
Revoking a device's certificate will cause the device to be unable to authenticate. It will not prevent it from being re-provisioned. If you wish to deny access to a device, use the **Manage Access** link in the device's row on the **Management and Control > View by Device** form.

Delete Certificate

The **✖ Delete certificate** link removes the certificate from the list. Certificates can be deleted even if they are still valid. This will have the effect of revoking them at the same time as deleting them.

Figure 92 *The Delete Certificate Form*



Delete Certificate	
Certificate Details Details about the certificate and its owner.	
Issued To:	 Amigopod Local Certificate Authority
Valid From:	 Thursday, 24 May 2012, 01:27 PM
Valid To:	 Friday, 24 May 2013, 01:57 PM
Subject:	Country US State California Locality Sunnyvale Organization Aruba Networks Common Name Amigopod Local Certificate Authority Email Address myName@myexamplecompany.com
Confirm:	<input type="checkbox"/> Delete this server certificate Select this checkbox to confirm the certificate deletion.
 	



The **Delete Certificate** form is displayed. Mark the **Delete this client certificate** check box to confirm the certificate's deletion, and then click **✖ Delete Certificate**.

Working with Certificate Signing Requests

Certificate signing requests can be managed through the **Certificate Management** list view at **Onboard > Management and Control > View by Certificate**. This allows server certificates, subordinate Certificate Authorities, and other client certificates not associated with a device to be issued by the Onboard Certificate Authority.

Click a certificate request to select it. You can then select from the **View Request**, **Export Request**, **Sign Request**, **Reject Request**, and **Delete Request** actions:

View Request

The  **View request** link displays the properties of the certificate request. Click  **Cancel** to close the certificate request properties.

Export Request


The  **Export request** link displays the **Export Certificate Request** form.

Figure 93 *The Export Certificate Form*



The screenshot shows a web form titled "Export Certificate". It contains the following fields and options:

- * Format:** A dropdown menu with "PKCS#12 Certificate & Key (.p12)" selected. Below it is the instruction: "Select the file format for the exported item."
- Trust Chain:** A checkbox labeled "Include certificate trust chain" is checked. Below it is the instruction: "Select this option to include the certificates for the CA and any intermediate certificate authorities in the PKCS#12 container."
- * Passphrase:** An empty text input field. Below it is the instruction: "Passphrase to protect the PKCS#12 file."
- * Confirm Passphrase:** An empty text input field. Below it is the instruction: "Re-enter the passphrase."

At the bottom of the form are two buttons: "Export Certificate" (with a document icon) and "Cancel" (with a red circle and slash icon).

Use the **Format** drop-down list on the **Export Certificate** form to select the format in which the certificate signing request should be exported. The following formats are supported:

- **PKCS#10 Certificate Request (.p10)** – Exports the certificate signing request in binary format.
- **Base-64 Encoded (.pem)** – Exports the certificate signing request as a base-64 encoded text file. This is also known as “PEM format”.

If you choose **Base-64 Encoded**, the form expands to include the **Trust Chain** row. You can use this option to create and export a certificate bundle that includes the Intermediate CA and Root CA and can be imported in ClearPass Policy Manager as the server certificate (ClearPass Policy Manager does not accept PKCS#7). To include the trust chain in a certificate bundle that can be imported as the server certificate in ClearPass Policy Manager, mark the **Include certificate trust chain** check box, then click **Export Certificate**.

Click **Export Request** to download the certificate signing request file in the selected format.

Sign Request






The  **Sign request** link opens the **Sign Request** form. Use this action to approve the request for a certificate and issue the certificate.

Figure 94 The Sign Request Form

Sign Request	
Request Details Details about the request and its owner.	
Issue To:	 Example Certificate Authority
Subject:	Country US State California Locality Sunnyvale Organization MyCompany Common Name Example Certificate Authority Email Address example@mycompany.com
Certificate Options Options that affect the signing of the certificate.	
* Expiration:	<input type="text" value="365"/> days The number of days before the certificate will expire.
Confirm:	<input type="checkbox"/> Sign this request Select this checkbox to sign the request and issue a certificate.
<div style="text-align: right;"> </div>	

Use the **Expiration** text field to specify how long the issued certificate should remain valid.

Mark the **Sign this request** check box to confirm that the certificate should be issued, and then click  **Sign Request**. The certificate will be issued and will then replace the certificate signing request in the list view.

Reject Request


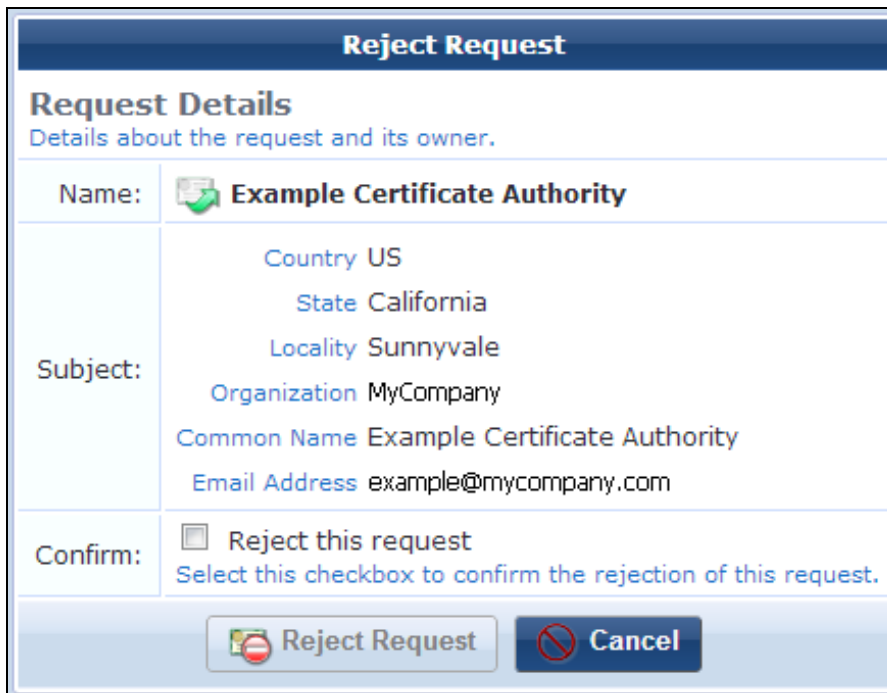



The  **Reject request** link opens the **Reject Request** form. Use this action to reject the request for a certificate. Rejected requests are automatically deleted according to the data retention policy.

Figure 95 *The Reject Request Form*



Reject Request	
Request Details Details about the request and its owner.	
Name:	 Example Certificate Authority
Subject:	Country US
	State California
	Locality Sunnyvale
	Organization MyCompany
	Common Name Example Certificate Authority
	Email Address example@mycompany.com
Confirm:	<input type="checkbox"/> Reject this request Select this checkbox to confirm the rejection of this request.
 	

Mark the **Reject this request** check box to confirm that the certificate signing request should be rejected, and then click the  **Reject Request** button.

Delete Request


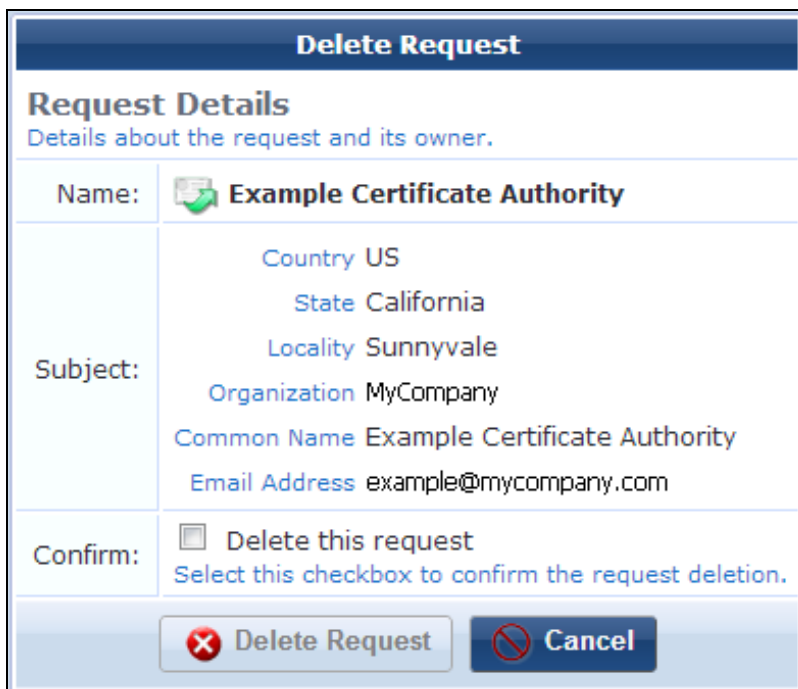



The  **Delete request** link opens the **Delete Request** form. You can use this form to remove the certificate signing request from the list. This option is only available if the data retention policy is configured to permit the certificate signing request's deletion.

Figure 96 *The Delete Request Form*



Delete Request	
Request Details Details about the request and its owner.	
Name:	 Example Certificate Authority
Subject:	Country US
	State California
	Locality Sunnyvale
	Organization MyCompany
	Common Name Example Certificate Authority
	Email Address example@mycompany.com
Confirm:	<input type="checkbox"/> Delete this request Select this checkbox to confirm the request deletion.
 	

Mark the **Delete this request** check box to confirm the certificate signing request's deletion, and then click **Delete Request**.

Importing a Code-Signing Certificate

ClearPass Onboard supports importing a code-signing certificate chain and private key for signing the Windows provisioning application. Certificates can be uploaded as PFX, PKCS-12, SPC, or PKCS-7, and can include a chain of certificates. An operator's profile must include the Import Code-Signing Certificate privilege in order to access this feature. Code-signing certificates can also be used as profile-signing certificates.

To import a trusted certificate, see "[Importing a Trusted Certificate](#)" on page 154.

To import a code-signing certificate, do one of the following:

- Go to **Onboard > Management and Control > View by Certificate** and click the **Upload a code-signing certificate** link.
- Go to **Onboard > Deployment and Provisioning > Provisioning Settings**. You can either click the **Create new provisioning settings** link at the top of the page, or click the **Edit** link for a configuration set in the list. In the page that opens, click the **Upload a code-signing certificate** link in the upper-right corner.

The **Code-Signing Certificate Import** form opens.

Figure 97 *The Code-Signing Certificate Import Form*

Table 39: *The Code-Signing Certificate Import Form*

Field	Description
Certificate	Click Choose File to navigate to the code-signing certificate file to upload.
Private Key	If the private key for the code-signing certificate was issued as a separate file, click the Choose File button to navigate to the private key file.
Private Key Passphrase	Passphrase that was used to encrypt the private key. If the private key is not encrypted, leave empty.
Upload Certificate	Uploads the certificate. The certificate chain is displayed.

To use the certificate for code-signing:

1. Go to **Onboard > Deployment and Provisioning > Provisioning Settings > Windows tab**.
2. In the **Windows Provisioning** area, use the **Code-Signing Certificate** drop-down list to select the uploaded certificate.

Figure 98 *The Windows Provisioning Area*



To create a test certificate:

1. Go to **Onboard > Management and Control > View by Certificate** and click the **Generate a new certificate signing request** link. The **Certificate Request Settings** form opens.
2. In the **Certificate Type** drop-down list, choose **Code-Signing**.
3. Complete the rest of the form with your information. Mark the **Issue this certificate immediately** check box, then click **Create Certificate Request**.

The test certificate is displayed in the list on the **Certificate Management** page, and can be selected on the **Provisioning Settings** form.

Importing a Trusted Certificate

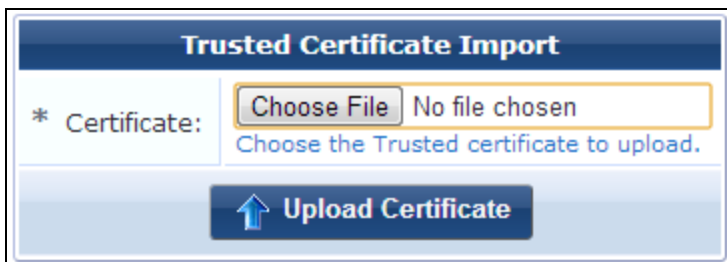
Onboard's **Certificate Management** page supports importing trusted certificates. Certificates may be uploaded in PEM format (*.pem).

(To import a code-signing certificate, see "[Importing a Code-Signing Certificate](#)" on page 153)

To import a trusted certificate:

1. Go to **Onboard > Management and Control > View by Certificate** and click the **Upload a trusted certificate** link. The **Trusted Certificate Import** form opens.

Figure 99 *The Trusted Certificate Import Form*



2. Click **Choose File** to browse to the certificate on your system, and then click **Upload Certificate**. A confirmation message is displayed, and the imported certificate is included in the **Certificate Management** list. You can click the **Show Certificate** link next to the certificate's name to view the certificate's details.

Figure 100 *The Certificate Information View*



3. You can use the following additional options in the upper-right corner of the **Import Trusted Certificate** page:
 - Click the **Upload another trusted certificate** link to upload additional certificates.

- Click the **Edit <certificate name> trust settings** link to open the **Trust** tab of the **Network Settings** form.

Creating a Certificate


To create a new certificate, go to **Onboard > Management and Control > View by Certificate**. The **Certificate Management** page opens. Click the  **Generate a new certificate signing request** link. The **Certificate Request Settings** form opens.

Figure 101 *The Certificate Request Settings Form*

Certificate Request Settings	
* Certificate Authority:	Local Certificate Authority ▼ <small>Select the certificate authority that will be used to sign this request.</small>
* Certificate Type:	TLS Client Certificate ▼ <small>Select the type of certificate to create from this signing request.</small>
Identity <small>These details are used to create a Distinguished Name for the certificate request.</small>	
* Country:	<input type="text"/> <small>Enter the 2-letter ISO country code of your country.</small>
* State:	<input type="text"/> <small>Enter the full name of your state or province.</small>
* Locality:	<input type="text"/> <small>Enter the name of your locality (town or city).</small>
* Organization:	<input type="text"/> <small>Enter the name of your organization or company.</small>
Organizational Unit:	<input type="text"/> <small>Enter the name of your organizational unit (e.g. section or division of the company).</small>
* Common Name:	<input type="text"/> <small>Enter a name for the certificate authority. This is the 'common name' of the digital certificate.</small>
* Email Address:	<input type="text"/> <small>Enter an email address.</small>
Private Key <small>These options are used to create a private key for the certificate request.</small>	
* Key Type:	2048-bit RSA ▼ <small>Select the type of private key to create for the certificate.</small>

To create a new certificate or certificate signing request:

1. In the **Certificate Authority** drop-down list, select the Certificate Authority that will be used to sign the request.
2. In the **Certificate Type** drop-down list, select the type of certificate you want to create:
 - **TLS Client Certificate**—Use this option when the certificate is to be issued to a client, such as a user or a user's device.
 - When this option is selected, the issued certificate's extended key usage property will contain a value of "Client Auth", indicating that the certificate may be used to identify a client.
 - When you create a TLS Client certificate, corresponding entries are created in the **Onboard > Management and Control > View by Device** and **Onboard > Management and Control > View by Username** lists.

- **Trusted Certificate**—Use this option when the certificate is to be issued to a network server, such as a Web server or as the EAP-TLS authentication server.
 - When this option is selected, the issued certificate’s extended key usage property will contain a value of “Server Auth”, indicating that the certificate may be used to identify a server. Trusted certificates include the id-kp-eapOverLAN extended key usage.
- **Certificate Authority**—Use this option when the certificate is for a subordinate Certificate Authority.
 - When this option is selected, the issued certificate will contain an extension identifying it as an intermediate Certificate Authority, and the extended key usage property will contain the three values “Client Auth”, “Server Auth” and “OCSP Signing”.
- **Code Signing**—Use this option for signing the Windows provisioning application.
- **HTTPS**—Use this option to create certificates suitable for use as HTTPS server certificates.

The fields available on the rest of the **Certificate Request Settings** form depend on your selection in the **Certificate Type** field. For information on configuring these fields, see the following section, ["Specifying the Identity of the Certificate Subject" on page 156](#).

Specifying the Identity of the Certificate Subject

In the **Identity** area of the **Certificate Request Settings** form, provide the identity of the person or device for which the certificate is to be issued (the “subject” of the certificate). Together, these fields are collectively known as a distinguished name, or “DN”:

Table 40: *Certificate Request Settings Form, Identity and Private Key Areas*

Field	Description
Country	Two-letter ISO country code for your organization. This value forms part of the distinguished name for the certificate.
State	Full name of the state or province for your organization. This value forms part of the distinguished name for the certificate.
Locality	Name of the town or city where your organization is located. This value forms part of the distinguished name for the certificate.
Organization	Name of your organization. This value forms part of the distinguished name for the certificate.
Organizational Unit	(Optional) Name of your organizational unit (section or division of the organization). This value forms part of the distinguished name for the certificate.

Table 40: Certificate Request Settings Form, Identity and Private Key Areas(Continued)

Field	Description
Common Name	Descriptive name for the certificate. This value is used to identify the certificate as the issuer of other certificates, notably the signing certificate.
Email Address	Contact email address. This email address is included in the root and signing certificates, and provides a way for users of the certificate authority to contact your organization.
Key Type	<p>Specifies the type of private key that should be created for the certificate. Options include:</p> <ul style="list-style-type: none"> ● 1024-bit RSA – lower security ● 2048-bit RSA – recommended for general use ● 4096-bit RSA – higher security <hr/> <p>Using a private key containing more bits will increase security, but will also increase the processing time required to create the certificate and authenticate the device. The additional processing required will also affect the battery life of a mobile device. It is recommended to use the smallest private key size that is feasible for your organization.</p>



Figure 102 *The Subject Alternative Name Area*

Subject Alternative Name
These details are used to add a 'subjectAltName' extension to the certificate request.

Device Type:	<input type="text"/>
Device Name:	<input type="text"/>
Device UDID:	<input type="text"/>
Device IMEI:	<input type="text"/>
Device ICCID:	<input type="text"/>
Device Serial:	<input type="text"/>
MAC Address:	<input type="text"/>
Product Name:	<input type="text"/>
Product Version:	<input type="text"/>
User Name:	<input type="text"/>
Custom Field:	<input type="text"/>
User Email Address:	<input type="text"/>

Issue Certificate
Checking this option will immediately issue the certificate for the request.

Approval: Issue this certificate immediately

If you have selected **TLS Client** as the certificate type, the **Subject Alternative Name** area is also included on the **Certificate Request Settings** form. The alternative name can be used to specify additional identification details for the certificate's subject. If one or more of these options are provided, the issued certificate will contain a subject AltName extension with the specified values.

Table 41 explains the fields that may be included as part of the subject alternative name.

Table 41: Subject Alternative Name Fields Supported When Creating a TLS Client Certificate Signing Request

Field	Description
Device Type	Type of device, such as "iOS", "Android", etc.
Device Name	The hostname of the device at the time of enrollment.
Device UDID	Unique device identifier (UDID) for this device. This is typically a 64-bit, 128-bit or 160-bit number represented in hexadecimal (16, 32 or 40 characters, respectively).
Device IMEI	International Mobile Equipment Identity (IMEI) number allocated to this device.
Device ICCID	Integrated Circuit Card Identifier (ICCID) number from the Subscriber Identity Module (SIM) card present in the device.
Device Serial	Serial number of the device.
MAC Address	IEEE MAC address of this device.
Product Name	Product string identifying the device and often including the hardware version information.
Product Version	Software version number for the device.
User Name	Username of the user who provisioned the device.
Custom Field	A custom field to be used as needed.
User Email Address	The email address of the user who provisioned a device.

Issuing the Certificate Request

To create the certificate, when you have completed the other fields on the **Certificate Request Settings** form, mark the **Issue this certificate immediately** check box.

Click  **Create Certificate Request** to save your changes.

- If the "Issue this certificate immediately" check box is marked, the certificate will be issued immediately and will be displayed in the **Certificate Management** list view.
- If the "Issue this certificate immediately" check box is **not** marked, the certificate request will be displayed in the **Certificate Management** list view. The certificate can then be issued or rejected at a later time.

While the certificate request is displayed in the **Certificate Management** list view, the options for the request let you view details, export, sign, reject, or delete the request.

Figure 103 The Certificate Management List View, Request Information Form

Common Name	Certificate Authority	Serial Number	Type
Authentication Server	Local Certificate Authority		tls-client
View request	Export request	Sign request	Reject request Delete request

Request Information

Request Details

Details about the request and its owner.

Name:	Authentication Server
Subject:	Country US Locality Sunnyvale Organization ACME Sprockets Common Name Authentication Server Org.Unit Visitor Services State California Email Address info@example.com
Received At:	Friday, 23 October 2015, 1:34 AM

Cancel

Requesting a Certificate

To access the **Certificate Signing Request** form, on the **Onboard > Management and Control > View by Certificate** page, click the **Upload a certificate signing request** link.

Providing a Certificate Signing Request in Text Format

If you have a certificate signing request in text format, click the **Copy and paste certificate signing request as text** radio button on the **Certificate Signing Request** form.

Figure 104 The Certificate Signing Request Form for Text

The screenshot shows a web form titled "Certificate Signing Request". It is divided into two steps. Step 1, "Select the format of your certificate signing request.", has two radio buttons: "Copy and paste certificate signing request as text" (which is selected) and "Upload certificate signing request file". Step 2, "Provide the certificate signing request here.", contains a large text area labeled "* Certificate Signing Request:" with a scroll bar. Below the text area is a note: "Copy and paste the certificate signing request here. This is a block of encoded text and should include the 'BEGIN CERTIFICATE REQUEST' and 'END CERTIFICATE REQUEST' lines." Below the text area are two more fields: "Certificate Type:" with a dropdown menu set to "TLS Client Certificate" and a note "Select the type of certificate to create from this signing request"; and "Approval:" with a checkbox labeled "Issue this certificate immediately". At the bottom of the form is a blue button with a document icon and the text "Submit Certificate Signing Request".

Paste the text into the **Certificate Signing Request** text field. Be sure to include the complete block of text, including the beginning and ending lines.

A complete certificate signing request looks like the following:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIB7DCCAVUCAQAwwgasxCzAJBgNVBAYTA1VTMRMwEQYDVQQIEwpDYWxpZm9ybm1h
MRIwEAYDVQQHEw1TdW5ueXZhbGUxZjZAVBgNVBAoTDkFDTUUgU3Byb2NrZXRzMRkw
FwYDVQQLEXBWaxNpdG9yIFN1cnZpY2VzMR4wHAYDVQQDExVBdXRozW50aWNhdGlv
biBTZXJ2ZXIuXzAdBgkqhkiG9w0BCQEWEGluZm9AZXhhbXBsZS5jb20wgZ8wDQYJ
KoZlIhvcNAQEBBQADgY0AMIGJAoGBALR4wRSH26w1cf3OEPEIh34iXRQIUrnYnDfo
+ZezeB/i4NZUhRvLMvhPW7DcLpiZJ17ILj3aPPUXWDBYYiIUOkmuFX3dG7eKCLMH
Z4E9z1ozK5Znm8cWIj56kg691e7QrAZBYrd5QaBTmxEe0F9CGFsYbFx1viMUMxN6
EJILaCTBAGMBAAGgADANBgkqhkiG9w0BAQUFAAOBgQB8/So9KU5BS3oxjyxftIwF
dWvNP2CNruKyQaba5RQ1ixdHAsPE+3uYIHNvlqqIpSzb1fYkr21S4DdR3SSC3bXy
t4l/fyMuC1cEG/RpPSxdDALpet8MuogV1JonKo2BDitOEd4y5SXGmHmDBHrPW2Nd
gthkrtBb/a2WakNcrfDuiQ==
-----END CERTIFICATE REQUEST-----
```

Providing a Certificate Signing Request File

Alternatively, if you have the certificate signing request as a file, click the **Upload certificate signing request file** radio button.

Figure 105 *The Certificate Signing Request Form for a File*

Step 1
Select the format of your certificate signing request.

* Format: Copy and paste certificate signing request as text
 Upload certificate signing request file

Step 2
Upload the certificate signing request file here.

* Certificate Signing Request: Browse...
Choose a digital certificate signing request to upload. This should be a PEM encoded PKCS#10 certificate request file.

* Certificate Type: TLS Client Certificate
Select the type of certificate to create from this signing request

Approval: Issue this certificate immediately

Submit Certificate Signing Request

Use the **Certificate Signing Request** field to select the appropriate file for upload.



The file should be a base-64 encoded (PEM format) PKCS#10 certificate signing request.

Specifying Certificate Properties

On the **Certificate Signing Request** form, select the type of certificate from the **Certificate Type** drop-down list. Choose from one of the following options:

Table 42: *Certificate Type Options*

Certificate Type	Description
TLS Client Certificate	Use this option if the certificate is to be issued to a client, such as a user or a user's device. When this option is selected, the issued certificate's extended key usage property will contain a value of "Client Auth", indicating that the certificate may be used to identify a client.
Trusted Certificate	Use this option if the certificate is to be issued to a network server, such as a Web server or the EAP-TLS authentication server. When this option is selected, the issued certificate's extended key usage property will contain a value of "Server Auth", indicating that the certificate may be used to identify a server. Trusted certificates include the id-kp-eapOverLAN extended key usage.
Certificate Authority	Use this option if the certificate is for a subordinate Certificate Authority. When this option is selected, the issued certificate will contain an extension identifying it as an intermediate Certificate Authority, and the extended key usage property will contain the three values "Client Auth", "Server Auth", and "OCSP Signing".
Code Signing	Use this option for signing the Windows provisioning application.

Table 42: Certificate Type Options(Continued)

Certificate Type	Description
HTTPS	Use this option to create certificates suitable for use as HTTPS server certificates.
Issue this certificate immediately	To automatically issue the certificate, mark this check box.
Submit Certificate Signing Request	<p>Saves your changes.</p> <ul style="list-style-type: none"> If the Issue this certificate immediately check box is marked, the certificate will be issued immediately and will be displayed in the Certificate Management list view. If the Issue this certificate immediately check box is <u>not</u> marked, the certificate request will be displayed in the Certificate Management list view. The certificate can then be issued or rejected at a later time.

Onboard Usage



The **Onboard Usage** page displays all current license usage and certificate counts for Onboard devices. To see the usage list, go to **Onboard > Management and Control > Usage**. The **Onboard Usage** list view opens.

Figure 106 *The Onboard Usage List View*

Onboard Usage				
License Usage:	2 The above number represents the number of devices with valid certificates.			
Devices:	Device Type	Enrolled	Not Enrolled	Denied
	OS X	0	1	0
	Windows	1	0	0
	iOS	1	1	0
	Android	0	2	0
	Total	2	4	0
Summary statistics of Onboard devices by device type.				
Certificates:	Certificate Authority	Valid	Expired	Revoked
	Local Certificate Authority	2	0	0
	Total	2	0	0
Summary statistics of Onboard client certificates by Certificate Authority.				

Table 43: Onboard Usage List

Field	Description
License Usage	The license count expressed as the total number of onboarded devices with currently valid certificates. This is the count as of the time of the query; it is not an average. When this number is exceeded, no further certificates can be issued. A device can only be listed as enrolled if it has a valid certificate.
Devices	Summary of Onboard device statistics. Information categories include Enrolled , Not Enrolled , and Denied for each device type, as well as the Total count for each category for all device types.
Certificates	Summary of certificate statistics. Information categories include Valid , Expired , and Revoked for each Certificate Authority , as well as the Total count for each category for all Certificate Authorities.

Onboard Configuration



Onboard lets you create and manage the configuration settings that can be provisioned to onboarded devices. To manage configuration settings, go to **Onboard > Configuration > Start Here**. The index page opens. It includes with command links for accessing the different configuration settings as well as the configuration profiles that use them.

- For network settings, see "[Network Settings](#)" on page 163
- For iOS device settings, see "[iOS Settings](#)" on page 177
- For configuration profiles, see "[Configuration Profiles](#)" on page 216

Network Settings



You can define multiple network settings that can be sent to provisioned devices. Each network you configure is also a "configuration unit" that you can include in a configuration profile.

To create and work with network settings, go to **Onboard > Configuration > Network Settings**. The **Networks** list view opens.

Figure 107 *The Networks List View*

Name	Network Type	SSID
cpg-qa-onboard	Wireless	cpg-qa-onboard
Example Network Connect to the example network.	Wireless	Example-TLS
Show Details Edit Duplicate Show Usage		
test	Both	Example-TLS

Showing 1 - 3 of 3
Refresh 1 20 rows per page

All networks that have been provisioned are included in the list. You can click a network's row in the list for additional options:

Table 44: *The Network Settings List*







Field	Description
Show Details	Displays details for the network. The form expands to show its name, description, and configuration values for network access, wireless networks, enterprise protocols, enterprise authentication, enterprise trust, Windows networking, and proxy settings.
Edit	Edit any of a network's attributes. The Network Settings form opens.
Duplicate	Creates a copy of a network configuration to use as a basis for a new network. The Network Settings form opens with all attributes prepopulated and "Copy" appended to its name. You can rename the new configuration, and edit any of its attributes.
Show Usage	Displays a list of configuration profiles that use the network.
Create new network	To create a new network, click this link in the upper right corner. The Network Settings form opens.

For information on creating, editing, or duplicating a Network Settings configuration, see:

- ["Configuring Basic Network Access Settings "](#) on page 164
- ["Configuring Enterprise Protocol Settings"](#) on page 167
- ["Configuring Device Authentication Settings"](#) on page 170
- ["Configuring Certificate Trust Settings"](#) on page 171
- ["Configuring Windows-Specific Network Settings"](#) on page 174
- ["Configuring Proxy Settings"](#) on page 175

Configuring Basic Network Access Settings

1. On the **Onboard > Configuration > Network Settings** list view, to configure the network settings that will be provisioned to devices, click the network's **Edit** link. To create a new network, click the **Create new network** link in the upper-right corner. The **Network Settings** form opens with the **Access** tab displayed. The configuration process is the same for editing an existing network and for creating a new network. The **Network Access** form is divided into several tabs:

Tab	Description
 Access	Specifies basic network properties, such as the name of the wireless network and the type of security that is used. This form is described below.
 Protocols	Specifies the 802.1X authentication protocols that are used by the network. See " Configuring Enterprise Protocol Settings " on page 167.
 Authentication	Specifies the type of device authentication to be used for the network. See " Configuring Device Authentication Settings " on page 170.
 Trust	Specifies options related to mutual authentication. See " Configuring Certificate Trust Settings " on page 171.
 Windows	Specifies networking options used only by devices using the Windows operating system. See " Configuring Windows-Specific Network Settings " on page 174.
 Proxy	Specifies a proxy server to be used by devices connecting to the network. See " Configuring Proxy Settings " on page 175.



Navigating between different tabs will save the changes you have made in each tab. The modified settings are indicated with a “#” marker in the tab. The settings used for device provisioning are not modified in the database until you click **Create Network**.

To edit the network’s basic and wireless network access options, click the  **Access** tab:

Figure 108 The Access Tab of the Network Settings Form

Network Settings >> Network Access

Access Protocols Authentication Trust Windows Proxy

Network Access
Options for basic network access.

* Name: Example Network
Enter a name for the network.

Description: Connect to the example network.
Enter a description for the network.

* Network Type: Wireless only
Select which types of network will be provisioned. Enterprise security (802.1X) will be selected if wired networks are to be supported.

* Security Type: Enterprise (802.1X)
Select the authentication method used for the network. Enterprise security (802.1X) will be selected if wired networks are to be supported.

Wireless Network Settings
Options for wireless network access.

* Security Version: WPA2 with AES (recommended)
Select the WPA encryption version for the wireless network. This setting is used for Windows, Android and Legacy OS X (10.5/6) devices only. iOS and OS X 10.7+ (Lion or later) devices auto-detect the WPA version.

* SSID: Example-TLS
Enter the SSID of the wireless network to connect to.

Wireless: Hidden network
Select this option if the wireless network is not open or broadcasting.






Auto Join: Automatically join network
Select this option to automatically join the wireless network.

Next Save Changes Cancel

Table 45: Network Settings Form, Access Tab

Field	Description
Name	Name of the network.
Description	(Optional) You may enter additional identifying information.
Network Type	The type of network to be provisioned. Options include: <ul style="list-style-type: none"> Both — Wired and Wireless – Configures both wired (Ethernet) and wireless network adapters. Use this option when you have 802.1X configured for all types of network access.

Table 45: Network Settings Form, Access Tab(Continued)

Field	Description
	<ul style="list-style-type: none"> • Wireless only – Configures only wireless network adapters. • Wired only – Configures only wired (Ethernet) network adapters. <hr/> <p>Wired-only networks are not supported for Android, iOS, or OS X 10.7+ clients.</p> <hr/>
Security Type	<p>Authentication method used for the network. Options include:</p> <ul style="list-style-type: none"> • Enterprise (802.1X) – Use this option to setup a network that requires user authentication. This option is the only available choice when the Network Type is set to “Wired only”. • Personal (PSK) – Use this option to setup a network that requires only a Pre-Shared Key (password) to access the network. This option is only available when the Network Type is set to “Wireless only”. <p>Selecting the PSK security type will hide the  Protocols,  Authentication, and  Trust tabs.</p>
Security Version	The field lets you set the encryption version for the wireless network to WPA with TKIP or WPA2 with AES .
SSID	The SSID of the wireless network to connect to.
Password	If the Personal (PSK) security type is selected, you must provide the Pre-Shared Key in this field. The minimum password length is six characters.
Wireless	If the wireless network is not open or broadcasting, select the Hidden network check box in this row.
Auto Join	If the device should be automatically connected to the network when it is provisioned, select the Automatically join network check box in this row. If only one network is available to the user, the device will be connected automatically. If multiple networks are available, the user will be able to choose the network to connect to. If the Automatically join network option is not selected on this form, an option to manually connect to the network will be shown to the user.
Next	Opens the  Protocols tab.
Save Changes	Saves your changes. The new network configuration settings take effect.
Cancel	Discards your changes. The Onboard > Configuration > Network Settings list view opens.

For information about the list of network settings, see "[Network Settings](#)" on page 163. For more information about configuration profiles, see "[Configuration Profiles](#)" on page 216

Configuring Enterprise Protocol Settings

To configure enterprise protocols for a network, on the **Onboard > Configuration > Network Settings** form, click the **Protocols** tab.

Use this form to specify the authentication methods required by your network infrastructure. The default EAP type is TLS for all platforms that support this method.

The following best practices are recommended when choosing the 802.1X authentication methods to provision:

- Configure PEAP with MS-CHAPv2 for Onboard devices – Android, Windows, and legacy OS X (10.5/10.6).
- Configure EAP-TLS for iOS devices and OS X (10.7 or later).

- Other EAP methods, while possible, are limited in their applicability and should only be used if you have a specific requirement for that method.

Figure 109 *The Protocols Tab of the Network Settings Form*

Network Settings » Enterprise Protocols

Access
 Protocols
 Authentication
 Trust
 Windows
 Proxy

Enterprise Protocols

Options for 802.1X protocols supported on the network.

iOS & OS X EAP

Accepted EAP Types

TLS
 PEAP
 EAP-SIM
 TTLS
 EAP-FAST

Select the authentication protocols to use when configuring an iOS or OS X 10.7+ (Lion or later) device.

Legacy OS X EAP

Legacy OS X EAP: PEAP with MSCHAPv2
The authentication protocol to use when configuring OS X 10.5/6 (Leopard/Snow Leopard) devices.

Android EAP

Android EAP: TLS ▼
Select the authentication protocol to use when configuring an Android device.

Windows EAP

Windows EAP: PEAP with MSCHAPv2 ▼
The authentication protocol to use when configuring a Windows device.

Fast Reconnect: Enable Fast Reconnect

Quarantine: Enforce Network Access Protection
This setting is labeled 'Enable Quarantine checks' in older versions of Windows.

Cryptobinding: Enforce Cryptobinding

Ubuntu EAP

Ubuntu EAP: TLS ▼
The authentication protocol to use when configuring an Ubuntu device.

← Previous
Next →
Save Changes
Cancel

Table 46: *Network Settings Form, Protocols Tab*

Field	Description
iOS & OS X EAP	Authentication protocol to use when configuring iOS or OS X 7+ devices. This option supports: <ul style="list-style-type: none"> ● TLS ● TTLS ● PEAP ● EAP-FAST ● EAP-SIM
Legacy OS X EAP	Authentication protocol to use when configuring OS X 10.5/6 devices. This option supports: <ul style="list-style-type: none"> ● PEAP with MSCHAPv2
Android EAP	Authentication protocol to use when configuring an Android device. This option supports: <ul style="list-style-type: none"> ● EAP-SIM ● TLS ● PEAP with MSCHAPv2 ● PEAP with GTC ● TTLS with MSCHAPv2 ● TTLS with GTC ● TTLS with PAP
Windows EAP	Authentication protocol to use when configuring a Windows device. This option supports: <ul style="list-style-type: none"> ● TLS ● PEAP with MSCHAPv2
Fast Reconnect	To enable Fast Reconnect for the Windows device, select the Enable Fast Reconnect check box in this row. Fast Reconnect is a PEAP property that enables wireless clients to move between wireless access points on the same network without being re-authenticated each time they associate with a new access point. If TLS is selected, Fast Reconnect is not available.
Quarantine	To obtain a system statement-of-health (SSoH) for the Windows device from the OnGuard or Microsoft NAP Agent and send it to the authentication server during the 802.1X authentication process, select the Enforce Network Access Protection check box in this row. Use this option to enforce network access control (NAC) protections on the network. If TLS is selected, Enforce Network Access Protection is not available.
Cryptobinding	To enforce cryptobinding for the Windows device, select the Enforce Cryptobinding check box in this row. Cryptobinding is a process that protects the authentication protocol negotiation against man-in-the-middle attacks. The cryptobinding request and response performs a two-way handshake between the peer and the authentication server using key materials. If TLS is selected, Enforce Cryptobinding is not available.
Ubuntu	Authentication protocol to use when configuring an Ubuntu device. This option supports: <ul style="list-style-type: none"> ● TLS ● PEAP with MSCHAPv2
Previous	Opens the Access tab.
Next	Opens the Authentication tab.
Save Changes	Saves your changes. The new network configuration settings take effect.
Cancel	Discards your changes. The Onboard > Configuration > Network Settings list view opens.

For information about the list of network settings, see "Network Settings " on page 163. For more information about configuration profiles, see "Configuration Profiles" on page 216

Configuring Device Authentication Settings

To configure authentication settings for a network, on the **Onboard > Configuration > Network Settings** form, click the **Authentication** tab.

The **Windows Authentication** area is included on this tab if **TLS** was chosen for **Windows EAP** on the **Protocols** tab.

Figure 110 The Authentication Tab of the Network Settings Form

The screenshot shows the 'Authentication' tab of the 'Network Settings' form. The title bar reads 'Network Settings » Enterprise Authentication'. Below the title bar are tabs for 'Access', 'Protocols', 'Authentication' (selected), 'Trust', 'Windows', and 'Proxy'. The main content area is titled 'Enterprise Authentication' with a subtitle 'Options for 802.1X authentication used on the network.' There are two main sections: 'iOS & OS X Authentication' and 'Windows Authentication'. In the 'iOS & OS X Authentication' section, the '* iOS & OS X Credentials:' dropdown is set to 'Certificate'. Below it is a note: 'Select the type of credentials to provision for iOS and OS X 10.7+ (Lion or later) devices.' In the 'Windows Authentication' section, the '* Certificate Store:' dropdown is set to 'User'. Below it is a note: 'Select the certificate store where the client certificate will be provisioned when configuring a Windows device.' At the bottom of the form are four buttons: 'Previous', 'Next', 'Save Changes', and 'Cancel'.

Table 47: Network Settings Form, Authentication Tab

Field	Description
Android Authentication	
Certificate Store	Specifies the certificate store where the client certificate will be provisioned when configuring an Android device. Options include: <ul style="list-style-type: none"> • Private – This is the default. • System – Certificates will be available for use by other applications but might require additional security prompts during provisioning.
iOS and OS X Authentication	
iOS & OS X Credentials	Specifies the type of credentials to provision for iOS and OS X 10.7+ devices. Options include: <ul style="list-style-type: none"> • Certificate – A device certificate will be provisioned and used for EAP-TLS client authentication. When this option is selected, EAP-TLS must be selected on the Protocols tab. • Username & Password – A device certificate will be provisioned, but the client authentication will use unique device credentials (as for Onboard devices). When this option is selected, EAP-TTLS or PEAP must be selected on the Protocols tab.
Windows Authentication	
Certificate Store	Specifies the certificate store where the client certificate will be provisioned when configuring a Windows device. Options include: <ul style="list-style-type: none"> • User – Use user-only credentials. This is the default. • Machine – Use computer-only credentials. • Machine and User – Use computer-only credentials or user-only credentials. When a user is

Table 47: Network Settings Form, Authentication Tab(Continued)

Field	Description
	logged on, the user's credentials are used for authentication. When no user is logged on, computer-only credentials are used for authentication.
Previous	Opens the Protocols tab.
Next	Opens the Trust tab.
Save Changes	Saves your changes. The new network configuration settings take effect.
Cancel	Discards your changes. The Onboard > Configuration > Network Settings list view opens.

For information about the list of network settings, see "Network Settings " on page 163. For more information about configuration profiles, see "Configuration Profiles" on page 216

Configuring Certificate Trust Settings

To configure trust settings for a network, on the **Onboard > Configuration > Network Settings** form, click the **Trust** tab.

Figure 111 The Trust Tab of the Network Settings Form, Automatic Configuration Selected

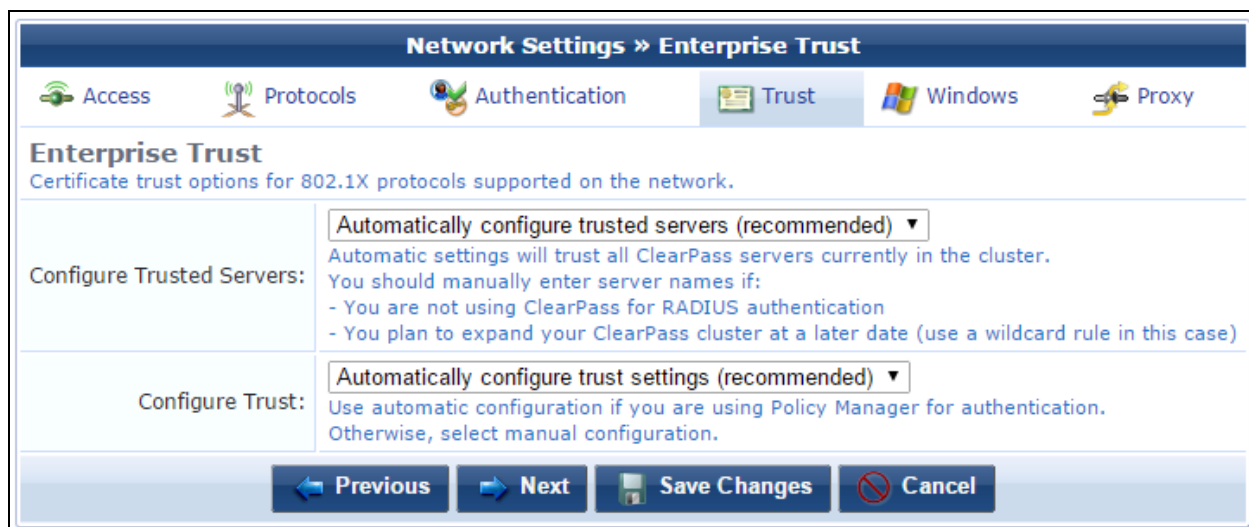




Figure 112 *The Trust Tab of the Network Settings Form, Manual Configuration Selected*

Table 48: *Network Settings, Trust Tab*

Field	Description
Configure Trusted Servers	Specifies automatic or manual configuration of trusted certificate servers. Options include: <ul style="list-style-type: none"> Automatically configure trusted servers (recommended) — Default. The common names of all ClearPass appliances in the cluster will be trusted. Manually configure certificate trusted servers — If you are not using ClearPass for RADIUS authentication, or if you plan to expand your ClearPass cluster, you should select manual configuration. You may use a wildcard in this field if will be expanding your cluster later.
Trusted Server Names	For manual trusted server configuration, enter the certificate names that can be expected from the authentication server. If a server presents a certificate that is not in this list, it will not be trusted. Enter each name on a separate line. Wildcards may be used.
Configure Trust	Specifies automatic or manual configuration of trust settings. Options include: <ul style="list-style-type: none"> Automatically configure trust settings (recommended) — Select this option if you are using Policy Manager for authentication. Onboard automatically determines the appropriate certificate trust configuration for your deployment. The complete trust chain is included in the profile download. Manually configure trust settings — To change the recommended default setting and configure trust settings manually, select this option. The form expands to include configuration options.
Trusted Certificate	Specifies the certificates the device should use during authentication. This should include the root CA that has issued the authentication server's certificate. The recommended certificate is selected by

Table 48: Network Settings, Trust Tab(Continued)

Field	Description
tes	default. You may click the field to open the drop-down list and select a different certificate the client should trust. You can select multiple certificates. You should include the root certificate that issued the authentication server's certificate, and you should provide the certificate for each authentication server a provisioned device will use.
Upload Certificate	Lets you import additional trusted certificates. Click Choose File to navigate to the file on your computer, and then click Upload . The certificate is imported, and the certificate name is displayed above the form. You can click the Show certificate link next to the name to view certificate details. The certificate is also displayed in the Certificate Management list with the type "trusted."
Dynamic Trust 	If selected, allows trust decisions to be made by the user (a dialog box will be presented to them). <hr/> You should avoid marking the Allow trust exceptions check box – the network administrator should make all trust decisions. Users will not generally review certificates for potential issues before accepting them. Letting the user make trust decisions is an insecure configuration, as the user can override a security warning if a man-in-the-middle attack occurs. <hr/>
Android Area	
Trusted Certificate	Specifies the certificate the Android device should trust. Android supports only a single trusted certificate; this must be the root CA that issued the authentication server's certificate. Be aware that if None is selected, 802.1x authentication might not work.
Windows Area	
Validate Certificate 	Leave this check box selected to have the provisioned device check that the server certificate is valid before using the server for authentication. <hr/> Disabling the Validate Certificate option is an insecure configuration. An attacker could provide another server certificate which the client would not verify. <hr/>
Previous	Opens the Authentication tab.
Next	Opens the Windows tab.
Save Changes	Saves your changes. The new network configuration settings take effect.
Cancel	Discards your changes. The Onboard > Configuration > Network Settings list view opens.

For information about the list of network settings, see "[Network Settings](#)" on page 163. For more information about configuration profiles, see "[Configuration Profiles](#)" on page 216

Configuring Windows-Specific Network Settings

To configure settings for Windows devices on a network, on the **Onboard > Configuration > Network Settings** form, click the **Windows** tab.

Figure 113 *The Windows Tab of the Network Settings Form*

The screenshot shows the 'Windows Network Settings' tab of the Network Settings form. The form is titled 'Network Settings » Windows Network Settings' and has a navigation bar with tabs for Access, Protocols, Authentication, Trust, Windows (selected), and Proxy. Below the navigation bar, the section is titled 'Windows Networking Settings' with a note: 'These settings are only applicable to Windows devices.' The settings are organized into several sections:

- NAP Services:** Enable NAP services. See also 'Enforce Network Access Protection' on the Protocols tab.
- Admin Username:** [Text input field]. Enter if configuration of networking requires administrator credentials. NOTE: This cannot be used on Windows 8 or above due to operating system limitations.
- Admin Password:** [Text input field]. Enter if configuration of networking requires administrator credentials.
- IP Address:** Assign IP address using DHCP
- DNS:** Assign DNS using DHCP
- DNS Registration:** Register IP address with DNS

Below these settings is the 'Windows XP Networking' section:

- Configure Using:** Use Windows to configure wireless
- Notification Icon:** Show icon in notification
- Notify Connectivity:** Notify when connectivity is limited

At the bottom of the form are four buttons: Previous, Next, Save Changes, and Cancel.

Table 49: Network Settings Form, Windows Tab

Field	Description
NAP Services	<p>If selected, enables NAP for Microsoft Windows clients. You will also need to mark the Enable Quarantine Checks check box on the Protocols tab.</p> <p>Network Access Protection (NAP) is a feature in Windows Server 2008 that controls access to network resources based on a client computer's identity and compliance with corporate governance policy. NAP allows network administrators to define granular levels of network access based on who a client is, the groups to which the client belongs, and the degree to which that client is compliant with corporate governance policy. If a client is not compliant, NAP provides a mechanism to automatically bring the client back into compliance and then dynamically increase its level of network access.</p> <p>Deploying NAP requires a NAP-compatible authentication server, so that appropriate policies may be implemented based on the statement of health provided by the NAP client.</p>
Admin Username	<p>If configuration of networking requires administrator credentials, enter the admin username in this field.</p> <p>Embedding administrator credentials allows privileged operations such as application installation to be done during onboarding by end users who otherwise do not have admin privileges. (Not supported by Windows 8 or above)</p>
Admin Password	<p>If configuration of networking requires administrator credentials, enter the admin password in this field.</p> <p>Embedding administrator credentials allows privileged operations such as application installation to be done during onboarding by end users who otherwise do not have admin privileges. (Not supported by Windows 8 or above)</p>
IP Address	If selected, assigns an IP address using DHCP,
DNS	If selected, assigns DNS using DHCP,
DNS Registration	If selected, registers IP address with DNS,
Configure Using	If selected, uses Windows to configure wireless,
Notification Icon	If selected, shows icon in notification,
Notify Connectivity	If selected, notifies when connectivity is limited,
Previous	Opens the Trust tab.
Next	Opens the Proxy tab.
Save Changes	Saves your changes. The new network configuration settings take effect.
Cancel	Discards your changes. The Onboard > Configuration > Network Settings list view opens.

For information about the list of network settings, see "[Network Settings](#)" on page 163. For more information about configuration profiles, see "[Configuration Profiles](#)" on page 216

Configuring Proxy Settings

To configure proxy settings for a network, on the **Onboard > Configuration > Network Settings** form, click the **Proxy** tab.

Figure 114 The Proxy Tab of the Network Settings Form

Table 50: Network Settings Form, Proxy Tab

Field	Description
Proxy Type	Specifies the network's proxy server configuration type. Options include: <ul style="list-style-type: none"> None– No proxy server will be configured. Manual– A proxy server will be configured, if the device supports it. Specify the proxy server settings in the Server and Server Port fields. Automatic– The device will configure its own proxy server, if the device supports it. Specify the location of a proxy auto-config file in the PAC URL text field.
Server	Enter the proxy server's network address.
Server Port	Enter the proxy server's port number.
PAC URL	Enter the URL of the PAC file that defines the proxy configuration.
Previous	Opens the Windows tab.
Save Changes	Saves your changes. The new network configuration settings take effect.
Cancel	Discards your changes. The Onboard > Configuration > Network Settings list view opens.

For information about the list of network settings, see "Network Settings " on page 163. For more information about configuration profiles, see "Configuration Profiles" on page 216

iOS Settings



You can manage iOS device settings for provisioned devices. A variety of settings are available, including such things as contacts, email, passcode policy, VPN, and Web clips settings. After you define each of the settings you wish to use, you can include them in configuration profiles. The configuration profiles are available in the **Provisioning Settings** form, and can be associated with a device provisioning configuration set.

To create and work with iOS settings, go to **Onboard > Configuration > iOS Settings**. The **iOS Settings** list view opens.

Figure 115 *The iOS Settings List View*

Add New	
Name	Type
Example ActiveSync Settings My ActiveSync 1	ActiveSync Settings
Example Calendar Settings	Calendar Settings
Example SSO Settings	SSO Settings

Show Details Edit Duplicate Delete Show Usage

Refresh 1 Showing 1 - 3 of 3 10 rows per page

All iOS settings that have been configured are included in the list. Each setting's name and type are shown in the list. You can click an iOS setting's row in the list for additional options:

Table 51: *The iOS Settings List*

Field	Description
Show Details	Displays details for the iOS setting. The form expands to show its name, description, and configuration values specific to the type of setting.
Edit	Edit the iOS setting's configuration. The Settings form for the type of iOS setting opens.
Duplicate	Creates a copy of an iOS setting to use as a basis for a new setting. The Settings form specific to the type of setting opens with all attributes prepopulated and "Copy" appended to its name. You can rename the new setting, and edit any of its attributes.
Delete	Deletes the iOS setting. You will be asked to confirm the deletion.
Show Usage	Displays a list of configuration profiles that use the iOS setting.
Add New	To create a new iOS setting, click this link above the table. The Settings form specific to the type of iOS setting opens.

For information on creating, editing, or duplicating the different types of iOS settings, see:

- "Configuring ActiveSync Settings" on page 178
- "Configuring AirPlay Settings" on page 181
- "Configuring AirPrint Settings" on page 183

- "Configuring APN Settings" on page 184
- "Configuring Calendar (CalDAV) Settings" on page 185
- "Configuring Contacts (CardDAV) Settings" on page 187
- "Configuring Device Restrictions Settings" on page 189
- "Configuring Email Settings" on page 197
- "Configuring an iOS Device Passcode Policy " on page 200
- "Configuring Calendar Subscription Settings" on page 203
- "Configuring an iOS Device VPN Connection" on page 204
- "Configuring Web Clips" on page 213

Configuring ActiveSync Settings



Exchange ActiveSync configurations you define can be used in configuration profiles to automatically configure an email account on an iOS device. Use an ActiveSync configuration when you have an Exchange mail server and want to automatically provide the email settings to users provisioning their mobile devices. You can define multiple ActiveSync settings.

Exchange ActiveSync settings are only supported by iOS devices; they will be ignored by all other device types.

To create and work with Exchange ActiveSync configurations, go to **Onboard > Configuration > iOS Settings**. Either click an existing ActiveSync setting's name in the list; or click **Add New**, select **ActiveSync Settings** in the **Settings Type** drop-down list, and click **Create**. The **Exchange ActiveSync Settings** form opens.

Figure 116 The Exchange ActiveSync Settings Form, General Area

Exchange ActiveSync Settings	
* Name:	<input type="text"/> Enter a name for the ActiveSync settings.
Description:	<input type="text"/> Enter a description for the ActiveSync settings.
General Settings Common settings for Exchange ActiveSync.	
* ActiveSync Host:	<input type="text"/> Hostname or IP address of the server the device will connect to. A hostname will only be accepted if the corresponding IP address can be resolved.
Use SSL:	<input checked="" type="checkbox"/> Send all communication through secure socket layer Select this option to ensure that communications are encrypted.
Magic String:	<input type="text"/> This string is sent as the value of the "X-Apple-Config-Magic" header in each EAS HTTP request. This is available only in iOS 7.0 and later.
Allow Move:	<input checked="" type="checkbox"/> Allow user to move messages from this account When unselected, messages may not be moved out of this email account into another account. This also prevents forwarding or replying from a different account than the message was originated from.
Allow Recent Address Sync:	<input checked="" type="checkbox"/> Include this account in recent address syncing
Use Only in Mail:	<input checked="" type="checkbox"/> Send outgoing mail from this account only from the Mail app When selected, this account is not available for sending mail in third-party applications.

Table 52: Exchange ActiveSync Settings Form, Basic Properties and General Area

Field	Description
Name	(Required) Enter a short name that identifies the ActiveSync configuration clearly. ActiveSync configuration names can include spaces. If you are duplicating a configuration, the original name has a number appended to it. You may highlight this name and replace it with a new name.
Description	Brief description of the ActiveSync setting.
ActiveSync Host	(Required) Enter the hostname or IP address of the server the device will connect to.
Use SSL	If selected, specifies that all communications are encrypted.
Magic String	Value to send as the "X-Apple-Config-Magic" header in each EAS HTTP request.
Allow Move	If selected, allows the user to move messages out of this email account into another account. Leave this field blank to prevent moving messages between accounts, and to prevent forwarding or replying from other than the message's originating account.
Allow Recent Address Sync	If selected, includes this email account in recent address syncing.
Use Only in Mail	If selected, sends outgoing mail from this account only from the Mail app, and prevents sending mail in third-party applications.

Figure 117 *The Account Settings Area*

Account Settings

These options configure the user account.

* Account Details:	<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">Provisioning - values acquired during device provisioning ▾</div> <small>Select how user account information is to be supplied.</small>
Domain:	<input style="width: 100%;" type="text"/> <small>Domain for the account.</small>
Email Address:	<input checked="" type="radio"/> Let system define - "Domain\User"@ActiveSync-Host" <input type="radio"/> Same as username <input type="radio"/> Generate using username

Sync Settings

These options configure mail synchronization.

* Days of Mail:	<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">3 days ▾</div> <small>The number of past days of mail to synchronize.</small>
-----------------	--

Save Changes

Table 53: *Exchange ActiveSync Settings Form, Account Settings and Sync Settings Areas*

Field	Description
Account Details	(Required) Specifies how user account information is supplied. Options include: <ul style="list-style-type: none"> ● User provided — entered by user on device. This option requires the user to enter their credentials on the device to access their email. ● Identity certificate — created during provisioning. This option uses the device's TLS client certificate to authenticate the user. Using this option requires configuration of the ActiveSync server to authenticate a user based on the client certificate. ● Provisioning — values acquired during device provisioning. ● Shared preset values — testing only. This option provides a fixed set of credentials to the device. These settings cannot be modified for each user when provisioning a device, so it is recommended that these settings only be used when testing Exchange integration.
Domain	You may enter the domain for the account.
Email Address	Specifies how the email address for the user account will be defined. Options include: <ul style="list-style-type: none"> ● Let system define ● Same as username ● Generate using username.
When to Add Email Address Domain	If "Generate using username" was selected in the Email Address field, this field is added. Options include: <ul style="list-style-type: none"> ● Only if username is not a valid email address ● Always append
User	If "Shared preset values - testing only" was chosen in the Account Details field, the form includes these fields for login credentials. Enter the login information for testing in the User , Password , and Confirm Password fields. The minimum password length is six characters. If both the Domain and User fields are blank, the device will prompt the user.
Password	

Table 53: Exchange ActiveSync Settings Form, Account Settings and Sync Settings Areas (Continued)

Field	Description
Confirm	
Days of Mail	Specifies the number of past days of mail to synchronize. Options include: <ul style="list-style-type: none">• No Limit• 1 day• 3 days• 1 week• 2 weeks• 1 month
Save Changes	Saves your changes and creates the ActiveSync setting. The Exchange ActiveSync setting is available as a configuration unit on the Configuration Profile form.

For more information about configuration profiles, see ["Configuration Profiles"](#) on page 216

Configuring AirPlay Settings



AirPlay settings you define can be used in configuration profiles for an iOS device. An AirPlay setting includes its name and description, the destinations that are available to the device, and passwords for each destination. You can define multiple AirPlay settings.

AirPlay settings are only supported by iOS 7 devices; they will be ignored by all other device types.

To configure an AirPlay setting, go to **Onboard > Configuration > iOS Settings**. Either click an existing AirPlay setting's name in the list; or click **Add New**, select **AirPlay Settings** in the **Settings Type** drop-down list, and click **Create**. The **AirPlay Settings** form opens.

Figure 118 *The AirPlay Settings Form*

The screenshot shows the 'AirPlay Settings' form. At the top is a dark blue header with the text 'AirPlay Settings'. Below this are several input fields. The first is labeled '* Name:' and contains the text 'Example AirPlay Settings'. Below it is a hint: 'Enter a name for the AirPlay settings.' The second field is labeled 'Description:' and contains the text 'My example AirPlay settings'. Below it is a hint: 'Enter a description for the AirPlay setting.' The third section is titled 'General Settings' with the subtitle 'Common settings for AirPlay.' It contains a field labeled 'AirPlay Destinations:' with the value '11:22:33:44:55:66'. Below this field is an information icon and the text: 'This is supported by Supervised devices only. Enter the device id of the AirPlay destinations available to the device, one per line. If left empty, all the AirPlay destinations are available to the device. Device Id should be of format xx:xx:xx:xx:xx:xx'. The fourth section is labeled 'AirPlay Destination Passwords:' and contains a table with two columns: 'Device Name' and 'Password'. The 'Device Name' column has the value 'New Device' and the 'Password' column has a masked password '.....'. Below the table is a hint: 'Enter passwords for the known AirPlay destinations.' At the bottom of the form is a blue button with a floppy disk icon and the text 'Save Changes'.

Table 54: *AirPlay Settings Form*

Field	Description
Name	(Required) Enter a short name that identifies the AirPlay configuration clearly. AirPlay configuration names can include spaces. If you are duplicating a configuration, the original name has a number appended to it. You may highlight this name and replace it with a new name.
Description	Brief description of the AirPlay setting.
AirPlay Destinations	Specifies the device ID of each AirPlay destination that will be available to the device. Each device ID must be entered on a new line. To make all destinations available, leave this field empty.
AirPlay Destination Passwords	You may enter a device password for each destination. The minimum password length is six characters.
Save Changes	Saves your changes and creates the AirPlay setting. The AirPlay setting is available as a configuration unit on the Configuration Profile form.

For more information about configuration profiles, see "[Configuration Profiles](#)" on page 216

Configuring AirPrint Settings



AirPrint settings you define can be used in configuration profiles for an iOS device. An AirPrint setting includes its name and description, and AirPrint printer locations that are available to the user. You can define multiple AirPrint settings.

AirPrint settings are only supported on iOS 7 devices; they are ignored by all other devices.

To configure an AirPrint setting, go to **Onboard > Configuration > iOS Settings**. Either click an existing AirPrint setting's name in the list; or click **Add New**, select **AirPrint Settings** in the **Settings Type** drop-down list, and click **Create**. The **AirPrint Settings** form opens.

Figure 119 The AirPrint Settings Form

Table 55: AirPrint Settings Form

Field	Description
Name	(Required) Enter a short name that identifies the AirPrint configuration clearly. AirPrint configuration names can include spaces. If you are duplicating a configuration, the original name has a number appended to it. You may highlight this name and replace it with a new name.
Description	Brief description of the AirPrint setting.
AirPrint Printers	(Required) Specifies the Destination IP address and Resource Path of each AirPrint location that will be available to the user.
Save Changes	Saves your changes and creates the AirPrint setting. The AirPrint setting is available as a configuration unit on the Configuration Profile form.

For more information about configuration profiles, see "Configuration Profiles" on page 216

Configuring APN Settings



APN settings you define can be used in configuration profiles for an iOS device. An APN setting includes its name and description, carrier and proxy server information, and user account provisioning details. You can define multiple APN settings.

APN settings are only supported on iOS devices; they are ignored by all other devices.

To configure an APN setting, go to **Onboard > Configuration > iOS Settings**. Either click an existing APN setting's name in the list; or click **Add New**, select **APN Settings** in the **Settings Type** drop-down list, and click **Create**. The **APN Settings** form opens.

Figure 120 *The APN Settings Form*

APN Settings	
* Name:	<input type="text" value="Example APN Settings"/> <small>Enter a name for the APN settings.</small>
Description:	<input type="text" value="My example APN settings"/> <small>Enter a description for the APN settings.</small>
General Settings <small>Common settings for APN.</small>	
* Access Point Name:	<input type="text" value="Example Carrier"/> <small>The name of the carrier (GPRS) access point.</small>
Proxy Server:	<input type="text" value="192.0.2.213"/> <small>Enter the fully qualified address of the proxy server.</small>
Port:	<input type="text" value="8080"/> <small>Port number of the proxy server.</small>
Account Settings <small>Options for the APN user account.</small>	
* Account Details:	<input type="text" value="Provisioning - values acquired during device provisioning"/> <small>Select how user account information is to be supplied.</small>
<input type="button" value="Save Changes"/>	

Table 56: APN Settings Form

Field	Description
Name	(Required) Enter a short name that identifies the APN configuration clearly. APN configuration names can include spaces. If you are duplicating a configuration, the original name has a number appended to it. You may highlight this name and replace it with a new name.
Description	Brief description of the APN setting.
Access Point Name	(Required) Enter the name of the carrier (GPRS) access point.
Proxy Server	Fully-qualified address of the proxy server.
Port	Port number of the proxy server.
Account Details	(Required) Specifies how the user account information should be supplied. Options include: <ul style="list-style-type: none">• User provided - entered by user on device• Provisioning - values acquired during device provisioning• Shared preset values - testing only
Access Point Username	Username to connect to the access point.
Access Point Password	Password to connect to the access point.
Confirm Password	
Save Changes	Saves your changes and creates the APN setting. The APN setting is available as a configuration unit on the Configuration Profile form.

For more information about configuration profiles, see "[Configuration Profiles](#)" on page 216

Configuring Calendar (CalDAV) Settings



CalDAV settings you define can be used in configuration profiles for an iOS device. CalDAV accounts give a provisioned device access to scheduling information on a remote server. A CalDAV setting includes its name and description, the account description and hostname, port, principal URL, and whether SSL is enabled, as well as additional account details. You can define multiple CalDAV settings.

APN settings are only supported on iOS devices; they are ignored by all other devices.

To configure a CalDAV account, go to **Onboard > Configuration > iOS Settings**. Either click an existing Calendar setting's name in the list; or click **Add New**, select **Calendar Settings** in the **Settings Type** drop-down list, and click **Create**. The **CalDAV Account Settings** form opens.

Figure 121 *The CalDAV Account Settings Form*

CalDAV Account Settings

* Name:
Enter a name for the calendar settings.

Description:
Enter a description for the calendar settings.

General Settings
Common settings for CalDAV.

Account Description:
The display name of the account, e.g. "Company CalDAV Account".

* Account Hostname:
Hostname or IP address of the CalDav server.
A hostname will only be accepted if the corresponding IP address can be resolved.

* Port:
Port number of the server.

Use SSL: Enable secure socket layer communication with CalDAV server

Account Principal URL:
The principal URL for the CalDAV account.

Account Settings
Options for the CalDAV user account.

* Account Details:
Select how user account information is to be supplied.

Table 57: *CalDAV Account Settings Form*

Field	Description
Name	(Required) Enter a short name that identifies the CalDAV configuration clearly. CalDAV configuration names can include spaces. If you are duplicating a configuration, the original name has a number appended to it. You may highlight this name and replace it with a new name.
Description	Brief description of the calendar settings.
Account Description	Display name for the account.
Account Hostname	(Required) Enter the hostname or IP address of the CalDAV server.
Port	(Required) Enter the port number of the CalDAV server.

Table 57: CalDAV Account Settings Form(Continued)

Field	Description
Use SSL	If selected, enables secure socket layer communication with the CalDAV server.
Account Principal URL	You may enter the principal URL for the CalDAV account.
Account Details	(Required) Specifies how user account information should be supplied. Options include: <ul style="list-style-type: none">• User provided - entered by user on device• Provisioning - values acquired during device provisioning• Shared preset values - testing only
User	If "Shared preset values - testing only" was chosen in the Account Details field, the form includes these fields for login credentials. Enter the login information for testing in the User , Password , and Confirm Password fields. The minimum password length is six characters.
Password	
Confirm	
Save Changes	Saves your changes and creates the CalDAV setting. The CalDAV setting is available as a configuration unit on the Configuration Profile form.

For more information about configuration profiles, see ["Configuration Profiles"](#) on page 216

Configuring Contacts (CardDAV) Settings



CardDAV settings you define can be used in configuration profiles for an iOS device. CardDAV accounts allow users of a provisioned device to access and share contact data on a server. A CardDAV setting includes its name and description, the account description and hostname, port, principal URL, and whether SSL is enabled, as well as additional account details. You can define multiple CardDAV settings.

CardDAV account settings are only supported on iOS devices; they are ignored by all other devices.

To configure a CardDAV account, go to **Onboard > Configuration > iOS Settings**. Either click an existing CardDAV setting's name in the list; or click **Add New**, select **Contacts Settings** in the **Settings Type** drop-down list, and click **Create**. The **CardDAV Account Settings** form opens.

Figure 122 *The CardDAV Account Settings Form*

CardDAV Account Settings

* Name:
Enter a name for the contacts settings.

Description:
Enter a description for the contacts settings.

General Settings
Common settings for CardDAV.

Account Description:
The display name of the account, e.g. "Company CardDAV Account".

* Account Hostname:
Hostname or IP address of the CardDAV server.
A hostname will only be accepted if the corresponding IP address can be resolved.

* Port:
Port number of the server.

Use SSL: Enable secure socket layer communication with CardDAV server

Account Principal URL:
The principal URL for the CardDAV account.

Account Settings
Options for the CardDAV user account.

* Account Details:
Select how user account information is to be supplied.

Table 58: *CardDAV Account Settings Form*

Field	Description
Name	(Required) Enter a short name that identifies the contacts configuration clearly. Contacts configuration names can include spaces. If you are duplicating a configuration, the original name has a number appended to it. You may highlight this name and replace it with a new name.
Description	Brief description of the contacts settings.
Account Description	Display name for the account.
Account Hostname	(Required) Enter the hostname or IP address of the CalDAV server.
Port	(Required) Enter the port number of the CardDAV server.

Table 58: CardDAV Account Settings Form(Continued)

Field	Description
Use SSL	If selected, enables secure socket layer communication with the CardDAV server.
Account Principal URL	You may enter the principal URL for the CardDAV account.
Account Details	(Required) Specifies how user account information should be supplied. Options include: <ul style="list-style-type: none"> ● User provided - entered by user on device ● Provisioning - values acquired during device provisioning ● Shared preset values - testing only
Username	If "Shared preset values - testing only" was chosen in the Account Details field, the form includes these fields for login credentials. Enter the login information for testing in the User , Password , and Confirm Password fields. The minimum password length is six characters.
Password	
Confirm Password	
Save Changes	Saves your changes and creates the CalDAV setting. The CalDAV setting is available as a configuration unit on the Configuration Profile form.

For more information about configuration profiles, see ["Configuration Profiles" on page 216](#)

Configuring Device Restrictions Settings



Device Restrictions settings you define specify the activities that will be allowed and settings that will be enabled on a provisioned device. A device restrictions setting includes its name and description, and the applications, content settings, security and privacy settings, device functionality settings, iCloud settings, and game center settings that will be enabled or disabled on the provisioned device.

Device Restrictions settings are only supported by iOS devices; they will be ignored by all other device types.

To create and work with Device Restrictions configurations, go to **Onboard > Configuration > iOS Settings**. Either click an existing Device Restrictions setting's name in the list; or click **Add New**, select **Device Restrictions Settings** in the **Settings Type** drop-down list, and click **Create**. The **Device Restrictions Settings** form opens.

Figure 123 *The Device Restrictions Settings Form, Basic Properties Area*

Device Restrictions Settings

* Name:	<input style="width: 90%;" type="text" value="Example Device Restrictions"/> <small>Enter a name for the device restrictions settings.</small>
Description:	<div style="border: 1px solid #ccc; padding: 5px; min-height: 40px;"> My example device restrictions settings </div> <small>Enter a description for the device restrictions settings.</small>

Table 59: Device Restrictions Settings Form, Basic Properties Area

Field	Description
Name	(Required) Enter a short name that identifies the Device Restrictions configuration clearly. Device Restrictions configuration names can include spaces. If you are duplicating a configuration, the original name has a number appended to it. You may highlight this name and replace it with a new name.
Description	Brief description of the Device Restrictions settings.

Figure 124 The Device Restrictions Settings Form, Applications Area

Applications	
Allow Installing Apps:	<input checked="" type="checkbox"/> Allow apps to be installed on devices When unselected, the App Store is disabled and users will be unable to install or update their apps.
Allow Camera:	<input checked="" type="checkbox"/> Allow use of camera When unselected, the camera is completely disabled and users will be unable to take photographs.
Allow Video Conferencing:	<input checked="" type="checkbox"/> Allow FaceTime When unselected, the FaceTime application cannot be used.
Allow YouTube:	<input checked="" type="checkbox"/> Allow use of YouTube app When unselected, the YouTube app is disabled. Note: This is not applicable for iOS 6 and later.
Allow iTunes:	<input checked="" type="checkbox"/> Allow use of the iTunes store When unselected, the iTunes music store is disabled and users cannot preview, purchase, or download content.
Allow iBookstore:	<input checked="" type="checkbox"/> Allow use of iBookstore When unselected, the use of iBookstore from the iBooks app is disallowed. This setting is applicable only to supervised devices.
Allow Open In Unmanaged Apps:	<input checked="" type="checkbox"/> Allow open from managed to unmanaged When unselected, the documents in managed apps and accounts only open in other managed apps and accounts. This setting is available only in iOS 7.0 and later.
Allow Open In Managed Apps:	<input checked="" type="checkbox"/> Allow open from unmanaged to managed When unselected, the documents in unmanaged apps and accounts only open in other unmanaged apps and accounts. This setting is available only in iOS 7.0 and later.
Autonomous Single mode Apps:	<div style="border: 1px solid #ccc; height: 40px; width: 100%;"></div> Enter the apps identifiers (bundle ids), one per line, that are allowed to autonomously enter Single App Mode. This setting is applicable only to supervised devices. This setting is available only in iOS 7.0 and later.

In the **Applications** area, you can allow or enable application behavior.

Table 60: *Device Restrictions Settings Form, Applications Area*

Field	Description
Allow Installing apps	If selected, enables the App Store. Users can install or update their apps.
Allow Camera	If selected, enables the camera. Users can take photographs.
Allow Video conferencing	If selected, allows the Facetime application.
Allow YouTube	If selected, enables the YouTube app. (Not available for iOS 6 or later.)
Allow iTunes	If selected, enables the iTunes music store. Users can preview, purchase, and download content.
Allow iBookstore	If selected, allows the use of iBookstore from the iBooks app. (Only applies to supervised devices.)
Allow Open in Unmanaged Apps	If selected, documents in managed apps and accounts can be opened in unmanaged apps and accounts. If this option is deselected, documents in managed apps and accounts can only open in other managed apps and accounts. (Available only in iOS 7.0 and later.)
Allow Open in Managed Apps	If selected, documents in unmanaged apps and accounts can be opened in managed apps and accounts. If this option is deselected, documents in unmanaged apps and accounts can only open in other unmanaged apps and accounts. (Available only in iOS 7.0 and later.)
Autonomous single-mode apps	App identifiers (bundle IDs) that are allowed to autonomously enter Single App Mode. Enter each app identifier on a separate line. (Only applies to supervised devices. Available only in iOS 7.0 and later.)

Figure 125 *The Device Restrictions Settings Form, Safari Area*

Safari	
Allow Safari:	<input checked="" type="checkbox"/> Allow use of the Safari browser When unselected, the Safari web browser app is disabled and this will also prevent users from opening web clips.
Enable Autofill:	<input type="checkbox"/> Enable autofill for Safari Select this option if form content in Safari can be auto-filled.
Fraud Warning:	<input checked="" type="checkbox"/> Warn when visiting fraudulent websites When unselected, users will not be warned when they visit fraudulent websites.
Enable JavaScript:	<input checked="" type="checkbox"/> Enable JavaScript in Safari When unselected, JavaScript is disabled in the Safari browser.
Block Pop-ups:	<input type="checkbox"/> Block pop-ups in Safari Select this option to block pop-ups in the Safari browser.
Accept Cookies:	Always <input type="button" value="v"/> Controls when Safari accepts web browser cookies.

Table 61: Device Restrictions Settings Form, Safari Area

Field	Description
Allow Safari	If selected, enables the Safari Web browser. Users can also open Web clips.
Enable Autofill	If selected, enables autofill for Safari.
Fraud Warning	If selected, users are warned when they visit fraudulent Web sites.
Enable JavaScript	If selected, enables Javascript for Safari.
Block Pop-ups	if selected, pop-up windows are blocked for Safari.
Accept Cookies	Specifies when Safari should accept cookies. Options include: <ul style="list-style-type: none"> ● Never ● From visited sites ● Always

Figure 126 The Device Restrictions Settings Form, Content Settings Area

Content Settings

Rating Region:
Select the region for content ratings.

Explicit Music & Podcasts: Allow explicit music, podcasts & iTunes U
Select this option if music, videos and podcasts containing explicit material are allowed.

Movies:
Select the maximum allowed ratings for movies.

TV Shows:
Select the maximum allowed ratings for TV shows.

Apps:
Select the maximum allowed ratings for apps.

Books: Allow explicit erotic content
Select this option if you want to allow download of media from the iBookstore that has been tagged as erotica.

Allow In-App Purchase: Allow In-App purchase
When unselected, apps will not be able to perform in-app purchases.

Force iTunes password: Force iTunes password for each transactions
Select this option if you want to require the user to enter their iTunes password for each transaction.

Table 62: Device Restrictions Settings Form, Content Settings Area

Field	Description
Rating Region	Specifies the region (country or territory) for content ratings.
Explicit Music and Podcasts	If selected, allows music, videos, and podcasts containing explicit material.
Movies	Specifies the maximum allowed rating for movies. Options include: <ul style="list-style-type: none"> ● Don't allow movies ● G ● PG ● PG-13 ● R ● NC-17 ● All all movies
TV Shows	Specifies the maximum allowed rating for TV shows. Options include: <ul style="list-style-type: none"> ● Don't allow TV shows

Table 62: Device Restrictions Settings Form, Content Settings Area(Continued)

Field	Description
	<ul style="list-style-type: none"> ● TV-Y ● TV-Y7 ● TV-G ● TV-PG ● TV-14 ● TV-MA ● Allow all TV shows
Apps	Specifies the maximum allowed rating for apps. Options include: <ul style="list-style-type: none"> ● Don't allow apps ● 4+ ● 9+ ● 12+ ● 17+ ● Allow all apps
Books	If selected, allows download from the iBookstore of media that are tagged as erotica.
Allow In-App Purchase	If selected, apps can perform in-app purchases.
Force iTunes Password	If selected, requires the user to enter their iTunes password for each transaction.

Figure 127 The Device Restrictions Settings Form, Security and Privacy Settings Area

Security and Privacy Settings	
Allow Diagnostic Data:	<input type="checkbox"/> Allow diagnostic data to be sent to Apple <small>Select this option if the device should automatically submit diagnostic reports to Apple.</small>
Prompt For Untrusted TLS Certificate:	<input checked="" type="checkbox"/> Allow user to accept untrusted TLS certificates <small>When unselected, the device will automatically reject untrusted TLS certificates without prompting the user.</small>
Force Encrypted Backups:	<input type="checkbox"/> Force encrypted backups <small>Select this option if you want backups from the device to be encrypted.</small>
Allow PKI Updates:	<input checked="" type="checkbox"/> Allow over-the-air PKI updates <small>When unselected, OTA PKI updates will be disabled. This setting is available only in iOS 7.0 and later.</small>
Limit Ad Tracking:	<input checked="" type="checkbox"/> Force limiting ad tracking <small>When selected, limits ad tracking. This setting is available only in iOS 7.0 and later.</small>
Host Pairing:	<input checked="" type="checkbox"/> Allow host pairing <small>When unselected, host pairing is disabled with the exception of the supervision host. If no supervision host certificate has been configured, all pairing is disabled. This setting is applicable only to supervised devices. This setting is available only in iOS 7.0 and later.</small>

Table 63: Device Restrictions Settings Form, Security and Privacy Settings Area

Field	Description
Allow Diagnostic Data	If selected, the device automatically submits diagnostic reports to Apple.
Prompt for Untrusted TLS Certificate	If selected, displays a prompt and allows the user to accept untrusted TLS certificates. If deselected, the device automatically rejects untrusted TLS certificates without prompting the user.
Force Encrypted Backups	If selected, backups from the device are encrypted.

Table 63: Device Restrictions Settings Form, Security and Privacy Settings Area(Continued)

Field	Description
Allow PKI Updates	If selected, enables OTA PKI updates. (Available only in iOS 7.0 and later.)
Limit Ad Tracking	If selected, limits ad tracking. (Available only in iOS 7.0 and later.)
Host Pairing	If selected, enables host pairing. If deselected, disables host pairing with the exception of the supervision host. If no supervision host is configured, disables all host pairing. (Only applies to supervised devices. Available only in iOS 7.0 and later.)

Figure 128 The Device Restrictions Settings Form, Device Functionality Settings Area

Device Functionality Settings	
Screen Capture:	<input checked="" type="checkbox"/> Allow screen capture When unselected, users will be unable to save a screenshot of the display.
Automatic Sync:	<input type="checkbox"/> Allow automatic sync while roaming Select this option to allow automatic sync while roaming.
Allow Assistant:	<input checked="" type="checkbox"/> Allow Siri When unselected, the use of Siri on the device is not allowed.
Allow Assistant on lock:	<input checked="" type="checkbox"/> Allow Siri while device is locked When unselected, users will be unable to use Siri when the device is locked. This restriction doesn't apply if device doesn't have a passcode set.
Allow Assistant for user-generated content:	<input checked="" type="checkbox"/> Allow Siri to query user-generated content from the web When unselected, prevents Siri from querying user-generated content from the web. This setting is applicable only to supervised devices. This setting is available only in iOS 7.0 and later.
Allow Voice Dialing:	<input checked="" type="checkbox"/> Allow voice dialing When unselected, users will not be able to use the voice dialing feature.
Allow Fingerprint:	<input checked="" type="checkbox"/> Allow fingerprint for unlock When unselected, prevents Touch ID from unlocking the device. This setting is available only in iOS 7.0 and later.
Allow Passbook on lock:	<input checked="" type="checkbox"/> Allow Passbook while device is locked When unselected, Passbook notifications will not be shown on the lock screen.
Control Center on lock:	<input checked="" type="checkbox"/> Show Control Center on the lock screen When unselected, prevents Control Center from appearing on the lock screen. This setting is available only in iOS 7.0 and later.
Notifications View on lock:	<input checked="" type="checkbox"/> Show Notifications view on the lock screen When unselected, the Notifications view in Notification Center on the lock screen is disabled. This setting is available only in iOS 7.0 and later.
Today View on lock:	<input checked="" type="checkbox"/> Show Today view on the lock screen When unselected, the Today view in Notification Center on the lock screen is disabled. This setting is available only in iOS 7.0 and later.
Configuration Profile Installation:	<input checked="" type="checkbox"/> Allow interactive installation of configuration profiles and certificates When unselected, the user is prohibited from installing configuration profiles and certificates interactively. This setting is applicable only to supervised devices.
Accounts:	<input checked="" type="checkbox"/> Allow account modification When unselected, prevents adding, removing, or modifying accounts in Mail, Contacts, Calendars. This setting is applicable only to supervised devices. This setting is available only in iOS 7.0 and later.
Cellular Data Use:	<input checked="" type="checkbox"/> Allow changes to cellular data usage for apps This setting is applicable only to supervised devices. This setting is available only in iOS 7.0 and later.
Find My Friends:	<input checked="" type="checkbox"/> Allow changes to Find My Friends When unselected, locks the friends list and the current settings. This setting is applicable only to supervised devices. This setting is available only in iOS 7.0 and later.
Allow AirDrop:	<input checked="" type="checkbox"/> Allow AirDrop When unselected, AirDrop is disabled. This setting is applicable only to supervised devices. This setting is available only in iOS 7.0 and later.

Table 64: *Device Restrictions Settings Form, Device Functionality Settings Area*

Field	Description
Screen Capture	If selected, users can save a screenshot of the display.
Automatic Sync	If selected, allows autosync while roaming.
Allow Assistant	If selected, allows using Siri on the device.
Allow Assistant on Lock	If selected, allows using Siri when the device is locked. This restriction only applies if a passcode has been set on the device.
Allow Assistant for User-Generated Content	If selected, allows Siri to query user-generated content from the Web. (Only applies to supervised devices. Available only in iOS 7.0 and later.)
Allow Voice Dialing	If selected, users can use the voice dialing feature.
Allow Fingerprint	If selected, Touch ID can be used to unlock the device. (Available only in iOS 7.0 and later.)
Allow Passbook on Lock	If selected, Passbook notifications will be shown on the lock screen.
Control Center on Lock	If selected, Control Center will appear on the lock screen. (Available only in iOS 7.0 and later.)
Notifications View on Lock	If selected, enables the Notifications view in the Notification Center on the lock screen. (Available only in iOS 7.0 and later.)
Today View on Lock	If selected, enables the Today view in the Notification Center on the lock screen. (Available only in iOS 7.0 and later.)
Configuration Profile Installation	If selected, the user can install configuration profiles and certificates interactively. (Only applies to supervised devices.)
Accounts	If selected, accounts can be added, removed, or modified in Mail, Contacts, and Calendars. (Only applies to supervised devices. Available only in iOS 7.0 and later.)
Cellular Data Use	If selected, allows changes to cellular data usage for apps. (Only applies to supervised devices. Available only in iOS 7.0 and later.)
Find My Friends	If selected, allows changes to the friends list and the current settings. (Only applies to supervised devices. Available only in iOS 7.0 and later.)
Allow AirDrop	If selected, enables AirDrop. (Only applies to supervised devices. Available only in iOS 7.0 and later.)

Figure 129 *The Device Restrictions Settings Form, iCloud Settings Area*

iCloud Settings	
Allow Backup:	<input checked="" type="checkbox"/> Allow backing up the device to iCloud When unselected, backups to iCloud are not allowed.
Allow Document Sync:	<input checked="" type="checkbox"/> Allow document and key-value sync to iCloud When unselected, documents and key-values will not be synced to iCloud.
Allow Photo Stream:	<input checked="" type="checkbox"/> Allow photo stream When unselected, photo stream is disallowed and this can cause data loss.
Allow Shared Photo Streams:	<input checked="" type="checkbox"/> Allow shared photo streams When unselected, shared photo streams in iCloud are not allowed.
Allow Keychain Sync:	<input checked="" type="checkbox"/> Allow keychain sync to iCloud When unselected, keychain will not be synced to iCloud. This setting is available only in iOS 7.0 and later.

Table 65: *Device Restrictions Settings Form, iCloud Settings Area*

Field	Description
Allow Backup	If selected, allows backups to iCloud.
Allow Document Sync	If selected, documents and key-values are synced to iCloud.
Allow Photo Stream	If selected, allows photostream. If deselected, photostream is not allowed, which can result in some data loss.
Allow Shared Photo Streams	If selected, allows shared photo streams in iCloud.
Allow Keychain Sync	If selected, keychain is synced to iCloud. (Available only in iOS 7.0 and later.)

Figure 130 *The Device Restrictions Settings Form, Game Center Settings Area*

Game Center Settings	
Game Center:	<input checked="" type="checkbox"/> Allow Game Center When unselected, Game Center is disabled and its icon is removed from the Home screen. This setting is applicable only to supervised devices.
Multiplayer gaming:	<input type="checkbox"/> Allow multiplayer gaming on the device Select this option to allow multiplayer gaming on the device.
Game Center Friends:	<input type="checkbox"/> Allow adding Game Center friends Select this option to allow adding Game Center friends.

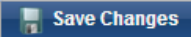


Table 66: *Device Restrictions Settings Form, Game Center Settings Area*

Field	Description
Game Center	If selected, enables Game Center and its icon is displayed on the Home screen. (Only applies to supervised devices.)
Multiplayer Gaming	If selected, allows multiplayer gaming on the device.
Game Center Friends	If selected, allows adding Game Center friends.

When your changes are complete on the **Device Restrictions Settings** form, click **Save Changes**. The device restrictions settings are available as a configuration unit on the **Configuration Profile** list view.

Configuring Email Settings



Email settings you define can be used in configuration profiles for an iOS device. You can define multiple Email settings.

Email settings are only supported on iOS devices; they are ignored by all other devices.

To configure email settings, go to **Onboard > Configuration > iOS Settings**. Either click an existing email setting's name in the list; or click **Add New**, select **Email Settings** in the **Settings Type** drop-down list, and click **Create**. The **Email Settings** form opens.

Figure 131 *The Email Settings Form, Basic Properties and General Settings Area*

Email Settings	
* Name:	<input type="text"/> <small>Enter a name for the email settings.</small>
Description:	<input type="text"/> <small>Enter a description for the email settings.</small>
General Settings <small>Common settings for the email account.</small>	
Account Description:	<input type="text" value="Company Mail Account"/> <small>The display name of the mail account, e.g. "Company Mail Account".</small>
Account Type:	IMAP <input type="button" value="v"/> <small>Select the protocol for accessing the email account.</small>
* Get Email Address From:	Provisioning - values acquired during device provisioning <input type="button" value="v"/> <small>Select how the user's email address is to be supplied.</small>
Email Address Domain:	<input type="text"/> <small>Select the domain name to be appended to the username. If the username is "user" and the domain is "example.com", the full email address will be "user@example.com".</small>
When to Add Email Address Domain:	Only if username is not a valid email address <input type="button" value="v"/> <small>Select when the email address domain should be added to the username.</small>
Allow Move:	<input checked="" type="checkbox"/> Allow user to move messages from this account <small>When unselected, messages may not be moved out of this email account into another account. This also prevents forwarding or replying from a different account than the message was originated from.</small>
Allow Recent Address Sync:	<input checked="" type="checkbox"/> Include this account in recent address syncing
Use Only in Mail:	<input checked="" type="checkbox"/> Send outgoing mail from this account only from the Mail app <small>When selected, this account is not available for sending mail in third-party applications.</small>

Table 67: *Email Settings Form, Basic and General Settings Areas*

Field	Description
Name	(Required) Short name that identifies the email setting clearly. Email settings names can include spaces. If you are duplicating an email settings, the original name has "Copy" appended to it. You may highlight this name and replace it with a new name.
Description	Brief description of the characteristics of the email settings.
Account Description	Display name for the mail account.
Get Email Address From	(Required) Specifies how the user's email address should be supplied. Options include: <ul style="list-style-type: none"> • User provided - entered by user on device • Provisioning - values acquired during device provisioning

Table 67: Email Settings Form, Basic and General Settings Areas(Continued)

Field	Description
	<ul style="list-style-type: none"> Shared preset values - testing only <p>The fields available in the General Settings area will vary according to your choice in the this drop-down list.</p>
Email Address	Full email address for the account.
Email Address Domain	Domain name to append to the username. For example, if the username is "user" and the domain is "example.com", the full email address would be "user@example.com".
When to Add Email Address Domain	Specifies when the email address domain should be added to the username. Options include: <ul style="list-style-type: none"> Only if username is not a valid email address Always add the domain
Allow Move	If selected, allows the user to move messages out of the account into another account. If deselected, messages may not be moved by the user, and the user also cannot forward or reply from a different account than the one where the message originated.
Allow Recent Address Sync	If selected, includes the account in recent address syncing.
Use Only in Mail	If selected, outgoing mail for this account is only sent from the Mail app, and the account is not available for sending mail in third-party applications.

Figure 132 *The Email Settings Form, Incoming Mail Server Settings Area*

Incoming Mail Server Settings

Settings for retrieving incoming mail.

* Incoming Mail Server:	<input style="width: 100%;" type="text"/> <small>Hostname or IP address of the server for incoming mail. A hostname will only be accepted if the corresponding IP address can be resolved.</small>
* Port:	<input style="width: 100%;" type="text" value="143"/> <small>Port number of the server for incoming mail.</small>
Use SSL:	<input checked="" type="checkbox"/> Retrieve incoming mail through secure socket layer <small>Select this option to ensure that communications are encrypted.</small>
Authentication Type:	<input style="width: 100%;" type="text" value="Password"/> <small>Select the authentication method for the incoming mail server.</small>
* Account Details:	<input style="width: 100%;" type="text" value="Provisioning - values acquired during device provisioning"/> <small>Select how user account information is to be supplied.</small>

Table 68: Email Settings Form, Incoming Mail Server Settings Form

Field	Description
Incoming Mail Server	(Required) Hostname or IP address of the server for the incoming mail (for example, mail.exampleprovider.com). The hostname will only be accepted if the corresponding IP address can be resolved.
Port	(Required) Click this field and use the counter to select the port number of the server for incoming mail.
Use SSL	If selected, enables secure socket layer communication with the server and ensures that incoming communications are encrypted.
Authentication Type	Specifies the authentication method for the incoming mail server. Options include: <ul style="list-style-type: none"> ● Password ● MD5 Challenge-Response ● NTLM ● HTTP MD5 Digest ● None
Account Details	Specifies how user account information should be supplied. Options include: <ul style="list-style-type: none"> ● User provided - entered by user on device ● Provisioning - values acquired during device provisioning ● Shared preset values - testing only
Username	If Shared preset values - testing only is selected in the Account Details drop-down list, the Username field is added to the form. Enter the username for connecting to the server for incoming mail.
Password	If Shared preset values - testing only is selected in the Account Details drop-down list, the password fields are added to the form. Enter the CalDAV password for connecting to the server for incoming mail. The minimum password length is six characters.
Confirm Password	

Figure 133 The Email Settings Form, Outgoing Mail Server Settings Area

Outgoing Mail Server Settings

Settings for sending outgoing mail.

* Outgoing Mail Server:	<input style="width: 100%;" type="text"/> <small style="color: #0070C0;">Hostname or IP address of the server for outgoing mail. A hostname will only be accepted if the corresponding IP address can be resolved.</small>
* Port:	<input style="width: 100%;" type="text" value="587"/> <small style="color: #0070C0;">Port number of the server for outgoing mail.</small>
Use SSL:	<input checked="" type="checkbox"/> Send outgoing mail through secure socket layer <small style="color: #0070C0;">Select this option to ensure that communications are encrypted.</small>
Authentication Type:	<input style="width: 100%;" type="text" value="Password"/> <small style="color: #0070C0;">Select the authentication method for the outgoing mail server.</small>
* Account Details:	<input style="width: 100%;" type="text" value="Provisioning - values acquired during device provisioning"/> <small style="color: #0070C0;">Select how user account information is to be supplied.</small>
Outgoing Password Same As Incoming:	<input checked="" type="checkbox"/> SMTP authentication uses the same password as POP/IMAP <small style="color: #0070C0;">When selected, the same password will be used for both incoming and outgoing mail.</small>
Use S/MIME:	<input type="checkbox"/> This account supports S/MIME

Table 69: Email Settings Form, Outgoing Mail Server Settings Area

Field	Description
Outgoing Mail Server	(Required) Hostname or IP address of the server for the outgoing mail (for example, smtp.exampleprovider.com).
Port	(Required) Click this field and use the counter to select port number of the server to use for outgoing mail.
Use SSL	If selected, enables secure socket layer communication with the server and ensures that outgoing communications are encrypted.
Authentication Type	Specifies the authentication method for the outgoing mail server. Options include: <ul style="list-style-type: none">• Password• MD5 Challenge-Response• NTLM• HTTP MD5 Digest• None
Account Details	Specifies how user account information should be supplied. Options include: <ul style="list-style-type: none">• User provided - entered by user on device• Provisioning - values acquired during device provisioning• Shared preset values - testing only
User Name	If Shared preset values - testing only is selected in the Account Details drop-down list, Username field is added to the form. Enter the username for connecting to the server for outgoing mail.
Outgoing Password Same as Incoming	If selected, the same password is used for incoming and outgoing mail.
Use S/MIME	If selected, the email account supports S/MIME.

When you have completed your changes on this form, click **Save Changes**. The application set is available as a configuration unit on the **Configuration Profile** list view.

For more information about configuration profiles, see "[Configuration Profiles](#)" on page 216

Configuring an iOS Device Passcode Policy



Passcode policy settings are typically used when you provision a corporate-owned device, or when a user is given remote access to sensitive information. Passcode policy settings you define can be used in configuration profiles for an iOS device. You can define multiple passcode policy settings.

Passcode policy settings are only supported by iOS devices; they are ignored by all other device types.

To configure a passcode policy, go to **Onboard > Configuration > iOS Settings**. Either click an existing passcode policy setting's name in the list; or click **Add New**, select **Passcode Policy Settings** in the **Settings Type** drop-down list, and click **Create**. The **Passcode Policy Settings** form opens.

Figure 134 *The Passcode Policy Settings Form*

Passcode Policy Settings	
* Name:	<input type="text"/> Enter a name for the passcode policy.
Description:	<input type="text"/> Enter a description for the passcode policy.
Force PIN:	<input type="checkbox"/> Force a passcode to be set on devices Determines whether the user is forced to set a PIN. Simply setting this value (and not others) forces the user to enter a passcode, without imposing a length or quality.
Allow Simple:	<input checked="" type="checkbox"/> Allow simple passcodes Determines whether a simple passcode is allowed. A simple passcode is defined as one containing repeated characters, or increasing/decreasing characters (such as 123 or CBA).
Require Alphanumeric:	<input type="checkbox"/> Require alphabetic characters Specifies whether the user must enter alphabetic characters ("abcd"), or if numbers are sufficient.
Max Failed Attempts:	<input type="text"/> attempts Specifies the number of allowed failed attempts to enter the passcode at the device's lock screen. Once this number is exceeded, the device is locked and must be connected to its designated iTunes in order to be unlocked.
Max Inactivity:	<input type="text" value="Unlimited"/> Specifies the number of minutes for which the device can be idle (without being unlocked by the user) before it gets locked by the system. Once this limit is reached, the device is locked and the passcode must be entered. Note: This is the maximum allowed, the user may still set a value lower than this.
Max PIN Age:	<input type="text"/> days Specifies the number of days for which the passcode can remain unchanged. After this number of days, the user is forced to change the passcode before the device is unlocked.
Min Complex Chars:	<input type="text"/> characters Specifies the minimum number of complex characters that a passcode must contain. A "complex" character is a character other than a number or a letter, such as &%\$#.
Max Grace Period:	<input type="text" value="4 Hours"/> The maximum grace period, in minutes, to unlock the device without entering a passcode. Note: This is the maximum allowed, the user may still set a value lower than this.
Min Length:	<input type="text"/> characters Specifies the minimum number of characters that a passcode must contain.
PIN History:	<input type="text"/> entries When the user changes the passcode, it has to be unique within the last N entries in the history.
	

Table 70: Passcode Policy Settings Form

Field	Description
Name	(Required) Short name that identifies the passcode policy clearly. Passcode policy names can include spaces. If you are duplicating a passcode policy, the original name has "Copy" appended to it. You may highlight this name and replace it with a new name.
Description	Brief description of the characteristics of the passcode policy.
Force PIN	If selected, requires the user to create a passcode.
Allow Simple	If selected, no restrictions are placed on the passcode for repeated or sequential characters. A simple passcode can include repeated characters, or increasing or decreasing characters such as 123 or CBA.
Require Alphanumeric	If selected, the passcode must include alphabetic characters in addition to numbers.
Max Failed Attempts	Use the counter to limit the number of times the passcode may be entered incorrectly before the device is locked.
Max Inactivity	Specifies the number of minutes the device is allowed to be idle before it is locked and the user must re-enter the passcode. Options include: <ul style="list-style-type: none"> • Unlimited • 2 • 5 • 10 • 15 The user may set a lower number.
Max PIN Age	Use the counter to specify a maximum duration for the passcode. After the specified number of days, the device is locked and the user must change their passcode.
Min Complex Chars	Specifies whether the passcode must include complex characters. Use the counter to specify how many complex characters it must contain. Complex, or special, characters are non-alphanumeric, such as &%\$#.
Max Grace Period	Specifies a maximum time in which the user may unlock the device without re-entering the passcode. Use the counter to select a number of minutes. The user may set a lower number.
Min Length	Use the counter to specify the minimum number of characters the passcode must include.
PIN History	Specifies that when the user changes their passcode the new value cannot be one that was used within a defined period of the passcode's history. Use the counter to specify the number of recent passwords whose values will not be allowed.

When you have completed your changes on this form, click **Save Changes**. The passcode policy is available as a configuration unit on the **Configuration Profile** form.

For more information about configuration profiles, see ["Configuration Profiles" on page 216](#)

Configuring Calendar Subscription Settings



Subscribed calendar settings let you configure the calendar subscriptions that will be sent to the provisioned device. A calendar subscription's settings include its name and description, the account description, server, and whether SSL is enabled, as well as additional account details. Subscribed calendar settings you define can be used in configuration profiles for an iOS device. You can define multiple subscribed calendar settings.

Subscribed calendar settings are only supported on iOS devices; they are ignored by all other devices.

To configure a calendar subscription setting, go to **Onboard > Configuration > iOS Settings**. Either click an existing subscribed calendar setting's name in the list; or click **Add New**, select **Subscribed Calendar Settings** in the **Settings Type** drop-down list, and click **Create**. The **Subscribed Calendar Settings** form opens.

Figure 135 *The Calendar Subscription Settings Form*

Calendar Subscription Settings	
* Name:	<input type="text"/> Enter a name for the calendar subscription settings.
Description:	<input type="text"/> Enter a description for the calendar subscription settings.
Settings Settings for the subscription to the calendar.	
Account Description:	<input type="text" value="Company Calendar Subscription"/> The description of the calendar subscription.
* Server:	<input type="text"/> Enter the URL of the calendar file.
Use SSL:	<input checked="" type="checkbox"/> Enable secure socket layer communication with the server
Account Settings Options for the calendar subscription user account.	
* Account Details:	<input type="text" value="Shared preset values — testing only"/> Select how user account information is to be supplied.
Username:	<input type="text"/> Enter the username for this subscribed calendar.
Password:	<input type="password"/> Enter the password for this subscribed calendar.
Confirm Password:	<input type="password"/> Re-enter the password.
<input type="button" value="Save Changes"/>	

Table 71: Calendar Subscription Settings Form

Field	Description
Name	(Required) Short name that identifies this calendar subscription setting clearly. Calendar subscription settings names can include spaces. If you are duplicating a calendar subscription setting, the original name has "Copy" appended to it. You may highlight this name and replace it with a new name.
Description	Brief description of the characteristics of the calendar subscription setting.
Account Description	Display name for the calendar subscription.
Server	(Required) URL of the calendar file.
Use SSL	If selected, enables secure socket layer communication with the server.
Account Details	Specifies how user account information should be supplied. Options include: <ul style="list-style-type: none"> • User provided - entered by user on device • Provisioning - values acquired during device provisioning • Shared preset values - testing only
Username	If Shared preset values - testing only is selected in the Account Details drop-down list, the username field is added to the form. Enter the username to be used for the subscribed calendar.
Password	If Shared preset values - testing only is selected in the Account Details drop-down list, the password fields are added to the form. Enter the password to be used for the subscribed calendar. The minimum password length is six characters.
Confirm Password	

When you have completed your changes on this form, click **Save Changes**. The calendar settings are available as a configuration unit on the **Configuration Profile** form.

For more information about configuration profiles, see ["Configuration Profiles" on page 216](#)

Configuring an iOS Device VPN Connection



Use VPN configuration profiles when you have deployed a VPN infrastructure and want to automatically provide the secure connection settings to users at the time of device provisioning. You can automatically configure virtual private network (VPN) settings on iOS and OS X 10.7+ devices. VPN settings you define can be used in configuration profiles for an iOS device. You can define multiple VPN settings.

VPN configuration profiles are only supported by iOS and OS X 10.7+ (Lion or later) devices; they are ignored by all other device types.

For information on configuring VPN connections, see:

- ["Configuring an iOS Device VIA Connection " on page 205](#)
- ["Configuring an iOS Device L2TP, PPTP, or IPsec Connection " on page 209](#)

Configuring an iOS Device VIA Connection

Aruba VIA is a remote access solution that provides secure connections for Enterprise networks. VIA detects the user's network environment (trusted and un-trusted) and automatically connects the user to their enterprise network.

To configure the Aruba VIA solution on an iOS device, go to **Onboard > Configuration > iOS Settings**. Either click a VPN setting's name in the list; or click **Add New**, select **VPN Settings** in the **Settings Type** drop-down list, and click **Create**. The **VPN Settings** form opens.

Figure 136 The VPN Settings Form, Basic and General Settings Areas for VIA

The screenshot shows the 'VPN Settings' form. It has a dark blue header with the title 'VPN Settings'. Below the header, there are three main sections:

- Name:** A text input field containing 'via-profile'. Below it is a blue link that says 'Enter a name for the VPN.'
- Description:** A large text area. Below it is a blue link that says 'Enter a description for the VPN.'
- General Settings:** A section with the subtitle 'Common settings for the Virtual Private Network.' Below this is a dropdown menu for 'Connection Type' which is currently set to 'Aruba VIA'. Below the dropdown is a blue link that says 'The type of connection enabled by this policy.'

Table 72: VPN Settings Form, Basic and General Settings Areas

Field	Description
Name	(Required) Short name that identifies the VPN setting clearly. VPN configuration names can include spaces. If you are duplicating a VPN configuration, the original name has "Copy" appended to it. You may highlight this name and replace it with a new name.
Description	Brief description of the characteristics of the VPN configuration.
Connection Type	(Required) Select Aruba VIA in the drop-down list. The VPN Settings form expands to include additional options.

Figure 137 The VPN Settings Form, Aruba VIA Settings Area

Aruba VIA Settings

These options configure the Aruba VIA connection.

* Server:	<input style="width: 90%;" type="text"/> <small>Hostname or IP address of the server the device will connect to. A hostname will only be accepted if the corresponding IP address can be resolved.</small>						
IKE Version:	<input style="width: 80%;" type="text" value="v2"/> <small>Version of the IKE protocol.</small>						
Authentication:	<input style="width: 80%;" type="text" value="Certificate"/> <small>Authentication type for the connection.</small>						
Internal IP:	<input style="width: 90%;" type="text"/> <small>Internal IP address of the controller, used for SSL fallback and configuration download after the tunnel is setup.</small>						
DNS Suffix:	<input style="width: 90%;" type="text"/> <small>DNS domain name to resolve internal resources.</small>						
Split Tunneling:	<input checked="" type="checkbox"/> Enable Split Tunneling <small>Allow split tunneling of traffic</small>						
Split Tunnels:	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr style="background-color: #2c4e64; color: white;"> <th style="width: 50%;">IP Address*</th> <th style="width: 50%;">Netmask*</th> </tr> </thead> <tbody> <tr style="text-align: center;"> <td colspan="2"> i No tunnels have been added to the list. </td> </tr> <tr> <td colspan="2" style="text-align: center;"> <input style="width: 100%; border: none; background-color: #e6f2ff;" type="button" value="Add a tunnel to match"/> </td> </tr> </tbody> </table> <small>Addresses to which data will be tunneled through VIA.</small>	IP Address*	Netmask*	i No tunnels have been added to the list.		<input style="width: 100%; border: none; background-color: #e6f2ff;" type="button" value="Add a tunnel to match"/>	
IP Address*	Netmask*						
i No tunnels have been added to the list.							
<input style="width: 100%; border: none; background-color: #e6f2ff;" type="button" value="Add a tunnel to match"/>							
On Demand:	<input checked="" type="checkbox"/> Enable VPN on Demand <small>Allow a list of domain and host names to automatically establish a VPN connection.</small>						
On Demand Match:	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr style="background-color: #2c4e64; color: white;"> <th style="width: 50%;">Match Domain or Host*</th> <th style="width: 50%;">On Demand Action</th> </tr> </thead> <tbody> <tr style="text-align: center;"> <td colspan="2"> i No domain or host names have been added to the list. </td> </tr> <tr> <td colspan="2" style="text-align: center;"> <input style="width: 100%; border: none; background-color: #e6f2ff;" type="button" value="Add a domain or host name to match"/> </td> </tr> </tbody> </table> <small>Domain and host names that will establish a VPN connection.</small>	Match Domain or Host*	On Demand Action	i No domain or host names have been added to the list.		<input style="width: 100%; border: none; background-color: #e6f2ff;" type="button" value="Add a domain or host name to match"/>	
Match Domain or Host*	On Demand Action						
i No domain or host names have been added to the list.							
<input style="width: 100%; border: none; background-color: #e6f2ff;" type="button" value="Add a domain or host name to match"/>							

Table 73: VPN Settings Form, Aruba VIA Settings Area

Field	Description
Server	(Required) Hostname or IP address of the server the device should connect to.
IKE Version	Specifies the version number for the Internet Key Exchange (IKE) protocol. Options include: <ul style="list-style-type: none"> ● v2 - IKEv2 supports a wider variety of authentication mechanisms and it is faster when compared to IKEv1 method. IKEv2 has only single phase authentication process ● v1 - This protocol performs the authentication in two phases.
Authentication	Specifies the authentication type for the connection. The options available in this list depend on the selection you made in the IKE Version field. <ul style="list-style-type: none"> ● If you choose the IKEv1 protocol, you can specify the following authentication types: <ul style="list-style-type: none"> ■ Certificate – The client certificate issued during device provisioning will also be used as the identity certificate for VPN connections. This option requires configuring your VPN server to allow VIA authentication using a client certificate. ■ Shared Secret / Group Name – An optional group name may be specified. A shared secret (Pre-Shared Key) is used to establish the VIA connection. Authentication is performed with a username and password. ● If you choose the IKEv2 protocol, you can specify the following authentication types. For VIA deployments that use IKEv2, the VPN server always uses a certificate for IKEv2 authentication phase. However, the devices can use certificates, EAP-MSCHAPv2, or EAP-TLS: <ul style="list-style-type: none"> ■ Certificate

Table 73: VPN Settings Form, Aruba VIA Settings Area(Continued)

Field	Description
	<ul style="list-style-type: none"> ■ EAP-TLS ■ EAP-MSCHAPv2
Internal IP	Internal IP address assigned to the controller. This is used for SSL fallback and configuration after the tunnel is set up.
DNS Suffix	DNS domain name for the resolution of the internal resources.
Split Tunneling	If selected, all the traffic to the VIA tunneled networks goes through the controller and the rest is bridged directly on the device.
Split Tunnels	If the Enable Split Tunnel option is selected, the Split Tunnels field is added to the form. You must specify the addresses and netmask to which data will be tunneled through VIA. Click the Add a tunnel to match link and enter the information for each IP address and netmask.
On Demand	If selected, the VPN connection will be automatically established when accessing certain domains.
On Demand Match	If the Enable VPN on Demand option is selected, the On Demand Match field is added to the form. You must specify the domain names and the on-demand action that need to be applied to these domains. Click the Add a domain or host name to match link and enter the information for each domain and action.

Figure 138 The VPN Settings Form, VIA Connection, Advanced Area

Advanced Settings

Advanced Settings: Show Advanced Settings
Select this option to configure advanced settings for VIA.

Hash Algorithm: OAKLEY_SHA ▼
Hash algorithm to use.

Encryption Algorithm: OAKLEY_AES_CBC ▼
Encryption algorithm to use.

DH Group: MODP1024 ▼
Diffie-Hellman group to use.

Phase2 Auth Algorithm: SHA1 ▼
Phase 2 auth algorithm to use.

Phase2 Encryption Algorithm: AES ▼
Phase 2 encryption algorithm to use.

PFS: Enable PFS
Configure perfect forward secrecy.

Suite B: Enable Suite B
Configure Suite B cryptography.

FIPS: Enable FIPS
Configure FIPS mode for VIA.

VPN Custom Data:

Key	Value
There are no items in the list.	
Add a new item	

VPN specific custom data using key and value pairs.

Table 74: VPN Settings Form, VIA Connection, Advanced Area

Field	Description
Show Advanced Settings	If selected, the advanced configuration options for VIA are added to this form.
Hash Algorithm	Hash algorithm to use. Options include: <ul style="list-style-type: none">● OAKLEY_SHA● OAKLEY_SHA_256● OAKLEY_SHA_384● OAKLEY_SHA_512● OAKLEY_MD5
Encryption Algorithm	Encryption algorithm to use. Options include: <ul style="list-style-type: none">● OAKLEY_AES_CBC● OAKLEY_3DES_CBC
DH Group	Diffie-Hellman group to use. Options include: <ul style="list-style-type: none">● MODP1024● MODP768● ECP256● ECP384
Phase2 Auth Algorithm	Phase 2 authentication algorithm to use. Options include: <ul style="list-style-type: none">● SHA1● MD5
Phase2 Encryption Algorithm	Phase 2 encryption algorithm to use. Options include: <ul style="list-style-type: none">● AES● GCM● 3DES
PFS	If selected, enables perfect forward secrecy.
Suite B	If selected, enables Suite B cryptography.
FIPS	If selected, enables FIPS mode for VIA.
VPN Custom Data	Lets you enter VPN-specific custom data. Click the Add a new item link and enter the key and value pairs.

Figure 139 The VPN Settings Form, VIA Connection, Proxy Settings Area

Proxy Settings
Configures proxies to be used with this VPN connection.

* Proxy Setup:

Server and Port: :
Hostname (or IP address) and port number of the proxy the device should connect to. A hostname will only be accepted if the corresponding IP address can be resolved.

Authentication:
Username used when connecting to the proxy.

Password:
Password used when connecting to the proxy.

Confirm:
Re-enter the proxy password.

Save Changes

Table 75: VPN Settings Form, VIA Connection, Proxy Settings Area

Field	Description
Proxy Setup	Specifies the proxy server to use when the VPN connection is active. Options include: <ul style="list-style-type: none"> • None — No proxy server will be configured with this VPN profile. • Manual — A proxy server will be configured with this VPN profile. Specify the proxy server settings in the Server and Port field. • Automatic — The proxy server will be automatically configured with this VPN profile. Specify the location of a proxy auto-config file in the Proxy Server URL field.
Proxy Server URL	If Automatic was selected in the Proxy Setup field, enter the URL used to retrieve the proxy settings.
Server and Port	If Manual was selected in the Proxy Setup field, enter the hostname or IP address and the port number of the proxy the device should connect to. The hostname will only be accepted if the corresponding IP address can be resolved.
Authentication	If authentication is required to access this proxy, enter the proxy username.
Password	If authentication is required to access this proxy, enter the proxy password. The minimum password length is six characters.
Confirm	

When you have completed your changes on this form, click **Save Changes**. The VPN configuration is available as a configuration unit on the **Configuration Profile** form.

For more information about configuration profiles, see "[Configuration Profiles](#)" on page 216

Configuring an iOS Device L2TP, PPTP, or IPsec Connection

You can use VPN settings when you have deployed a VPN infrastructure and want to automatically provide the secure connection settings to users at the time of device provisioning.

To configure the L2TP, PPTP, or IPsec VPN settings, go to **Onboard > Configuration > iOS Settings**. Either click a VPN setting's name in the list; or click **Add New**, select **VPN Settings** in the **Settings Type** drop-down list, and click **Create**. The **VPN Settings** form opens.

Figure 140 The VPN Settings Form, Basic and General Settings Areas for L2TP, PPTP, or IPsec

The screenshot shows the 'VPN Settings' form. At the top is a dark blue header with the text 'VPN Settings'. Below the header are three main sections. The first section is for 'Name', with a text input field and a blue prompt 'Enter a name for the VPN.' The second section is for 'Description', with a larger text area and a blue prompt 'Enter a description for the VPN.' The third section is titled 'General Settings' with the subtitle 'Common settings for the Virtual Private Network.' It contains a 'Connection Type' dropdown menu currently set to 'PPTP' and a blue prompt 'The type of connection enabled by this policy.'

Table 76: VPN Settings Form, Basic and General Settings Areas for L2TP, PPTP, or IPsec

Field	Description
Name	(Required) Short name that identifies the VPN setting clearly. VPN configuration names can include spaces. If you are duplicating a VPN configuration, the original name has "Copy" appended to it. You may highlight this name and replace it with a new name.
Description	Brief description of the characteristics of the VPN configuration.
Connection Type	(Required) Select either L2TP, PPTP, or IPsec in the drop-down list, as appropriate. The VPN Settings form expands to include additional options specific to that connection type. <ul style="list-style-type: none"> ● L2TP — Uses the Layer 2 Tunneling Protocol. ● PPTP — Uses the Point-to-Point Tunneling Protocol. ● IPsec — Uses the Internet Protocol with security extensions.

Figure 141 The VPN Settings Form, Area for L2TP, PPTP, or IPsec Settings

L2TP Connection Settings	
These options configure the L2TP connection.	
* Server:	<input type="text"/> Hostname or IP address of the server the device will connect to. A hostname will only be accepted if the corresponding IP address can be resolved.
Override Routing:	<input type="checkbox"/> Send all traffic through the VPN connection Select this option to override the primary route and send all traffic over the VPN connection.
Machine Authentication	
Shared Secret:	<input type="text"/> Shared secret for the connection. Leave blank to prompt the user on the device.
Confirm:	<input type="text"/> Re-enter the shared secret for the connection.
User Authentication	
* Account:	<input type="text"/> User account for authenticating the connection. Leave blank to prompt the user on the device.
User Authentication:	<input type="radio"/> Password <input type="radio"/> RSA SecurID Authentication type for the connection.

The options available in the **Settings** area depend on your selection in the **Connection Type** field.

Table 77: VPN Settings Form, Settings Area for L2TP, PPTP, or IPsec

Field	Description
Server	(Required) Hostname or IP address of the server the device should connect to.
Override Routing	If selected, overrides the primary route and sends all traffic through the VPN connection.
Encryption Level	Specifies the level of data encryption to apply to the PPTP connection. Options include: <ul style="list-style-type: none"> • None • Automatic • Maximum (128-bit)
Authentication Type	(Required) Specifies the type of authentication to use for the IPsec connection. Options include: <ul style="list-style-type: none"> • Identity Certificate — The client certificate issued during device provisioning will also be used as the identity certificate for VPN connections. This option requires configuring your VPN server to allow IPsec authentication using a client certificate. • Shared Secret / Group Name — An optional group name may be specified. A shared secret (Pre-Shared Key) is used to establish the IPsec VPN. Authentication is performed with a username and password.
Group Name	Group identity for the IPsec connection.
Shared Secret	Shared secret for the L2TP or IPsec connection. If this field is left blank, the user will be prompted to create the shared secret.
Confirm	
Hybrid Authentication	If selected, authentication for this IPsec connection will use the secret, name, and server-side certificate.

Table 77: VPN Settings Form, Settings Area for L2TP, PPTP, or IPsec(Continued)

Field	Description
Account	User account for authenticating the connection. If this field is left blank, the user will be prompted to enter the account information.
User Authentication	Authentication type for the L2TP or PPTP connection. Options include: <ul style="list-style-type: none"> • Password • RSA SecurID
Password Prompt	Specifies whether the password for the IPsec connection must be entered every time. Options include: <ul style="list-style-type: none"> • Save and reuse the password — greater convenience • Always ask for the password — greater security

Figure 142 The VPN Settings Form, Proxy Settings Area

Proxy Settings
Configures proxies to be used with this VPN connection.

* Proxy Setup:

Server and Port: :
Hostname (or IP address) and port number of the proxy the device should connect to. A hostname will only be accepted if the corresponding IP address can be resolved.


Authentication:
Username used when connecting to the proxy.

Password:
Password used when connecting to the proxy.

Confirm:
Re-enter the proxy password.

Table 78: VPN Settings Form, Proxy Settings Area

Field	Description
Proxy Setup	Specifies the proxy server to use when the VPN connection is active. Options include: <ul style="list-style-type: none"> • None — No proxy server will be configured with this VPN profile. • Manual — A proxy server will be configured with this VPN profile. Specify the proxy server settings in the Server and Port field. • Automatic — The proxy server will be automatically configured with this VPN profile. Specify the location of a proxy auto-config file in the Proxy Server URL field.
Proxy Server URL	If Automatic was selected in the Proxy Setup field, enter the URL used to retrieve the proxy settings.
Server and Port	If Manual was selected in the Proxy Setup field, enter the hostname or IP address and the port number of the proxy the device should connect to. The hostname will only be accepted if the corresponding IP address can be resolved.
Authentication	If authentication is required to access this proxy, enter the proxy username.
Password	If authentication is required to access this proxy, enter the proxy password. The minimum password length is six characters.
Confirm	

When you have completed your changes on this form, click  **Save Changes**. The VPN configuration is available as a configuration unit on the **Configuration Profile** form.

For more information about configuration profiles, see "[Configuration Profiles](#)" on page 216

Configuring Web Clips



When you create a Web clip, you can make any URL look like a native app on your device. You can assign it an icon, and when the icon is selected, the URL opens in its own frame. Web clip settings let you create a library of Web clips and bookmarks that can be sent to the provisioned device. A Web clip's settings include its name and description, the icon if one was chosen, the URL, and whether the user can remove it. Web clip settings you define can be used in configuration profiles for an iOS device. You can define multiple Web clip settings.

Web clip settings are only supported on iOS devices; they are ignored by all other devices.

To configure a Web clip setting, go to **Onboard > Configuration > iOS Settings**. Either click an existing Web clip setting's name in the list; or click **Add New**, select **Web Clip Settings** in the **Settings Type** drop-down list, and click **Create**. The **Web Clip Settings** form opens.

Figure 143 *The Web Clip Settings Form*

Web Clip Settings	
* Name:	<input type="text" value="Example Web Clip"/> <small>Enter a name for the web clip.</small>
Description:	<input type="text"/> <small>Enter a description for the web clip.</small>
Web Clip Settings	
Icon:	
* URL:	<input type="text" value="http://www.youtube.com/watch?v=nhQz2eWYFI4"/> <small>The URL to be displayed when selecting the web clip.</small>
Removable:	<input checked="" type="checkbox"/> User can remove the web clip
Choose New Icon:	<input type="checkbox"/> Specify an icon for the web clip <small>If no icon is assigned to the web clip, a white square will be shown to the user.</small>
<input type="button" value="Save Changes"/>	

Table 79: Web Clip Settings Form

Field	Description
Name	(Required) Short name that identifies the Web clip clearly. Web clip names can include spaces. If you are duplicating a Web clip, the original name has "Copy" appended to it. You may highlight this name and replace it with a new name.
Description	Brief Description of the characteristics of the Web clip.
Icon	If an icon was uploaded through Configuration > Content Manager , it is displayed in this field.
URL	The URL of the Web clip.
Removable	If selected, the user can remove the Web clip.
Choose New Icon	If selected, you can specify an icon for the Web clip. The form expands to include the Custom Icon field.
Custom Icon	If icon files have been uploaded in Content Manager, they are displayed in the Custom Icon field. Highlight the icon to be used. If no images are displayed, upload your icon image or images to Content Manager, then return to this form. If no icon is assigned to the Web clip, a white square is shown to the user.
Save Changes	Saves your changes. The Web clip is available as a configuration unit on the Configuration Profile form.

For more information about configuration profiles, see ["Configuration Profiles" on page 216](#)

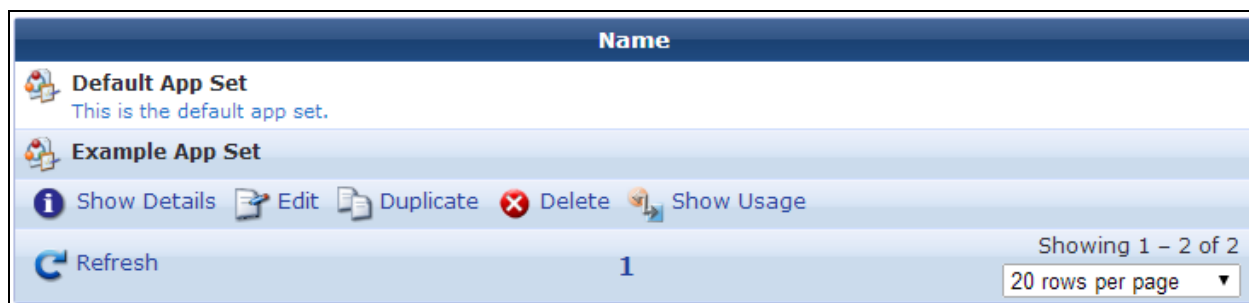
Windows Applications



Application sets let you specify either individual apps or groups of apps that should be installed during device provisioning, and indicate whether they should be restarted when the device is provisioned. After you define each of the sets you wish to use, you can include them in configuration profiles. The configuration profiles are available in the **Provisioning Settings** form, and can be associated with a device provisioning configuration set.

To create and work with Windows application sets, go to **Onboard > Configuration > Windows Applications**. The **App Sets** list view opens.

Figure 144 *The App Sets List View*



All Windows application sets that have been configured are included in the list. Each set's name is shown in the list. You can click a Windows application set's row in the list for additional options.

Table 80: The Windows App Set List

Field	Description
Show Details	Displays details for the Windows application set. The form expands to show its name, description, and configuration values.
Edit	Edit the Windows application set's configuration. The App Set form opens.
Duplicate	Creates a copy of a Windows application set to use as a basis for a new set. The App Set form opens with all attributes prepopulated and "Copy" appended to its name. You can rename the new app set, and edit any of its attributes.
Delete	Deletes the Windows application set. You will be asked to confirm the deletion.
Show Usage	Displays a list of configuration profiles that use the Windows application set.
Create new app set	To create a new Windows application set, click this link above the table. The App Set configuration form opens.

For information on configuring a Windows app set, see ["Configuring App Sets" on page 215](#).

Configuring App Sets

Windows app sets you define let you specify an app or group of apps to be installed during device provisioning, and whether an app requires the device to be restarted after provisioning.

To configure an app set, go to **Onboard > Configuration > Windows Applications**, and then either click the **Edit** link for an app set in the list, or click the **Create new app set** link in the upper-right corner. The **App Set** form opens.

Figure 145 *The App Set Form*

App Set

* Name:
Enter a name for the app set.

Description:
Enter a description for the app set.

Windows Applications
Options for installing applications on Windows devices. Applications may be uploaded using Content Manager.

Installers:	Application Installer	Install	Restart
	ClearPassOnGuardInstall.exe ClearPass OnGuard installer for Windows	<input type="checkbox"/> Install application	<input type="checkbox"/> Requires restart

Select the applications that are to be installed when a Windows device is provisioned.

Table 81: App Set Form

Field	Description
Name	Short name that identifies the app set clearly. App set names can include spaces. If you are duplicating an app set, the original name has "Copy" appended to it. You may highlight this name and replace it with a new name.
Description	Brief description of the characteristics of the app set.
Installers	Apps you have downloaded to Content Manager are listed in this field. <ul style="list-style-type: none">To specify that an app should be installed during provisioning, mark its Install application check box.To specify that the device needs to be restarted after the app is installed, mark its Requires restart check box.
Save Changes	Saves your changes. The app set is available as a configuration unit on the Configuration Profile form.

To add or manage apps in Content Manager, click the **Content Manager** link above the form. You can download apps to your system as content items, then upload them to Content Manager.

For more information about configuration profiles, see ["Configuration Profiles" on page 216](#)

Deployment and Provisioning



Onboard lets you configure deployment and provisioning settings. Configuration profiles let you define the profile settings that will be provisioned to devices, including configuration units. Provisioning settings let you define the settings for device provisioning. The configuration profiles are available in the Provisioning Settings form.

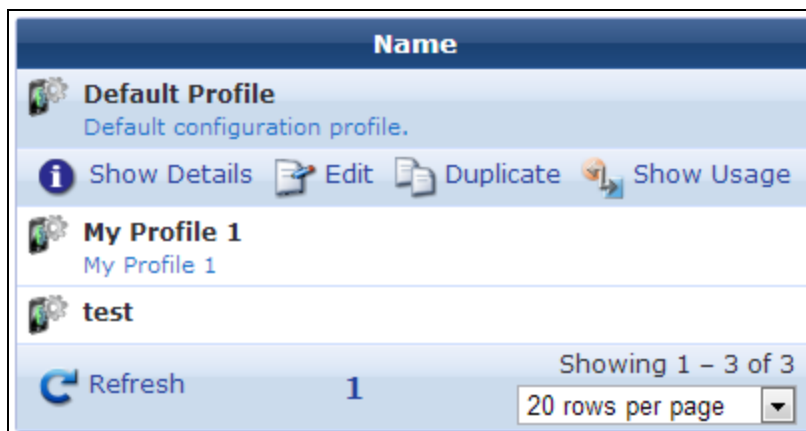
- To create and manage configuration profiles, see ["Configuration Profiles" on page 216](#)
- To create and manage provisioning settings, see ["Provisioning Settings" on page 220](#)

Configuration Profiles



Onboard lets you create and manage multiple configuration profiles to choose from for your captive portal pages. To manage the configuration profiles that will be provisioned to onboarded devices, go to **Onboard > Deployment and Provisioning > Configuration Profiles**. The **Configuration Profiles** list view opens.

Figure 146 *The Configuration Profile List View*



All configuration profiles that have been created are included in the list. You can click a profile's row in the list for additional options.

Table 82: *Configuration Profiles*

Field	Description
Show Details	Displays details of the configuration profile: The device's name and description, a list of the configuration units that will be provisioned to it, and a list of supervised devices. For information on configuration units, see "Onboard Configuration" on page 163.
Edit	Opens the Configuration Profile form, where you can edit any of the configuration profile's attributes.
Duplicate	Creates a copy of the configuration profile to use as a basis for a new profile. The Configuration Profile form opens with all attributes prepopulated and a number appended to the profile's name. You can rename the new profile, and edit any of its attributes.
Delete	Deletes the configuration profile. You will be asked to confirm the deletion. This option is not available for the default profile or for configuration profiles that are currently used for device provisioning.
Show Usage	Displays a list of the provisioning settings that use the configuration profile. For more information, see "Provisioning Settings" on page 220.
Create new configuration profile	Opens the Configuration Profile form, where you can create a new configuration profile.

For information on creating, editing, or duplicating a configuration profile, see ["Creating and Editing Configuration Profiles"](#) on page 217.

Creating and Editing Configuration Profiles

To create or edit a configuration profile, go to **Onboard > Deployment and Provisioning > Configuration Profiles**, and then either click the **Create new configuration profile** link or click the **Edit** or **Duplicate** link for a profile in the list. The **Configuration Profile** form opens.

Figure 147 The Configuration Profile Form

Profile	
* Name:	<input type="text" value="Default Profile"/> Enter a name for the profile.
Description:	<div style="border: 1px solid #ccc; padding: 5px; min-height: 80px;">Default configuration profile.</div> Enter a description for the profile.
AirPlay:	<input type="text" value="None"/> ▾ Choose the AirPlay settings to include in the profile.
AirPrint:	<input type="text" value="None"/> ▾ Choose the AirPrint settings to include in the profile.
Access Point Name (APN):	<input type="text" value="None"/> ▾ Choose the APN settings to include in the profile.
App Set:	<input type="text" value="Default App Set"/> ▾ Choose the app set to include in the profile.
Calendar:	<input type="text" value="None"/> ▾ Choose the calendar settings to include in the profile.
Contacts:	<input type="text" value="None"/> ▾ Choose the contacts settings to include in the profile.
Device Restrictions:	<input type="text" value="None"/> ▾ Choose the device restrictions settings to include in the profile.
Email:	<input type="text" value="None"/> ▾ Choose the email settings to include in the profile.
Exchange ActiveSync:	<input type="text" value="None"/> ▾ Choose the ActiveSync settings to include in the profile.
Networks:	<input checked="" type="checkbox"/> Example Network Choose the networks to include in the profile.
Passcode Policy:	<input type="text" value="None"/> ▾ Choose the passcode policy to include in the profile.
Subscribed Calendar:	<input type="text" value="None"/> ▾ Choose the calendar subscription settings to include in the profile.
VPN Settings:	<input type="text" value="None"/> ▾ Choose the VPN configuration to include in the profile.
Web Clips:	<u>(no items)</u> Choose the web clips to include in the profile.

Table 83: Configuration Profile Form

Field	Description
Name	(Required) Short name that identifies the configuration profile clearly. Configuration profile names can include spaces. If you are duplicating a profile, the original name has a number appended to it. You may highlight this name and replace it with a new name.
Description	Brief description of the characteristics of the profile.
AirPlay	Specifies AirPlay settings to include in the profile. AirPlay settings in this list were created on the Onboard > Configuration > iOS Settings > AirPlay Settings form. For more information, see " Configuring AirPlay Settings " on page 181.
AirPrint	Specifies AirPrint settings to include in the profile. AirPrint settings in this list were created on the Onboard > Configuration > iOS Settings > AirPrint Settings form. For more information, see " Configuring AirPrint Settings " on page 183.
Access Point Name (APN)	Specifies APN settings to include in the profile. APN settings in this list were created on the Onboard > Configuration > iOS Settings > APN Settings form. For more information, see " Configuring APN Settings " on page 184.
App Set	Specifies app sets to included in the profile. App sets in this list were created on the Onboard > Configuration > Windows Applications form. For more information, see " Configuring App Sets " on page 215.
Calendar	Specifies calendar sets to include in the profile. Calendar sets in this list were created on the Onboard > Configuration > iOS Settings > Calendar Settings form. For more information, see " Configuring Calendar (CalDAV) Settings " on page 185.
Contacts	Specifies contacts settings to include in the profile. Contacts settings in this list were created on the Onboard > Configuration > iOS Settings > Contacts Settings form. For more information, see " Configuring Contacts (CardDAV) Settings " on page 187.
Device Restrictions	Specifies device restrictions settings to include in the profile. Device restrictions settings in this list were created on the Onboard > Configuration > iOS Settings > Device Restrictions Settings form. For more information, see " Configuring Device Restrictions Settings " on page 189.
Email	Specifies email settings to include in the profile. Email settings in this list were created on the Onboard > Configuration > iOS Settings > Email Settings form. For more information, see " Configuring Email Settings " on page 197.
Exchange ActiveSync	Specifies Exchange ActiveSync settings to include in the profile. ActiveSync configuration settings in this list were created on the Onboard > Configuration > iOS Settings > Exchange ActiveSync Settings form. For more information, see " Configuring ActiveSync Settings " on page 178.
Networks	Specifies networks to include in the profile. Select the check box of each network to include. Networks available here were created on the Onboard > Configuration > Network Settings form. For more information, see " Configuring Basic Network Access Settings " on page 164 and the related topics for the form.
Passcode Policy	Specifies passcode policy settings to include in the profile. Passcode policy settings in this list were created on the Onboard > Configuration > iOS Settings > Passcode Policy Settings form. For more information, see " Configuring an iOS Device Passcode Policy " on page 200.
Subscribed Calendar	Specifies calendar subscription settings to include in the profile. Calendar subscription settings in this list were created on the Onboard > Configuration > iOS Settings > Calendar Subscription Settings form. For more information, see " Configuring Calendar "

Field	Description
	Subscription Settings" on page 203.
VPN Settings	Specifies VPN settings to include in the profile. VPN settings in this list were created on the Onboard > Configuration > iOS Settings > VPN Settings form. For more information, see "Configuring an iOS Device VPN Connection" on page 204.
Web Clips	Specifies Web clip settings to include in the profile. This drop-down list is only available if you have defined Web clip settings on the Onboard > Configuration > iOS Settings > Web Clip Settings form. For more information, see "Configuring Web Clips" on page 213.

When you have completed your changes on this form, click **Save Changes**, the configuration profile is included in the **Configuration Profile** drop-down list on the **Provisioning Settings** form and can be associated with a device provisioning configuration set.








Provisioning Settings



The Provisioning Settings page lists all your device provisioning configuration settings, and lets you define multiple device provisioning configurations for Onboard captive portal pages. You can assign different network settings to each of them. You can also choose from a variety of configuration profiles you have already defined, such as application sets, ActiveSync settings, passcode policies, or VPN settings.

To view the list of device provisioning configuration sets and work with them, go to **Onboard > Deployment and Provisioning > Provisioning Settings**. The **Provisioning Settings** list view opens. All device provisioning configuration settings that have been created are included in the list. Information shown for each setting includes its name, Certificate Authority (CA), and the configuration profile assigned to it.

Figure 148 *The Provisioning Settings List View*

Name	CA	Profile
 Local Device Provisioning This is the default configuration set for device provisioning.	Local Certificate Authority	Default Profile
 Show Details  Edit  Duplicate  Delete  Test		
 Refresh 1 Showing 1 - 1 of 1		
20 rows per page 		



You can click a provisioning setting's row in the list for additional options:

Table 84: Provisioning Settings List View








Field	Description
Show Details	Displays details of the provisioning setting. The form expands to show a summary of the settings defined for it, including information for identity, authorization, supported devices, Web login page, device provisioning, profile signing, and reconnect behavior.
Edit	Opens the Device Provisioning Settings form. You can edit any of the provisioning setting's attributes.
Duplicate	Creates a copy of the provisioning setting to use as a basis for a new configuration. The Device Provisioning Settings form opens with all attributes prepopulated and "Copy" appended to its name. You can rename the new configuration, and edit any of its attributes.
Delete	Deletes the provisioning set. You will be asked to confirm the deletion.
Test	<p>To view and test a device provisioning Web login page, this link opens the page in a new tab as it would appear to a user. The default login page includes the username and password fields. If you have configured sponsorship confirmation, it will also include the sponsor's email field:</p> <div data-bbox="414 714 1490 1297" style="border: 1px solid black; padding: 10px;"> <p>Please login to the network using your ClearPass username and password.</p> <div style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <div style="background-color: #003366; color: white; text-align: center; padding: 5px;">Login</div> <div style="display: flex; justify-content: space-between; margin-top: 5px;"> <div style="width: 60%;">* Username:</div> <input style="width: 35%; border: 1px solid #ccc;" type="text"/> </div> <div style="display: flex; justify-content: space-between; margin-top: 5px;"> <div style="width: 60%;">* Password:</div> <input style="width: 35%; border: 1px solid #ccc;" type="password"/> </div> <div style="text-align: center; margin-top: 10px;"> <input style="background-color: #003366; color: white; padding: 5px 15px; border: none;" type="button" value="Log In"/> </div> </div> <p>* required field</p> <p>Contact a staff member if you are experiencing difficulty logging in.</p> </div>
Create new provisioning settings	Opens the Device Provisioning Settings form, where you can create a new provisioning set.

For information on creating, editing, or duplicating a configuration profile, see "About Configuring Provisioning Settings " on page 221.

About Configuring Provisioning Settings

On the **Onboard > Deployment and Provisioning > Provisioning Settings** list view, to modify a provisioning set for Onboard captive portal pages, click its  **Edit** link. To create a new provisioning set, click the  **Create new provisioning settings** link. The **Device Provisioning Settings** form opens with the **General** tab displayed.

The configuration process is the same for editing an existing provisioning set and for creating a new set. The **Device Provisioning Settings** form is divided into several tabs:

Tab	Description
 General	Specifies basic provisioning settings such as information about identity settings, authorization, and actions. See "Configuring General Provisioning Settings" on page 222.
 Supported Devices	Lets you specify the supported operating systems for which devices may be enabled for provisioning, and specify some OS-specific or Web-based information. See "Configuring Provisioning Settings for Supported Devices" on page 227.
 Web Login	Specifies options for the Web login captive portal page such as the page name, redirect, authentication, labels and messages, skin, header and footer HTML, Social Logins configuration, and access control. See "Configuring Provisioning Settings for the Web Login Page" on page 229.
 Instructions & Messages	Specifies text for labels and messages shown before, during, and after provisioning. It includes general messages as well as sections for messages specific to each operating system. See "Configuring Provisioning Settings for Instructions and Messages" on page 238
 iOS/OS X Profile	Specifies options for Apple iOS and OS X device provisioning such as display text, profile security, and certificate source. See "Configuring Provisioning Settings for iOS and OS X Profiles" on page 259.
 Onboard Client	Specifies options for Windows, Android, and legacy OS X (10.5/6) device provisioning such as provisioning address and access, certificate validation, logo, and support information. See "Configuring Options for Onboard Client Devices" on page 261.
 Sponsorship Confirmation	Specifies sponsor confirmation and authentication, sponsor email configuration, and UI overrides. See "Configuring Provisioning Settings for Sponsorship Confirmation" on page 265"Configuring Provisioning Settings for Sponsorship Confirmation" on page 265.

Configuring General Provisioning Settings

To configure basic provisioning settings, go to **Onboard > Deployment and Provisioning > Provisioning Settings**. The **Provisioning Settings** list opens. Either click the **Edit** link for a configuration set in the list, or click the **Create new provisioning settings** link to open the **Provisioning Settings** configuration form. This form has several tabs. The first tab that opens is the **General** tab, and is used to specify basic information about Onboard provisioning.

Figure 149 *The General Tab, Device Provisioning Settings Form*



The screenshot shows the "Device Provisioning Settings" form with the "General" tab selected. The form contains the following fields:

- * Name:** A text input field containing "Local Device Provisioning". Below the field is the instruction: "Enter a name for this configuration set."
- Description:** A text area containing "This is the default configuration set for device provisioning." Below the text area is the instruction: "Enter a description for the configuration set."
- * Organization:** A text input field containing "Example Organization". Below the field is the instruction: "Enter an organization name for this configuration set. The organization name is displayed by the device during provisioning."

The top of the form has a navigation bar with tabs for: General, Supported Devices, Web Login, Instructions & Messages, iOS/OS X Profile, Onboard Client, and Sponsorship Confirmation #.

Table 85: Provisioning Settings, General Tab, Basic Information Area

Field	Description
Name	(Required) Name of this configuration set. This name is used internally to identify this set of Onboard settings for the network administrator. This value is never displayed to the user during device provisioning.
Description	Brief description of this configuration set. This description is used internally to identify this set of Onboard settings for the network administrator. This value is never displayed to the user during device provisioning.
Organization	(Required) The name of your organization. This is displayed to the user during the device provisioning process.

Figure 150 The Provisioning Settings Form, General Tab, Identity and Authorization Areas

Identity

These options control the generation of device credentials.

- * Certificate Authority: Local Certificate Authority ▼
Select the certificate authority that will be used to sign profiles and messages.
- * Signer: Onboard Certificate Authority ▼
Select the source that will be used to sign TLS client certificates.
- * TLS Certificate Authority: Local Certificate Authority ▼
Select the certificate authority that will be used to sign TLS client certificates.
- * Key Type: 2048-bit RSA - created by device ▼
Select the type of private key to use for TLS certificates.
- * Unique Device Credentials: Include the username in unique device credentials
When checked, the username is prefixed to the device's PEAP credentials. This unique set of credentials is used to identify the user and device on the network.

Authorization

These options control how a device is authorized during provisioning.

- * Authorization Method: App Authentication — check using Aruba Application Authentication ▼
Select the method used to authorize devices.
- Use SSO: Single Sign-On – Enable SSO for device provisioning
If enabled then users will be required to authenticate via SSO
- * Configuration Profile: Default Profile ▼
Select the configuration profile that will be provisioned to devices.
- * Maximum Devices: 0
The maximum number of devices that a user may provision. Use 0 for unlimited.



If you use Active Directory Certificate Services (ADCS), you might need to add your ADCS certificate to the Trust List. When connecting to ADCS to issue an Onboard certificate, the server certificate is verified against the ClearPass Trust List.

Table 86: Provisioning Settings Form, General Tab, Identity Area

Field	Description
Certificate Authority	(Required) Specifies the Certificate Authority (CA) used to sign profiles and messages (see "Creating a New Certificate Authority" on page 117). Options include: <ul style="list-style-type: none"> ● Local Certificate Authority ● SCEP-RA
Signer	(Required) Specifies the source to use for signing TLS client certificates. Options include: <ul style="list-style-type: none"> ● Onboard Certificate Authority ● Active Directory Certificate Services — The ADCS URL and ADCS Template rows are added to the form. ACDS can only be used with certificate-based authentication; it cannot be used with username/password authentication.
TLS Certificate Authority	(Required) Specifies the Certificate Authority (CA) used to use to sign TLS client certificates. Options include: <ul style="list-style-type: none"> ● Local Certificate Authority ● SCEP-RA
ADCS URL	(Required) If Active Directory Certificate Services was chosen in the Signer field, enter the URL of the ADCS server in the field. This URL should be the Web interface for ADCS, and is typically http://<server>/certsrv/ .
ADCS Template	(Required) If Active Directory Certificate Services was chosen in the Signer field, enter the name of the template to use when requesting the certificate. If the name is not known, you can use the default name of "user".
Key Type	(Required) Specifies the type of private key to use when issuing a new certificate. Options include: <ul style="list-style-type: none"> ● 1024-bit RSA – created by server: Lower security. ● 1024-bit RSA – created by device: Lower security. Uses SCEP to provision the EAP-TLS certificate. ● 2048-bit RSA – created by server: Recommended for general use. ● 2048-bit RSA – created by device: Recommended for general use. Uses SCEP to provision the EAP-TLS certificate. ● 4096-bit RSA – created by server: Higher security. ● X9.62/SECG curve over a 256 bit prime field - created by server ● NIST/SECG curve over a 384 bit prime field - created by server See Note below this table.
Unique Device Credentials	(Required) If selected, includes the username as a prefix in the device's PEAP credentials.

Using a private key containing more bits will increase security, but will also increase the processing time required to create the certificate and authenticate the device. The additional processing required will also affect the battery life of a mobile device. It is recommended to use the smallest private key size that is feasible for your organization. The "created by device" options use SCEP to provision the EAP-TLS device certificate, so the private key is known only to the device rather than also known by the user. When a "created by device" option is selected, the generated key is used instead of a username/password authentication defined in Network Settings.



Table 87: Provisioning Settings Form, General Tab, Authorization Area

Field	Description
Authorization Method	Specifies the authorization method for devices. Options include: <ul style="list-style-type: none"> ● App Auth – check using Aruba Application Authentication ● RADIUS – check using a RADIUS request
Use SSO	If selected, users will be required to authenticate using Single Sign-On (SSO). (SSO support is enabled at Policy Manager > Configuration > Identity > Single Sign-On.)
Configuration Profile	(Required) Specifies the configuration profile to provision to devices. All configuration profiles that have been created are included in this list. A configuration profile specifies an application set, Exchange ActiveSync settings, network settings, passcode policy, VPN, and other settings. For more information, see "Onboard Configuration" on page 163.
Maximum Devices	(Required) Enter a number to specify the maximum number of devices that each user may provision. To be enrolled, a device must have a currently valid certificate, and its status set to Allowed (at Onboard > Management and Control > View by Device).

Figure 151 The Provisioning Settings Form, General Tab, Actions Area

Actions
These options control actions that may be taken after device provisioning.

Certificate Expiry:	<input checked="" type="checkbox"/> Notify users before their device credentials expire <small>If checked users will receive an email notification when their device's network credentials are due to expire.</small>
* Send Email Notification:	4 weeks prior to expiration ▾ <small>Select the time to send an email notification.</small>
* If Email is Unknown:	Do not send any message ▾ <small>Specify where to send emails to if the user's certificate doesn't have an email address recorded.</small>
* Subject Line:	Your network credentials are about to expire <small>Enter a subject for the notification email.</small>
* Email Message:	Certificate Expiry ▾ <small>The plain text or HTML print template to use when generating an email message.</small>
* Email Skin:	(Use Default: Use the default skin) ▾ <small>The format in which to send email receipts.</small>
* Send Copies:	Do not send copies ▾ <small>Specify when to send to the recipients in the Copies To list.</small>
Revoke Inactive:	<input checked="" type="checkbox"/> Revoke certificates for inactive devices <small>If checked the certificates for devices will be revoked after a period where the device is not seen on the network.</small>
	This feature relies on data from ClearPass Insight. You must have an Insight master node enabled and with an appropriate data retention period configured for inactivity calculations to work correctly.
* Inactivity Period:	30 days <small>If a device does not authenticate on the network after this period its certificate will be revoked.</small>
Delete Duplicates:	<input checked="" type="checkbox"/> Delete duplicate certificates for devices <small>If checked then old certificates from previous enrollments of a device will be automatically deleted.</small>
* Deletion Delay:	30 days <small>Any duplicate certificates will be deleted after the specified number of days have passed since re-enrollment.</small>

Next
Save Changes
Cancel

Table 88: Provisioning Settings Form, General Tab, Actions Area

Field	Description
Certificate Expiry	Specifies that users will receive an email notification when their device's network credentials are about to expire. The form expands to include options for configuring the notification email.
Send Email Notification	(Required) Specifies when to send the notification email. Options include: <ul style="list-style-type: none"> • 1 week prior to expiration • 2 weeks prior to expiration • 3 weeks prior to expiration • 4 weeks prior to expiration
If Email is Unknown	(Required) Specifies action to take if the user's email address is not recorded with the certificate. Options include: <ul style="list-style-type: none"> • Do not send any message • Send a message to a fixed email address • Send a message to username@domain
Unknown Address	Address to use when no email address is known for the user.
Unknown Domain	Domain to append to the username to form an email address.
Subject Line	(Required) Subject line for the notification email.
Email Message	(Required) Plain text or HTML print template to use when generating the email message. Options include: <ul style="list-style-type: none"> • Account List • Certificate Expiry • Download Receipt • GuestManager Receipt • One account per page • SMS Receipt • Sponsorship Confirmation • Two-column scratch cards
Email Skin	(Required) Format to use for email receipts. Options include: <ul style="list-style-type: none"> • Use the default skin • No skin - Plain text only • No skin - HTML only • No skin - Native receipt format • Aruba ClearPass Skin • Blank Skin • ClearPass Guest Skin • Custom Skin 1 • Custom Skin 2 • Galleria Skin • Galleria Skin 2
Send Copies	(Required) Specifies how to send copies to the recipients in the Copies To list. Options include: <ul style="list-style-type: none"> • Do not send copies • Always send using "cc:"

Field	Description
	<ul style="list-style-type: none"> Always send using "Bcc:"
Revoke Inactive	If selected, certificates for devices are revoked after a specified amount of time that the device is not seen on the network. You must have an Insight master node enabled with an appropriate data retention period configured.
Inactivity Period	(Required) Number of days that a device should be absent from the network before its certificate is revoked.
Delete Duplicates	If selected, old certificates from previous enrollments are automatically deleted.
Deletion Delay	(Required) Number of days that should pass after re-enrollment before old (duplicate) certificates are deleted.
Provisioning Address	Hostname or IP address to use for device provisioning.

Click **Next** to proceed to the next tab, or **Save Changes** to complete your edits.

To return to the list of links to all Provisioning Settings tabs, see ["About Configuring Provisioning Settings" on page 221](#).

Configuring Provisioning Settings for Supported Devices

To configure which operating systems to support for device provisioning, and to specify some OS-specific or Web-based information, go to **Onboard > Deployment and Provisioning > Provisioning Settings**, expand the provisioning setting's row in the list, and click its **Edit** link. In the **Device Provisioning Settings** form, click the **Supported Devices** tab.

When you enable a device operating system on the **Supported Devices** tab, fields are added for it on the **Instructions & Messages** tab. You cannot configure instructions or instructions for a device type until it is enabled on the **Supported Devices** tab.

Table 89: *Provisioning Settings, Supported Devices Configuration*

Field	Description
Android Provisioning Area	
Android Devices	If selected, enables Android devices for provisioning. An Android application is downloaded and executed on the user's device to complete provisioning.
Android Rootkit Detection	Specifies whether Android devices with a rootkit may be provisioned. Options include: <ul style="list-style-type: none"> Provision all devices— All Android devices will be provisioned. Do not provision rooted devices—Onboard will detect a jailbroken Android device and will not provision the device if it has been compromised.
Android Browser Check	If selected, forces Android users to provision with the default browser (Chrome). A warning message is displayed if a non-default browser is detected.
Chromebook Provisioning Area	
Chromebook Devices	If selected, enables Chromebook devices for provisioning. A certificate is provided to Chromebook devices. The device must be under management and the QuickConnect extension must be configured for pre-installation.

Table 89: Provisioning Settings, Supported Devices Configuration(Continued)

Field	Description
Setup Instructions	You must configure the Chromebook extension in the Google admin console. Go to Device Management > Chrome > User Settings and configure Pre-installed Apps and Extensions . Search for ClearPass Onboard in the Chrome Web Store and add it to the pre-installation list.
Chromebook Token	Specifies the hardware token to store the certificates against. Options include: <ul style="list-style-type: none"> • User-Specific • System-Wide
iOS Provisioning Area	
iOS Devices	If selected, enables iOS devices for provisioning. The iOS devices are provisioned by Apple's "Over-the-Air" profile delivery process.
iOS Browser Check	If selected, forces iOS users to use the default browser (Safari). A warning message is displayed if a non-default browser is detected.
OS X Provisioning Area	
OS X Devices	If selected, enables OS X 10.7+ (Lion or later) devices for provisioning. The OS X devices are provisioned by Apple's "Over-the-Air" profile delivery process.
Profile Type	Specifies the type of profile to create when provisioning OS X 10.7+ (Lion or later) devices. Options include: <ul style="list-style-type: none"> • User • System
Legacy OS X Provisioning Area	
OS X 10.5/6 Devices	If selected, enables OS X 10.5 (Leopard) and 10.6 (Snow Leopard) devices for provisioning. An OS X application is downloaded and executed on the user's device to complete provisioning.
Ubuntu Provisioning Area	
Ubuntu Devices	If selected, enables Ubuntu devices for provisioning. An Ubuntu application is downloaded and executed on the user's device to complete provisioning.
Windows Provisioning Area	
Windows Devices	If selected, enables Windows devices for provisioning. A Windows application is downloaded and executed on the user's device to complete provisioning.
Web-Based Provisioning Area	
Web-Based Devices	If selected, enables Web-based devices for provisioning. A certificate is generated for manual installation on devices for which there is no Onboard client support.
Override Device Type Detection Area	
Detection Override	Specifies whether users can override browser device detection. In cases where a non-default browser is used and the operating system can't be detected, this option allows users to identify their operating system in a drop-down list.

Click **Next** to proceed to the next tab, or **Save Changes** to complete your edits.

To return to the list of links to all **Provisioning Settings** tabs, see "About Configuring Provisioning Settings " on page 221.

Configuring Provisioning Settings for the Web Login Page

Onboard creates a default Web login page that is used to start the device provisioning process. You can configure options such as the page name, redirect, authentication, labels and messages, skin, header and footer HTML, social logins configuration, and access control.

To configure the Web login captive portal page, go to **Onboard > Deployment and Provisioning > Provisioning Settings**, expand the provisioning setting's row in the list, and click its **Edit** link. In the **Provisioning Settings** form, click the **Web Login** tab.

Basic and Login Form Areas

Figure 152 The Provisioning Settings Form, Web Login Tab, Basic and Login Form Areas

Table 90: Provisioning Settings Form, Web Login Tab, Basic and Login Form Areas

Field	Description
Page Name	(Required) The page name (filename) for the Web login page. This will be part of the URL for accessing the page — for example, "/guest/page_name.php".
Page Redirect Area	
Security Hash	Specifies the level of checking to apply to URL parameters passed to the Web login page. Use a security hash to detect when URL parameters such as the MAC address have been modified by the user. Security hash is not supported by all vendors. Options include: <ul style="list-style-type: none"> ● Do not check - login will always be permitted ● Permit login on validation error - validation errors will be logged ● Deny login on validation error - login will not be permitted

Table 90: Provisioning Settings Form, Web Login Tab, Basic and Login Form Areas(Continued)

Field	Description
URL Hash Key	(Required) The shared secret (64 characters) used by ClearPass and the NAD for the hash key to validate the redirect URL. This must be entered twice in order to verify the key.
Confirm Key	
Login Form Area	
Authentication	<p>Specifies the authentication requirement. Options include:</p> <ul style="list-style-type: none"> • Credentials - Require a username and password • Access Code - Only require username for authentication — Requires a single code (username) to be entered, and requires the account to have the Username Authentication field set. • Anonymous - Do not require a username or password — Allows a blank form requiring just the terms or a Log In button. Requires a pre-existing account, and requires the account to have the Username Authentication field set. • Auto - Do not require a username or password and automatically submit the page — Similar to Anonymous, but the page is automatically submitted.
Auto-Generate	If selected, auto-generates the anonymous account. The account is created without a session limit or expiration time, and with the Guest role (ID 2).
Anonymous User	(Required) Account to use for anonymous authentication. The password will be visible in the HTML. The account Session Limit should be increased to the number of guests to be supported. To use a specific username, enter it in this field. To randomly generate a user name, leave this field blank.
Prevent CNA	If selected, enables bypassing the Apple Captive Network Assistant (CNA). The CNA is the pop-up browser shown when joining a network that has a captive portal. This option might not work with all vendors; it depends on how the captive portal is implemented.
Custom Form	If selected, you must provide your own HTML login form in the header and footer areas.
Custom Labels	If selected, allows you to modify the login form's labels and error messages. The form expands to include the Username Label , Password Label , and Log In Label fields. Complete these fields with your customized label text.
Terms	If selected, forces the user to accept a "Terms and Conditions" statement. The form expands to include the Terms Label , Terms Text , Terms Layout , and Terms Error fields. Complete these fields with your customized values.
Custom Fields	<p>You can click in this field to open a drop-down list where you can select additional fields to be displayed on the login form. The values entered in these fields will be added to the subject alt-name of the client's certificate.</p> <p>To configure sponsorship confirmation in order for a user to enroll their device, select Sponsor's Email: (sponsor_email) in this list, and then complete the Sponsorship Confirmation tab.</p>

Login Page Area

Figure 153 *The Provisioning Settings Form, Web Login Tab, Login Page Area*

Login Page	
Options for controlling the look and feel of the login page.	
* Skin:	<input type="text" value="(Default)"/> Choose the skin to use when this web login page is displayed.
Title:	<input type="text" value="Register Your Device"/> The title to display on the web login page.
Header HTML:	<pre>{\$pre_login_instructions} {nwa_cookiecheck} {* Onboard instructions can be edited on a per device type basis under Onboard Provisioning Settings *}</pre> <input type="text" value="Insert content item..."/> <input type="text" value="Insert self-registration link..."/> HTML template code displayed before the login form.
Footer HTML:	<pre>{nwa_text id=7979}<p> Contact a staff member if you are experiencing difficulty logging in. </p>{/nwa_text}</pre> <input type="text" value="Insert content item..."/> <input type="text" value="Insert self-registration link..."/> HTML template code displayed after the login form.

Table 91: *Provisioning Settings Form, Web Login Tab, Login Page Area*

Field	Description
Skin	(Required) Specifies the skin to use for the Web login page. Options include: <ul style="list-style-type: none"> • (Default) • Aruba ClearPass Skin • Blank Skin • ClearPass Guest Skin • Custom Skin 1 • Custom Skin 2 • Galleria Skin • Galleria Skin 2
Title	Title that will be displayed on the Web login page.
Header HTML	Default text for the header and footer is shown in these fields and may be edited. You can also use the drop-down lists in these fields to add images or other content items or to insert a self-registration link.
Footer HTML	

Social Logins Area

Figure 154 The Provisioning Settings Form, Web Login Tab, Social Logins Area: Enabling Social Logins

Social Logins
Optionally present guests with various social login options.

Social Login: Enable login with social network credentials

Add new authentication provider

Use the form below to add an authentication provider to this login.

Properties

* Provider:	Facebook
Enabled:	<input checked="" type="checkbox"/>
* Client ID:	37Signals (Basecamp)
* Client Secret:	Amazon
Advanced:	Bitbucket
Endpoint Attributes:	Bitly
Provider Specific	Box
Email:	Buffer
Friends:	Clever
	Copy
	Dailymotion
	Discogs
	Disqus
	Dropbox
	Dropbox OAuth V2
	Etsy
	Eventful
	Facebook
	Facebook WiFi
	Fitbit
	Flickr

* required field

Provider	Client ID
There are no authentication providers defined.	

Buttons:
Refer to the help for more details.

Debug: Log debugging data

Table 92: Provisioning Settings Form, Web Login Tab, Social Logins Area: Enabling Social Logins

Field	Description
Social Login	If selected, enables the use of social network credentials to log in. The form expands to include Authentication Providers social login configuration options.
Authentication Providers	After you enable social logins, options in this area let you specify and configure the options for the social network provider.
Add new authentication provider	Opens the properties form for adding and configuring a social network provider.
Buttons	Shows the syntax for displaying social network login buttons on the page. You must add <code>{nwa_social_logins}</code> to either the HTML Header or HTML Footer area.
Debug	If selected, social logins debugging will be included in the application log.

Figure 155 The Provisioning Settings Form, Social Logins Area, Authentication Providers Area (Facebook selected as an example provider)

Authentication Providers:

Add new authentication provider

Use the form below to add an authentication provider to this login.

Properties	
* Provider:	Facebook ▼
Enabled:	<input checked="" type="checkbox"/> Use this provider
* Client ID:	<input type="text"/> <small>The Client ID associated to your provider. They may use a different label.</small>
* Client Secret:	<input type="text"/> <small>The Client Secret associated to your provider. They may use a different label.</small>
Advanced:	<input checked="" type="checkbox"/> Show advanced properties
Destination:	<input type="text"/> <small>Guests authenticating with this provider will be redirected to this URL after login.</small>
Auto Redirect:	<input type="checkbox"/> Automatically redirect the guest to this provider <small>Checking this box will remove the ability to support local logins, or any other providers. We recommend also enabling "Custom Form:" in the "Web Login" itself.</small>
Endpoint Attributes:	Do not create additional attributes ▼ <small>Creating attributes is only needed if you are creating specialized enforcement policies on them.</small>
Username Prefix:	<input type="text"/> <small>Prepend this text to all usernames. A prefix or suffix can be useful if you are providing a means to login using a variety of providers.</small>
Username Suffix:	<input type="text"/> <small>Append this text to all usernames.</small>
Icon Label:	<input type="text"/> <small>Override the default label on this provider's icon.</small>
Hostname:	<input type="text"/> <small>If specified, use this hostname when redirecting the user to authenticate. This is optional – leave blank if unsure.</small>
Notes:	<input style="width: 100%;" type="text"/> <small>Enter comments or notes about this provider. This description is only shown to administrators.</small>
Provider Specific Options	
Email:	<input type="checkbox"/> Request access to the guest's email address <small>Access requires an additional permission for this provider.</small>
Friends:	<input type="checkbox"/> Retrieve the guest's friends <small>Access requires an additional permission for this provider.</small>
<input type="button" value="Add"/> <input type="button" value="Cancel"/>	
* required field	
Provider	Client ID
i There are no authentication providers defined.	

Table 93: Provisioning Settings Form, Web Login Tab, Social Logins Area, Authentication Providers Area

Field	Description
Provider	(Required) Specifies the social network provider to use. All social network providers that have been configured are included in this list. The following options presented in the Authentication Providers area depend on the provider selected in this drop-down list.
Enabled	If this check box is selected, the specified provider can be used.
Admin SDK Refresh Token	(Required) (Google Apps) Valid Google API admin refresh token. To generate a new refresh token, clear this value. You will need to generate a new authorization code.

Field	Description
Advanced	If selected, displays additional options on this form.
Allow Guests	(Google Apps) If selected, allows Google accounts that are not part of your domain to log in as guests. The <code>social_vip</code> flag will be set to false for these users.
Authorization Code	(Required) (Google Apps) When you generate a new code, it is automatically entered in this field, and you can close the redirect window.
Auto Redirect	If selected, local logins and other providers will not be supported. If this option is selected, we recommend you also enable Custom Form in the Login Form area.
Client ID	(Required) Client ID to use with this provider. The provider might use a different label.
Client Secret	(Required) Client secret to use with this provider. The provider might use a different label.
Delete	Removes the provider from the list and deletes its configuration. You will be asked to confirm the deletion.
Destination	URL to which guests authenticating with this provider will be redirected after logging in.
Disable	Disables the provider. To enable it again, click the Enable link.
Disconnect Action	(Facebook WiFi) For the Facebook Wi-Fi provider, specifies the action to take when a disconnect is requested by Facebook. Options include: <ul style="list-style-type: none"> • Terminate Session • Cisco - Disable Host-Port • Cisco - Bounce-Host-Port • Cisco - Reauthenticate Session
District ID	(Clever) Identifier for the school district. During authentication, this ID is compared to the ID returned by a Clever Instant Login. If no value is entered in this field, Clever's District Picker will handle the details.
Edit	Opens the Properties form. You can edit any of the configuration options for the provider.
Email	If selected, allows access to the guest's email address. Access requires additional permission for the provider.
Endpoint Attributes	Specifies whether to create endpoint attributes, and how they will be handled. Options include: <ul style="list-style-type: none"> • Do not create additional attributes • Create Endpoint attributes converting any arrays to JSON • Create Endpoint attributes flattening the entire data set If one of the Create options is selected, an endpoint attribute is created for every attribute returned by the user. This is only needed if you are creating specialized enforcement policies on them.
Flatten Prefix	If Endpoint Attributes was selected, you may enter text to prepend to all keys when flattening. This stores a normalized version of all the returned attributes in the endpoint. If nothing is entered in this field, the default "social" will be used.
Friends	(Facebook) If selected, allows a list of the guest's friends to be retrieved, if permission is granted by the guest. The list is limited to only those friends who also use your application ID.
Generate Code	To generate a new authorization code, click the link in this field. You will be redirected to a new window to generate an authorization code.

Field	Description
Google Apps VIP	Name of the user record attribute to apply to the <code>social_vip</code> flag. For more information, refer to the Google Directory API for retrieving users.
Google Groups	(Google Apps) If selected, all groups associated with the account will be retrieved and stored as a list of group names and a list of matching email addresses. The Admin SDK Refresh Token and Authorization Code must also be regenerated.
Google Plus	(Google) if selected, allows access to the guest's Google Plus profile. Access requires additional permission for the provider.
Group Membership	(Microsoft Azure) If selected, all groups associated with the account will be retrieved and stored as a list of group names and a list of matching email addresses.
Hostname	If specified, overrides the hostname guests are redirected to for authentication. This field is optional; leave it empty if you are unsure.
Icon Label	Overrides the default label on the provider's icon.
LinkedIn VIP	(LinkedIn) Enter a LinkedIn Distance value (0 - 3). If the guest is within this distance, the <code>social_vip</code> flag will be enabled for them.
Move Up Move Down	Moves the provider up or down in the list.
Notes	You may enter additional notes or comments about the provider. This description is only seen by administrators.
Twitter VIP	(Twitter) Name of a Twitter account. If the guest follows this account, they will have the "social_vip" flag enabled.
Username Prefix	Text to prepend to all usernames. A prefix can be useful if you are providing a way to log in using a variety of providers.
Username Suffix	Text to append to all usernames. A suffix can be useful if you are providing a way to log in using a variety of providers.
VIP Attribute	(Google Apps; Microsoft Azure) Name of the user record attribute to apply to the <code>social_vip</code> flag. For more information, refer to the Microsoft Graph API for retrieving users.
Add	When your entries are complete on the Properties, form, click this button. The Properties form closes and the provider is included in the Authentication Providers list.

Multi-Factor Authentication Area

Options in the **Multi-Factor Authentication** area let you require a secondary factor when authenticating. When the guest enters their username to log in, they are sent a code which they must successfully retrieve and enter to complete the login. For more information, see ["About Multi-Factor Authentication" on page 412](#).

Figure 156 *The Provisioning Settings Form, Web Login Tab, Multi-Factor Authentication Area*

Multi-Factor Authentication	
Require a secondary factor when authenticating.	
Provider:	Duo Security - Two Factor Authentication ▼
Authentication Order:	Credentials and then device ▼
* Duo AKEY:	<input type="text"/> <small>Your akey is a string that you should generate and keep secret from Duo. It should be at least 40 characters long. Reference the Duo website for tips on generating this key.</small>
* Duo Integration Key:	<input type="text"/>
* Duo Secret Key:	<input type="text"/>
* Duo API Hostname:	<input type="text"/>
Header HTML:	<input type="text"/> Insert... <small>HTML template code displayed before the provider's vendor-specific authentication area.</small>
Footer HTML:	<input type="text"/> Insert... <small>HTML template code displayed after the provider's vendor-specific authentication area.</small>

Table 94: *Provisioning Settings Form, Web Login Tab, Multi-Factor Authentication Area*

Field	Description
Provider	Specifies the multi-factor authentication provider. Options include: <ul style="list-style-type: none"> • No multi-factor authentication • Duo Security - Two Factor Authentication • Facial Networks - ZOOM Multi-Factor Authentication • Kasada - authenticator • Kasada - authenticator (legacy) • ImageWare Systems - GoMobile Interactive • SMS Verification Codes
App Name	(Required) App name to use with this provider.
Authentication Order	Specifies the authentication order. Options include: <ul style="list-style-type: none"> • Credentials and then device • Device and then credentials
Client ID	(Required) Client ID to use for this provider.
Duo AKEY	(Required) A string that you should generate and keep secret from Duo. The string should be at least 40 characters long. The Duo Web site provides tips for how to generate this key.
Duo API Hostname	(Required) The Duo API hostname.
Duo	(Required) The Duo ikey.

Table 94: Provisioning Settings Form, Web Login Tab, Multi-Factor Authentication Area(Continued)

Field	Description
Integration Key	
Duo Secret Key	(Required) The Duo skey.
Email	If selected, emails will be sent during application enrollment. If deselected, the user must scan the QR code.
Enroll	If selected, usernames will be automatically enrolled with the provider.
Factors	The number of factors to require. For some providers, options are included to specify types of factor, such as: <ul style="list-style-type: none"> • photolock - The Photo • fingerprint - The Fingerprint • gridlock - The Pattern • onetap - The Onetap • password - The Password
Footer HTML	HTML template code displayed after the provider’s vendor-specific authentication area. This is the login “wait” page displayed to the user while the authentication code is sent to and submitted by them. You can also use the drop-down lists to add images or other content items, or to insert a self-registration link. To appear in this list, content items must first be uploaded to the Content Manager.
Grace Period	Specifies the number of hours between multi-factor authentication checks. If the user logs in again before this interval expires, they can skip the secondary check if the device name and username have not changed. To require full authentication every time, leave this field empty. The default interval is 24 hours.
Header HTML	HTML template code to display before the provider’s vendor-specific authentication area. This is the login “wait” page displayed to the user while the authentication code is sent to and submitted by them. You can also use the drop-down lists to add images or other content items, or to insert a self-registration link. To appear in this list, content items must first be uploaded to the Content Manager.
Hostname	(Required) Hostname of the ImageWare server.
Password	(Required) Password to use with this provider.
Phone Attribute	(Required) For SMS Verification Codes, the attribute name containing mobile numbers. Names should be entered as a comma-separated list. The order of the list determines the lookup priority.
Role	Your role ID.
Secret Key	(Required) The Facial Networks client secret.
Service Provider	Service provider to use when sending SMS messages.

Table 94: Provisioning Settings Form, Web Login Tab, Multi-Factor Authentication Area(Continued)

Field	Description
Tenant Name	(Required) Tenant name to use with the GoMobile provider. A tenant is a company or other entity that has created a tenant account with ImageWare in order to use the GoMobile server for security.
Username	(Required) Username to use with this provider.
Verify Template	The full URL of the verification template.

Network Login Access Area

Figure 157 The Provisioning Settings Form, Web Login Tab, Network Login Access Area

Table 95: Provisioning Settings Form, Web Login Tab, Network Login Access Area

Field	Description
Allowed Access	Enter the IP addresses and networks from which logins will be allowed. (IPv4 and IPv6 are both supported)
Denied Access	Enter the IP addresses and networks from which logins will be denied. (IPv4 and IPv6 are both supported)
Deny Behavior	(Required) Specifies the response shown to the user if their login request is denied. Options include: <ul style="list-style-type: none"> • Send HTTP 404 Not Found status • Show Access Denied page • Show a blank page.

Click **Next** to proceed to the next tab, or **Save Changes** to complete your edits.

To return to the list of links to all Provisioning Settings tabs, see "[About Configuring Provisioning Settings](#) " on page 221.

Configuring Provisioning Settings for Instructions and Messages

To configure the text for labels and messages shown before, during, and after provisioning, including messages specific to each operating system, go to **Onboard > Deployment and Provisioning**, expand the provisioning

setting's row in the list, and click its **Edit** link. In the **Device Provisioning Settings** form, click the **Instructions & Messages** tab.



To add the fields for a device's operating system to the **Provisioning Settings > Instructions & Messages** tab, you must first enable provisioning for that operating system on the **Supported Devices** tab.

This section describes the following areas on the **Onboard > Deployment and Provisioning > Provisioning Settings > Instructions & Messages** tab:

- "Provisioning Instructions Area" on page 240
- "Device Status Area" on page 242
- "Android Instructions Area" on page 244
- "Chromebook Instructions Area" on page 246
- "iOS Instructions Area" on page 248
- "OS X Instructions Area" on page 250
- "Legacy OS X Instructions Area" on page 252
- "Ubuntu Instructions Area" on page 254
- "Windows Instructions Area" on page 256
- "Web-Based Instructions Area" on page 258

Provisioning Instructions Area

Figure 158 The Provisioning Settings Form, Instructions & Messages Tab, Provisioning Instructions Area

Provisioning Instructions
Instructions displayed during and after device provisioning.

* Provisioning Device:	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 2px;">Use custom message ▼</div> <p>Message shown to the user during the provisioning process (after login).</p>
Provisioning Message:	<div style="border: 1px solid #ccc; padding: 5px; min-height: 100px;"> <pre>{nwa_icontext type=info} {nwa_text id=16344}In order to connect to this network, your device must be configured for enhanced security. This wizard will guide you through the configuration process.{/nwa_text} {/nwa_icontext} {onboard_device_message} {onboard_device_link}</pre> </div> <div style="border: 1px solid #ccc; padding: 2px; margin-top: 2px; width: fit-content; margin-left: auto;">Insert...</div> <p>Enter the HTML code to display. Smarty template functions can be used here. You can use the {onboard_device_message} Smarty template to insert the configured device specific messages. You can use the {onboard_device_link} Smarty template to insert a download link for the current step.</p>
* Complete, Reconnected:	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 2px;">Use default message ▼</div> <p>Message shown to the user after enrollment is complete and device has automatically reconnected. Only Android, iOS, Windows and Ubuntu devices support automatically reconnecting. Additionally Insight must be enabled and a single-SSID setup used for iOS devices to reconnect.</p>
* Complete, Reconnect Required:	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 2px;">Use default message ▼</div> <p>Message shown to the user after enrollment is complete and the user must manually reconnect their device. Chromebook, OS X and Web-Based enrollments require manual reconnection. If Insight is not enabled or a dual-SSID setup is used, iOS devices also require manual reconnection.</p>

Table 96: Provisioning Settings Form, Instructions & Messages Tab, Provisioning Instructions Area

Field	Description
Provisioning Device	<p>Specifies how to configure the message that is shown to the user after they log in and during provisioning. Options include:</p> <ul style="list-style-type: none"> ● Use default message ● Use custom message
Provisioning Message	<p>Enter the instructions that are shown to the user after they log in and during provisioning. The text can be entered as HTML code, and you can use Smarty template functions. If this field is left empty, the default text will be displayed.</p> <p>You may use the Insert content item drop-down list to add an image file or link.</p> <p>To insert the configured device-specific message, you can use the {onboard_device_message} Smarty template.</p> <p>To insert a download link for the current step, you can use the {onboard_device_link} Smarty template.</p>
Complete, Reconnected	<p>Specifies how to configure the message that is shown to the user after enrollment is complete and the device has automatically reconnected. Options include:</p> <ul style="list-style-type: none"> ● Use default message ● Use custom message <p>Automatic reconnection is only supported by Android, iOS, Windows, and Ubuntu devices. For iOS devices to reconnect, Insight must be enabled and a single-SSID setup must be used.</p>

Table 96: *Provisioning Settings Form, Instructions & Messages Tab, Provisioning Instructions Area(Continued)*

Field	Description
Complete, Reconnected Message	<p>Enter the instructions that are shown to the user after enrollment is complete and the device has automatically reconnected. The text can be entered as HTML code, and you can use Smarty template functions. If this field is left empty, the default text will be displayed.</p> <p>You may use the Insert content item drop-down list to add an image file or link.</p> <p>To insert the configured device-specific message, you can use the <code>{onboard_device_message}</code> Smarty template.</p>
Complete, Reconnect Required	<p>Specifies how to configure the message that is shown to the user after enrollment is complete and the user must manually reconnect their device. Options include:</p> <ul style="list-style-type: none">● Use default message● Use custom message <p>Manual reconnection is required by Chromebook, OS X, and Web-based enrollments.</p> <p>If Insight is not enabled or a dual-SSID setup is used, iOS devices also require manual reconnection.</p>
Complete, Reconnect Required Message	<p>Enter the instructions that are shown to the user after enrollment is complete and the user must manually reconnect their device. The text can be entered as HTML code, and you can use Smarty template functions. If this field is left empty, the default text will be displayed.</p> <p>You may use the Insert content item drop-down list to add an image file or link.</p> <p>To insert the configured device-specific message, you can use the <code>{onboard_device_message}</code> Smarty template.</p>

To return to the list of links to all **Provisioning Settings** tabs, see ["About Configuring Provisioning Settings "](#) on page 221.

Device Status Area

Figure 159 *The Provisioning Settings Form, Instructions & Messages Tab, Device Status Area*

Device Status
Messages related to the status of the user's device.

* Denied Device:	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 2px;">Use custom message ▼</div> <small>Error shown to a user when their device has been denied access.</small>
Denied Device Message:	<div style="border: 1px solid #ccc; padding: 5px; min-height: 100px;"> <pre>{nwa_icontext type=error} {nwa_text id=9651}Your certificate for this device has been revoked. This device is no longer authorized to use the network.{/nwa_text} {/nwa_icontext}</pre> </div> <div style="border: 1px solid #ccc; padding: 2px; margin-top: 2px; width: fit-content;">Insert... ▼</div> <small>Enter the HTML code to display. Smarty template functions can be used here.</small>
* Expired Device:	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 2px;">Use default message ▼</div> <small>Message shown to a user when their device credentials have expired. This message is displayed above the normal login page.</small>
* Override Device Detection:	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 2px;">Use default message ▼</div> <small>Message that allows the user to override the detected device type.</small>
* Reprovision Device:	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 2px;">Do not display a message, allow normal provisioning ▼</div> <small>Message shown to a user when their device has already been enrolled.</small>
* Unsupported Browser:	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 2px;">Use default message ▼</div> <small>Error shown to the user if they attempt to provision using an unsupported browser.</small>
* Unsupported Device:	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 2px;">Use default message ▼</div> <small>Error shown to the user if they attempt to provision an unsupported device.</small>

Table 97: *Provisioning Settings Form, Instructions & Messages Tab, Device Status Area*

Field	Description
Denied Device	Specifies how to configure the error that is shown to the user when their device is denied access. Options include: <ul style="list-style-type: none"> ● Use default message ● Use custom message
Denied Device Message	Enter the instructions that are shown to the user when their device is denied access. The text can be entered as HTML code, and you can use Smarty template functions. If this field is left empty, the default text will be displayed. You may use the Insert content item drop-down list to add an image file or link.
Expired Device	Specifies how to configure the message that is shown to the user when their device credentials have expired. This message is displayed above the normal login page. Options include: <ul style="list-style-type: none"> ● Use default message ● Use custom message
Expired Device Message	Enter the instructions that are shown to the user when their device credentials have expired. The text can be entered as HTML code, and you can use Smarty template functions. If this field is left empty, the default text will be displayed. You may use the Insert content item drop-down list to add an image file or link.
Override Device Detection	Specifies how to configure the message that allows the user to override the detected device type. Options include: <ul style="list-style-type: none"> ● Use default message ● Use custom message
Reprovision Device	Specifies how to configure the message that is shown to the user if their device is already enrolled. Options include: <ul style="list-style-type: none"> ● Do not display a message, allow normal provisioning ● Use default message ● Use custom message

Table 97: Provisioning Settings Form, Instructions & Messages Tab, Device Status Area(Continued)

Field	Description
Reprovision Device Message	<p>Enter the instructions that are shown to the user if their device is already enrolled. The text can be entered as HTML code, and you can use Smarty template functions. If this field is left empty, the default text will be displayed.</p> <p>You may use the Insert content item drop-down list to add an image file or link.</p> <p>To insert a link to the provisioning page, you can use the <code>{ \$reprovision_link }</code> Smarty variable.</p>
Unsupported Browser	<p>Specifies how to configure the error that is shown to the user if they attempt to provision using an unsupported browser. Options include:</p> <ul style="list-style-type: none">● Use default message● Use custom message
Unsupported Browser Message	<p>Enter the instructions that are shown to the user if they attempt to provision using an unsupported browser. The text can be entered as HTML code, and you can use Smarty template functions. If this field is left empty, the default text will be displayed.</p> <p>You may use the Insert content item drop-down list to add an image file or link.</p> <p>To insert the name of the supported browser for the device, you can use the <code>{ \$supported_browser }</code> Smarty variable.</p>
Unsupported Device	<p>Specifies how to configure the error that is shown to the user if they attempt to provision an unsupported device. Options include:</p> <ul style="list-style-type: none">● Use default message● Use custom message
Unsupported Device Message	<p>Enter the instructions that are shown to the user if they attempt to provision an unsupported device. The text can be entered as HTML code, and you can use Smarty template functions. If this field is left empty, the default text will be displayed.</p> <p>You may use the Insert content item drop-down list to add an image file or link.</p>

To return to the list of links to all **Provisioning Settings** tabs, see ["About Configuring Provisioning Settings "](#) on page 221.

Android Instructions Area

To add the **Android Instructions** area to the **Provisioning Settings > Instructions & Messages** tab, you must first enable Android provisioning on the **Supported Devices** tab.

Figure 160 The Provisioning Settings Form, Instructions & Messages Tab, Android Instructions Area

Android Instructions	
These options control messages shown during Android device provisioning.	
* Pre-Login:	Use custom message Instructions shown to the user before they log in using an Android device.
Pre-Login Message:	<input type="text"/> Insert... Enter the HTML code to display. Smarty template functions can be used here.
* App Download:	Use default message Instructions shown to the user when asked to download the Android app.
* Profile Download:	Use default message Instructions shown to the user when asked to download the Android profile.
* Installing Profile:	Use default message Instructions shown to the user while the Android profile installs.
* Complete:	Use default message Instructions shown to the user when Android provisioning is complete.
* Link Text:	Use default labels Controls the labels shown on download links during Android provisioning.

Table 98: Provisioning Settings Form, Instructions & Messages Tab, Android Instructions Area

Field	Description
Pre-Login	Specifies how to configure the instructions that are shown to the user before they log in using an Android device. Options include: <ul style="list-style-type: none"> ● Use default message ● Use custom message
Pre-Login Message	Enter the instructions that are shown to the user before they log in using an Android device. The text can be entered as HTML code, and you can use Smarty template functions. If this field is left empty, the default text will be displayed. You may use the Insert content item drop-down list to add an image file or link.
App Download	Specifies how to configure the instructions that are shown to the user when they are asked to download the Android app. Options include: <ul style="list-style-type: none"> ● Use default message ● Use custom message
App Download Message	Enter the instructions that are shown to the user when they are asked to download the Android app. The text can be entered as HTML code, and you can use Smarty template functions. If this field is left empty, the default text will be displayed. You may use the Insert content item drop-down list to add an image file or link.
Profile Download	Specifies how to configure the instructions that are shown to the user when they are asked to download the Android profile. Options include: <ul style="list-style-type: none"> ● Use default message ● Use custom message
Profile Download Message	Enter the instructions that are shown to the user when they are asked to download the Android profile. The text can be entered as HTML code, and you can use Smarty template functions. If this field is left empty, the default text will be displayed. You may use the Insert content item drop-down list to add an image file or link.

Table 98: Provisioning Settings Form, Instructions & Messages Tab, Android Instructions Area(Continued)

Field	Description
Installing Profile	Specifies how to configure the instructions that are shown to the user while the Android profile is installed. Options include: <ul style="list-style-type: none">● Use default message● Use custom message
Installing Profile Message	Enter the instructions that are shown to the user while the Android profile is installed. The text can be entered as HTML code, and you can use Smarty template functions. If this field is left empty, the default text will be displayed. You may use the Insert content item drop-down list to add an image file or link.
Complete	Specifies how to configure the instructions that are shown to the user when Android provisioning is complete. Options include: <ul style="list-style-type: none">● Use default message● Use custom message
Complete Message	Enter the instructions that are shown to the user when Android provisioning is complete. The text can be entered as HTML code, and you can use Smarty template functions. If this field is left empty, the default text will be displayed. You may use the Insert content item drop-down list to add an image file or link.
Link Text	Specifies how to configure the labels that are shown on download links during Android provisioning. Options include: <ul style="list-style-type: none">● Use default labels● Use custom labels
App Link Command	Enter the short description that is shown for Android app download.
App Link Text	Enter the detailed description that is shown for Android app download.
App Link Skip	Enter the text to display on the link to skip the app download step.
Profile Link Command	Enter the short description that is shown for Android profile download.
Profile Link Text	Enter the detailed description that is shown for Android profile download.

To return to the list of links to all **Provisioning Settings** tabs, see ["About Configuring Provisioning Settings "](#) on page 221.

Chromebook Instructions Area

To add the **Chromebook Instructions** area to the **Provisioning Settings > Instructions & Messages** tab, you must first enable Chromebook provisioning on the **Supported Devices** tab.

Figure 161 *The Provisioning Settings Form, Instructions & Messages Tab, Chromebook Instructions Area*

Chromebook Instructions
These options control messages shown during Chromebook device provisioning.

* Pre-Login:	Use custom message ▼ Instructions shown to the user before they log in using an Chromebook device.
Pre-Login Message:	<input type="text"/> Insert... ▼ Enter the HTML code to display. Smarty template functions can be used here.
* Plugin Launch:	Use default message ▼ Instructions shown to the user when asked to launch the Chromebook plugin.
* Installing Profile:	Use default message ▼ Instructions shown to the user while the Chromebook certificate installs.
* Complete:	Use default message ▼ Instructions shown to the user when Chromebook provisioning is complete.
* Link Text:	Use default labels ▼ Controls the labels shown on download links during Chromebook provisioning.

Table 99: *Provisioning Settings Form, Instructions & Messages Tab, Chromebook Instructions Area*

Field	Description
Pre-Login	Specifies how to configure the instructions that are shown to the user before they log in using a Chromebook device. Options include: <ul style="list-style-type: none"> ● Use default message ● Use custom message
Pre-Login Message	Enter the instructions that are shown to the user before they log in using a Chromebook device. The text can be entered as HTML code, and you can use Smarty template functions. If this field is left empty, the default text will be displayed. You may use the Insert content item drop-down list to add an image file or link.
Plugin Launch	Specifies how to configure the instructions that are shown to the user when they are asked to launch the Chromebook plugin. Options include: <ul style="list-style-type: none"> ● Use default message ● Use custom message
Plugin Launch Message	Enter the instructions that are shown to the user when they are asked to launch the Chromebook plugin. The text can be entered as HTML code, and you can use Smarty template functions. If this field is left empty, the default text will be displayed. You may use the Insert content item drop-down list to add an image file or link.
Installing Profile	Specifies how to configure the instructions that are shown to the user while the Chromebook certificate is installed. Options include: <ul style="list-style-type: none"> ● Use default message ● Use custom message
Installing Profile Message	Enter the instructions that are shown to the user while the Chromebook certificate is installed. The text can be entered as HTML code, and you can use Smarty template functions. If this field is left empty, the default text will be displayed. You may use the Insert content item drop-down list to add an image file or link.
Complete	Specifies how to configure the instructions that are shown to the user when Chromebook provisioning is complete. Options include:

Table 99: *Provisioning Settings Form, Instructions & Messages Tab, Chromebook Instructions Area(Continued)*

Field	Description
	<ul style="list-style-type: none">● Use default message● Use custom message
Complete Message	Enter the instructions that are shown to the user when Chromebook provisioning is complete. The text can be entered as HTML code, and you can use Smarty template functions. If this field is left empty, the default text will be displayed. You may use the Insert content item drop-down list to add an image file or link.
Link Text	Specifies how to configure the labels that are shown on download links during Chromebook provisioning. Options include: <ul style="list-style-type: none">● Use default labels● Use custom labels
Plugin Launch Command	Enter the short description that is shown for Chromebook plugin launch.
Plugin Launch Text	Enter the detailed description that is shown for Chromebook plugin launch.

To return to the list of links to all **Provisioning Settings** tabs, see "[About Configuring Provisioning Settings](#) " on page 221.

iOS Instructions Area

To add the **iOS Instructions** area to the **Provisioning Settings > Instructions & Messages** tab, you must first enable iOS provisioning on the **Supported Devices** tab.

Figure 162 The Provisioning Settings Form, Instructions & Messages Tab, iOS Instructions Area

iOS Instructions	
These options control messages shown during iOS device provisioning.	
* Pre-Login:	Use custom message ▼ Instructions shown to the user before they log in using an iOS device.
Pre-Login Message:	<input type="text"/> Insert... ▼ Enter the HTML code to display. Smarty template functions can be used here.
* Root Certificate Download:	Use default message ▼ Instructions shown to the user when asked to download the iOS root certificate.
* Profile Download:	Use default message ▼ Instructions shown to the user when asked to download the iOS profile.
* Installing Profile:	Use default message ▼ Instructions shown to the user while the iOS profile installs.
* Complete:	Use default message ▼ Instructions shown to the user when iOS provisioning is complete.
* Link Text:	Use default labels ▼ Controls the labels shown on download links during iOS provisioning.

Table 100: Provisioning Settings Form, Instructions & Messages Tab, iOS Instructions Area

Field	Description
Pre-Login	Specifies how to configure the instructions that are shown to the user before they log in using an iOS device. Options include: <ul style="list-style-type: none"> ● Use default message ● Use custom message
Pre-Login Message	Enter the instructions that are shown to the user before they log in using an iOS device. The text can be entered as HTML code, and you can use Smarty template functions. If this field is left empty, the default text will be displayed. You may use the Insert content item drop-down list to add an image file or link.
Root Certificate Download	Specifies how to configure the instructions that are shown to the user when they are asked to download the iOS root certificate. Options include: <ul style="list-style-type: none"> ● Use default message ● Use custom message
Root Certificate Download Message	Enter the instructions that are shown to the user when they are asked to download the iOS root certificate. The text can be entered as HTML code, and you can use Smarty template functions. If this field is left empty, the default text will be displayed. You may use the Insert content item drop-down list to add an image file or link.
Profile Download	Specifies how to configure the instructions that are shown to the user when they are asked to download the iOS profile. Options include: <ul style="list-style-type: none"> ● Use default message ● Use custom message
Profile Download Message	Enter the instructions that are shown to the user when they are asked to download the iOS profile. The text can be entered as HTML code, and you can use Smarty template functions. If this field is left empty, the default text will be displayed. You may use the Insert content item drop-down list to add an image file or link.

Table 100: Provisioning Settings Form, Instructions & Messages Tab, iOS Instructions Area(Continued)

Field	Description
Installing Profile	Specifies how to configure the instructions that are shown to the user while the iOS profile is installed. Options include: <ul style="list-style-type: none">● Use default message● Use custom message
Installing Profile Message	Enter the instructions that are shown to the user while the iOS profile is installed. The text can be entered as HTML code, and you can use Smarty template functions. If this field is left empty, the default text will be displayed. You may use the Insert content item drop-down list to add an image file or link.
Complete	Specifies how to configure the instructions that are shown to the user when iOS provisioning is complete. Options include: <ul style="list-style-type: none">● Use default message● Use custom message
Complete Message	Enter the instructions that are shown to the user when iOS provisioning is complete. The text can be entered as HTML code, and you can use Smarty template functions. If this field is left empty, the default text will be displayed. You may use the Insert content item drop-down list to add an image file or link.
Link Text	Specifies how to configure the labels that are shown on download links during iOS provisioning. Options include: <ul style="list-style-type: none">● Use default labels● Use custom labels
Root Certificate Command	Enter the short description that is shown for iOS root certificate download.
Root Certificate Text	Enter the detailed description that is shown for iOS root certificate download.
Profile Link Command	Enter the short description that is shown for iOS profile download.
Profile Link Text	Enter the detailed description that is shown for iOS profile download.

To return to the list of links to all **Provisioning Settings** tabs, see ["About Configuring Provisioning Settings "](#) on page 221.

OS X Instructions Area

To add the **OS X Instructions** area to the **Provisioning Settings > Instructions & Messages** tab, you must first enable OS X provisioning on the **Supported Devices** tab.

Figure 163 The Provisioning Settings Form, Instructions & Messages Tab, OS X Instructions Area

OS X Instructions	
These options control messages shown during OS X device provisioning.	
* Pre-Login:	Use custom message ▼ Instructions shown to the user before they log in using an OS X device.
Pre-Login Message:	[Text Area] Insert... ▼ Enter the HTML code to display. Smarty template functions can be used here.
* Root Certificate Download:	Use default message ▼ Instructions shown to the user when asked to download the OS X root certificate.
* Profile Download:	Use default message ▼ Instructions shown to the user when asked to download the OS X profile.
* Installing Profile:	Use default message ▼ Instructions shown to the user while the OS X profile installs.
* Complete:	Use default message ▼ Instructions shown to the user when OS X provisioning is complete.
* Link Text:	Use default labels ▼ Controls the labels shown on download links during OS X provisioning.

Table 101: Provisioning Settings Form, Instructions & Messages Tab, OS X Instructions Area

Field	Description
Pre-Login	Specifies how to configure the instructions that are shown to the user before they log in using an OS X device. Options include: <ul style="list-style-type: none"> ● Use default message ● Use custom message
Pre-Login Message	Enter the instructions that are shown to the user before they log in using an OS X device. The text can be entered as HTML code, and you can use Smarty template functions. If this field is left empty, the default text will be displayed. You may use the Insert content item drop-down list to add an image file or link.
Root Certificate Download	Specifies how to configure the instructions that are shown to the user when they are asked to download the OS X root certificate. Options include: <ul style="list-style-type: none"> ● Use default message ● Use custom message
Root Certificate Download Message	Enter the instructions that are shown to the user when they are asked to download the OS X root certificate. The text can be entered as HTML code, and you can use Smarty template functions. If this field is left empty, the default text will be displayed. You may use the Insert content item drop-down list to add an image file or link.
Profile Download	Specifies how to configure the instructions that are shown to the user when they are asked to download the OS X profile. Options include: <ul style="list-style-type: none"> ● Use default message ● Use custom message
Profile Download Message	Enter the instructions that are shown to the user when they are asked to download the OS X profile. The text can be entered as HTML code, and you can use Smarty template functions. If this field is left empty, the default text will be displayed. You may use the Insert content item drop-down list to add an image file or link.

Table 101: Provisioning Settings Form, Instructions & Messages Tab, OS X Instructions Area(Continued)

Field	Description
Installing Profile	Specifies how to configure the instructions that are shown to the user while the OS X profile is installed. Options include: <ul style="list-style-type: none">● Use default message● Use custom message
Installing Profile Message	Enter the instructions that are shown to the user while the OS X profile is installed. The text can be entered as HTML code, and you can use Smarty template functions. If this field is left empty, the default text will be displayed. You may use the Insert content item drop-down list to add an image file or link.
Complete	Specifies how to configure the instructions that are shown to the user when OS X provisioning is complete. Options include: <ul style="list-style-type: none">● Use default message● Use custom message
Complete Message	Enter the instructions that are shown to the user when OS X provisioning is complete. The text can be entered as HTML code, and you can use Smarty template functions. If this field is left empty, the default text will be displayed. You may use the Insert content item drop-down list to add an image file or link.
Link Text	Specifies how to configure the labels that are shown on download links during OS X provisioning. Options include: <ul style="list-style-type: none">● Use default labels● Use custom labels
Root Certificate Command	Enter the short description that is shown for OS X root certificate download.
Root Certificate Text	Enter the detailed description that is shown for OS X root certificate download.
Profile Link Command	Enter the short description that is shown for OS X profile download.
Profile Link Text	Enter the detailed description that is shown for OS X profile download.

To return to the list of links to all **Provisioning Settings** tabs, see ["About Configuring Provisioning Settings "](#) on page 221.

Legacy OS X Instructions Area

To add the **Legacy OS X Instructions** area to the **Provisioning Settings > Instructions & Messages** tab, you must first enable Legacy OS X provisioning on the **Supported Devices** tab.

Figure 164 *The Provisioning Settings Form, Instructions & Messages Tab, Legacy OS X Instructions Area*

Table 102: *Provisioning Settings Form, Instructions & Messages Tab, Legacy OS X Instructions Area*

Field	Description
Pre-Login	Specifies how to configure the instructions that are shown to the user before they log in using a legacy OS X device. Options include: <ul style="list-style-type: none"> ● Use default message ● Use custom message
Pre-Login Message	Enter the instructions that are shown to the user before they log in using a legacy OS X device. The text can be entered as HTML code, and you can use Smarty template functions. If this field is left empty, the default text will be displayed. You may use the Insert content item drop-down list to add an image file or link.
App Download	Specifies how to configure the instructions that are shown to the user when they are asked to download the legacy OS X app. Options include: <ul style="list-style-type: none"> ● Use default message ● Use custom message
App Download Message	Enter the instructions that are shown to the user when they are asked to download the legacy OS X app. The text can be entered as HTML code, and you can use Smarty template functions. If this field is left empty, the default text will be displayed. You may use the Insert content item drop-down list to add an image file or link.
Installing Profile	Specifies how to configure the instructions that are shown to the user while the legacy OS X certificate is installed. Options include: <ul style="list-style-type: none"> ● Use default message ● Use custom message
Installing Profile Message	Enter the instructions that are shown to the user while the legacy OS X certificate is installed. The text can be entered as HTML code, and you can use Smarty template functions. If this field is left empty, the default text will be displayed. You may use the Insert content item drop-down list to add an image file or link.
Complete	Specifies how to configure the instructions that are shown to the user when legacy OS X provisioning is complete. Options include:

Table 102: *Provisioning Settings Form, Instructions & Messages Tab, Legacy OS X Instructions Area(Continued)*

Field	Description
	<ul style="list-style-type: none">● Use default message● Use custom message
Complete Message	Enter the instructions that are shown to the user when legacy OS X provisioning is complete. The text can be entered as HTML code, and you can use Smarty template functions. If this field is left empty, the default text will be displayed. You may use the Insert content item drop-down list to add an image file or link.
Link Text	Specifies how to configure the labels that are shown on download links during legacy OS X provisioning. Options include: <ul style="list-style-type: none">● Use default labels● Use custom labels
App Download Command	Enter the short description that is shown for legacy OS X app download.
App Download Text	Enter the detailed description that is shown for legacy OS X app download.

To return to the list of links to all **Provisioning Settings** tabs, see "[About Configuring Provisioning Settings](#) " on page 221.

Ubuntu Instructions Area

To add the **Ubuntu Instructions** area to the **Provisioning Settings > Instructions & Messages** tab, you must first enable Ubuntu provisioning on the **Supported Devices** tab.

Figure 165 *The Provisioning Settings Form, Instructions & Messages Tab, Ubuntu Instructions Area*

Ubuntu Instructions
These options control messages shown during Ubuntu device provisioning.

* Pre-Login:	Use custom message ▼ Instructions shown to the user before they log in using an Ubuntu device.
Pre-Login Message:	<input type="text"/> Insert... ▼ Enter the HTML code to display. Smarty template functions can be used here.
* App Download:	Use default message ▼ Instructions shown to the user when asked to download the Ubuntu app.
* Installing Profile:	Use default message ▼ Instructions shown to the user while the Ubuntu certificate installs.
* Complete:	Use default message ▼ Instructions shown to the user when Ubuntu provisioning is complete.
* Link Text:	Use default labels ▼ Controls the labels shown on download links during Ubuntu provisioning.

Table 103: *Provisioning Settings Form, Instructions & Messages Tab, Ubuntu Instructions Area*

Field	Description
Pre-Login	Specifies how to configure the instructions that are shown to the user before they log in using an Ubuntu device. Options include: <ul style="list-style-type: none"> ● Use default message ● Use custom message
Pre-Login Message	Enter the instructions that are shown to the user before they log in using an Ubuntu device. The text can be entered as HTML code, and you can use Smarty template functions. If this field is left empty, the default text will be displayed. You may use the Insert content item drop-down list to add an image file or link.
App Download	Specifies how to configure the instructions that are shown to the user when they are asked to download the Ubuntu app. Options include: <ul style="list-style-type: none"> ● Use default message ● Use custom message
App Download Message	Enter the instructions that are shown to the user when they are asked to download the Ubuntu app. The text can be entered as HTML code, and you can use Smarty template functions. If this field is left empty, the default text will be displayed. You may use the Insert content item drop-down list to add an image file or link.
Installing Profile	Specifies how to configure the instructions that are shown to the user while the Ubuntu certificate is installed. Options include: <ul style="list-style-type: none"> ● Use default message ● Use custom message
Installing Profile Message	Enter the instructions that are shown to the user while the Ubuntu certificate is installed. The text can be entered as HTML code, and you can use Smarty template functions. If this field is left empty, the default text will be displayed. You may use the Insert content item drop-down list to add an image file or link.
Complete	Specifies how to configure the instructions that are shown to the user when Ubuntu provisioning is complete. Options include:

Table 103: *Provisioning Settings Form, Instructions & Messages Tab, Ubuntu Instructions Area(Continued)*

Field	Description
	<ul style="list-style-type: none">● Use default message● Use custom message
Complete Message	Enter the instructions that are shown to the user when Ubuntu provisioning is complete. The text can be entered as HTML code, and you can use Smarty template functions. If this field is left empty, the default text will be displayed. You may use the Insert content item drop-down list to add an image file or link.
Link Text	Specifies how to configure the labels that are shown on download links during Ubuntu provisioning. Options include: <ul style="list-style-type: none">● Use default labels● Use custom labels
App Download Command	Enter the short description that is shown for Ubuntu app download.
App Download Text	Enter the detailed description that is shown for Ubuntu app download.

To return to the list of links to all **Provisioning Settings** tabs, see "[About Configuring Provisioning Settings](#) " on page 221.

Windows Instructions Area

To add the **Windows Instructions** area to the **Provisioning Settings > Instructions & Messages** tab, you must first enable Windows provisioning on the **Supported Devices** tab.

Figure 166 *The Provisioning Settings Form, Instructions & Messages Tab, Windows Instructions Area*

Table 104: *Provisioning Settings Form, Instructions & Messages Tab, Windows Instructions Area*

Field	Description
Pre-Login	Specifies how to configure the instructions that are shown to the user before they log in using a Windows device. Options include: <ul style="list-style-type: none"> ● Use default message ● Use custom message
Pre-Login Message	Enter the instructions that are shown to the user before they log in using a Windows device. The text can be entered as HTML code, and you can use Smarty template functions. If this field is left empty, the default text will be displayed. You may use the Insert content item drop-down list to add an image file or link.
App Download	Specifies how to configure the instructions that are shown to the user when they are asked to download the Windows app. Options include: <ul style="list-style-type: none"> ● Use default message ● Use custom message
App Download Message	Enter the instructions that are shown to the user when they are asked to download the Windows app. The text can be entered as HTML code, and you can use Smarty template functions. If this field is left empty, the default text will be displayed. You may use the Insert content item drop-down list to add an image file or link.
Installing Profile	Specifies how to configure the instructions that are shown to the user while the Windows certificate is installed. Options include: <ul style="list-style-type: none"> ● Use default message ● Use custom message
Installing Profile Message	Enter the instructions that are shown to the user while the Windows certificate is installed. The text can be entered as HTML code, and you can use Smarty template functions. If this field is left empty, the default text will be displayed. You may use the Insert content item drop-down list to add an image file or link.
Complete	Specifies how to configure the instructions that are shown to the user when Windows provisioning is complete. Options include:

Table 104: *Provisioning Settings Form, Instructions & Messages Tab, Windows Instructions Area(Continued)*

Field	Description
	<ul style="list-style-type: none">● Use default message● Use custom message
Complete Message	Enter the instructions that are shown to the user when Windows provisioning is complete. The text can be entered as HTML code, and you can use Smarty template functions. If this field is left empty, the default text will be displayed. You may use the Insert content item drop-down list to add an image file or link.
Link Text	Specifies how to configure the labels that are shown on download links during Ubuntu provisioning. Options include: <ul style="list-style-type: none">● Use default labels● Use custom labels
App Download Command	Enter the short description that is shown for Ubuntu app download.
App Download Text	Enter the detailed description that is shown for Ubuntu app download.

To return to the list of links to all **Provisioning Settings** tabs, see "[About Configuring Provisioning Settings](#) " on page 221.

Web-Based Instructions Area

To add the **Web-Based Instructions** area to the **Provisioning Settings > Instructions & Messages** tab, you must first enable Web-based provisioning on the **Supported Devices** tab.

Figure 167 The Provisioning Settings Form, Instructions & Messages Tab, Web-Based Instructions Area

Web-Based Instructions
These options control messages shown during Web-Based device provisioning.

* Pre-Login:
Instructions shown to the user before they log in using a web-based device.

Pre-Login Message:

Enter the HTML code to display. Smarty template functions can be used here.

* App Download:
Instructions shown to the user when asked to download the web app.

* Complete:
Instructions shown to the user when web provisioning is complete.

* Link Text:
Controls the labels shown on download links during web-based provisioning.

Table 105: Provisioning Settings Form, Instructions & Messages Tab, Web-Based Instructions Area

Field	Description
Pre-Login	Specifies how to configure the instructions that are shown to the user before they log in using a Web-based device. Options include: <ul style="list-style-type: none"> ● Use default message ● Use custom message
Pre-Login Message	Enter the instructions that are shown to the user before they log in using a Web-based device. The text can be entered as HTML code, and you can use Smarty template functions. If this field is left empty, the default text will be displayed. You may use the Insert content item drop-down list to add an image file or link.
App Download	Specifies how to configure the instructions that are shown to the user when they are asked to download the Web app. Options include: <ul style="list-style-type: none"> ● Use default message ● Use custom message
App Download Message	Enter the instructions that are shown to the user when they are asked to download the Web app. The text can be entered as HTML code, and you can use Smarty template functions. If this field is left empty, the default text will be displayed. You may use the Insert content item drop-down list to add an image file or link.
Complete	Specifies how to configure the instructions that are shown to the user when Web provisioning is complete. Options include: <ul style="list-style-type: none"> ● Use default message ● Use custom message
Complete Message	Enter the instructions that are shown to the user when Web provisioning is complete. The text can be entered as HTML code, and you can use Smarty template functions. If this field is left empty, the default text will be displayed. You may use the Insert content item drop-down list to add an image file or link.
Link Text	Specifies how to configure the labels that are shown on download links during Web-based provisioning. Options include:

Table 105: Provisioning Settings Form, Instructions & Messages Tab, Web-Based Instructions Area(Continued)

Field	Description
	<ul style="list-style-type: none"> ● Use default labels ● Use custom labels
App Download Command	Enter the short description that is shown for Web-based certificate download.
App Download Text	Enter the detailed description that is shown for Web-based certificate download.

To return to the list of links to all **Provisioning Settings** tabs, see "About Configuring Provisioning Settings " on page 221.

Configuring Provisioning Settings for iOS and OS X Profiles

To specify provisioning settings related to iOS and OS X devices, go to **Onboard > Deployment and Provisioning > Provisioning Settings**, expand the provisioning setting's row in the list, and click its **Edit** link. On the **Provisioning Settings** form, click the **iOS & OS X Profile** tab.

Figure 168 The Provisioning Settings Form, iOS/OS X Profile Tab, iOS/OS X Provisioning Area

Device Provisioning Settings

General # Supported Devices # Web Login # Instructions & Messages # **iOS/OS X Profile #** Onboard Client # Sponsorship Confirmation #

iOS & OS X Provisioning
These options control Apple iOS (iPad, iPod, iPhone) and OS X (Lion or later) device provisioning.

* Display Name:
Example: 'Device Enrollment'.
This text is displayed as the title of the 'Install Profile' screen on the device.

* Profile Description:
Enter the description to display on the 'Install Profile' screen of the device.
This should provide help text for the user and instruct them to install the profile.

* Profile Security:
Select when the configuration profile may be removed.


* Removal Password:
Enter the password required to remove the configuration profile.

* Confirm Removal Password:
Re-enter the password required to remove the configuration profile.

Edit ID: Change the profile ID
The current profile ID is 'com.example.device.provisioning.6d2249a3-e412-4a2c-8b86-b39f875171db'

* ID:
Once set, this ID should rarely be changed.
Changing this ID will cause a **re-provisioned device** to install an **additional** profile instead of **updating** its existing profile.
Example: 'com.example.device.provisioning'.
A reverse-DNS name, used to uniquely identify the profile service.

Table 106: Provisioning Settings Form, iOS/OS X Profile Tab, iOS/OS X Provisioning Area

Field	Description
iOS and OS X Provisioning Area	
Display Name	Enter text for the title that is displayed on the “Install Profile” screen of the device.
Profile Description	<p>Enter text for the description that is displayed on the “Install Profile” screen of the device. This should provide help text for the user and instruct them to install the profile.</p> 
Profile Security	<p>Specifies when the configuration profile may be removed. Options include:</p> <ul style="list-style-type: none"> • Always allow removal – The user may remove the configuration profile at any time, which will also remove the associated device configuration and unique device credentials. • Remove only with authorization – The user may remove the configuration profile if they also provide a password. The administrator must specify the password in the Removal Password and Confirm Removal Password fields. • Never allow removal – The user cannot remove the configuration profile. This option should be used with caution, as the only way to remove the profile is to reset the device to factory defaults, and destroy all data on the device.
Removal Password	If Remove only with authorization was selected in the Profile Security drop-down list, enter the password to use when removing the profile. The minimum password length is six characters.
Confirm Removal Password	
Edit ID	<p>To change the profile ID, select the check box in this row. The profile ID is a unique value associated with the configuration profile. It is used to identify the configuration settings as being from a particular source, and should be globally unique.</p> <p>When an iOS device receives a new configuration profile that has the same profile ID as an existing profile, the existing profile will be replaced with the new profile.</p>
ID	If the Change the profile ID check box is selected in the Edit ID row, you may edit the ID displayed in this field. The ID is a reverse-DNS name used to uniquely identify the profile service. Changing the ID will cause the reprovisioned device to install an additional profile - it does <u>not</u> update the existing profile.



Changing the profile ID will affect any device that has already been provisioned with the existing profile ID. The default value is automatically generated and is globally unique. You should only change this value during initial

Figure 169 *The Provisioning Settings Form, iOS/OS X Profile Tab, Profile Signing Area*

Profile Signing
These options control the way profiles are signed for iOS and OS X devices.

* Certificate Source:	<input type="text" value="Generate using the Onboard CA"/> <small>Choose how to obtain the certificate used to sign iOS and OS X 10.7+ profiles.</small>
* Common Name:	<input type="text" value="Device Enrollment (Profile Signing)"/> <small>Enter the common name to use for the certificate used to sign iOS and OS X 10.7+ profiles. This will appear as the "Signed" field on the install profile dialog.</small>

Table 107: *Provisioning Settings Form, iOS/OS X Profile Tab, Profile Signing Area*

Field	Description
Certificate Source	Specifies how to obtain the certificate used to sign the iOS and OS X 10.7+ profiles. Options include: <ul style="list-style-type: none"> ● Generate using the Onboard CA -- This method establishes a trust chain when the CA certificate is already installed. ● Use an uploaded certificate -- This method can be used for public access situations, and allows a .mobileconfig profile to be signed using a public SSL certificate (for example, one issued by VeriSign).
Common Name	Enter the display name of the certificate used to sign the configuration profile. This certificate will be automatically created by the Certificate Authority, and appears as the "Signed" field on the device when the user authorizes the device provisioning.

Click **Next** to proceed to the next tab, or **Save Changes** to complete your edits.

To return to the list of links to all **Provisioning Settings** tabs, see "[About Configuring Provisioning Settings](#)" on page 221.

Configuring Options for Onboard Client Devices

The **Onboard Client** tab is used to edit basic configuration options for Windows, Android, and legacy OS X (10.5 and 10.6) devices. This form is not used for iOS or OS X 10.7+ devices.

To specify provisioning settings related to Onboard-capable devices, go to **Onboard > Deployment and Provisioning > Provisioning Settings**, expand the provisioning setting's row in the list, and click its **Edit** link. On the **Provisioning Settings** form, click the **Onboard Client** tab.

Figure 170 *The Provisioning Settings Form, Onboard Client Tab*

Device Provisioning Settings	
<p>General Supported Devices Web Login Instructions & Messages iOS/OS X Profile Onboard Client Sponsorship Confirmation</p>	
Device Provisioning Options for Windows, Android and Legacy OS X (10.5/6) device provisioning. These settings are not used for iOS or OS X 10.7+ (Lion or later) devices.	
* Code-Signing Certificate:	<p>None — Do not sign the application</p> <p>Select a code signing certificate for signing the Windows provisioning application.</p>
* Provisioning Address:	<p>10.17.4.197 (Management Port)</p> <p>Select the hostname or IP address to use for device provisioning.</p>
Provisioning Access:	<p>To be provisioned, devices must be able to access 10.17.4.197 via HTTP.</p> <p>HTTPS is not enabled. User's credentials will be transmitted over the network unencrypted.</p> <p>It is highly recommended that you require HTTPS for users (guests). The use of HTTPS is configured on the Authentication page.</p>
* Validate Certificate:	<p>No, do not validate this web server's certificate</p> <p>Specify whether the web server's certificate is to be validated during device provisioning. When testing with the default self-signed web server certificate, you may need to disable validation. This option applies to Windows, Android, and OS X 10.5/6 devices only.</p>
Bypass Proxy:	<p><input checked="" type="checkbox"/> Bypass proxy server</p> <p>If checked, the proxy server configured on the client will not be used during the Onboard enrollment process.</p>
Logo Image:	 <p>Select an image to use in the provisioning wizard. New images can be uploaded using the Content Manager.</p>
* Wizard Title:	<p>Onboard Wizard</p> <p>Enter a title for the wizard used on Windows and Legacy OS X (10.5/6) devices.</p>
Password Recovery URL:	<p>Enter the URL displayed to users who have forgotten their password.</p>
Helpdesk URL:	<p>Enter the URL displayed to users who require helpdesk assistance.</p>
<p>Previous Next Save Changes Cancel</p>	

Table 108: Provisioning Settings Form, Onboard Client Tab




Field	Description
Code-Signing Certificate	Specifies the code-signing certificate to use for signing the Windows provisioning application.
Provisioning Address 	<p>Specifies the hostname or IP address to use for device provisioning. Options include:</p> <ul style="list-style-type: none"> ● The system's hostname (requires DNS resolution) – Select this option to use the system hostname for device provisioning. <hr/> <p>This option requires that the device be able to resolve the listed hostname at the time the device is provisioned.</p> <hr/> <ul style="list-style-type: none"> ● The system's IP address (network adapter name) – Select this option to use the IP address of the system for device provisioning. The drop-down list includes one option for each of the IP addresses detected on the system. ● Use this option when DNS resolution of the system's hostname is not available for devices that are in a provisioning role. ● Other IP address or hostname... – Select this option to override the hostname or IP address to be specified during device provisioning. The administrator must enter the hostname or IP address in the "Address" text field. <p>Use this option when special DNS or NAT conditions apply to devices that are in a provisioning role.</p>
Address	If you chose Other IP address or hostname in the Provisioning Address drop-down list, enter the hostname or IP address to use for device provisioning.
Provisioning Access 	<p>This warning message is displayed when HTTPS is not required for guest access. HTTPS is recommended for all deployments as it secures the unique device credentials that will be issued to the device.</p> <hr/> <p>When using HTTPS for device provisioning, you must obtain a commercial SSL certificate. Self-signed SSL certificates, and SSL server certificates that have been issued by an untrusted or unknown root Certificate Authority, will cause iOS device provisioning to fail with the message "The server certificate for ... is invalid".</p> <hr/>
Bypass Proxy	If selected, the proxy server configured on the client will not be used during the Onboard enrollment process.
Validate Certificate	<p>Specifies whether the SSL server's certificate should be validated as trusted. Options include:</p> <ul style="list-style-type: none"> ● Yes, validate this web server's certificate (recommended) — If selected, a certificate validation failure on the client device will cause device provisioning to fail. This is the default option. ● No, do not validate this web server's certificate — Use this option only during testing, or if you are waiting for a commercial SSL certificate.

Table 108: *Provisioning Settings Form, Onboard Client Tab(Continued)*

Field	Description
Logo Image	To display your enterprise's logo in the provisioning wizard, select an image from the list in this field. Go to Administration > Content Manager to upload new images to use as the logo. The native size of the logo used in the QuickConnect client is 188 pixels wide, 53 pixels high. You may use an image of a different size and it will be scaled to fit, but for the best quality results it is recommended that you provide an image that is already the correct size.
Wizard Title	Specifies the title displayed to users on the wizard for Windows or legacy OS X (10.5/6) devices.
Password Recovery URL  Helpdesk URL	If provided, these fields may be used to provide additional resources to users who encounter trouble in provisioning their devices. <hr/> Ensure that users in the provisioning role can access these URLs. <hr/>

Click **Next** to proceed to the next tab, or **Save Changes** to complete your edits.

To return to the list of links to all **Provisioning Settings** tabs, see "[About Configuring Provisioning Settings](#)" on page 221.

Configuring Provisioning Settings for Sponsorship Confirmation

To specify provisioning settings related to sponsorship confirmation and UI overrides, go to **Onboard > Deployment and Provisioning > Provisioning Settings**, expand the provisioning setting's row in the list, and click its **Edit** link. On the **Provisioning Settings** form, click the **Sponsorship Confirmation** tab.

Sponsorship Confirmation Area

Figure 171 The Provisioning Settings Form, Sponsorship Confirmation Tab, Sponsorship Confirmation Area

The screenshot shows the 'Device Provisioning Settings' form with the 'Sponsorship Confirmation' tab selected. The form is divided into several sections:

- Enabled:** A checkbox labeled 'Require sponsor confirmation prior to enabling the account' is checked.
- Authentication:** A checkbox labeled 'Require sponsors to provide credentials prior to sponsoring' is checked. Below it, text reads: 'If checked, the sponsor will need to successfully authenticate prior to approving the request. The sponsor's operator profile must have the Guest Manager > Remove Accounts privilege.'
- Email Delivery:** This section contains several fields:
 - * Email Field:** A dropdown menu with '(Use Default: sponsor_email)' selected. Below it, text reads: 'The field containing the sponsor's email address.'
 - Email Confirmation:** A dropdown menu with '(Use Default: Sponsor Device Provisioning)' selected. Below it, text reads: 'The plain text or HTML print template to send to the sponsor.'
 - * Email Skin:** A dropdown menu with '(Use Default: Use the default skin)' selected. Below it, text reads: 'The format in which to send email receipts.'
 - * Send Copies:** A dropdown menu with 'Do not send copies' selected. Below it, text reads: 'Specify when to send visitor account receipts to the recipients in the Copies To list.'
 - Reply-To:** A checkbox labeled 'Allow the reply-to address to be overridden' is checked. Below it, text reads: 'If checked, the reply-to address will be overridden by the guest's email field.'
 - Override From:** A checkbox labeled 'Override the from address instead of using reply-to' is checked. Below it, text reads: 'If checked, the from address will be overridden in lieu of the reply-to value above. Note, this feature may require configuration on your mail server to allow the override.'

Table 109: Provisioning Settings Form, Sponsorship Confirmation Tab, Sponsorship Confirmation Area

Field	Description
Enabled	If selected, sponsor confirmation is required prior to enabling the account. You must also add the field for the sponsor's email to the login form as a custom field. See "Configuring Provisioning Settings for the Web Login Page" on page 229.
Authentication	If selected, the sponsor must successfully authenticate prior to approving the request. The sponsor's profile must include the Guest Manager > Remove Accounts privilege.
Email Field	Specifies the attribute to use for field containing the sponsor's email address. The default is sponsor_email .
Email Confirmation	Specifies the plain text or HTML print template to send to the sponsor for email confirmation. The default is Sponsor Device Provisioning .
Email Skin	Specifies the skin to use for email confirmations. Options include: <ul style="list-style-type: none"> • No skin - Plain text only • No skin - HTML only • No skin - Native receipt format • (Use the default skin • Aruba ClearPass Skin • Blank Skin • ClearPass Guest Skin • Custom Skin 1 • Custom Skin 2

Table 109: *Provisioning Settings Form, Sponsorship Confirmation Tab, Sponsorship Confirmation Area (Continued)*

Field	Description
	<ul style="list-style-type: none"> ● Galleria Skin ● Galleria Skin 2
Send Copies	<p>Specifies when to send visitor account receipts to the recipients in the Copies To list. Options include:</p> <ul style="list-style-type: none"> ● Do not send copies ● Always send using "cc:" ● Always send using "Bcc:"
Copies To	<p>List of email addresses to which copies of visitor account receipts will be sent. To have the email sent to the sponsor's email address, enter _admin.</p>
Reply-To	<p>If selected, the Reply- To Address will be overridden by the visitor's email field.</p>
Override From	<p>If selected, the From Address will be overridden instead of using the Reply-To value. This might require configuration of your mail server to allow the override.</p>

UI Overrides Area

Figure 172 The Provisioning Settings Form, Sponsorship Confirmation Tab, UI Overrides Area

UI Overrides

UI Overrides: Display fields to override UI text and labels

Subject Line:
 Template specifying the subject line for emailed visitor account receipts.
 Leave blank to use the default (Device provisioning request from: `{if $email}{$email}{else}{$username}{/if}`)

Confirmation Title:
 Override the default page title (Device Provisioning Request).

Header HTML:

 HTML template code displayed before the login form.

Form Override: Override the form

Confirm Button:
 Override the default confirm button (Confirm).

Reject Button:
 Override the default reject button (Reject).

Footer HTML:

 HTML template code displayed after the confirmation form.

Pending Approval:

 HTML template code displayed on the pending approval page.

Table 110: Provisioning Settings Form, Sponsorship Confirmation Tab, QuickAccess and UI Overrides Areas

Field	Description
UI Overrides	If selected, the form expands to include fields for configuring overrides to UI text and labels.
Subject Line	You may specify the template to use for the subject line for emailed visitor account receipts. If this field is left blank, the default will be used (Device provisioning request from: <code>{if \$email}{else}{ \$username}{/if}</code>).
Confirmation Title	You may specify text to override the default page title. If this field is left blank, the default will be used (Device Provisioning Request).
Header HTML	You may enter HTML template code for the header that is displayed before the login form. If this field is left empty, the default text will be displayed. You may use the Insert content item drop-down list to add an image file or link.
Form Override	If selected, allows overriding the form.
Confirm Button	You may specify text to override the default confirm button. If this field is left blank, the default will be used (Confirm).

Table 110: *Provisioning Settings Form, Sponsorship Confirmation Tab, QuickAccess and UI Overrides Areas (Continued)*

Field	Description
Reject Button	You may specify text to override the default reject button. If this field is left blank, the default will be used (Reject).
Footer HTML	You may enter HTML template code for the footer that is displayed after the confirmation form. If this field is left empty, the default text will be displayed. You may use the Insert content item drop-down list to add an image file or link.
Pending Approval	You may enter HTML template code for the message that is displayed on the pending approval page. If this field is left empty, the default text will be displayed. You may use the Insert content item drop-down list to add an image file or link.

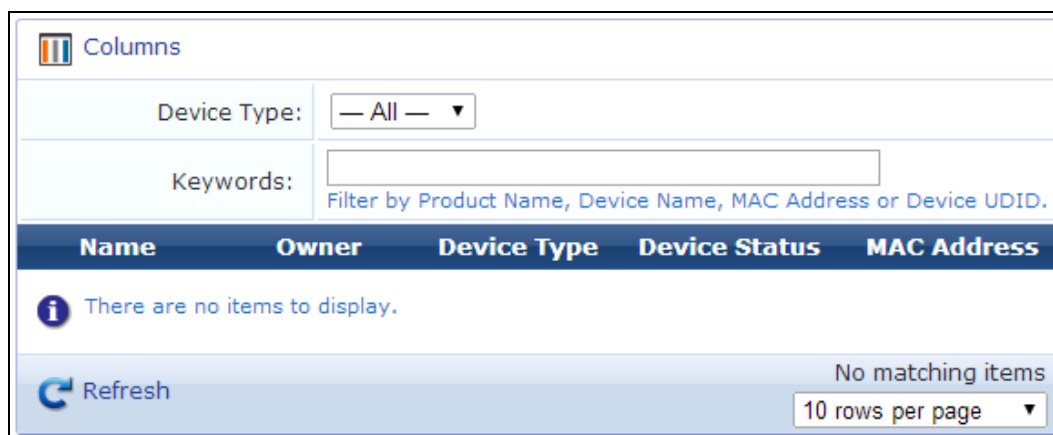
Click **Next** to proceed to the next tab, or **Save Changes** to complete your edits.

To return to the list of links to all **Provisioning Settings** tabs, see "[About Configuring Provisioning Settings](#)" on page 221.

About the Self-Service Portal

The Self-Service Portal allows users to manage their onboarded BYOD devices without requiring IT intervention.

Figure 173 *The Self-Service Portal List View*



The **Self-Service Portal** list displays Onboard devices. Select the type from the **Device Type** drop-down list in the filter area. Information shown for each device includes the device's name, owner's name, device type, the device's network access status, and the device ID (MAC address).



¹Log in as the local user in the Self-Service portal to view the list of your devices. For more information on configuring the local user credentials, see the section, *Adding and Modifying Local Users* in the latest ClearPass Policy Manager *User Guide*.

Guest users can perform the following operations:

- View, enable, disable, or delete a device.
- Report a device as lost or stolen.

In addition, ClearPass operators can revoke a device's client certificate.

For more information on various device actions, see "[Device Management \(View by Device\)](#)" on page 136.

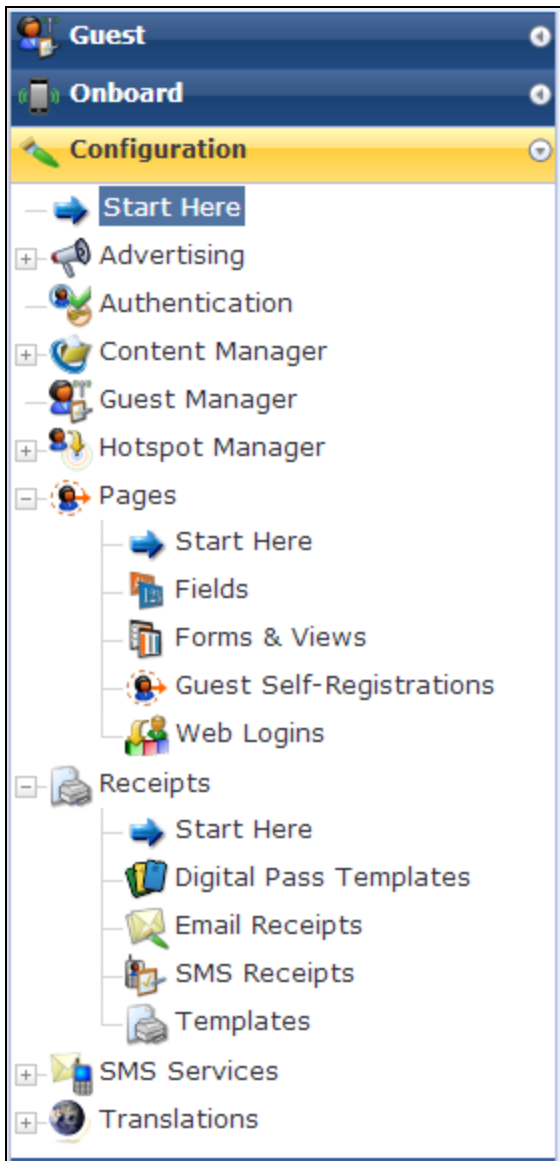


ClearPass Guest's Configuration editor lets you customize many aspects of the appearance, settings, and behavior of the application. Areas you can customize include:

- Advertising services. See ["Advertising Services"](#) on page 473.
- Authentication settings. See ["Configuring ClearPass Guest Authentication "](#) on page 273.
- Content asset management. See ["Content Manager"](#) on page 273.
- Guest Manager configuration. See ["Configuring Guest Manager "](#) on page 277.
- Hotspot Manager. See ["Hotspot Manager"](#) on page 507.
- Pages, including:
 - Fields, forms, and views in ClearPass Guest. See ["Customizing Fields"](#) on page 294 and ["Customizing Forms and Views"](#) on page 305.
 - Guest self-registration processes and forms. See ["Customizing Guest Self-Registration"](#) on page 341.
 - Web login pages. See ["Managing Web Logins"](#) on page 396.
 - Web pages. See ["Managing Web Pages"](#) on page 414.
- Receipts, including:
 - Digital passes. See ["Digital Passes"](#) on page 420.
 - Settings for emailing visitor account receipts. See ["Email Receipts and SMTP Services"](#) on page 435.
 - SMS visitor account receipt settings. See ["Customizing SMS Receipt"](#) on page 442.
 - Guest Manager print templates. See ["Customizing Print Templates "](#) on page 444.
- SMS services. See ["SMS Services"](#) on page 453.
- Translation packs. See ["About Translations"](#) on page 465.

Accessing Configuration

To access ClearPass Guest's application customization features, click the **Configuration** link in the left navigation.



Configuring ClearPass Guest Authentication

You can use the Configuration module to modify authentication settings for the ClearPass Guest application.

To configure ClearPass Guest's authentication settings, go to **Configuration > Authentication**. The **Authentication Settings** form opens.

Figure 174 *The Authentication Settings Form*

Authentication Settings	
Dynamic Authorization:	<input type="checkbox"/> Send a disconnect/re-authorization message to the NAS Global to automatically send disconnects when enabled/role values change. Requires a NAS Type supporting RFC-3576.
NAS Type:	Aruba Networks (RFC 3576 support) [v] Select the default type for network access servers.
RFC-3576 Bind Address:	0.0.0.0 Force a specific bind address for RFC-3576 requests. This may be needed in an AirGroup environment.
* Internal Auth Type:	PAP [v] Controls the RADIUS authentication type used for internal RADIUS authentication requests.
Security:	<input type="checkbox"/> Require HTTPS for guest access If checked, HTTP access by guests will be redirected to use HTTPS instead.
<input type="button" value="Save Changes"/>	

Table 111: *Authentication Settings Form*

Field	Description
Dynamic Authorization	If selected, Guest sends automatic disconnect or re-authorization messages when enabled values or role values change. This requires a network access server (NAS) type that supports RFC-3576.
NAS Type	Specifies the default type for network access servers.
RFC-3576 Bind Address	To force a specific bind address for RFC-3576 requests, enter a value. This might be needed in an AirGroup environment.
Internal Auth Type	Specifies the RADIUS authentication type used for internal RADIUS requests. Options include: <ul style="list-style-type: none">● PAP● CHAP● MS-CHAP
Security	If selected, redirects HTTP access to use HTTPS instead.
Save Changes	Saves your changes.

Content Manager



The Content Manager allows you to upload content items to ClearPass Guest. Content items are assets such as text, images, and animations. To work with your content items, go to **Configuration > Content Manager > Start Here**.

Content assets are organized into private files and public files. Private files are only available within the ClearPass application. Public files are accessible via HTTP/HTTPS for guest access using the application's built-in Web server.

This section includes:

- "Managing Content: Private Files and Public Files" on page 274
- "Uploading Content " on page 275
- "Downloading Content" on page 276
- "Creating a New Content Directory" on page 276

Managing Content: Private Files and Public Files

Content items are assets such as text, images, and animations. After you upload them to ClearPass, you can use them in registrations, receipts, digital passes, and so on.

To use a content item, you can insert a reference to it into any custom HTML editor within the application. To do this, select the content item you want to insert from the drop-down list located in the lower right corner of the HTML editor. The item will be inserted using HTML that is most suited to the type of content inserted. To manually reference a content item, you can use the URL of the item directly. For example, an item named **logo.jpg** could be accessed using a URL such as: **http://192.0.2.23/public/logo.jpg**.

Content items are organized into two categories, private files and public files, and stored and accessed separately:

- **Private Files**—Content items in the **Private Files** list are only available within the ClearPass application. These files are not accessible to guests. To work with your private content items, go to **Configuration > Content Manager > Private Files**. The **Private Files** list view opens.
- **Public Files**—Public files are accessible via HTTP/HTTPS for guest access using the application's built-in Web server. To work with your public content items, go to **Configuration > Content Manager > Public Files**. The **Public Files** list view opens.

The list views and procedures are the same for both private and public files. Columns in the list show the filename, owner, file type, last modification date, and file size.

Figure 175 *The List Views for the Public Files and for the Private Files Are Similar*

Name	Owner	Type	Date Modified	Size
autumnGraphic1.PNG	admin	image/png	2012-10-30 14:22	40.4 KB
autumnOffersContent1.txt	admin	text/plain	2012-10-30 14:23	0.0 KB
springGrapic1.PNG	admin	image/png	2012-10-30 14:23	40.4 KB

Table 112: Content Files List View, Private Files or Public Files

Field	Description
Upload New Content	Add a new content item from your system. See "Uploading Content " on page 275.
Download New Content	Add a new content item from another Web server. See "Downloading Content" on page 276.
Create New Directory	Add a new subdirectory under the currently displayed directory. See "Creating a New Content Directory" on page 276.
Properties	Displays the content file's properties. Information includes the file's owner, filename, description, type, image size, date modified, and file size.
Delete	Deletes the content file from the directory. You will be asked to confirm the deletion.
Rename	Modify the file's name or move it to another directory.
Download	Download a copy of the file to your local Downloads folder.
View Content	Opens a preview of the content item in a new browser tab.
Quick View	Displays a preview of the content item within the file's row in the list.

Uploading Content

1. To add a new content item using your Web browser, go to **Configuration > Content Manager**, and then go to either **Private Files** or **Public Files**, as appropriate. The list view opens. The procedures are the same for both private and public files.
2. Click the **Upload New Content** tab . The **Add Content** form opens.

Figure 176 The Add Content Form

The screenshot shows the 'Add Content' form with the following fields and options:

- Size Limit:** Maximum file upload size: 15.0 MB.
- * File:** Choose File button, No file chosen, Choose a file to upload from your computer.
- Description:** Text area, Enter an optional description of this content item.
- Overwrite:** Replace existing item with same name, Select this option to overwrite an existing content item that has the same name.
- Buttons:** Upload Content, Cancel

3. In the **File** row, click **Browse** to navigate to the file you wish to upload. The Maximum file size is 15 MB. You can upload single content files, multiple content asset files and folders, or a Web deployment archive. To upload multiple assets, first compress the files as a "tarball" or zip file, then browse to it in the File field. Allowed file formats are .tgz, .tar.gz, .tb2, .tar.bz2, or .zip. When you have uploaded the file, the Extract option lets you create the new directory, navigate into it, and view and extract the files. Directory structure is preserved when extracting.
4. You may enter a description of the content assets in the **Description** text area.

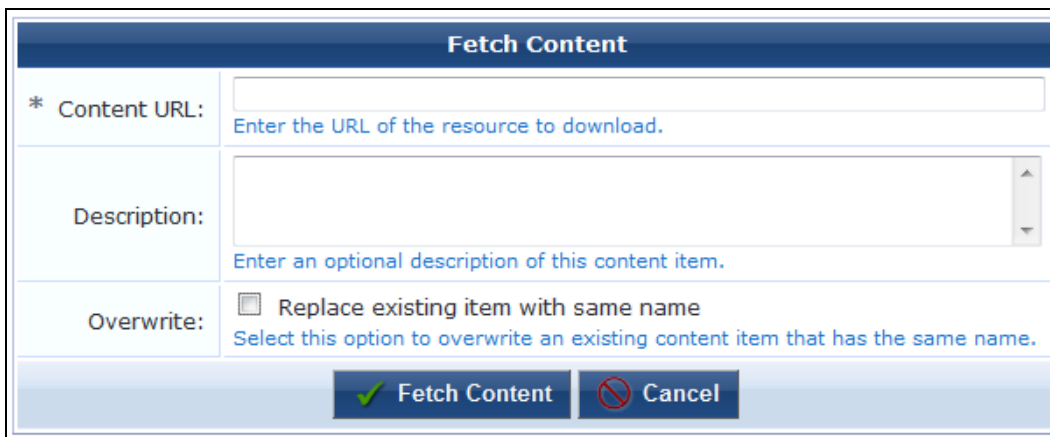
- To overwrite a previous file of the same name, mark the **Overwrite** check box.
- Click **Upload Content** to upload the file.

If you clicked the **Upload New Content** link on the **Private Files** list view, the file is added to the **private** directory in ClearPass. If you clicked the link on the **Public Files** list view, it is added to the **public** directory on the Web server. You can reference the file when creating custom HTML templates.

Downloading Content

- To add a new content item from the internet or another Web server, go to **Configuration > Content Manager**, and then go to either **Private Files** or **Public Files**, as appropriate. The list view opens. The procedures are the same for both private and public files.
- Click the **Download New Content** tab. The **Fetch Content** form opens.

Figure 177 *The Fetch Content Form*



Fetch Content	
* Content URL:	<input type="text"/> Enter the URL of the resource to download.
Description:	<input type="text"/> Enter an optional description of this content item.
Overwrite:	<input type="checkbox"/> Replace existing item with same name Select this option to overwrite an existing content item that has the same name.
<input type="button" value="Fetch Content"/> <input type="button" value="Cancel"/>	

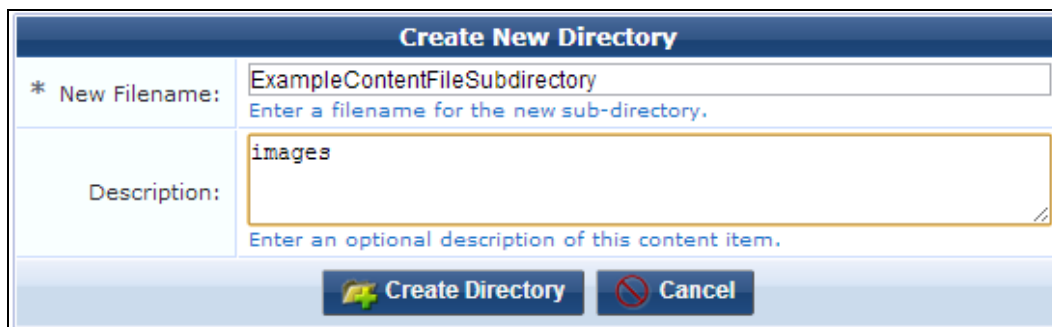
- In the **Content URL** row, enter the URL of the content item to download. Allowed formats are HTTP, HTTPS, and FTP only.
- You may enter a description of the content assets in the **Description** text area.
- To overwrite a previous file of the same name, mark the **Overwrite** check box.
- Click **Fetch Content** to download the file.

If you clicked the **Upload New Content** link on the **Private Files** list view, the file is added to the **private** directory in ClearPass. If you clicked the link on the **Public Files** list view, it is added to the **public** directory on the Web server. You can reference the file when creating custom HTML templates.

Creating a New Content Directory

- To add a new content subdirectory under either the private or public directory, go to **Configuration > Content Manager**, and then go to either **Private Files** or **Public Files**, as appropriate. The list view opens. The procedures are the same for both private and public files.
- Click the **Create New Directory** tab. The **Create New Directory** form opens.

Figure 178 *The Create New Directory Form*



Create New Directory	
* New Filename:	ExampleContentFileSubdirectory Enter a filename for the new sub-directory.
Description:	images Enter an optional description of this content item.
<input type="button" value="Create Directory"/> <input type="button" value="Cancel"/>	

3. In the **New Filename** row, enter the name for the new subdirectory.
4. You may enter a description of the directory in the **Description** text area.
5. Click **Create Directory**.

If you clicked the **Create New Directory** link on the **Private Files** list view, the subdirectory is added under the **private** directory in ClearPass. If you clicked the link on the **Public Files** list view, it is added under the **public** directory on the Web server. You can reference files in this subdirectory when creating custom HTML templates.

Configuring Guest Manager



The Guest Manager module allows the entire guest account provisioning process to be customized. This is useful in many different situations, such as:

- **Self-registration** — Allow your guests to self-register and create their own temporary visitor accounts.
- **Visitor surveys** — Define custom fields to store data of interest to you, and collect this information from guests using customized forms.
- **Branded print receipts** — Add your own branding images and text to print receipts.
- **SMS and email receipts** — Include a short text message with your guest's username and password, or send HTML emails containing images.
- **Advanced customization** — ClearPass Guest is flexible and can be used to provide location sensitive content and advertising.

Default Settings for Account Creation

The **Configure Guest Manager** plugin configuration form lets you control the default settings for account creation.

To modify settings for the Guest Manager plugin configuration, go to **Configuration > Guest Manager**. The **Configure Guest Manager** form opens.

You can also access this form from the **Administration > Plugin Manager > Guest Manager > Configuration** link.

Figure 179 *The Configure Guest Manager Form, Username Options Area*

Configure Guest Manager	
Username Options	
* Username Type:	<input type="text" value="Random digits"/> <small>The method used to generate random account usernames.</small>
* Username Length:	<input type="text" value="8"/> <small>The length, in characters, of generated account usernames.</small>
Username Example:	29087953 Generate
Initial Sequence:	<input type="text"/> <small>Create multi next available sequence number. These values will be used when multi_initial_sequence is set to -1.</small>

Table 113: *Configure Guest Manager Form, Username Options Area*

Field	Description
Username Type	(Required) Specifies the default method used to generate random account usernames (when creating groups of accounts). This may be overridden by using the random_username_method field.
Username Length	(Required) Default length of random account usernames (when creating groups of accounts). This may be overridden by using the random_username_length field. This field is displayed if the Username Type is set to "Random digits", "Random letters", "Random letters and digits" or "Sequential numbering".
Username Example	Displays a sample username generated according to the rules specified by the selections in the Username Type and Username Length fields. You can click the Generate link to view different examples.
Username Format	Specifies the format of the username to be created. This field is displayed if the Username Type is set to "Format picture". See " Format Picture String Symbols " on page 736 for a list of the special characters that may be used in the format string. This may be overridden by using the random_username_picture field.
Initial Sequence	This field contains the next available sequence number for each username prefix that has been used. Automatic sequence numbering is used when the value of the multi_initial_sequence field is set to -1. The username prefix is taken from the multi_prefix field when usernames are automatically generated using the "nwa_sequence" method. You can edit the values stored here to change the next sequence numbers that will be used. This is an automatically managed field; in most situations there is no need to edit it.

Figure 180 *The Configure Guest Manager Form, Password Options Area*

Password Options	
* Random Password Type:	<input type="text" value="Random digits"/> The method used to generate a random account password.
* Random Password Length:	<input type="text" value="8"/> Number of characters to include in randomly-generated account passwords.
* Password Complexity:	<input type="text" value="No password complexity requirement"/> Password complexity to enforce for manually-entered guest passwords. Requires the random password type 'A password matching the password complexity requirements' and the field validator 'NwaisValidPasswordComplexity' for manual password entry.
* Minimum Password Length:	<input type="text" value="8"/> The minimum number of characters that a guest password must contain.
* Disallowed Password Characters:	<input type="text"/> Characters which cannot appear in a user-generated password.
Disallowed Password Words:	<input type="text"/> Comma separated list of words disallowed in the random words password generator. Note there is an internal exclusion list built into the server.
Password Example:	33248842 Generate
Password Logging:	<input checked="" type="checkbox"/> Log guest account passwords Whether to record passwords for guest accounts in the application log.
Password Display:	<input type="checkbox"/> View guest account passwords If selected, guest account passwords may be displayed in the list of guest accounts. This is only possible if operators have the View Passwords privilege.

Table 114: *Configure Guest Manager Form, Password Options Area*

Field	Description
Random Password Type	(Required) Default method used to generate random account passwords (when creating groups of accounts). This may be overridden by using the random_password_method field.
Random Password Length	(Required) Default length of random account passwords (when creating groups of accounts). This may be overridden by using the random_password_length field.
Password Format	(Required) Specifies the format of the password to be created. This may be overridden by using the random_password_picture field. This field is displayed if the Password Type field is set to "Format picture". See " Format Picture String Symbols " on page 736 for a list of the special characters that may be used in the format string.
Password Complexity	(Required) Policy to enforce when guests change their account passwords using the guest self-service user interface. Different levels of password complexity can require guests to select passwords that contain different combinations of uppercase letters, lowercase letters, digits and symbols (!#\$%&()*+,-./:;<=>?@[\\]^_{ }~.). Options include: <ul style="list-style-type: none"> • No password complexity requirement • At least one uppercase and one lowercase letter • At least one digit • At least one letter and one digit • At least one of each: uppercase letter, lowercase letter, digit • At least one symbol • At least one of each: uppercase letter, lowercase letter, digit, and symbol
Minimum Password Length	(Required) Minimum acceptable password length for guests changing their account passwords. The original default password length is six characters.
Disallowed	(Required) Special characters that should not be allowed in a guest password. Spaces are not

Table 114: *Configure Guest Manager Form, Password Options Area(Continued)*

Field	Description
Password Characters	allowed by default. You can specify special characters, numbers, and letters to exclude from passwords—for example, letters and numbers that can look similar, such as i, l, 1, 0, O, o, 5, S, 8, B.
Disallowed Password Words	Comma- separated list of words that are disallowed and will not be created by the random words password generator.
Password Example	Displays a sample password generated according to the rules specified by the selections in the Password Type and Password Length fields. You can click the Generate link to view different examples.
Password Logging	If selected, passwords for created guest accounts are logged in the application log and may be recovered from there. For increased security, you may prevent this password from being logged by deselecting this check box.
Password Display	If selected, enables the display of visitor account passwords in the user list. To reveal passwords, the password field must be added to the “guest_users” or “guest_edit” view, and the operator profile in use must also have the View Passwords privilege.

Figure 181 *The Configure Guest Manager Form, Expiration Options Area*

Expiration Options

* **Expire Action:** Disable at specified time
Default action to take when the expire_time is reached.
 Note that a logout can only occur if the NAS is RFC-3576 compliant.

* **Expiration Options:** 1 | 1 hour
2 | 2 hours
3 | 3 hours
4 | 4 hours
6 | 6 hours
8 | 8 hours
12 | 12 hours
16 | 16 hours
20 | 20 hours
The available options to select from when choosing the expiration time of a guest account (expire_after).
 Expiration times are specified in hours.

* **Modify Expiration Options:** none | Account will not expire
now | Now
plus 1h | Lengthen expiration time
by 1 hour
plus 1d | Lengthen expiration time
by 1 day
plus 1w | Lengthen expiration time
by 1 week
minus 1h | Shorten expiration time
The available options to select from when modifying an account's expiration (modify_expire_time).
 Note some items may be dynamically removed based on the state of the account.

* **Lifetime Options:** 0 | N/A
60 | 1 hour
120 | 2 hours
180 | 3 hours
240 | 4 hours
360 | 6 hours
480 | 8 hours
720 | 12 hours
1440 | 1 day
The available options to select from when choosing the lifetime of a guest account (expire_postlogin).
 Lifetime values are specified in minutes.

Table 115: *Configure Guest Manager Form, Expiration Options Area*

Field	Description
Expire Action	(Required) Default action when the expiration time is reached. Available options available are: <ul style="list-style-type: none"> ● Disable at specified time ● Delete and logout at specified time ● Delete at specified time ● Disable and logout at specified time
Expiration Options	(Required) The options that should be available to select from when choosing the expiration time of a guest account (expire_after). These options are displayed as the values of the “Expires After” field when creating a user account. Values are in hours for relative account expiration times.
Modify Expiration Options	(Required) The options that should be available to select from when modifying an account's expiration (modify_expire_time). Some items may be dynamically removed based on the state of the account.
Lifetime Options	(Required) The options that should be available to select from when choosing the lifetime for a guest account (expire_postlogin). These options are displayed as the values of the “Account Lifetime” field when creating a user account. Values are in minutes for relative account lifetimes.

Figure 182 *The Configure Guest Manager Form, Expiration Warning Options Area*

Expiration Warning Options

Account Expiry Warning: Notify users before their user credentials expire
If checked users will receive an email notification when their device's network credentials are due to expire.

* If Email is Unknown:
Specify where to send emails to if the users account doesnt have an email address recorded

* Subject Line:
Enter a subject for the notification email.

* Email Message:
The plain text or HTML print template to use when generating an email message

* Email Skin:
The format in which to send email receipts

* Send Copies:
Specify when to send to the recipients in the Copies To list.

Table 116: *Configure Guest Manager Form, Expiration Warning Options Area*

Field	Description
Account Expiry Warning	If selected, users will receive an email notification before their device's network credentials are about to expire. Expiration warning configuration options are added to the form.
Account Expiry Notification	(Required) Number of days before account expiration that the notification email will be sent. You may specify a number from 1 through 30.
If Email is Unknown	(Required) Specifies where to send emails if the user's account does not have an email address recorded. Options include: <ul style="list-style-type: none"> ● Do not send any message ● Send a message to a fixed email address ● Send a message to username@domain
Subject Line	(Required) Enter the subject line for the notification email.
Email	(Required) Specifies the print template to use when generating the email message. Options

Table 116: *Configure Guest Manager Form, Expiration Warning Options Area(Continued)*

Field	Description
Message	include: <ul style="list-style-type: none"> ● Account List ● Certificate Expiry ● Download Receipt ● Guest Account Expiry ● GuestManager Receipt ● One account per page ● SMS Receipt ● SMS Sponsor Confirmation Alert ● Sponsorship Confirmation ● Two-column scratch cards
Email Skin	(Required) Specifies the format for the email receipts. Options include: <ul style="list-style-type: none"> ● No skin - Plain text only ● No skin - HTML only ● No skin - Native receipt format ● Use the default skin ● Aruba ClearPass Skin ● Blank Skin ● ClearPass Guest Skin ● Custom Skin 1 ● Custom Skin 2 ● Galleria Skin ● Galleria Skin 2
Send Copies	(Required) Specifies when to send to recipients in the Copies To list. Options include: <ul style="list-style-type: none"> ● Do not send copies ● Always send using "cc:" ● Always send using "Bcc:"

Figure 183 *The Configure Guest Manager Form, Receipt Options Area*

Receipt Options	
Site SSID:	<input type="text" value="Aruba"/> <p><small>The SSID of the wireless LAN, if applicable. This will appear on guest account print receipts.</small></p>
Site WPA Key:	<input type="text"/> <p><small>The WPA key for the wireless LAN, if applicable. This will appear on guest account print receipts.</small></p>
Receipt Printing:	<input type="checkbox"/> Require click to print <small>Guest receipts can print simply by selecting the template in the dropdown, or by clicking a link.</small>

Table 117: *Configure Guest Manager Form, Receipt Options Area*

Field	Description
Site SSID	Public name of the wireless local area network (WLAN). The default setting for this field is Aruba , and can be changed. The site SSID is displayed in the guest receipt as the WiFi Network , shown below this table.
Site WPA Key	Encryption key used to secure the wireless network. If a value is entered in this field, it will appear on guest print receipts.
Receipt Printing	<p>If selected, the receipt page provides a drop-down list of print templates and a Print link that must be clicked to display the account receipt:</p> <div style="border: 1px solid #ccc; padding: 5px; margin: 5px 0;"> Select a print template... Print </div> <p>If this option is <u>not</u> selected, the default behavior is to provide a drop-down list of print templates and to open a new window when one is selected:</p> <div style="border: 1px solid #ccc; padding: 5px; margin: 5px 0;"> Open print window using template... </div>

Figure 184 *Example Guest Receipt, Showing Site SSID Displayed as the WiFi Network*

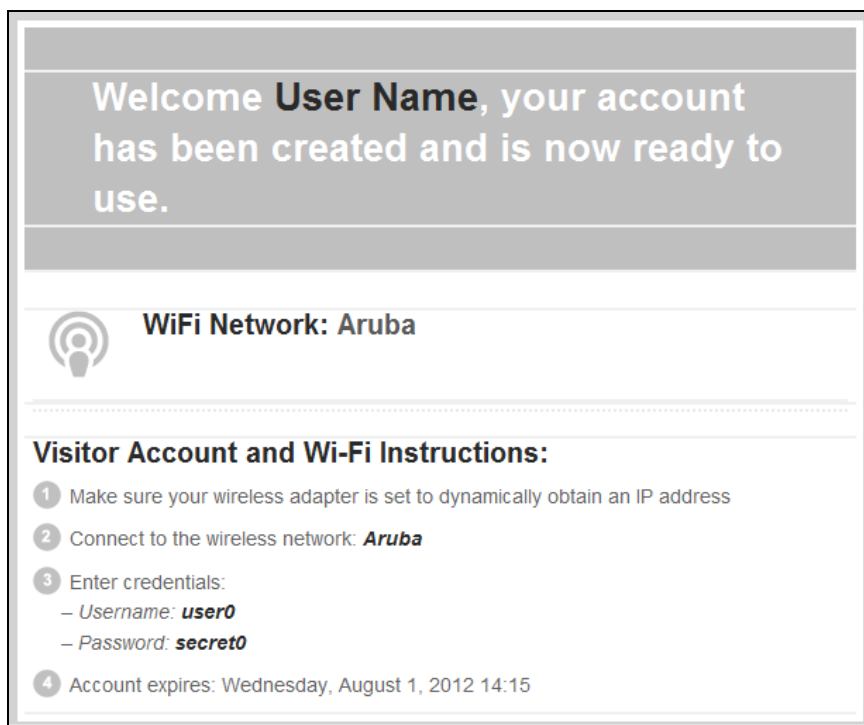


Figure 185 *The Configure Guest Manager Form, General Options Area*

General Options	
Terms Of Use URL:	<input type="text" value="terms.php"/> <p>The URL of a terms and conditions page. The URL will appear in any terms checkbox with: {nwa_global name=guest_account_terms_of_use_url} It is recommended to upload your terms in Content Manager, where the files will be referenced with the "public/" prefix. Alternatively, you can edit Terms and Conditions under Configuration > Pages > Web Pages. If your site is hosted externally, be sure the proper access control lists (ACLs) are in place. If terms are not required, it is recommended to edit the terms field on your forms to a UI type "hidden" and an Initial Value of 1.</p>
Active Sessions:	<input type="text" value="1"/> <p>Enable limiting the number of active sessions a guest account may have. Enter 0 to allow an unlimited number of sessions.</p>
About Guest Network Access:	<input type="text" value="Insert..."/> <p>Template code to display on the Guest Manager start page, under the "About Guest Network Access" heading. Leave blank to use the default text, or enter a hyphen ("-") to remove the default text and the heading.</p>
<input type="button" value="Save Configuration"/>	

Table 118: *Configure Guest Manager Form, General Options Area*

Field	Description
Terms of Use URL	URL of a terms and conditions page provided to sponsors. The default, terms.php , displays the preconfigured Web page provided at Configuration > Pages > Web Pages > Terms and Conditions . You can edit that page, or you can use Content Manager to upload an HTML file describing the terms and conditions of use (See " Managing Content: Private Files and Public Files " on page 274). <ul style="list-style-type: none"> • If your site is hosted externally, be sure the proper access control lists (ACLs) are in place. • If terms are required, it is best practice to edit the terms field on you forms to a UI type "hidden" and an initial value of 1.
Active Sessions	Default maximum number of active sessions that should be allowed for a guest account. This may be overridden by using the simultaneous_use field when creating or editing a guest account.
About Guest Network Access	Specifies the template code to display on the Guest Manager start page under the "About Guest Network Access" heading. <ul style="list-style-type: none"> • To use the default text, leave this field blank. • To specify custom text, select an item in the drop-down list. • To remove the default text and the heading, enter a single hyphen (-) in this field.

About Fields, Forms, and Views

- A field is a named item of information. It may be used to display information to a user as static text, or it may be an interactive field where a user can select an option or enter text.
- A form is a group of fields that is used to collect information from an operator.
- A view is a grouping of fields that is used to display information to an operator.

Business Logic for Account Creation

When guest accounts are created, there are certain rules that must be followed in order to create a valid account. These rules apply to all accounts, regardless of how the account was created.

The business logic rules that control all guest account creation are described below. To see the display name corresponding to a field name, go to **Configuration > Pages > Fields** and scroll to the field name. Display names are shown in the **Column Title** column.

For information on customizing fields, see "[Customizing Fields](#)" on page 294.

Verification Properties

The following table describes the verification properties fields for guest account creation at **Configuration > Pages > Fields**.

Table 119: *Verification Properties Fields*

Field	Description
creator_accept_terms	This field must be set to 1, indicating the creator has accepted the terms of use for creating the account. If the field is not present or is not set to 1, the visitor account is not created.
password2	If this field is specified, its value must be equal to the “password” field, or else the visitor account is not created.
auto_update_account	If this field is present and set to a non-zero value, account creation will not fail if the username already exists – any changes will be merged into the existing account using an update instead.

Basic User Properties

The following table describes the basic user properties fields for guest account creation at **Configuration > Pages > Fields**.

Table 120: *Basic User Properties Fields*

Field	Description
username	This field is the name for the visitor account and may be provided directly. If this field is not specified, then use the email address from the email field, and if that is also not specified, then randomly generate a username (according to the value of the random_username_method and random_username_length fields).
modify_password	This field controls password modification for the visitor account. It may be set to one of these values: <ul style="list-style-type: none">• “reset” to randomly generate a new password according to the values of the random_password_method and random_password_length fields• “password” to use the password specified in the password field• “random_password” to use the password specified in the random_password field• If blank or unset, the default password behavior is used, which is to use any available value from the random_password field and the password field, or assume that “reset” was specified otherwise.
password	This field is the password for the visitor account and may be provided directly. If this field is not specified, then randomly generate a password (according to the values of the random_password_method and random_password_length fields).
role_id	This field is the role to assign to the visitor account and may be specified directly. If this field is not specified, then determine the role ID from the role_name field. If no valid role ID is able to be determined, the visitor account is not created.
simultaneous_use	This field determines the maximum number of concurrent sessions allowed for the visitor account. If this field is not specified, the default value from the GuestManager configuration is used.
random_username_method	The method used to generate a random account username. If not specified, the default value from the GuestManager configuration is used.

Table 120: Basic User Properties Fields(Continued)

Field	Description
random_username_length	The length in characters of random account usernames. If not specified, the default value from the GuestManager configuration is used.
random_password_method	The method used to generate a random account password. If not specified, the default value from the GuestManager configuration is used.
random_password_length	The length in characters of random account passwords. If not specified, the default value from the GuestManager configuration is used. The default password length is six characters.

Visitor Account Activation Properties

The following table describes the visitor account activation properties fields for guest account creation at **Configuration > Pages > Fields**.

Table 121: Visitor Account Activation Properties Fields

Field	Description
enabled	This field determines whether the account is enabled or disabled; if not specified, the default is 1 (account is enabled).
do_schedule	<p>These fields are used to determine the time at which the visitor account will be activated.</p> <ul style="list-style-type: none"> If modify_schedule_time is "none", then the account is disabled and has no activation time set. If modify_schedule_time is "now", then the account is enabled and has no activation time set. If modify_schedule_time is a value that specifies a relative time change, for example "+1h", then the visitor account's activation time is modified accordingly. If modify_schedule_time is a value that specifies an absolute time, for example "2010-12-31 17:00", then the visitor account's activation time is set to that value. If modify_schedule_time is "schedule_after" or "schedule_time", then the activation time is determined according to the schedule_after or schedule_time fields as explained below. <ul style="list-style-type: none"> If schedule_after is set and not zero, then add that time in hours to the current time and use it as the activation time (setting do_schedule to 1); enabled will be set to zero. Otherwise, if schedule_after is zero, negative or unset, and schedule_time has been specified, use that activation time (set do_schedule to 1 and enabled to 0). If the schedule_time specified is in the past, set do_schedule to 0 and enabled to 1. Otherwise, if schedule_time if not specified, then the visitor account has no activation time and do_schedule will default to zero.
modify_schedule_time	
schedule_after	
schedule_time	

Visitor Account Expiration Properties

The following table describes the visitor account expiration properties fields for guest account creation at **Configuration > Pages > Fields**.

Table 122: *Visitor Account Expiration Properties Fields*

Field	Description
do_expire	<p>These fields are used to determine the time at which the visitor account will expire.</p> <ul style="list-style-type: none">• If modify_expire_time is "none", then the account has no expiration time set.• If modify_expire_time is "now", then the account is disabled and has no expiration time set.• If modify_expire_time is a value that specifies a relative time change, for example "+1h", then the visitor account's expiration time is modified accordingly.
modify_expire_time	<ul style="list-style-type: none">• If modify_expire_time is a value that specifies an absolute time, for example "2010-12-31 17:00", then the visitor account's expiration time is set to that value.• If modify_expire_time is "expire_after" or "expire_time", then the expiration time is determined according to the expire_after or expire_time fields as explained below.• If expire_after is set and not zero and the account will be activated immediately, then add the value in hours to the current time to determine the expiration time.• If expire_after is set and not zero and account activation is set for a future time (schedule_time) instead of the current time, then the expiration time is calculated relative to the activation time instead of the current time.
expire_after	<ul style="list-style-type: none">• Otherwise, if expire_after is zero, negative or unset, and expire_time has been specified, use that expiration time. If the expire_time specified is in the past, set do_expire to 0 and ignore the specified expiration time.
expire_time	<ul style="list-style-type: none">• If the expire_timezone field is used in conjunction with expire_time and a time zone and date are selected, the date calculation is adjusted relative to the time zone.• Otherwise, if expire_time is not specified, then the expire_time is not set and do_expire will always be set to zero.• If the do_expire field is not included in the form, the default expiration action is 4, Logout and Delete. This can be configured on the Customize Guest Manager page.
expire_postlogin	<p>This field determines the amount of time after the initial login for which the visitor account will remain valid. If this field is not specified, the default value is 0 (account lifetime not set).</p>
expire_usage	<p>This field determines the total amount of login time permitted for the visitor account. If this field is not specified, the default value is 0 (account usage is unlimited).</p>

Other Properties

- All other properties specified at creation time are stored with the visitor account (for example, **email**, **visitor_name**, **visitor_company**, **visitor_phone**, **sponsor_name** as well as any custom fields that have been defined).

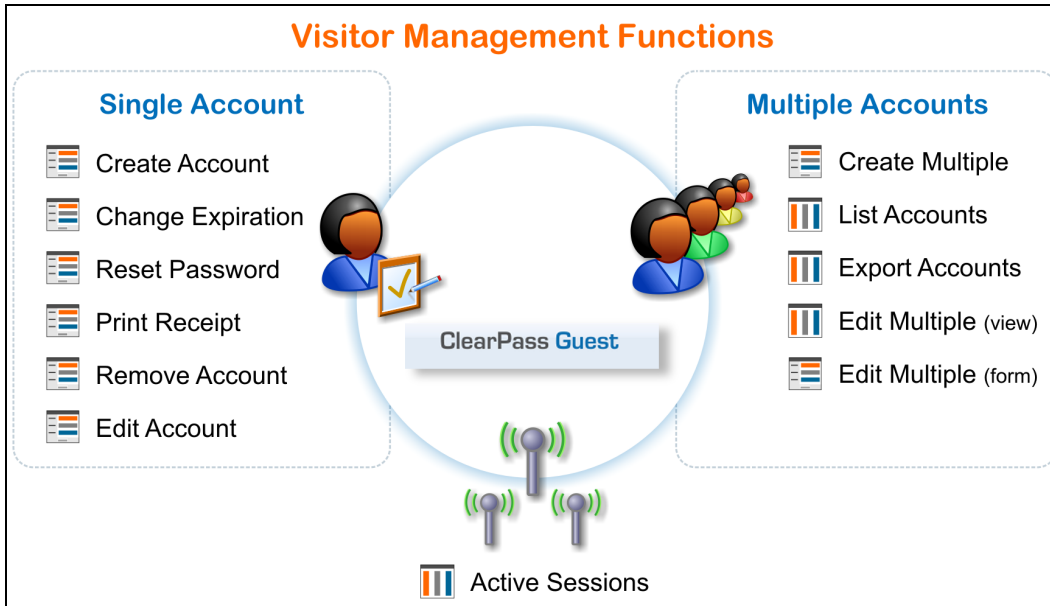
Standard Fields

See "[Field, Form, and View Reference](#)" on page 724 for a listing of the standard fields shipped with ClearPass Guest.

Standard Forms and Views

The figure below shows the standard forms and views in the application.

Figure 186 Standard Forms and Views in the ClearPass Guest Application



The table below lists all the forms and views used for visitor management.

Table 123: Visitor Management Forms and Views

Name	Type	Visitor Management Function	Editable?
change_expiration	Form	Change Expiration	Yes
create_multi	Form	Create Multiple	Yes
create_user	Form	Create Account	Yes
guest_edit	Form	Edit Account	Yes
guest_export	View	Export Accounts	Yes
guest_multi	View	Edit Multiple Accounts	Yes
guest_multi_form	Form	Edit Multiple Accounts	Yes
guest_receipt	Form	Print Receipt	No
guest_register	Form	Guest Self-Registration	Yes
guest_register_receipt	Form	Guest Self-Registration Receipt	Yes
guest_sessions	View	Active Sessions	Yes
guest_users	View	List Accounts	Yes
remove_account	Form	Remove Account	No
reset_password	Form	Reset Password	No

These forms are accessed directly:

- **create_multi** form – multiple account creation
- **create_user** form – sponsored account creation
- **guest_register** form – guest self-registration form

These forms are accessed through the action row of the **guest_users** view:

- **change_expiration** form – change expiration time for a single account
- **guest_multi_form** form – editing multiple accounts
- **guest_edit** form – editing single account
- **reset_password** form – reset password for a single account

These forms are the standard self-registration forms:

- **guest_register** form – self-registration form
- **guest_register_receipt** form – self-registration receipt

These standard views are defined in Guest Manager:


- **guest_export** view – view used when exporting guest account information
- **guest_multi** view – displays a list of guest accounts optimized for working with multiple accounts
- **guest_sessions** view – displays a list of current or historical sessions (See "[Active Sessions Management](#)" on page 35.)
- **guest_users** view – displays a list of guest accounts optimized for working with individual accounts

Configuring Access Code Logins

This section explains how to configure Guest Manager to create multiple accounts that have the ability to log in with only the username. We will refer to this as an **Access Code**.

Customize Random Username and Passwords

In this example we will set the random usernames and passwords to be a mix of letters and digits.

1. Go to **Configuration > Guest Manager**. The **Configure Guest Manager** form opens.
2. In the **Username Type** field, select **Random Letters and digits**. The generator matching the complexity will also include a mix of upper and lower case letters.
3. In the **Username Length field**, select **6** characters.
4. Configure other settings. See "[Default Settings for Account Creation](#)" on page 277 for a description. Click  **Save Configuration** to save your changes.

Create the Print Template

By default, the print templates include username, password, and expiration, as well as other options. For the purpose of access codes, we only want the username presented. This access code login example bases the print template off an existing scratch card template.


1. Go to **Configuration > Receipts > Templates**.
2. Select **Two-column scratch cards**, and then click **Duplicate**.
3. Select the **Copy of Two-column scratch cards** template, and then click  **Edit**.
4. In the **Name** field, substitute **Access Code** for **Username** as shown below.

Figure 187 *The Edit Print Template Form*

Edit Print Template	
* Name:	Copy of Two-column access codes <small>A name for the print template. This name is used to select which template to use when printing a list of accounts.</small>
Enabled:	<input checked="" type="checkbox"/> Allow the use of this print template
* Layout:	2-column list <small>Choose how the guest account list will be printed when using this template.</small>
User Account HTML:	<pre> <tr> <th class="nwaTop" colspan="3">Access Details</th> </tr> </thead> <tbody> <tr> <td class="nwaBody" rowspan="99" valign="top"></td> <th class="nwaLeft">Access Code</th> <td class="nwaBody" style="width:12em">{\$u.username escape}</td> </tr> <tr> <th class="nwaLeft">Error</th> <td class="nwaBody">{\$u.create_result.message escape}</td> </tr> </tbody> </table> </pre>

5. Remove extraneous data from the **User Account HTML** field. Example text is shown below.

```

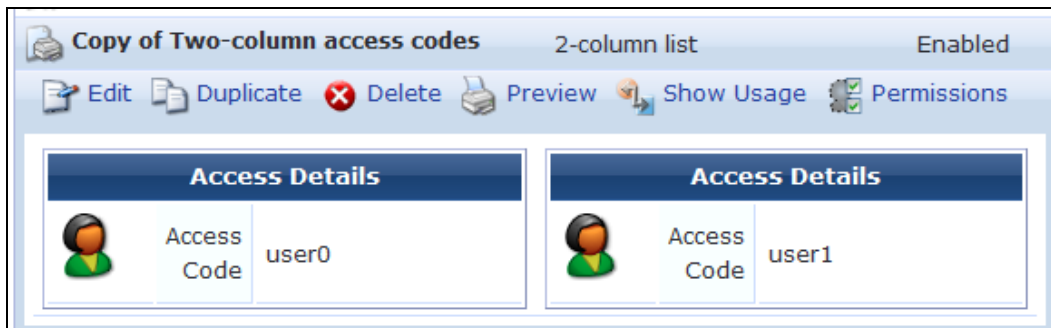
<table {$table_class_content}>
  <thead>
  <tr>
    <th class="nwaTop" colspan="3">Access Details</th>
  </tr>
</thead>
<tbody>
  <tr>
    <td class="nwaBody" rowspan="99" valign="top"></td>
    <th class="nwaLeft">Access Code</th>
<td class="nwaBody" style="width:12em">{$u.username|htmlspecialchars}</td>
  </tr>
  <tr>
    <th class="nwaLeft">Error</th>
    <td class="nwaBody"><span class="nwaError">{$u.create_result.message}</span></td>
  </tr>
</tbody>
</table>

```

6. Click  **Save Changes** to save your settings.

7. To preview the new template, select the template in the **Guest Manager Print Templates** list, then click **Preview**. The template is displayed. The template created by the example text given above would look like this:

Figure 188 Example Template

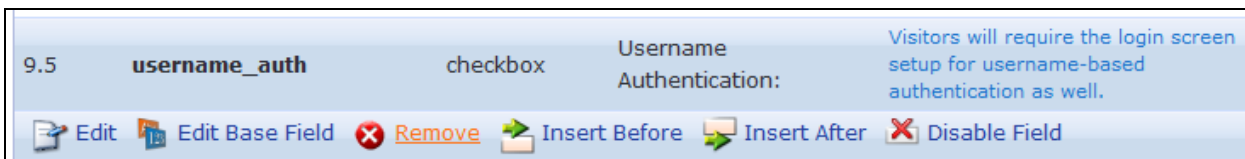


Customize the Guest Accounts Form

Next, modify the **Guest Accounts** form to add a flag that allows access-code based authentication.

1. Go to **Configuration > Pages > Forms & Views**.
2. In the **Customize Forms & Views** list, select **create_multi** and then click **Edit Fields**.
3. In the **Edit Fields** list, look for a field named **username_auth**. If the field exists but is not bolded and enabled, select it and click **Enable Field**.

Figure 189 The `username_auth` Field in the Customize Form Fields List View



If the field does *not* exist, select any field in the list (for example, **num_accounts**) and then select **Insert After**. Click the **Field Name** drop-down list, select **username_auth** and allow the page to refresh. The defaults should be acceptable, but feel free to customize the label or description.


4. Click **Save Changes** to save your settings. After the field is enabled or inserted, you should see it bolded in the list of fields.

Create the Access Code Guest Accounts

After the account fields have been customized, you can create new accounts.


1. Go to **Guest > Create Multiple**.
2. In the **Create Multiple Guest Accounts** form, select the check box in the **Username Authentication** row that was added in the procedure above (see "[Customize the Guest Accounts Form](#)" on page 291). If you do not select this check box and if the username is entered on the login screen, the authentication will be denied. The example shown below will create 10 accounts that will expire in two weeks, or four hours after the visitors first log in, whichever comes first.


Figure 190 *The Create Multiple Guest Accounts Form, Showing the Username Authentication Field*


Create Guest Accounts	
* Number of Accounts:	<input type="text" value="10"/> Number of visitor accounts to create.
Username Authentication:	<input checked="" type="checkbox"/> Allow visitor access using their username only Visitors will require the login screen setup for username-based authentication as well.
Account Activation:	<input type="text" value="Now"/> Select an option for changing the activation time of this account.
Account Expiration:	<input type="text" value="Account expires after..."/> Select an option for changing the expiration time of this account.
Expires After:	<input type="text" value="2 weeks"/> Amount of time before this visitor account will expire.
* Account Role:	<input type="text" value="[Contractor]"/> Role to assign to this visitor account.
	


3. Click **Create Accounts** to display the **Finished Creating Guest Accounts** page. If you create a large number of accounts, they are created at one time but might not all be displayed at the same time. (This will not affect the printing action in the following step.)

Figure 191 *The Account Details Displayed for Multiple Accounts*

Account Details		
	Username	01973984
	Password	47468940
	Role	[Contractor]
	Current State	Active
	Account Activation	Wednesday, 31 October 2012, 06:23 AM
	Account Expiration	Wednesday, 14 November 2012, 05:23 AM

Account Details		
	Username	30759520
	Password	71701546
	Role	[Contractor]
	Current State	Active
	Account Activation	Wednesday, 31 October 2012, 06:23 AM
	Account Expiration	Wednesday, 14 November 2012, 05:23 AM

Account Details		
	Username	28603627
	Password	69265462
	Role	[Contractor]
	Current State	Active
	Account Activation	Wednesday, 31 October 2012, 06:23 AM
	Account Expiration	Wednesday, 14 November 2012, 05:23 AM

Account Details		
	Username	77564827
	Password	68704971
	Role	[Contractor]
	Current State	Active
	Account Activation	Wednesday, 31 October 2012, 06:23 AM
	Account Expiration	Wednesday, 14 November 2012, 05:23 AM

4. Confirm that the accounts settings are as you expected with respect to letters and digits in the username and password, expiration, and role.
5. Click the **Open print window using template** drop-down list and select the new print template you created using this procedure See "[Create the Print Template](#)" on page 289 for a description of this procedure. A new window or tab will open with the cards.

Pages



The Pages area of the user interface lets you customize the pages that are available to guests and sponsors. To work with pages configuration, go to **Configuration > Pages > Start Here**.

This section includes:

- "Customizing Fields" on page 294
- "Customizing Forms and Views" on page 305
- "Customizing Guest Self-Registration" on page 341
- "Managing Web Logins" on page 396

Customizing Fields




Custom fields are fields that you define yourself to cater for areas of interest to your organization. You are able to define custom fields for your guest accounts as well as edit the existing fields.

In addition you can delete and duplicate fields. For your convenience you are also able to list any forms or views that use a particular field.



Fields that have a lock symbol  cannot be deleted.















Fields

Define custom fields for visitor accounts or change the behaviour of existing fields.

To work with fields or create a new field, go to **Configuration > Pages > Fields**. The **Customize Fields** list view opens.






Figure 192 *The Customize Fields List View*

	△ Name	Column Title	Type
	account_activation The current activation time in long form.	Activation	string 
	airgroup_enable Flag indicating that this account has been created for AirGroup use.	AirGroup	bool 
	airgroup_shared Flag indicating that this account has been created by an AirGroup administrator for sharing.	Shared	bool 
 Edit  Duplicate  Show Forms  Show Views			

All fields that have been defined are included in the list. To display only the fields that have been created, click the  **Custom Fields Only** link in the bottom row of the list view. To return to displaying all fields, click the  **All Fields** link.

You can click a field's row in the list or use the links provided on the page for additional options:

Table 124: *The Customize Fields List*

Field	Description
Edit	Edit a field's basic properties. The Edit Field form opens. You can make changes to the description or other properties. For an existing field, the name and type cannot be changed. See " Creating a Custom Field " on page 295.
Duplicate	Creates a copy of the field to use as a basis for a new field. The field is copied and the new field is added to the list with a number appended to the end of the field name—for example, if you were to duplicate the card_code field, the duplicated field would be card_code_1 . To rename the field, click Edit .
Show Forms	Expands the row to display a list of forms that use the field. You can click the  Edit Fields link next to a form in this list to edit the form's fields. You can click the  Use link to open the form that uses that field. If the field is used on multiple forms, you can select which form you would like to view.
Show Views	Expands the row to display a list of views that use the field. You can also click the  Edit Fields link next to a view in the list to edit the view's fields. You can click the  Use link to open the view that uses the field. If the field is used on multiple views, you are able to select which view you would like to see.
Delete	Deletes the field. You will be asked to confirm the deletion. A message indicates when the deletion is completed. Only fields that do not have a lock symbol  in the Type column can be deleted. A field that is currently in use on a form or view cannot be deleted.
Customize Forms & Views	To customize forms and views within the application, click this link in the upper right corner. The Customize Forms & Views list view opens.
Create new field	To create a new field, click this link in the upper right corner. The Define Custom Field form opens. See " Creating a Custom Field " on page 295.
Reset all to defaults	To reset all fields in the list to default values, click this link in the upper right corner. You will be asked to confirm the change.

For information on properties of some specific fields, see "[Business Logic for Account Creation](#)" on page 284.

Creating a Custom Field



To create a custom field, go to **Configuration > Pages > Fields** and click the  **Create** tab at the top of the form or the  **Create new field** link in the upper-right corner. The **Create Field** form is displayed.

Figure 193 *The Create Field Form, Basic Information Area*

Create Field	
* Field Name:	<input type="text"/> The unique name of this field. This is a single word that may consist of letters, digits and underscores.
* Field Type:	String <input type="button" value="v"/> The type of data that is stored in this field.
Description:	<input type="text"/> An optional description of this field.

Table 125: *Create Field Form, Basic Information Area*

Field	Description
Field Name	(Required) Unique name for this field. The field name cannot include spaces, but can include underscores.
Field Type	(Required) Type of data to store in this field. Options include: <ul style="list-style-type: none"> • String • Integer • Boolean • Scalar • No data type — Used for a label or a submit button
Description	Brief description of the field. If you enter a multiple-line description, multiple lines will be displayed on the form.

Figure 194 *The Create Field Form, Default View Display Properties Area*

Default View Display Properties

These options control the default values when used in a column.

Column Type:	<input style="width: 90%;" type="text" value="Sortable text"/>
	Type of column used to display this field.
* Column Title:	<input style="width: 90%;" type="text"/>
	The title text to display for this field's column.
Column Width:	<input style="width: 90%;" type="text" value="100"/>
	The default width of this field in pixels.
CSS Class:	<input style="width: 90%;" type="text"/>
	Optional CSS class name to apply to this form field.
CSS Style:	<input style="width: 90%;" type="text"/>
	Optional CSS style text to apply to this form field.
Column Format:	<input style="width: 90%;" type="text" value="Field Value"/>
	Describe how the value should be displayed onscreen.
Search:	<input type="checkbox"/> Include values when performing a quick search Many views include an ability to filter results. If checked, and this field is enabled, it will be included in the search.

The **Default View Display Properties** area lets you specify the default properties to use when adding this field to a view. For a list of the view display fields, including the Column Type and Column Format fields, see "View Field Editor" on page 339.

Table 126: *Create Field Form, Default View Display Properties Area*

Field	Description
Column Type	Specifies the default column type properties to use when adding this field to a view. Options include: <ul style="list-style-type: none"> ● Text ● Sortable text ● Sortable text, case insensitive ● Sortable numeric
Column Title	(Required) Header text to display for this field's column.
Column Width	Default width of this field in pixels.
CSS Class	CSS class name to apply to this form field.
CSS Style	CSS style text to apply to this form field.
Column Format	Specifies the default column format properties to use when adding this field to a view. Options include: <ul style="list-style-type: none"> ● Field Value ● Field Value (Unescaped) ● Boolean - Yes/No

Table 126: Create Field Form, Default View Display Properties Area(Continued)

Field	Description
	<ul style="list-style-type: none"> • Boolean - Enabled/Disabled • Boolean - On/Off • Date • Duration (from seconds) • Duration (from minutes) • Use form options • Custom expression
Display Expression	If Custom Expression was selected as the Column Format , you can enter the Javascript display expression for the field. The expression "data.F" returns the value of field "F".
Search	If selected, if this field is enabled it will be included in filter results for views that include filters.

Figure 195 The Create Field Form, Default Form Display Properties Area

Default Form Display Properties
 These properties control the default user interface displayed for this field.

User

Interface: The kind of user interface element to use when entering or editing this field.

The **Default Form Display Properties** area lets you specify the default properties to use when adding the field to a form. For a list of the available user interface types, see "[View Field Editor](#)" on page 339.

Table 127: Create Field Form, Default Form Display Properties Area

Field	Description
User Interface	Specifies the type of user interface element to use for this field (for example, drop-down list, CAPTCHA code, text field, and so on).
Label	Label to display for this field on the form.
Description	Brief description to display for this form on the field.
Label After (HTML)	HTML to display after the user interface element. Smarty template functions can be used. You can also use the drop-down list to add images or links.
CSS Class	CSS class name to apply to this form field.
CSS Style	CSS style text to apply to this form field.
Checkbox Value	Value to use for a selected check box. The default value is 1.
HTML	HTML text to display next to the check box as its label.
Legend	Title for the group of check boxes or radio buttons.
Options Generator	Specifies the function used to generate the list of available options for the multiple selection list or group of check boxes or radio buttons.

Table 127: Create Field Form, Default Form Display Properties Area(Continued)

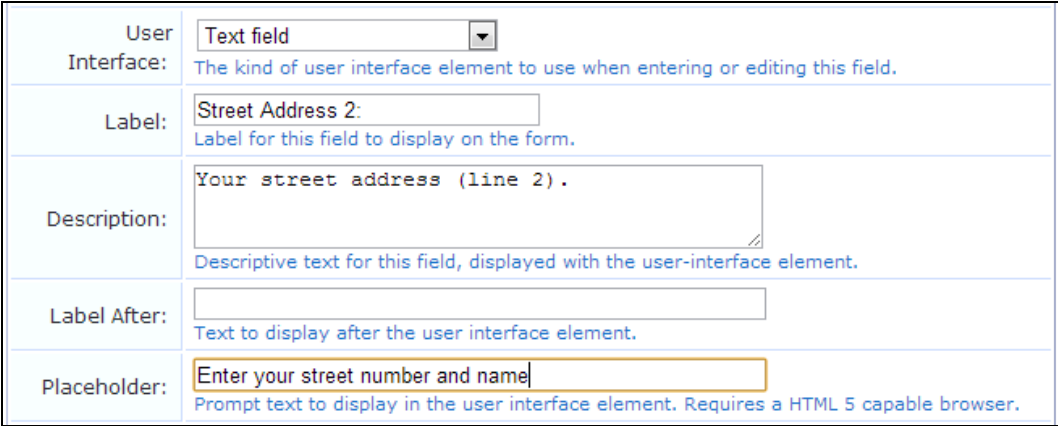
Field	Description
Options	List of available options. Enter each “key value” pair on a separate line, where the key and value are separated by a pipe character ().
Options Generator Param	Specifies the name of the field whose value will be supplied as the argument to the options.
Generator Arguments	Value to supply as the argument to the options generator.
Sort	Specifies the method to use to sort the available options. Options include: <ul style="list-style-type: none"> ● No sorting ● Sort options by key ● Sort options by value
Collapse	If selected, automatically hides the form field when only one choice is available.
Layout	Specifies the layout mode for the checklist options. Options include: <ul style="list-style-type: none"> Vertical Horizontal
Vertical Columns	Number of columns for the checklist.
Horizontal Rows	Number of rows for the checklist.
Searchable	If selected, enables searching and autocomplete with the “select2” user interface.
Max File Size	Maximum allowed size for an uploaded file.
Placeholder	<p>If Text or Password was selected as the User Interface type, you can use this field to enter a temporary value, such as a hint for how to complete the field, that can later be overridden by the user when they complete the form that uses this field.</p> 
Icon Image	Image to display with the user interface element.

Table 127: Create Field Form, Default Form Display Properties Area(Continued)

Field	Description
Columns	Number of columns to display in the user interface element.
Rows	Number of rows to display in the user interface element. Use -1 to automatically resize the height to fit the contents.
Max Length	Maximum number of characters that can be entered in the field.

Figure 196 The Create Field Form, Form Validation Properties Area

Form Validation Properties
 These properties control how the value of this field is checked.

Field Required:	<input type="checkbox"/> Field value must be supplied Select this option if the field cannot be omitted or left blank.
Initial Value:	<input type="text"/> Value to initialize this field with when the form is first displayed.
Validator:	(No validation) <input type="button" value="v"/> The function used to validate the contents of a field.

The **Form Validation Properties** area lets you specify the default validation rules that should be applied to this field when it is added to a form. See "Form Validation Properties" on page 326 in this chapter for further information about form validation properties.

Table 128: Create Field Form, Form Validation Properties Area

Field	Description
Field Required	If selected, the field cannot be omitted or left blank.
Initial Value	Value to initialize this field with when the form is first displayed.
Validator	Specifies the function used to validate the contents of a field.
Validator Param	Specifies the name of a field whose value will be supplied as the argument to the validator.
Validator Argument	Value to supply as the argument to a validator.
Validation Error	Error message to display if the field's value fails validation and the validator does not return an error message directly.

Figure 197 The Create Field Form, Advanced Properties Area


Advanced Properties
 These properties control conversion, display and dynamic behaviours.

Advanced:	<input type="checkbox"/> Show advanced properties
------------------	--

The **Advanced Properties** area lets you specify additional properties related to conversion, display, and dynamic form behavior. The fields displayed in the **Advanced** area will vary according to your selections on the rest of the **Create Field** form. See "[View Field Editor](#)" on page 339 in this chapter for more information about advanced properties.

Table 129: *Create Field Form, Advanced Properties Area*

Field	Description
Advanced	If selected, this form expands to include advanced options.
Conversion	Specifies the function used to convert an incoming field prior to validation.
Type Error	Error message to display if the field's value is not supplied, has an incorrect type, or if conversion fails.
Value Format	Specifies the function used to format a field value after validation.
Display Function	Specifies the function used to convert a field to a displayable value on the form.
Display Param	Name of the field whose value will be supplied as the argument to a display function.
Display Arguments	Value to supply as the argument to a display function.
Static Display Function	Specifies the function used to convert a static field to a displayable value on the form.
Static Display Param	Name of the field whose value will be supplied as the argument to a display function.
Static Display Arguments	Value to display as the argument to a display function.
Force Value	If selected, sets the field's value to the initial value specified above when the form is submitted.
Pre-Registration	<p>Specifies the pre-registration type. Options include:</p> <ul style="list-style-type: none"> ● Field was not pre-registered ● Guest must supply field ● Guest must supply field (match case) <p>Pre-registration applies to accounts that were created prior to registration. A field requiring a match will be searched in the account list. If a single match is found, the registration can continue.</p>
Enable If	Javascript conditional expression for this field's enabled property. The expression "f.value" returns the in-form value of field "f".
Visible If	Javascript conditional expression for this field's visibility. The expression "f.value" returns the in-form value of field "f".

When your changes are complete on this form, click  **Save Changes** to complete the creation of a new field. The new field is added at the top of the custom fields list at **Configuration > Pages > Fields**. To change the position of the new field, you can re-sort the list or you can reload the page.

Customizing AirGroup Registration Forms

AirGroup allows users to register their personal mobile devices on the local network and define a group of friends or associates who are allowed to share them. If AirGroup Services is enabled, AirGroup administrators can provision their organization's shared devices and manage access, and AirGroup operators can register and provision a limited number of their own personal devices for sharing. For complete AirGroup deployment information, refer to the AirGroup sections in the *ArubaOS User Guide* and the ClearPass Policy Manager documentation.

On the device registration forms for AirGroup administrators and operators, the default **Shared Locations** and **Shared Roles** fields are text boxes where the user enters the information. These fields can be configured as selection options populated with existing locations or roles.

Configuring the Shared Locations and Shared Role Fields

To configure a predefined list of shared locations or shared roles:

1. Go to **Configuration > Pages > Fields** and click the **airgroup_shared_location** or **airgroup_shared_role** row. The form expands to include the **Edit**, **Duplicate**, **Show Forms**, and **Show Views** links.
2. Click the **Edit** link. The **Define Custom Field** form opens. Scroll to the **Default Form Display Properties** area.

Figure 198 *The Define Custom Field Form, Default Form Display Properties Area*

Default Form Display Properties	
These properties control the default user interface displayed for this field.	
User Interface:	<input type="text" value="Checklist"/> The kind of user interface element to use when entering or editing this field.
Label:	<input type="text" value="Shared Locations:"/> Label for this field to display on the form.
Description:	<input type="text" value="Select the location IDs where this device will be shared. Leave blank to share with all locations."/> Descriptive text for this field, displayed with the user-interface element.
CSS Class:	<input type="text"/> Optional CSS class name to apply to this form field.
CSS Style:	<input type="text"/> Optional CSS style text to apply to this form field.
Legend:	<input type="text"/> Optional title for the checkbox or radio button group.
Options Generator:	<input type="text" value="(Use options)"/> The function used to generate the list of available options.
Options:	<input type="text" value="AP-Group=Location-1 Location One
AP-Group=Location-2 Location Two
AP=Location-3 Location Three"/> List of options available. Enter one or more lines containing 'key value' pairs, where the key and value are separated with a vertical bar .
Sort:	<input type="text" value="No sorting"/> Method to use to sort the available options.
Collapse:	<input type="checkbox"/> Hide when no options are selectable Select this option to automatically hide the form field when only one choice is available.
Layout:	<input type="text" value="Horizontal"/> Layout mode for the checklist options.
Horizontal Rows:	<input type="text"/> Number of rows to draw in the checklist.

- In the **User Interface** drop-down list, select **Checklist**.
- In the **Description** text box, delete the existing text, then enter **Select the location IDs where this device will be shared. Leave blank to share with all locations**.
- Delete any text from the **CSS Class** and the **CSS Style** fields.
- In the **Options Generator** drop-down list, select **(Use options)**.
- In the **Options** text box, enter a list of values to use as the checklist options that presented to the user.

The values you enter in the **Options** text box control both the values stored in the shared_location field in the database as well as the text displayed to the user in the checklist. Use the following format:

```
tag1=value1 | Option 1
tag2=value2 | Option 2
```

...where the tag=value pair **tag1=value1** represents the value stored in the shared_location field in the database, the pipe character (|) is a separator, and **Option 1** represents the text displayed in the checklist.


- (Optional) To sort the locations by key or value, choose an option from the **Sort** drop-down list.

- (Optional) To control the layout of the checklist on the form, first use the **Layout** drop-down list to select either **Vertical** or **Horizontal**. The name of the next field changes to correspond to your choice in this field. Enter the appropriate number in the **Vertical Rows** or **Horizontal Rows** field. If the **Layout** field is left blank, the default layout of a single list of checklist options is displayed.

To ensure the values are stored correctly as a comma-separated list:

- Scroll to the **Advanced Properties** section of the form and mark the check box in the **Advanced** row. The form expands to include the advanced options.

Figure 199 *The Define Custom Field Form, Advanced Properties Area*

Advanced Properties	
These properties control conversion, display and dynamic behaviours.	
Advanced:	<input checked="" type="checkbox"/> Show advanced properties
Conversion:	NwaImplodeComma The function used to convert an incoming field value prior to validation.
Type Error:	<input type="text"/> The error message to display if the field's value is not supplied, has an incorrect type, or if conversion fails.
Value Format:	(None) The function used to format a field value after validation.
Display Function:	NwaExplodeComma The function used to convert a field to a displayable value on the form.
Display Param:	_self Optional name of field whose value will be supplied as the argument to a display function.
Display Arguments:	<input type="text"/> Optional value to supply as the argument to a display function.
Static Display Function:	(None) The function used to convert a static field to a displayable value on the form.
Force Value:	<input type="checkbox"/> Always use initial value on form submit Sets the field's value to the initial value specified above when the form is submitted. Use this option when the field must have a certain value that cannot be overridden by a user.
Pre-Registration:	Field was not pre-registered Pre-Registration applies for accounts that have been created prior to registration. A field requiring a match will be searched in the account list. If a single match is found, the registration can continue.
Enable If:	<input type="text"/> Javascript conditional expression for this field's enabled property. The expression 'f.value' returns the in-form value of field 'f'.
Visible If:	<input type="text"/> Javascript conditional expression for this field's visibility. The expression 'f.value' returns the in-form value of field 'f'.
	

- In the **Conversion** drop-down list, select **NwaImplodeComma**. The form expands to include the **Type Error** row.

3. In the **Display Function** drop-down list, select **NwaExplodeComma**. The form expands to include the **Display Param** and **Display Arguments** rows.
4. In the **Display Param** text field, enter the value **_self**. Be sure to include the leading underscore character.
5. Click **Save Changes**.

Example:

If the layout is set to vertical and the following options are specified:

```
AP-Group=Location-1 | Location One
AP-Group=Location-2 | Location Two
AP-Location-3 | Location Three
```

The user interface appears as follows:


Figure 200 *The Register Shared Device Form Showing the Configured Fields*

Register Shared Device	
* Device Name:	<input type="text" value="LibraryPrinter2"/> <small>Enter a name to identify the device.</small>
* MAC Address:	<input type="text" value="AA-BB-CC-DD-EE-FF"/> <small>Enter the MAC address of the device.</small>
Shared Locations:	<input checked="" type="checkbox"/> Location One <input type="checkbox"/> Location Two <input checked="" type="checkbox"/> Location Three <small>Select the location IDs where this device will be shared. Leave blank to share with all locations.</small>
Shared With:	<input type="text"/> <small>Enter up to 10 usernames that will be able to use this device. Use a comma-separated list, e.g. user1,user2,user3, or blank for all users.</small>
Shared Roles:	<input type="text"/> <small>List the user roles that will be able to use this device. Use a comma-separated list, e.g. role1,role2,role3, or blank for all roles.</small>
<input type="button" value="Register Shared Device"/>	

Customizing Forms and Views



You can view a list of ClearPass Guest's forms and views. From this list view, you can change the layout of forms or views, add new fields to a form or view, or alter the behavior of an existing field.



Forms & Views
 Add new fields to forms, change existing fields, or reconfigure views of visitor accounts.

To view or customize forms and views, go to **Configuration > Pages > Forms & Views**. The **Customize Forms and Views** list view opens.

Figure 201 *The Customize Forms and Views List View*

Name	Title	Type
airgroup_shared_list List of shared devices managed by the administrator.	Shared Devices	view
change_expiration Change the expiration time of a single visitor account.	Change Expiration	form
create_multi Create multiple visitor accounts.	Create Guest Accounts	form
Edit Edit Fields Duplicate Use		
create_user Create a single visitor account.	New Visitor Account	form

All forms and views in the application are included in the list. You can click a field's row in the list or use the links provided on the page for additional options:

Table 130: *The Customize Forms & Views List*

Field	Description
Edit	Edit a form or view's basic properties. The row expands to include the Edit Properties form. See "Editing Forms and Views " on page 306.
Edit Fields	Edit the form's or view's fields. The Customize Form Fields list view for the form or view opens. You can add a new field to a form, reorder the fields, or make changes to an existing field. See "Editing Forms " on page 308 or "Editing Views " on page 337. Editing Views
Duplicate	Creates a copy of the form or view to use as a template in order to provide different forms and views to different operator profiles. See "Role-Based Access Control for Multiple Operator Profiles" on page 668 for a description. This enables you to provide different views of the underlying visitor accounts in the database depending on the operator's profile. The form or view is copied and the new one is added to the list with a number appended to the end of its name—for example, if you were to duplicate the change expiration form, the duplicated form would be change_expiration_1 . This name cannot be changed. Use the Title and Description properties of the duplicated item to describe the intended purpose for the form or view.
Show Usage	Expands the row to display a list of operator profiles that reference the form or view. You can click an operator profile's name in this list to edit the form's fields.
Use	Opens the form or view. The form or view opens in a separate tab, and the Forms and Views tab stays open so you can work in both.
Delete	Deletes the form or view. You will be asked to confirm the deletion. A form or view cannot be removed if it is referenced by an operator login account or an operator profile.
Reset to defaults	An asterisk (*) shown next to a form or view indicates that the form or view has been modified from the defaults. To reset a form or view to default values, click this link. You will be asked to confirm the change. Resetting a form or view is a destructive operation and cannot be undone.
Customize Fields	To customize fields used in the application, click this link in the upper right corner. The Customize Fields list view opens. See "Customizing Fields" on page 294.

Editing Forms and Views

You can change the general properties of a form or view such as its title and description. To edit the form or view, go to **Configuration > Pages > Forms & Views**, click the form's or view's row in the list, and then click


its  **Edit** link. The row expands to include the **Edit Properties** form.

Figure 202 *The Edit Properties Form*

Edit Properties

Name:	guest_multi <small>The name of the application page.</small>
Type:	view <small>The type of application page.</small>
Title:	<input type="text" value="Edit Accounts"/> <small>The title for this form or view.</small>
Description:	<div style="border: 1px solid #ccc; padding: 2px; min-height: 20px;">Edit multiple visitor accounts.</div> <small>An optional description of this form or view.</small>
Width:	<input type="text"/> <small>The width of the list view, in pixels.</small>

Page Properties

Page Title:	<input type="text"/> <small>The title to display on the page. Leave blank to use the default title.</small>
Header HTML:	<div style="border: 1px solid #ccc; padding: 2px; min-height: 20px;"></div> <div style="float: right; border: 1px solid #ccc; padding: 2px; font-size: small;">Insert content item... ▼</div> <small>HTML template code displayed before the form or view. Leave blank to use the default text, or enter a hyphen "-" to remove the default text.</small>
Footer HTML:	<div style="border: 1px solid #ccc; padding: 2px; min-height: 20px;"></div> <div style="float: right; border: 1px solid #ccc; padding: 2px; font-size: small;">Insert content item... ▼</div> <small>HTML template code displayed after the form or view. Leave blank to use the default text, or enter a hyphen "-" to remove the default text.</small>


 Save Changes

Table 131: *The Edit Properties Form*

Field	Description
Name	Filename of the application page.
Type	Page type, either form or view.
Title	Title of the form or view.
Description	Brief description of the form or view.
Width	Total width of the list view in pixels. If this field is left blank, a default value is used. The Width field is only displayed for views.
Page Title	Title that is displayed on the form or view in the user interface.

Table 131: *The Edit Properties Form(Continued)*

Field	Description
Header HTML	HTML template code displayed before the form or view. You can use the drop-down list to add images or links.
Footer HTML	HTML template code displayed after the form or view. You can use the drop-down list to add images or links.
Save Changes	Saves your changes to this form. On the Customize Forms & Views list, an asterisk (*) is shown next to the form or view to indicate that it has been modified. To reset it to default values, you can click the Reset to defaults link. You will be asked to confirm the change. Resetting a form or view is a destructive operation and cannot be undone.

Editing Forms


To add a new field to a form, reorder the fields, or make changes to an existing field, go to **Configuration > Pages > Forms & Views**, click the form’s row in the **Customize Forms & Views** list, and then click the  **Edit Fields** link. The **Customize Form Fields** list view opens and includes the fields that are used in the selected form or view.

Figure 203 *The Customize Form Fields List View*







Rank	Field	Type	Label	Description
10	sponsor_name	text	Sponsor’s Name:	Name of the person sponsoring this visitor account.
15	sponsor_email	text	Sponsor’s Email:	Email of the person sponsoring this visitor account.
20	visitor_name	text	Visitor’s Name:	Name of the visitor.
 Edit  Edit Base Field  Remove  Insert Before  Insert After  Disable Field				
25	visitor_phone	text	Phone Number:	The visitor’s phone number.
30	visitor_company	text	Company Name:	Company name of the visitor.
40	email	text	Email Address:	The visitor’s email address. This will become their username to log into the network.
50	modify_start_time	dropdown	Account Activation:	Select an option for changing the activation time of this account.

Table 132: *Customize Form Fields*

Field	Description
Rank	Specifies the relative ordering of the fields when displaying the form. This list always shows the fields in order by rank.
Field	The name of the field in the database.
Type	Controls what kind of user interface element is used to interact with the user.
Label	The label for this field as it is displayed on the form.
Description	The description for this field as it is displayed on the form.

To work with a form field, click its row in the list. The row expands to include configuration options:

Table 133: *Customize Form Fields, Options*

Field	Description
Edit	Make changes to an existing field. The Form Field Editor opens. Any changes made to the field using this editor will apply only to this field on this form. See "Form Field Editor " on page 309.
Edit Base Field	Make changes to an existing field's definition. The Edit Field form opens. Any changes made to the field using this editor will apply to all forms that are using this field (except where the form field has already been modified to be different from the underlying field definition). See "Creating a Custom Field " on page 295.
Remove	Removes the field from the form. To add a field back to the form after it has been removed, use the Insert Before or Insert After option and select it from the Field Name drop-down list in the Form Field Editor that opens.
Insert Before	Adds a new field to the form. Clicking one of these links opens a blank form field editor and automatically sets the rank number of the new field.
Insert After	
Disable Field	Disables this field on the form. To enable it on the form again, click Enable Field .
Preview Form	Opens an example of the form so you can see what it looks like. This preview form can be submitted to test the field validation rules you have defined. If all fields are able to be validated, the form submit is successful and a summary of the values submitted is displayed. This allows you to verify any data conversion and formatting rules you have set up.

Form Field Editor

The **Form Field Editor** is used to control both the data gathering aspects and user interface characteristics of a field.

To modify these aspects of a form field, go to **Configuration > Pages > Forms & Views**, click a form or view, click its **Edit Fields** link, click the field, and then click the field's **Edit** link. The **Form Field Editor** opens.

Figure 204 *The Form Field Editor Form*

The screenshot shows the 'Form Field Editor' window. At the top, there is a title bar with the text 'Form Field Editor'. Below the title bar, there is a label '* Field Name:' followed by a dropdown menu. The dropdown menu is currently open, showing the selected value 'visitor_name'. Below the dropdown menu, there is a blue link that says 'Select the field definition to attach to the form.'



Each field can only appear once on a form. The **Field Name** drop-down list specifies which underlying field is being represented on the form. This also determines which options are available in the rest of the **Form Field Editor**.

The rest of the **Form Field Editor** is split into three areas:

- **Form Display Properties** — See ["Form Display Properties"](#) on page 310
- **Form Validation Properties** — ["Form Validation Properties"](#) on page 326
- **Advanced Properties** — ["Advanced Form Field Properties"](#) on page 331

Form Display Properties

Figure 205 The Form Field Editor Form, Form Display Properties Area

Form Display Properties	
These properties control the user interface displayed for this field.	
Field:	<input checked="" type="checkbox"/> Enable this field When checked, the field will be included as part of the form.
* Rank:	<input type="text" value="20"/> Number indicating the relative ordering of user interface fields, which are displayed in order of increasing rank.
* User Interface:	<input type="text" value="Text field"/> The kind of user interface element to use when entering or editing this field.
Label:	<input type="text" value="Visitor's Name"/>  Label for this field to display on the form.
Description:	<input type="text" value="Name of the visitor"/>  Descriptive text for this field, displayed with the user-interface element.
CSS Class:	<input type="text"/> Optional CSS class name to apply to this form field.
CSS Style:	<input type="text" value="width: 240px;"/> Optional CSS style text to apply to this form field.
Label After:	<input type="text"/> Text to display after the user interface element.
Placeholder:	<input type="text"/> Prompt text to display in the user interface element. Requires a HTML 5 capable browser.
Max Length:	<input type="text"/> Maximum number of characters allowed to be entered in the field.

On the **Form Field Editor** (see "Form Field Editor " on page 309), the form display properties control the user interface this field will have. Different options are available in this section, depending on the selection you make in the **User Interface** drop-down list.



Fields with a green border use their base field's value. If you enter a different value to override the base field's value, a **Revert** option lets you return to the original value.

The available user interface elements are described below, together with an example of each.

Use Default

If the (**Use default**) user interface option is selected, the default user interface type defined for the field will be used.

No User Interface

If the **No user interface** option is selected, the field does not have a user interface specified. Using this value will cause a diagnostic message to be displayed ("Form element is missing the 'ui' element") when using the form.

CAPTCHA Security Code

If the **CAPTCHA** user interface is selected, a distorted image of several characters will be displayed to the user, as shown below:

Figure 206 A CAPTCHA Code Image in a Field

A new image may be generated, or the image may be played as an audio sample for visually impaired users. When using the recommended validator for this field (NwaCaptchalsValid), the security code must be matched or the form submit will fail with an error.

Figure 207 Form Display Properties Options for the CAPTCHA User Interface

* User Interface:	<input type="text" value="CAPTCHA security code"/>
	The kind of user interface element to use when entering or editing this field.
Label:	<input type="text" value="Security Code:"/>
	Label for this field to display on the form.
Description:	<input type="text" value="Please enter the security code shown in this image. This helps to prevent abuse of"/> <input type="button" value="Revert"/>
	Descriptive text for this field, displayed with the user-interface element.
CSS Class:	<input type="text"/>
	Optional CSS class name to apply to this form field.
CSS Style:	<input type="text"/>
	Optional CSS style text to apply to this form field.

Checkbox

If the **Checkbox** user interface is selected, a check box is displayed for the field, as shown below:

Figure 208 A Check Box in a Field

The check box label can be specified using HTML. If the check box is selected, the field is submitted with its value set to the check box value (default and recommended value 1). If the check box is not selected, the field is not submitted with the form.

Figure 209 Form Display Properties Options for the Check Box User Interface

* User Interface:	<input type="text" value="Checkbox"/> Revert The kind of user interface element to use when entering or editing this field.
Label:	<input type="text" value="Account Status:"/> Label for this field to display on the form.
Description:	<input type="text" value="Select an option for changing the status of this visitor account."/> Revert Descriptive text for this field, displayed with the user-interface element.
CSS Class:	<input type="text"/> Optional CSS class name to apply to this form field.
CSS Style:	<input type="text"/> Optional CSS style text to apply to this form field.
HTML:	<input type="text"/> HTML text to display next to the checkbox, as its clickable label.
Text:	<input type="text"/> Text to display next to the checkbox, if HTML is not supplied.
Checkbox Value:	<input type="text"/> Optional value to use for a checked checkbox; the default is '1'.

Checklist

If the **Checklist** user interface is selected, a list of check boxes is displayed, as shown below:

Figure 210 A Checklist in a Field

Sample Field:	<div style="border: 1px solid #ccc; padding: 5px;"> <p>Select Options</p> <p><input type="checkbox"/> Option One</p> <p><input type="checkbox"/> Option Two</p> <p><input type="checkbox"/> Option Three</p> <p>This is a sample field</p> </div>
---------------	---

The text displayed for each check box is the value from the options list. Zero or more check boxes may be selected. This user interface type submits an array of values containing the option key values of each selected check box. Because an array value may not be stored directly in a custom field, you should use the conversion and value formatting facilities to convert the array value to and from a string when using this user interface type.

To store a comma-separated list of the selected values:



1. Enable the **Advanced** options.
2. In the **Conversion** drop-down list, select **NwaImplodeComma**.
3. In the **Display Function** drop-down list, select **NwaExplodeComma**.
4. In the **Display Param** field, enter the field's name.

The “Vertical” and “Horizontal” layout styles control whether the check boxes are organized in top-to-bottom or left-to-right order. The default is “Vertical” if not specified. When using these options, you may also specify the desired number of columns or rows to adjust the layout appropriately.

Figure 211 Form Display Properties Options for the Checklist User Interface

* User Interface:	<input type="text" value="Checklist"/> Revert The kind of user interface element to use when entering or editing this field.
Label:	<input type="text" value="Account Status:"/> Label for this field to display on the form.
Description:	<input type="text" value="Select an option for changing the status of this visitor account."/> Revert Descriptive text for this field, displayed with the user-interface element.
CSS Class:	<input type="text"/>
CSS Style:	<input type="text"/>
Legend:	<input type="text"/>
Options Generator:	<input type="text" value="(Use options)"/> Revert The function used to generate the list of available options.
Options:	<input type="text" value="1 Enable visitor account\n0 Disable visitor account"/> Revert List of options available. Enter one or more lines containing 'key value' pairs, where the key and value are separated with a vertical bar .
Sort:	<input type="text" value="No sorting"/> Revert Method to use to sort the available options.
Collapse:	<input type="checkbox"/> <input type="text" value="Hide when no options are selectable"/> Select this option to automatically hide the form field when only one choice is available.
Layout:	<input type="text"/>
Vertical Columns:	<input type="text"/>

Figure 212 *Advanced Properties Options for the Checklist User Interface*

Advanced Properties	
These properties control conversion, display and dynamic behaviours.	
Advanced:	<input checked="" type="checkbox"/> Show advanced properties  Revert
Conversion:	<input type="text" value="NwalmplodeComma"/>  Revert The function used to convert an incoming field value prior to validation.
Type Error:	<input type="text"/> The error message to display if the field's value is not supplied, has an incorrect type, or if conversion fails.
Value Format:	<input type="text" value="(None)"/> The function used to format a field value after validation.
Display Function:	<input type="text" value="(None)"/> The function used to convert a field to a displayable value on the form.
Static Display Function:	<input type="text" value="(None)"/> The function used to convert a static field to a displayable value on the form.

For example, suppose the first two check boxes are selected (in this example, with keys "one" and "two"). The incoming value for the field will be an array containing 2 elements, which can be written as `array("one", "two")`. The `NwalmplodeComma` conversion is applied, which converts the array value into the string value "one,two", which is then used as the value for the field. Finally, when the form is displayed and the value needs to be converted back from a string, the `NwaExplodeComma` display function is applied, which turns the "one,two" string value into an array value `array("one", "two")`, which is used by the checklist to mark the first two items as selected.

Date/Time Picker

If the **Date/time picker** user interface is selected, a text field is displayed with an attached button that displays a calendar and time chooser. A date may be typed directly into the text field, or selected using the calendar.

The text value typed is submitted with the form. If using a date/time picker, you should validate the field value to ensure it is a date.

Certain guest account fields, such as **expire_time** and **schedule_time**, require a date/time value to be provided as a UNIX time value. In this case, the conversion and display formatting options should be used to convert a human-readable date and time to the equivalent UNIX time and vice versa.

Figure 213 Advanced Properties for the Date/time picker User Interface

Advanced Properties	
These properties control conversion, display and dynamic behaviours.	
Advanced:	<input checked="" type="checkbox"/> Show advanced properties
Conversion:	<input type="text" value="NwaConvertOptionalDateTime"/> The function used to convert an incoming field value prior to validation.
Type Error:	<input type="text" value="Please enter a valid date and time."/> The error message to display if the field's value is not supplied, has an incorrect type, or if conversion fails.
Value Format:	<input type="text" value="(None)"/> The function used to format a field value after validation.
Display Function:	<input type="text" value="NwaDateFormat"/> The function used to convert a field to a displayable value on the form.
Display Param:	<input type="text" value="expire_time"/> Optional name of field whose value will be supplied as the argument to a display function.
Display Arguments:	<input type="text" value="%Y-%m-%d %H:%M? :"/> Optional value to supply as the argument to a display function.

Drop-Down List

If the **Drop-down list** user interface is selected, the field is displayed allowing a single choice from a drop-down list.



Figure 214 A Drop-Down List in a Field

Sample Field:	<input type="text" value="Option One"/> This is a sample field.
---------------	--

The text displayed for each option is the value from the options list. When the form is submitted, the key of the selected value becomes the value of the field.

If the **Hide when no options are selectable** check box is selected, and there is only a single option in the drop-down list, it will be displayed as a static text item rather than as a list with only a single item in it.

Figure 215 Form Display Properties Options for the Drop-down list User Interface

* User Interface:	Drop-down list  Revert
Searchable:	<input type="checkbox"/> Enable searching and advanced UI Select this option to use the 'select2' user interface. This provides search, autocomplete and better management for multiple selection lists.
Label:	Your Name:  Revert Label for this field to display on the form.
Description:	Please enter your full name.  Revert Descriptive text for this field, displayed with the user-interface element.
CSS Class:	<input type="text"/> Optional CSS class name to apply to this form field.
CSS Style:	<input type="text"/> Optional CSS style text to apply to this form field.
No Changes:	<input type="checkbox"/> Add (No changes) Select if you want the list to insert a (No changes) option to the default set.
Options Generator:	(Use options)  The function used to generate the list of available options.
Options:	<input type="text"/> List of options available. Enter one or more lines containing 'key value' pairs, where the key and value are separated with a vertical bar .
Sort:	No sorting  Method to use to sort the available options.
Collapse:	<input type="checkbox"/> Hide when no options are selectable Select this option to automatically hide the form field when only one choice is available.

File Upload

If the **File upload** user interface is selected, a file selection text field and dialog box are displayed (the exact appearance differs from browser to browser).

File uploads cannot be stored in a custom field. This user interface type requires special form implementation support and is not recommended for use in custom fields.

Hidden Field

If the **Hidden Field** user interface is selected, the field is not displayed to the user, but is submitted with the form. This option is often used to force a specific value such as a user's role or an expiration date. However, it is possible for someone to use browser tools to modify the initial value when the form is submitted. If the value should be forced, use the **Force Value** setting under **Advanced Properties** to ensure the value cannot be overridden. For more information, see "[Advanced Form Field Properties](#)" on page 331.

To set the value to submit for this field, use the **Initial Value** option in the **Form Field Editor**.

Figure 216 Form Display Properties Options for the Hidden Field User Interface

* User Interface:	Hidden field <input type="button" value="Revert"/>
The kind of user interface element to use when entering or editing this field.	
Form Validation Properties These properties control how the value of this field is checked.	
Field Required:	<input checked="" type="checkbox"/> Field value must be supplied Select this option if the field cannot be omitted or left blank.
Initial Value:	<input type="text"/> Value to initialize this field with when the form is first displayed.
* Validator:	(No validation) <input type="button" value="Revert"/> The function used to validate the contents of a field.

Figure 217 Initial Values for a Form

✓ The form was submitted with the following values:

```
array (  
  'password' => 'password',  
  'sponsor_name' => 'Sponsor',  
  'visitor_name' => 'Visitor',  
  'visitor_company' => 'Company',  
  'email' => 'demo@example.com',  
  'expire_after' => 1,  
  'expire_time' => 0,  
  'role_id' => 2,  
  'creator_accept_terms' => true,  
  'submit' => NULL,  
  'sample_field' => 'value for sample_field',  
)
```

Multiple Selection List

If the **Multiple selection list** user interface is selected, a list of selectable options will be displayed.







The text displayed for each check box or radio button is the value from the options list. Zero or more check boxes may be selected. This user interface type submits an array of values containing the option key values of each selected check box. Because an array value may not be stored directly in a custom field, you should use the conversion and value formatting facilities to convert the array value to and from a string when using this user interface type.

To store a comma-separated list of the selected values:

1. Enable the **Advanced** options.
2. In the **Conversion** drop-down list, select **NwaImplodeComma**.
3. In the **Display Function** drop-down list, select **NwaExplodeComma**.
4. In the **Display Param** field, enter the field's name.

The "Vertical" and "Horizontal" layout styles control whether the check boxes are organized in top-to-bottom or left-to-right order. The default is "Vertical" if not specified. When using these options, you may also specify the desired number of columns or rows to adjust the layout appropriately.

Figure 218 Form Display Properties Options for the Multiple selection list User Interface

* User Interface:	Multiple selection list  Revert The kind of user interface element to use when entering or editing this field.
Searchable:	<input checked="" type="checkbox"/> Enable searching and advanced UI Select this option to use the 'select2' user interface. This provides search, autocomplete and better management for multiple selection lists.
Label:	Phone Number(s)  Revert Label for this field to display on the form.
Description:	The visitor's phone number or phone numbers.  Revert Descriptive text for this field, displayed with the user-interface element.
CSS Class:	<input type="text"/> Optional CSS class name to apply to this form field.
CSS Style:	<input type="text"/>  Revert Optional CSS style text to apply to this form field.
Options Generator:	(Use options)  The function used to generate the list of available options.
Options:	<input type="text"/> List of options available. Enter one or more lines containing 'key value' pairs, where the key and value are separated with a vertical bar .
Sort:	No sorting  Method to use to sort the available options.
Collapse:	<input checked="" type="checkbox"/> Hide when no options are selectable Select this option to automatically hide the form field when only one choice is available.




Password Text Field

If the **Password text field** user interface is selected, the field is displayed as a text field, with input from the user obscured. The text typed in this field is submitted as the value for the field.

Figure 219 A Text Field in a Form, with the User's Entry Obscured

Sample Field:	<input type="password" value="••••••"/> This is a sample field.
---------------	--

Figure 220 Form Display Properties Options for the Password text field User Interface

* User Interface:	Password text field  Revert The kind of user interface element to use when entering or editing this field.
Label:	Your Name:  Revert Label for this field to display on the form.
Description:	Please enter your full name.  Revert Descriptive text for this field, displayed with the user-interface element.
CSS Class:	<input type="text"/> Optional CSS class name to apply to this form field.
CSS Style:	<input type="text"/> Optional CSS style text to apply to this form field.
Placeholder:	<input type="text"/> Prompt text to display in the user interface element. Requires a HTML 5 capable browser.

Radio Buttons







If the **Radio buttons** user interface is selected, the field is displayed as a group of radio buttons, allowing one to be selected, as shown below:

Figure 221 Radio Buttons in a Field

Sample Field:	<input checked="" type="radio"/> Option One <input type="radio"/> Option Two <input type="radio"/> Option Three This is a sample field.
---------------	--

The text displayed for each option is the value from the options list. When the form is submitted, the key of the selected value becomes the value of the field.

Figure 222 Form Display Properties Options for the Radio buttons User Interface


* User Interface:	Radio buttons  Revert The kind of user interface element to use when entering or editing this field.
Label:	Your Name:  Revert Label for this field to display on the form.
Description:	Please enter your full name.  Revert Descriptive text for this field, displayed with the user-interface element.
CSS Class:	<input type="text"/> Optional CSS class name to apply to this form field.
CSS Style:	<input type="text"/> Optional CSS style text to apply to this form field.
Legend:	<input type="text"/> Optional title for the checkbox or radio button group.
No Changes:	<input type="checkbox"/> Add (No changes) Select if you want the list to insert a (No changes) option to the default set.
Options Generator:	(Use options)  The function used to generate the list of available options.
Options:	<input type="text"/> Select... Amex American Express Discover Discover MasterCard MasterCard  Revert List of options available. Enter one or more lines containing 'key value' pairs, where the key and value are separated with a vertical bar .
Sort:	No sorting  Method to use to sort the available options.
Collapse:	<input type="checkbox"/> Hide when no options are selectable Select this option to automatically hide the form field when only one choice is available.
Layout:	<input type="text"/> Layout mode for the checklist options.

The “Vertical” and “Horizontal” layout styles control whether the radio buttons are organized in top-to-bottom or left-to-right order. The default is “Vertical” if not specified.

Static Text

If the **Static text** user interface is selected, the field’s value is displayed as a non-editable text string. An icon image may optionally be displayed before the field’s value. A hidden element is also included for the field, thereby including the field’s value when the form is submitted.






Figure 223 A Static Text Field in a Form

Sample Field:	 value for sample_field This is a sample field.
---------------	---

If the **Hide when no options are selectable** check box is selected in the **Collapse** row, the field will be hidden if its value is blank.

To set the value of this field, use the **Initial Value** option in the **Form Validation Properties** area of the form field editor.

Figure 224 Form Display Properties Options for the Static text User Interface

* User Interface:	Static text  Revert The kind of user interface element to use when entering or editing this field.
Label:	Sample Field:  Revert Label for this field to display on the form.
Description:	This is a sample field  Revert Descriptive text for this field, displayed with the user-interface element.
CSS Class:	<input type="text"/> Optional CSS class name to apply to this form field.
CSS Style:	<input type="text"/> Optional CSS style text to apply to this form field.
Icon Image:	<input type="text"/> Image to display with the user interface element.
Collapse:	<input checked="" type="checkbox"/> Hide when no options are selectable  Revert Select this option to automatically hide the form field when only one choice is available.
Form Validation Properties These properties control how the value of this field is checked.	
Field Required:	<input type="checkbox"/> Field value must be supplied Select this option if the field cannot be omitted or left blank.
Initial Value:	<input type="text"/> Value to initialize this field with when the form is first displayed.
* Validator:	(No validation)  The function used to validate the contents of a field.

Static Text (Raw Value)






If the **Static text (Raw value)** user interface is selected, the field's value is displayed as a non-editable text string. HTML characters in the value are not escaped, which allows you to display HTML markup such as images, links and font formatting.

Figure 225 A Static Text Field in a Form, with HTML Formatting

Sample Field:	 value may contain HTML This is a sample field.
---------------	---

Use caution when using this type of user interface element, particularly if the field's value is collected from visitors. Allowing HTML from untrusted sources is a potential security risk.

Figure 226 Form Display Properties Options for the Static text (Raw value) User Interface

* User Interface:	Static text (Raw value)  Revert
The kind of user interface element to use when entering or editing this field.	
Label:	Sample Field:  Revert
Label for this field to display on the form.	
Description:	This is a sample field  Revert
Descriptive text for this field, displayed with the user-interface element.	
CSS Class:	<input type="text"/>
Optional CSS class name to apply to this form field.	
CSS Style:	<input type="text"/>
Optional CSS style text to apply to this form field.	
Icon Image:	<input type="text"/>
Image to display with the user interface element.	
Collapse:	<input checked="" type="checkbox"/> Hide when no options are selectable  Revert
Select this option to automatically hide the form field when only one choice is available.	
Form Validation Properties	
These properties control how the value of this field is checked.	
Field Required:	<input type="checkbox"/> Field value must be supplied
Select this option if the field cannot be omitted or left blank.	
Initial Value:	<input type="text"/>
Value to initialize this field with when the form is first displayed.	
* Validator:	(No validation) 
The function used to validate the contents of a field.	

If the **Hide when no options are selectable** check box is selected in the **Collapse** row, the field will be hidden if its value is blank.

To set the value of this field, use the **Initial Value** option in the **Form Validation Properties** area of the form field editor.

Static Text (Options Lookup)

If the **Static text (Options lookup)** user interface is selected, the value of the field is assumed to be one of the keys from the field's option list. The value displayed is the corresponding value for the key, as a non-editable text string.

An icon image may optionally be displayed before the field's value. A hidden element is also included for the field, thereby including the field's value when the form is submitted.

Figure 227 A Static Text Field in a Form, Displaying a Value from the Field's Options List




Sample Field:	 Option Two
This is a sample field.	

Figure 228 Form Display Properties Options for the Static text (Options lookup) User Interface

* User Interface:	Static text (Options lookup)  Revert The kind of user interface element to use when entering or editing this field.
Label:	Sample Field:  Revert Label for this field to display on the form.
Description:	This is a sample field  Revert Descriptive text for this field, displayed with the user-interface element.
CSS Class:	<input type="text"/> Optional CSS class name to apply to this form field.
CSS Style:	<input type="text"/> Optional CSS style text to apply to this form field.
Icon Image:	images/icon-key.png  Revert Image to display with the user interface element.
Options Generator:	(Use options)  The function used to generate the list of available options.
Options:	<input type="text"/> List of options available. Enter one or more lines containing 'key value' pairs, where the key and value are separated with a vertical bar .
Collapse:	<input checked="" type="checkbox"/> Hide when no options are selectable  Revert Select this option to automatically hide the form field when only one choice is available.

If the **Hide when no options are selectable** check box is selected in the **Collapse** row, the field will be hidden if its value is blank.

To set the value of this field, use the **Initial Value** option in the **Form Validation Properties** area of the form field editor.

Static Group Heading






If the **Static group heading** user interface is selected, the label and description of the field is used to display a group heading on the form, as shown below. The field's value is not used, and the field is not submitted with the form.

Figure 229 A Group Heading on a Form

Group Heading
This is a sample group heading

When using this user interface element, it is recommended that you use the "nwalimportant" CSS class to visually distinguish the group heading's title.

Figure 230 Form Display Properties Options for the Static group heading User Interface

* User Interface:	Static group heading  Revert The kind of user interface element to use when entering or editing this field.
Label:	Group Heading  Revert Label for this field to display on the form.
Description:	This is a sample group heading  Revert Descriptive text for this field, displayed with the user-interface element.
CSS Class:	<input type="text"/>  Revert Optional CSS class name to apply to this form field.
CSS Style:	<input type="text"/>  Revert Optional CSS style text to apply to this form field.

Submit Button

If the **Submit button** user interface is selected, the field is displayed as a clickable form submit button, with the label of the field as the label of the button.

Figure 231 A Button on a Form

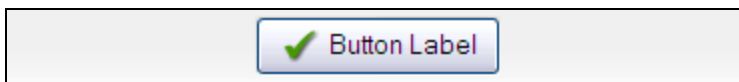








Figure 232 Form Display Properties Options for the Submit button User Interface

* User Interface:	Submit button  Revert The kind of user interface element to use when entering or editing this field.
Label:	Button Label  Revert Label for this field to display on the form.
Description:	<input type="text"/>  Revert Descriptive text for this field, displayed with the user-interface element.
CSS Class:	nwalimportant  Revert Optional CSS class name to apply to this form field.
CSS Style:	<input type="text"/>  Revert Optional CSS style text to apply to this form field.
Icon Image:	images/icon-checkmark.png  Revert Image to display with the user interface element.

The description is not used. The field's value is ignored, and will be set to NULL when the form is submitted. To place an image on the button, an icon may be specified.

To match the existing user interface conventions, you should ensure that the submit button has the highest rank number and is displayed at the bottom of the form.

Text Area

If the **Text area** user interface is selected, the field is displayed as a multiple-line text box. The text typed in this box is submitted as the value for the field.

Figure 233 A Text Area on a Form

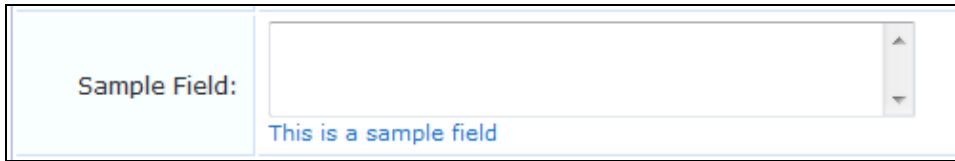


Figure 234 Form Display Properties Options for the Text area User Interface

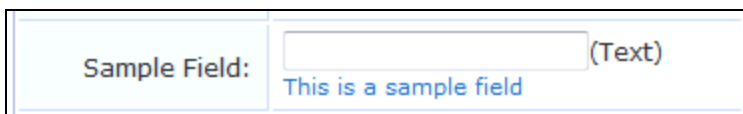
* User Interface:	Text area <input type="button" value="Revert"/>
Label:	Sample Field <input type="button" value="Revert"/> Label for this field to display on the form.
Description:	This is a sample field <input type="button" value="Revert"/> Descriptive text for this field, displayed with the user-interface element.
CSS Class:	nwalmimportant <input type="button" value="Revert"/> Optional CSS class name to apply to this form field.
CSS Style:	<input type="text"/> Optional CSS style text to apply to this form field.
Rows:	3 <input type="button" value="Revert"/> Number of rows to display in the user interface element.
Columns:	10 <input type="button" value="Revert"/> Number of columns to display in the user interface element.

We recommend that you specify the desired minimum dimensions of the text area, either with the **Rows** and **Columns** options, or by specifying a width in the **CSS Style** option (for example, “width: 460px; height: 100px;” specifies a 460 x 100 pixel minimum area).

Text Field





If the **Text field** user interface is selected, the field is displayed as a single-line text box. The text typed in this box is submitted as the value for the field.

Figure 235 A Text Field on a Form



A short text label may be placed after the text box using the **Label After** option. This field allows you to specify HTML (using Smarty template syntax) instead of plain text to be displayed after the input field.

Figure 236 Form Display Properties Options for the Text field User Interface

* User Interface:	Text field  Revert
Label:	Sample Field  Revert
Description:	This is a sample field  Revert
CSS Class:	<input type="text"/>
CSS Style:	width: 240px;  Revert
Label After:	<input type="text"/>
Placeholder:	<input type="text"/>
Max Length:	<input type="text"/>

If you select **Text** or **Password** as the **User Interface** type, the Placeholder row is added to this form. You may use this field to enter a temporary value, such as a hint for how to complete the field, that can later be overridden by the user completing the form that uses this field.

Form Validation Properties

On the **Form Field Editor** (see "Form Field Editor " on page 309), the form validation properties control the validation of data entered into a form. By specifying appropriate validation rules, you can detect when users attempt to enter incorrect data and require them to correct their mistake. All fields must be successfully validated before any form processing can take place. This ensures that the form processing always has user input that is known to be valid.

Figure 237 Form Field Editor, Form Validation Properties Area



Form Validation Properties	
These properties control how the value of this field is checked.	
Field Required:	<input checked="" type="checkbox"/> Field value must be supplied Select this option if the field cannot be omitted or left blank.
Initial Value:	value for sample field Value to initialize this field with when the form is first displayed.
* Validator:	IsNotEmpty 
Validator Param:	(None) 
Validator Argument:	<input type="text"/> Optional value to supply as the argument to a validator.
Validation Error:	You cannot leave this field blank The error message to display if the field's value fails validation and the validator does not return an error message directly.

Table 134: Form Field Editor, Form Validation Properties Area

Field	Description
Field Required	<p>If selected, the field cannot be omitted or left empty. Required fields are marked with an asterisk, as shown below:</p> <div data-bbox="391 310 1127 394" style="border: 1px solid gray; padding: 5px;"> <p>* Sample Field: <input type="text" value="This is a sample field."/></p> </div> <p>All values supplied for a required field are always validated, including blank values. An optional field may be left blank. In this case, the field is not validated as there is no value for the field. However, any value that is supplied for an optional field is subject to validation checks.</p>
Initial Value	<p>Initial value for the form field. Use this option when a field value has a sensible default. The initial value should be expressed in the same way as the field's value. In particular, for drop-down list and radio button selections, the initial value should be the key of the desired default option. Likewise, for date/time fields that have a display function set, the initial value should be a value that can be passed to the display function.</p>
Validator	<p>(Required) Specifies the validator function for the field. See "Form Field Validation Functions" on page 737 for a description of the built-in validators.</p>
Validator Param	<p>Specifies the name of the field on the form, the value of which should be passed to the validator as its argument. This could be used to validate one field based on the contents of another. However, in most deployments this does not need to be set. To provide a fixed value as the argument to the validator, set the Validator Param selection to its default value, (Use argument).</p>
Validator Argument	<p>Provides further instructions to the selected validator. Not all validators require an argument; a validator such as IsValidEmail is entirely self-contained and will ignore the Validator Argument. Validators such as IsEqual, IsInRange and IsRegexMatch use the argument to perform validation.</p>
Validation Error	<p>Error message to display if the field's value fails validation and the validator does not return an empty message directly. Validation errors are displayed to the user by highlighting the field(s) that are in error and displaying the validation error message with the field:</p> <div data-bbox="391 1178 1159 1293" style="border: 1px solid gray; padding: 5px;"> <p>* Visitor's Name: <input style="border: 2px solid red;" type="text" value="Name of the visitor."/> You cannot leave this field blank. Name of the visitor.</p> </div>

Examples of Form field Validation

Example 1 — Integer Value Between 1 and 100 (Inclusive)

To create a form field that requires an integer value between 1 and 100 (inclusive) to be provided, use the following settings in the **Form Field Editor** (see "Form Field Editor " on page 309):

Figure 238 Form Field Editor, Form Validation Properties Area, Example Range of Integer Values

Form Validation Properties	
These properties control how the value of this field is checked.	
Field Required:	<input checked="" type="checkbox"/> Field value must be supplied Select this option if the field cannot be omitted or left blank.
Initial Value:	<input type="text"/> Value to initialize this field with when the form is first displayed.
* Validator:	IsInRange <input type="text"/> The function used to validate the contents of a field.
Validator Param:	(None) <input type="text"/> Optional name of field whose value will be supplied as the argument to a validator.
Validator Argument:	array(1, 100) <input type="text"/> Optional value to supply as the argument to a validator.
Validation Error:	Please enter a number between 1 and 100. The error message to display if the field's value fails validation and the validator does not return an error message directly.



The form field will contain an integer value, so you should set the field's type to Integer when you create it.

In the **Validator** field, to specify the minimum and maximum values for the **IsInRange** validator, use the PHP syntax **array(1, 100)**. After saving changes on the form, this value will be internally converted to the equivalent code:

```
array (  
    0 => 1,  
    1 => 100,  
)
```

With these validator settings, users that enter an invalid value will now receive a validation error message:

Figure 239 Example Validation Error Message for an Invalid Range Value

* Sample Field:	<input type="text" value="123"/> (1 - 100) Please enter a number between 1 and 100. This is a sample field.
-----------------	---

Furthermore, be aware that blank values, or non-numeric values, will result in a different error message:

Figure 240 Example Validation Error Message for a Missing or Non-Numeric Entry

* Sample Field:	<input type="text" value="xyzy"/> (1 - 100) Parameter must be an integer This is a sample field.
-----------------	--

The reason for this is that in this case, the validation has failed due to a type error — the field is specified to have an integer type, and a blank or non-numeric value cannot be converted to an integer. To set the error message to display in this case, use the **Type Error** option in the **Advanced Properties** area.

Example 2 — Small Number of String Values

To create a form field that accepts one of a small number of string values, use the following settings in the form field editor:

Figure 241 *Form Field Editor, Form Validation Properties Area, Example Array Values*

Field Required:	<input checked="" type="checkbox"/> Field value must be supplied Select this option if the field cannot be omitted or left blank.
Initial Value:	sales Value to initialize this field with when the form is first displayed.
* Validator:	IsArrayValue The function used to validate the contents of a field.
Validator Param:	(None) Optional name of field whose value will be supplied as the argument to a validator.
Validator Argument:	array ("accounting", "hr", "research", "sales", "support") Optional value to supply as the argument to a validator.
Validation Error:	Please select from one of the following options. The error message to display if the field's value fails validation and the validator does not return an error message directly.

This example could be used for a string field named **visitor_department**. Because the values are known in advance, a drop-down list is the most suitable user interface. An initial value for the form field, as shown above, could be used if most visitors are in fact there to visit the sales team.

To match against a list of options used for a drop-down list or set of radio buttons, you can use the **IsInOptionsList** validator.

Example 3 — US Social Security Numbers

To create a form field that validates US social security numbers using a regular expression, use the following settings in the form field editor:

Figure 242 Form Field Editor, Form Validation Properties Area, Example Regular Expression Values

Field Required:	<input checked="" type="checkbox"/> Field value must be supplied Select this option if the field cannot be omitted or left blank.
Initial Value:	<input type="text"/> Value to initialize this field with when the form is first displayed.
* Validator:	IsRegexMatch <input type="button" value="v"/> The function used to validate the contents of a field.
Validator Param:	(None) <input type="button" value="v"/> Optional name of field whose value will be supplied as the argument to a validator.
Validator Argument:	<input type="text" value="/^\d\d\d-\d\d-\d\d\d\d\$/"/> Optional value to supply as the argument to a validator.
Validation Error:	<input type="text" value="Please a valid SSN."/> The error message to display if the field's value fails validation and the validator does not return an error message directly.

Notice that the regular expression used here includes beginning and ending delimiters (in this case the `/` character), and ensures that the whole string matches by the start-of-string marker `^` and the end-of-string marker `$`. The construct `\d` is used to match a single digit. Many equivalent regular expressions could be written to perform this validation task. See "Regular Expressions" on page 749 for more information about regular expressions.

Advanced Form Field Properties

Figure 243 Form Field Editor, Advanced Properties Area

Advanced Properties	
These properties control conversion, display and dynamic behaviours.	
Advanced:	<input checked="" type="checkbox"/> Show advanced properties
Conversion:	(Use default) <input type="button" value="v"/> The function used to convert an incoming field value prior to validation.
Type Error:	<input type="text"/> The error message to display if the field's value is not supplied, has an incorrect type, or if conversion fails.
Value Format:	(Use default) <input type="button" value="v"/> The function used to format a field value after validation.
Display Function:	(Use default) <input type="button" value="v"/> The function used to convert a field to a displayable value on the form.
Static Display Function:	(Use default) <input type="button" value="v"/> The function used to convert a static field to a displayable value on the form.
Force Value:	<input type="checkbox"/> Always use initial value on form submit Sets the field's value to the initial value specified above when the form is submitted. Use this option when the field must have a certain value that cannot be overridden by a user.
Pre-Registration:	Field was not pre-registered <input type="button" value="v"/> Pre-Registration applies for accounts that have been created prior to registration. A field requiring a match will be searched in the account list. If a single match is found, the registration can continue.
Enable If:	<input type="text"/> Javascript conditional expression for this field's enabled property. The expression 'f.value' returns the in-form value of field 'f'.
Visible If:	<input type="text"/> Javascript conditional expression for this field's visibility. The expression 'f.value' returns the in-form value of field 'f'.

On the **Form Field Editor** (see "Form Field Editor" on page 309), options in the **Advanced Properties** area control certain optional form processing behaviors. You can also specify JavaScript expressions to build dynamic forms similar to those found elsewhere in the application.

Table 135: Form Field Editor, Advanced Properties Area

Field	Description
Advanced	If selected, displays the advanced properties options in the Form Field Editor .
Conversion	Specifies the function used to convert an incoming field value prior to validation. This option can be used to enable certain form processing behavior. See "Form Field Conversion Functions" on page 744 and "Form Field Display Formatting Functions" on page 745.
Type Error	Error message to display if the field's value is not supplied, has an incorrect type, or the conversion fails.
Value Format	Specifies the function used to format the field value after validation. This option can be used to enable certain form processing behavior. See "Form Field Conversion Functions" on page 744 and "Form Field Display Formatting Functions" on page 745.

Table 135: Form Field Editor, Advanced Properties Area(Continued)

Field	Description
Display Function	Specifies the function used to convert a field to a displayable value on the form. This option can be used to enable certain form processing behavior. See "Form Field Conversion Functions" on page 744 and "Form Field Display Formatting Functions" on page 745 .
Display Param	Name of the field whose value will be supplied as the argument to a display function.
Display Arguments	Value to supply as the argument to a display function.
Static Display Function	Specifies the function used to convert a static field to a displayable value on the form.
Force Value	If selected, sets the field's value to the initial value specified above when the form is submitted. Prevents attempts to override the value set for the field. When this option is set, if a user modifies the field's value, it reverts to the specified initial value when the form is submitted. A similar effect can be achieved by using appropriate validation rules, but selecting this check box is easier. Using this option is recommended for hidden fields, particularly those related to security, such as role ID or expiration date.
Pre-Registration	For accounts that have been created prior to registration, specifies whether the guest's entry must match the preliminary value provided for the field during pre-registration. For pre-registered guest accounts, some fields may be completed during pre-registration and some fields may be left for the guest to complete at registration. Options include: <ul style="list-style-type: none"> ● Field was not pre-registered — Select this option if a value was not provided for a field when the account was created ● Guest must supply field — Select this option if a preliminary value was provided for the field but the guest's entered value does not need to match case or all characters. For example, a bulk account creation might use random usernames, and each visitor's entry in that field would not need to match exactly. ● Guest must supply field (match case) — Select this option if a preliminary value was provided for the field and the guest's entered value must match case or all characters. If the guest's entry does not successfully match the preregistered value, the account registration will not succeed. For example, if a list of email addresses and phone numbers was imported for pre-registration, each visitor's entries for those fields at registration must match.
Enable If	Javascript conditional expression for the field's enabled property. The expression "f.value" returns the in-form value of field "f".
Visible If	Javascript conditional expression for the field's visibility. The expression "f.value" returns the in-form value of field "f".
Save Changes	Saves your changes on this form and returns you to the Customize Form Fields list view at Configuration > Pages > Forms & Views .

Creating a Single Password for Multiple Accounts

You can create multiple accounts that have the same password. In order to do this, you first customize the **Create Multiple Guest Accounts** form to include the **Password** field.

To include the **Password** field on the **Create Multiple Guest Accounts** form:

1. Go to **Configuration > Pages > Forms & Views**. Click the **create_multi** row, then click its **Edit Fields** link. The **Customize Form Fields** view opens, showing a list of the fields included in the **Create Multiple Guest Accounts** form and their descriptions.

At this point, the **Password** field is not listed because the **Create Multiple Guest Accounts** form (create_multi) has not yet been customized to include it. You will create it for the form in the next step.

2. Click on any field in the list to expand a row, then click the **Insert After** link (you can modify this placement later). The **Customize Form Field** form opens.
3. In the **Field Name** row, choose **password** from the drop-down list. The form displays configuration options for this field.

Figure 244 Form Field Editor, Password Configuration Options

Form Field Editor	
* Field Name:	password <small>Select the field definition to attach to the form.</small>
Form Display Properties <small>These properties control the user interface displayed for this field.</small>	
Field:	<input checked="" type="checkbox"/> Enable this field <small>When checked, the field will be included as part of the form.</small>
* Rank:	4 <small>Number indicating the relative ordering of user interface fields, which are displayed in order of increasing rank.</small>
* User Interface:	Password text field <small>The kind of user interface element to use when entering or editing this field.</small>
Label:	Visitor Password: <small>Label for this field to display on the form.</small>

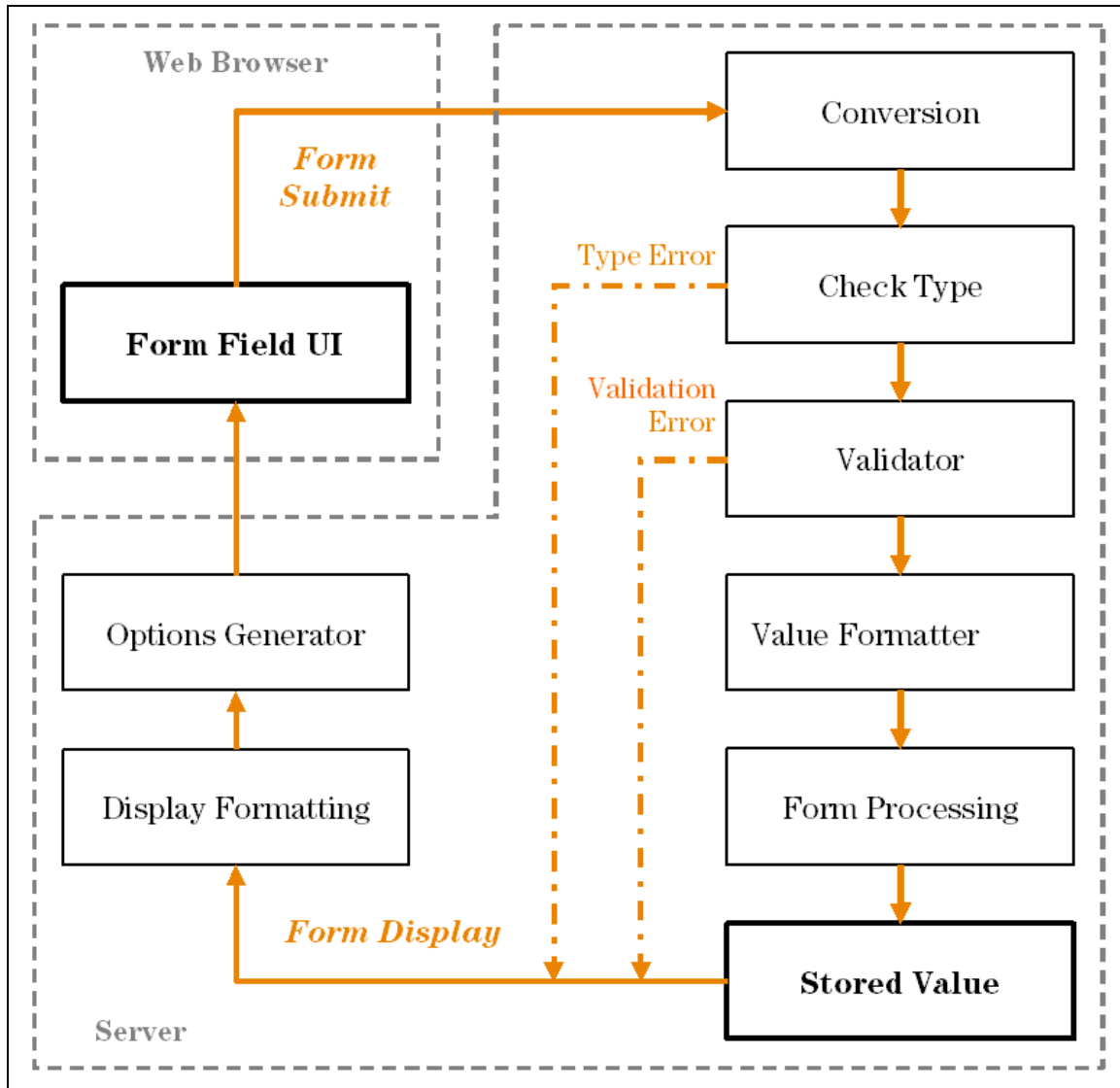
4. In the **Field** row, mark the **Enable this field** check box.
5. To adjust the placement of the password field on the **Create Multiple Guest Accounts** form, you may change the number in the **Rank** field.
6. In the **User Interface** row, choose **Password text field** from the drop-down list. The **Field Required** check box should now be automatically marked, and the **Validator** field should be set to **IsNotEmpty**.
7. Click **Save Changes**. The **Customize Form Fields** view opens again, and the password field is now included and can be edited.

To create the multiple accounts that all use the same password, see ["Creating Multiple Guest Accounts" on page 50](#).

Form Field Validation Processing Sequence

The following figure shows the interaction between the user interface displayed on a form and the various conversion and display options available on the **Form Field Editor** (see ["Form Field Editor " on page 309](#)).

Figure 245 Steps Involved in Form Field Processing



The Conversion step should be used when the type of data displayed in the user interface is different from the type required when storing the field.

For example, consider a form field displayed as a date/time picker, such as the **expire_time** field used to specify an account expiration time on the **create_user** form. The user interface is displayed as a text field, but the value that is required for the form processing is a UNIX time (integer value).

Figure 246 Form Field Editor, Advanced Properties Area for a Field Using a Date/Time Picker

Advanced Properties	
These properties control conversion, display and dynamic behaviours.	
Advanced:	<input checked="" type="checkbox"/> Show advanced properties
Conversion:	NwaConvertOptionalDateTime The function used to convert an incoming field value prior to validation.
Type Error:	Please enter a valid date and time. The error message to display if the field's value is not supplied, has an incorrect type, or if conversion fails.
Value Format:	(None) The function used to format a field value after validation.
Display Function:	NwaDateFormat The function used to convert a field to a displayable value on the form.
Display Param:	expire_time Optional name of field whose value will be supplied as the argument to a display function.
Display Arguments:	%Y-%m-%d %H:%M?: Optional value to supply as the argument to a display function.

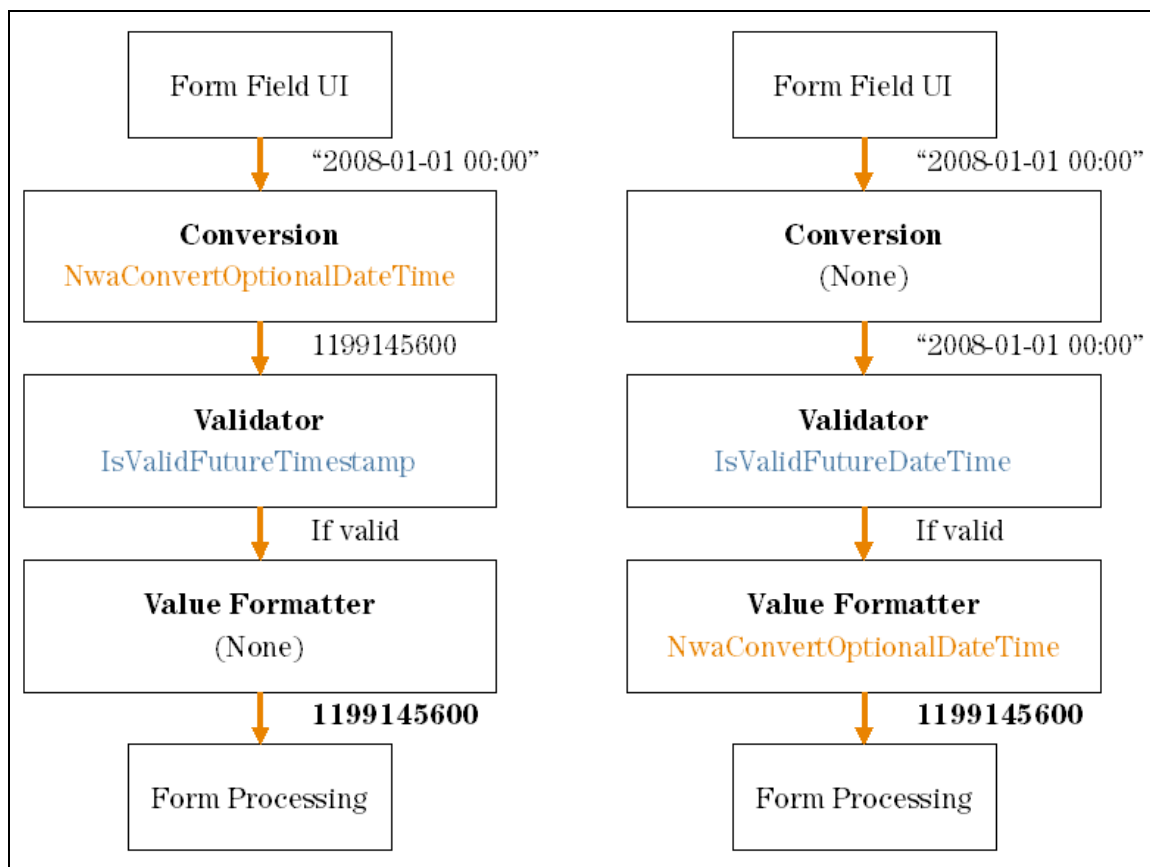
In this case, the Conversion function is set to NwaConvertOptionalDateTime to convert the string time representation from the form field (for example, "2008-01-01") to UNIX time (for example, 1199145600).

The Validator for the **expire_time** field is **IsValidFutureTimestamp**, which checks an *integer* argument against the current time.

The Value Formatter is applied after validation. This may be used in situations where the validator requires the specific type of data supplied on the form, but the stored value should be of a different type. In the **expire_time** field example, this is not required, and so the value formatter is not used. However, if the Conversion function had not been used, and the Validator had been set to **IsValidFutureDateTime** (which checks a *string* date/time value), then the Value Formatter would need to be set to NwaConvertOptionalDateTime to perform the data conversion before the form processing.

A comparison of these two approaches is shown below to illustrate the difference:

Figure 247 Comparison of Two Validation Approaches



When using a Conversion or Value Format function, you will almost always have to set up a Display Function for the form field. This function is used to perform the conversion in the reverse direction – between the internal stored value and the value displayed in the form field.

See ["Form Field Conversion Functions"](#) on page 744 for a detailed list of the options available to you for the Conversion and Value Format functions.

The **Display Param** is the name of a form field, the value of which will be passed to the Display Function. In almost all cases this option should contain the name of the form field.

Display Arguments are available for use with a form field and are used to control the conversion process. In the case of the **expire_time** form field, the Display Function is set to **NwaDateFormat** to perform a conversion from a UNIX time to a date/time string, and the Display Argument specifies the format to use for the conversion.

See ["Form Field Display Formatting Functions"](#) on page 745 for a detailed list of the options available to you for the Display Function and Static Display Function.

The **Enable If** and **Visible If** options in the **Form Field Editor** allow you to specify JavaScript expressions. The result obtained by evaluating these expressions is used to enable/disable, or show/hide the form field in real time, while an operator is using the form.

Unlike the other parts of the form field editor, the **Enable If** and **Visible If** expressions are evaluated by the operator's Web browser. These expressions are not used by the server for any other purpose.

The expression must be a Boolean expression in the JavaScript language; statements and other code should not be included as this will cause a syntax error when the form is displayed in a Web browser.

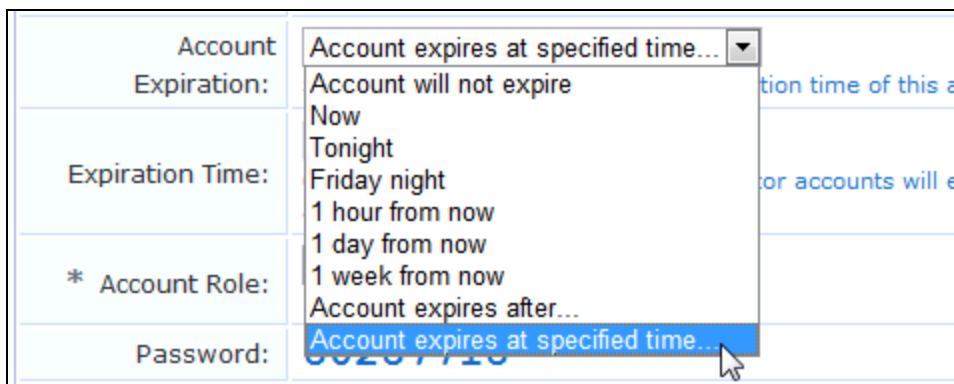
Because of the scoping rules of JavaScript, all of the user interface elements that make up the form are available as variables in the local scope with the same name as the form field. Thus, to access the current value of a text field named **sample_field** in a JavaScript expression, you would use the code **sample_field.value**.

Most user interface elements support the **value** property to retrieve the current value. For check boxes, however, use the **checked** property to determine if the check box is currently selected.

The most practical use for this capability is to hide a form field until a certain value of some other related field has been selected.

For example, the default **create_user** form has an **Account Expiration** drop-down list. One of the values in this list is special: the **-1** option displays the value **Account expires at a specified time...**

Figure 248 *The Account Expiration Drop-Down List*



When this option is selected, the form expands to include the **Expires After** row, allowing the user to specify a time other than one of the options in the list.

The **expire_time** field uses the JavaScript expression **expire_after.value < 0** for the **Visible If** option. When the **-1** option has been selected, this condition will become true and the field will be displayed.

If the **expire_timezone** field is used in conjunction with **expire_time** and a time zone and date are selected, the date calculation is adjusted relative to the time zone.

Additional examples of the **Visible If** conditional expressions can be found in the **guest_edit** form.

Editing Views

A view is a page in the application that displays data, similar to a form, but does not contain interactive fields the user can modify. It consists of one or more columns, each of which contains a single field. You can change which fields are displayed and how each field is displayed. You can also define your own fields using the **Customize Fields** page, and then add them to a view by choosing appropriate display options for each new column.

To add a new field to a view, reorder the fields, or make changes to an existing field in a view, go to **Configuration > Pages > Forms & Views**, click the view, and click its **Edit Fields** link. The **Customize View Fields** editor opens.

Figure 249 *The Customize View Fields List View*

Quick Help		Add Field		
Rank	Field	Type	Title	Width
10	username	sort	Username	160px
15	visitor_name	sort	Full Name	120px
20	visitor_company	sort	Company	100px
30	visitor_phone	sort	Phone	120px
40	creator_name	sort	Creator	100px
Edit Edit Base Field Remove Insert Before Insert After Enable Field				
50	sponsor_name	sort	Sponsor	100px
60	role_name	static_options	Role	120px
70	current_state	text	State	75px

The **Customize View Fields** list view includes the following columns:

- **Rank** — Specifies the relative ordering of the columns when displaying the view. The **Customize View Fields** editor always shows the columns in order by rank.
- **Field** — The field name.
- **Type** — The type of the field. This controls what kind of user interface element is used to display the column, and whether the column is to be sortable or not. Values displayed in *italics* are default values defined for the field being displayed.
- **Title** — The title of the column. Values displayed in *italics* are default values defined for the field being displayed.
- **Width** — The width of the column. Values displayed in *italics* are default values defined for the field being displayed.

All fields that have been defined for the view are included in the list. You can click a field's row in the list or use the links provided on the page for additional options:

Table 136: *Customize View Fields*

Field	Description
Edit	Make changes to an existing column. The row expands to include the View Field Editor . Any changes made to the field using this editor will apply only to this field on the view being edited. See "View Field Editor" on page 339 .
Edit Base Field	Make changes to an existing field definition. The Edit Field form opens. Any changes made to the field using this editor will apply to all views that are using this field (except where the view field has already been modified to be different from the underlying field definition). See "Creating a Custom Field" on page 295 .
Remove	Deletes the field from the view. You will be asked to confirm the deletion.
Insert Before	Adds a new column to the view. Opens a blank View Field Editor form and automatically sets the rank number of the new column. You can specify the field that this field should be above.
Insert After	Adds a new column to the view. Opens a blank View Field Editor form and automatically sets the rank number of the new column. You can specify the field that this field should be below.

Table 136: *Customize View Fields(Continued)*

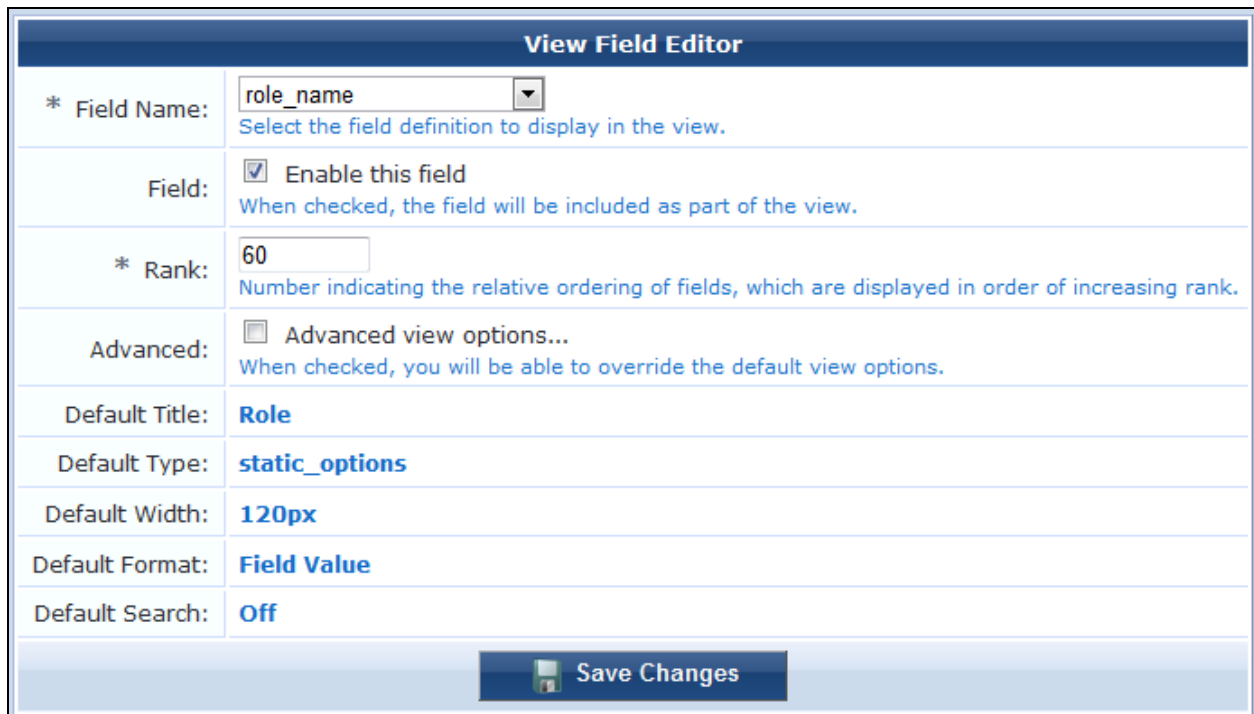
Field	Description
Enable Field	Immediately enables display of the column. A progress indicator is briefly displayed.
Disable Field	Immediately disables display of the column. A progress indicator is briefly displayed.
Customize fields	Lets you modify existing fields. The Customize Fields list view opens (Configuration > Pages > Fields). See "Customizing Fields" on page 294.
Back to list of forms & views	Returns to the parent page, the Customize Forms & Views list view (Configuration > Pages > Forms & Views). See "Customizing Forms and Views" on page 305.
Use this view	Opens the view in the application.

View Field Editor

The view field editor is used to control the data-display aspects of a column within the view. Each column in a view displays the value of a single field.

To edit a field for a view, go to **Configuration > Pages > Forms & Views**, click a view in the list, and click its **Edit Fields** link. In the **Customize View Fields** list, click a field and then click the field's **Edit** link. The row expands to include the **View Field Editor**.

Figure 250 *The View Field Editor*



The screenshot shows the 'View Field Editor' form with the following fields and values:

- * Field Name:** role_name (dropdown menu)
- Field:** Enable this field. When checked, the field will be included as part of the view.
- * Rank:** 60 (text input)
- Advanced:** Advanced view options... When checked, you will be able to override the default view options.
- Default Title:** Role
- Default Type:** static_options
- Default Width:** 120px
- Default Format:** Field Value
- Default Search:** Off

At the bottom of the form is a **Save Changes** button.

Table 137: View Field Editor

Field	Description
Field Name	(Required) Specifies the field definition to display in the view.
Field	If selected, enables the field. To use the default view display properties for a field, you only need to select this check box to enable the field to display in the column, and then click Save Changes . No further changes are needed on this form.
Rank	(Required) Indicates the field's position in the relative ordering of the fields. Fields are displayed in order of increasing rank.
Advanced	If selected, lets you override the default view options and customize the view display properties. This form expands to include the advanced options.
Default Title	Default title text for this field's column. The default value cannot be edited.
Column Title	Lets you override the default and specify title text to display for this field's column. To use the default, leave this text field empty.
Default Type	Default type of the column used for this field. The default value cannot be edited.
Column Type	Lets you override the default and specify the type of column used to display this field. To use the default, leave this drop-down selection empty. Options include: <ul style="list-style-type: none"> • Text – The column displays a value as text. • Sortable text – The column displays a value as text, and may be sorted by clicking on the column heading. • Sortable text, case-insensitive – The same as “Sortable text”, but the column sorting will treat uppercase and lowercase letters the same. • Sortable numeric – The column displays a numeric value, and may be sorted by clicking on the column heading.
Default Width	Default width for the field's column, in pixels. The default value cannot be edited.
Column Width	Lets you override the default and specify a width in pixels for the field's column. To use the default, leave this text field empty.
CSS Class	CSS class name to apply to the field.
Default CSS Style	Default CSS style text to apply to the field. The default value cannot be edited.
CSS Style	Lets you override the default and specify the CSS style text to apply to this field. To use the default, leave this field empty.
Default Format	Default format for displaying the field. The default value cannot be edited.
Column Format	Lets you override the default and specify how the field's value should be displayed. To use the default, leave this field empty. Options include: <ul style="list-style-type: none"> • Field Value — The value of the field is displayed as plain text. • Field Value (Unescaped) — The value of the field is displayed as HTML.

Table 137: View Field Editor(Continued)

Field	Description
	<ul style="list-style-type: none"> • Boolean - Yes/No — The value of the field is converted to Boolean and displayed as “Yes” or “No”. • Boolean - Enabled/Disabled — The value of the field is converted to Boolean and displayed as “Enabled” or “Disabled”. • Boolean - On/Off — The value of the field is converted to Boolean and displayed as “On” or “Off”. • Date — The value of the field is assumed to be a UNIX timestamp value and is displayed as a date and time. • Duration (from seconds) — The value of the field is assumed to be a time period measured in seconds and is displayed as a duration (for example, “23 seconds”, “45 minutes”) • Duration (from minutes) — The value of the field is assumed to be a time period measured in minutes and is displayed as a duration (for example, “45 minutes”, “12 hours”) • Use form options — The value of the field is assumed to be one of the keys from the field's option list. The value displayed is the corresponding value for the key. • Custom expression... — The Display Expression text area is displayed allowing a custom JavaScript expression to be entered. See "View Display Expression Technical Reference" on page 747 for technical information about this display expression and a list of the functions that are available to format the value.
Default Search	Default value for whether the field will be included in filter searches. The default value cannot be edited.
Search	Many views include the ability to filter results. If selected, and the field is enabled, it will be included in the search.
Save Changes	Saves your changes to the View Field Editor form.

Customizing Guest Self-Registration



Guest self-registration allows an administrator to customize the process for guests to create their own visitor accounts. Self-registration is also referred to as self-provisioned access. The registration process consists of a data collection step (the ‘registration page’) and a confirmation step (the ‘receipt page’):

- On the registration page, you can define what information is collected from visitors. New fields and data validation rules can be defined with the custom form editor. Specific details about the type of visitor accounts created are also set here.
- The receipt page typically contains static information about the guest account, but several different actions can be included, enabling visitors to obtain their receipt in different ways. The receipt page can also be used to automatically log the guest into a Network Access Server, enabling them to start using the network immediately.

Detailed user interface customization can be performed for all parts of the self-registration process. You can define page titles, template code for the page header and footer, and choose a skin that controls the overall look and feel of self-registration. The default user interface customization can be disabled.

A guest self-registration process consists of many different settings. The **Customize Guest Registration** form organizes these settings into the different stages of the registration process, each on its own section of the form. These sections are displayed as separate pages in the Configuration UI. When you create a new registration page, the process walks you through these pages of the form one at a time. When you edit a registration page, links let you go directly to the section for the stage of the process you want to edit.

This section includes:

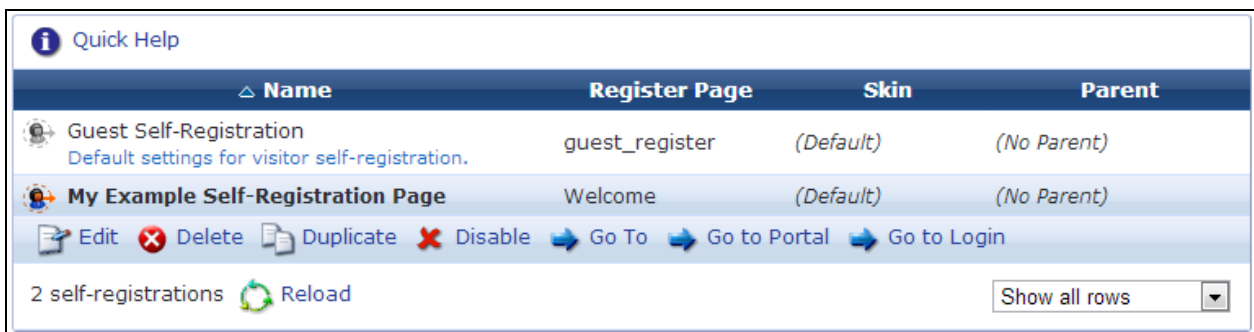
- "Accessing the Guest Self-Registration Customization Forms" on page 342
- "Self-Registration Sequence Diagram" on page 346
- "Editing Self-Registration Pages" on page 347
- "Creating a Self-Registration Page" on page 348
- "Configuring Basic Properties for Self-Registration" on page 350
- "Editing Registration Page Properties" on page 353
- "Editing the Default Self-Registration Form Settings" on page 355
- "Editing Guest Receipt Page Properties" on page 357
- "Editing Receipt Actions" on page 358
- "Editing Login Page Properties" on page 373
- "Editing Social Logins Properties" on page 379
- "Self-Service Portal Properties" on page 386
- "Resetting Passwords with the Self-Service Portal" on page 394
- "Enabling and Editing NAS Login Properties" on page 384

Accessing the Guest Self-Registration Customization Forms

To create a new guest self-registration page, go to **Configuration > Pages > Guest Self-Registrations** and click the **Create new self-registration page** link in the upper-right corner. The first part of the **Customize Guest Registration** form opens. See "Creating a Self-Registration Page" on page 348.

To work with an existing guest self-registration page, go to **Configuration > Pages > Guest Self-Registrations**. The **Guest Self-Registration** list view opens. All self-registration pages that have been created are included in this list.

Figure 251 *The Guest Self-Registrations List View*



Name	Register Page	Skin	Parent
Guest Self-Registration Default settings for visitor self-registration.	guest_register	(Default)	(No Parent)
My Example Self-Registration Page	Welcome	(Default)	(No Parent)

2 self-registrations Reload Show all rows

Click a page's row in the list to select it. The row expands to include options for working with the self-registration pages.

Table 138: Guest Self-Registrations

Field	Description
Edit	Edit any of the self-registration page's properties. The Customize Guest Registration workflow diagram opens. Links in the workflow diagram provide access to any section of the registration page's properties. For information on editing the different parts of the self-registration process, see "Editing Self-Registration Pages" on page 347 .
Delete	Deletes the guest self-registration page. You will be asked to confirm the deletion.
Duplicate	Creates a copy of the self-registration page and appends a number to page name. See "Duplicating a Self-Registration Page" on page 343 .
Enable	Enables the self-registration page so it can be used.
Disable	Disables the self-registration page for the user and displays a message. See "Disabling a Self-Registration Page" on page 344 .
Go To	Displays a preview of the Visitor Registration network access form. See "The "Go To" Option: The Registration Page" on page 344 .
Go to Portal	Displays a preview of the Self Service Login portal. See "The "Go to Portal" Option " on page 345 .
Go to Login	Displays a preview of the Network Login form. See "The "Go to Login" Option" on page 346 .
Create new self-registration	Create a new self-registration page. See "Creating a Self-Registration Page" on page 348 .

Duplicating a Self-Registration Page

When you choose the **Duplicate** option for a self-registration page, the row expands to include the **Duplicate Guest Registration** form. Complete the fields to rename the page and enter a name for the **Register Page**. You can also give the page a description and indicate the parent page.

The **Register** page does not exist until you create it here. There are no spaces in this name. This page name will become part of the URL used to access the self provisioning page. For example, the default "guest_register" page is accessed using the URL **guest_register.php**.

Figure 252 *The Duplicate Guest Registration Form*

The screenshot shows a form titled "Duplicate Guest Registration" with the following fields and options:

- * Name:** A text input field containing "Guest Self-Registration (1)". Below it is the instruction: "Enter a name to identify the guest self-registration instance. This is visible only to administrators."
- Description:** A text area containing "Default settings for visitor self-registration." Below it is the instruction: "Enter comments about this instance of guest self-registration. This is visible only to administrators."
- * Register Page:** A text input field containing "guest_register_1". Below it is the instruction: "Enter the base page name for the guest registration page."
- Parent:** Two radio button options: "Same as original" and "Use the original as the new parent". Below these is the instruction: "Fields and text will use the parent's value unless overridden. Simply edit a field to override the parent value."

At the bottom of the form are two buttons: "Save Changes" and "Cancel".

Disabling a Self-Registration Page

When you choose the **Disable** option for a self-registration page, the row expands to include the **Disable Guest Registration** form. In the **Disabled Message** text box, you may enter the HTML content to display on the page when guest registration is disabled. You can also use the drop-down list to add images or other content items.

Figure 253 *The Disable Guest Registration Form*

The screenshot shows a form titled "Disable Guest Registration" with the following fields and options:

- Enabled:** Two radio button options: "Enable: 'Guest Self-Registration'" and "Disable: 'Guest Self-Registration'". The "Disable" option is selected.
- Disabled Message:** A text area for entering HTML content. Below it is a drop-down menu labeled "Insert content item...". Below the text area is the instruction: "HTML template code displayed on the page if guest registration is disabled."


At the bottom of the form are two buttons: "Save Changes" and "Cancel".

The "Go To" Option: The Registration Page

When you choose the **Go To** option for a self-registration page, the row expands to show an active preview of the **Visitor Registration** page and form as the visitor would see it. This is the registration page and data collection step. You may test the behavior of the form.

Figure 254 *The Visitor Registration Form*

Please complete the form below to gain access to the network.

Visitor Registration	
* Your Name:	<input type="text"/> <small>Please enter your full name.</small>
* Email Address:	<input type="text"/> <small>Please enter your email address. This will become your username to log into the network.</small>
* Confirm:	<input type="checkbox"/> I accept the terms of use
	

* required field

Already have an account? [Sign In](#)

The Receipt Page

After the visitor successfully registers, the receipt page is their confirmation and provides their login and access information.

Figure 255 *The Visitor Registration Receipt*

The details for your guest account are shown below.

Visitor Registration Receipt	
Sponsor's Name:	admin
Guest's Name:	My Name
Account Username:	 myName@myCompany.com
Guest Password:	 29114430
Activation Time:	Monday, 09 December 2013, 10:38 PM
Expiration Time:	Tuesday, 10 December 2013, 10:38 PM
	
 Download account details	

The "Go to Portal" Option

When you choose the **Go To Portal** option for a self-registration page, the row expands to show an active preview of the **Self Service Login** page and form as the visitor would see it. This form lets the visitor access their account information. You may test the behavior of the form.

Figure 256 *The Self-Service Login Form*


Please log in to the Self Service area to access the details about your account.


Self Service Login

* Username:

* Password:

* required field

 [I've forgotten my password](#)

 [I don't have an account](#)

The "Go to Login" Option

When you choose the **Go To Login** option for a self-registration page, the row expands to show an active preview of the **Network Login** page and form as the visitor would see it. This is the page the visitor sees when they log in to the network. You may test the behavior of the form.

Figure 257 *The Network Login Form*

Please login to the network using your username and password.

Network Login

* Username:

* Password:

* Terms: [I accept the terms of use](#)

* required field

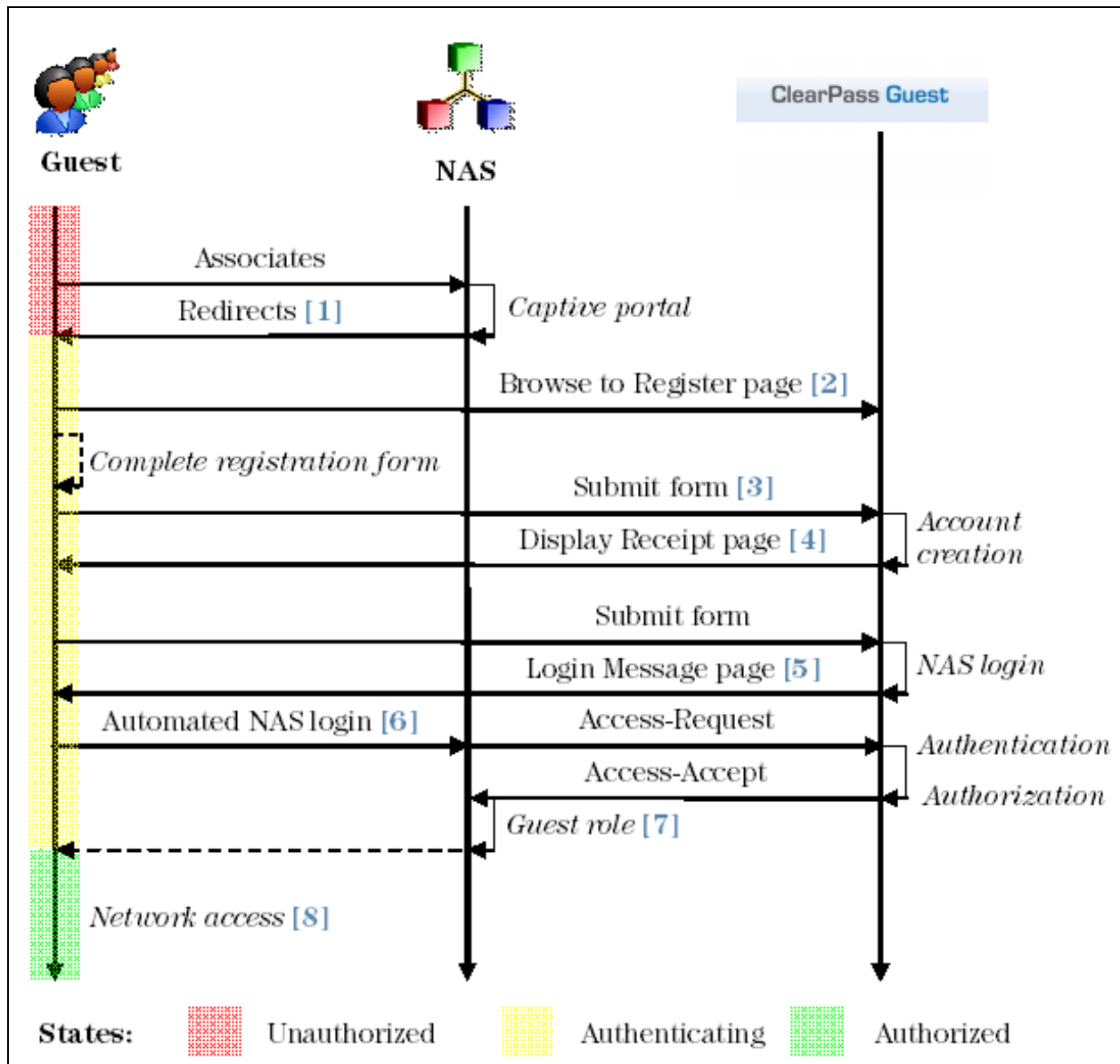
Need an account? [Click Here](#)

Self-Registration Sequence Diagram

To set up a captive portal with guest self-registration, you configure your Network Access Servers (NAS) to redirect guests to the URL of the 'Go To' link. To complete the portal, you ensure that the NAS is configured to authorize users with the ClearPass Guest RADIUS server, and set up the self-registration NAS login to redirect registered guests back to the NAS.

This process is shown below.

Figure 258 Sequence Diagram for Guest Self-Registration



In this diagram, the stages in the self-registration process are identified by the numbers in brackets, as follows:

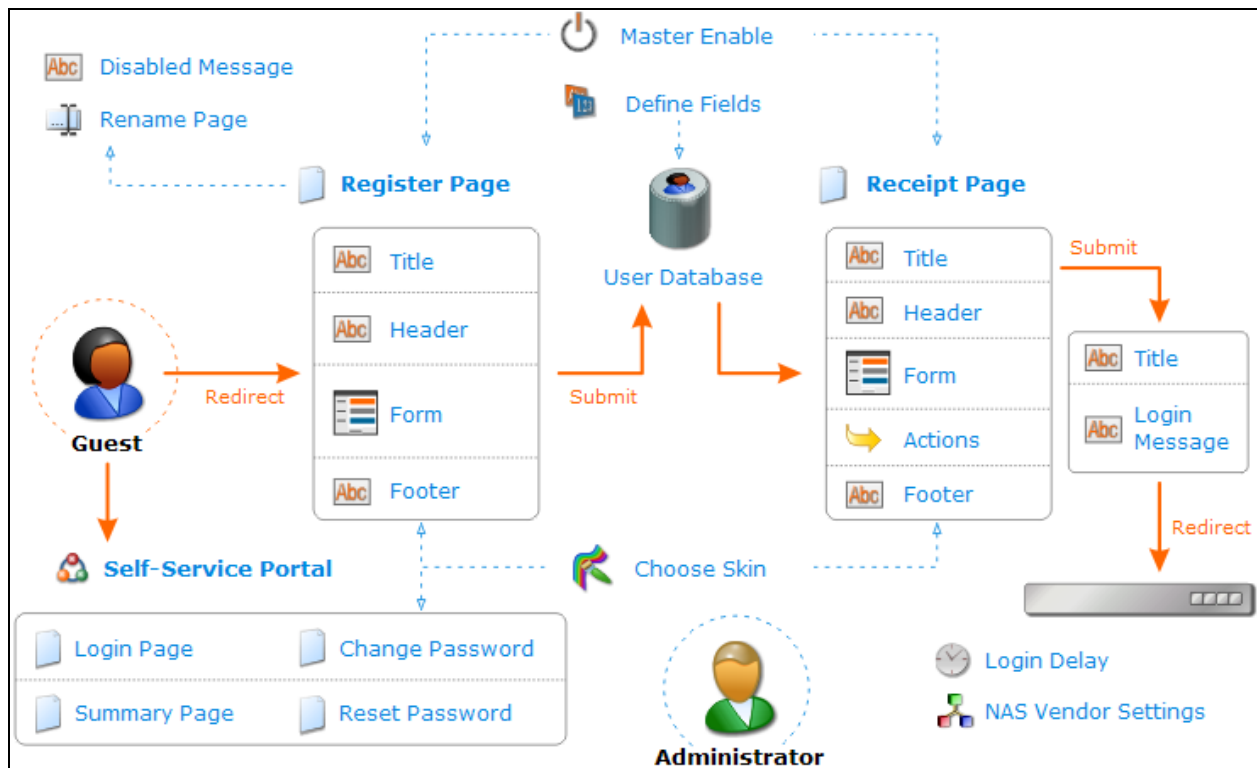
The captive portal redirects unauthorized users [1] to the registration page [2]. After submitting the registration form [3], the guest account is created and the receipt page is displayed [4] with the details of the guest account. If NAS login is enabled (the default), submitting the form on this page will display a login message [5] and automatically redirect the guest to the NAS login [6]. After authentication and authorization the guest's security profile is applied by the NAS [7], enabling the guest to access the network [8].

Editing Self-Registration Pages

When you edit a registration page, links let you go directly to the section of the **Customize Guest Registration** form that corresponds to the stage of the process you want to edit.

To edit a self-registration page, go to **Configuration > Pages > Guest Self-Registrations**, select the page in the list, and click its **Edit** link. The **Customize Guest Registration** workflow diagram opens.

Figure 259 Guest Self-Registration Workflow Diagram



The diagram shows the guest self-registration process. The solid orange arrows show the workflow for the visitor. The dotted blue arrows show the workflow for the administrator. The blue headings in the diagram are links to the corresponding sections of the **Customize Guest Registration** form. Click an icon or label in the diagram to jump directly to the editor for that item.

To view the **Visitor Registration** network access form (the registration page), click the **Launch this guest registration page** link in the upper-right corner. To view the self-service portal the visitor can use to log in to their account details after registration, click the **Launch self-service portal** link. To view the visitor's network access login form, click the **Launch network login** link.

Creating a Self-Registration Page

The **Customize Guest Registration** form is divided across several pages, which are displayed separately. When you create a new registration page, the process walks you through these pages of the form one at a time. As you complete each page of the form, you can click **Save and Continue** to move to the next section of the form. At any point, you can click **Save and Continue** or use your browser's **Back** button to move back and forth through the pages, or you can click **Save Changes** to exit the process and go to the self-registration process diagram.

To create a new guest self-registration page, go to **Configuration > Pages > Guest Self-Registration** and click the **Create new self-registration page** link. The first section of **Customize Guest Registration** form opens, where you can configure basic properties and access control. The registration page does not exist until you create it here.

Figure 260 *The Customize Guest Registration Form*

Customize Guest Registration

Basic Properties

Options controlling basic operation of guest self-registration.

* Name:	<input style="width: 90%;" type="text"/> <small>Enter a name to identify the guest self-registration instance. This is visible only to administrators.</small>
Description:	<input style="width: 90%; height: 40px;" type="text"/> <small>Enter comments about this instance of guest self-registration. This is visible only to administrators.</small>
Enabled:	<input checked="" type="checkbox"/> Enable guest self-registration
* Register Page:	<input style="width: 90%;" type="text"/> <small>Enter the base page name for the guest registration page.</small>
Parent:	<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">(No parent - standalone) ▼</div> <small>Fields and text will use the parent's value unless overridden. Simply edit a field to override the parent value.</small>
Hotspot:	<input type="checkbox"/> Prepare self-registration for Hotspot Transactions <small>Check this box if registrants will be required to pay for access.</small>
Authentication:	<input type="checkbox"/> Require operator credentials prior to registering the guest <small>If checked, access to this registration page will require operator credentials. The sponsor's operator profile must have the Guest Manager > Create New Guest Account privilege.</small>

Save Changes

Save and Continue

Table 139: *Customize Guest Registration*

Field	Description
Name	(Required) The name of this self-registration page to identify it—for example, "Guest Self-Registration". This name can include spaces. This name is only displayed to administrators within ClearPass; it is not seen by the visitor.
Description	You may enter comments to further identify or describe this page. This description is only displayed within ClearPass.
Enabled	When creation of this page is complete, select this check box to make it available to use. Deselect the check box if the page should not be used. When self-registration is enabled, you can edit, delete, duplicate or go to the page after it is created.
Register Page	(Required) The base page name for the guest registration page. Do not use spaces. Allowed characters are letters, numbers, underscores, and hyphens. This name becomes part of the URL used to access the self provisioning page. For example, the default "guest_register" page is accessed using the URL guest_register.php . This name is only displayed to administrators within ClearPass; it is not seen by the visitor.
Parent	The page to use as a basis for this page's configuration. If a parent page is selected from this dropdown list, the parent page's values will be used for the new page's configuration. These values can be edited. If the (No parent - standalone) option is selected, all values must be configured.

Table 139: *Customize Guest Registration(Continued)*

Field	Description
Hotspot	Select this check box if the page will be used for Hotspot transactions. Requires the visitor to pay for access.
Authentication	Requires operator credentials to access the page. The sponsor's operator profile must include the Guest Manager > Create New Guest Account privilege.
Save Changes	Saves your changes and creates the self-registration page. This form closes and the self registration process diagram opens.
Save and Continue	Saves your changes and creates the self-registration page. The next section of the Customize Guest Registration form opens.

Configuring Basic Properties for Self-Registration

To edit the basic settings for a guest self-registration, click either the **Master Enable**, **User Database**, **Choose Skin**, or **Rename Page** links on the diagram at **Configuration > Pages > Guest Self-Registrations > Edit link**.

Figure 261 *Customize Guest Registration, Basic Properties*

Customize Guest Registration

Basic Properties
Options controlling basic operation of guest self-registration.

* Name:	<input type="text" value="Guest Self-Registration"/> <small>Enter a name to identify the guest self-registration instance. This is visible only to administrators.</small>
Description:	<div style="border: 1px solid #ccc; padding: 5px; min-height: 40px;">Default settings for visitor self-registration.</div> <small>Enter comments about this instance of guest self-registration. This is visible only to administrators.</small>
Enabled:	<input type="checkbox"/> Enable guest self-registration
* Register Page:	<input type="text" value="guest_register"/> <small>Enter the base page name for the guest registration page.</small>
* User Database:	ClearPass Policy Manager <small>Self provisioned guest accounts are created using this service handler.</small>
* Skin:	<input type="text" value="(Default)"/> <small>Choose the skin for the self-registration pages.</small>
Prevent CNA:	<input type="checkbox"/> Enable bypassing the Apple Captive Network Assistant <small>The Apple Captive Network Assistant (CNA) is the pop-up browser shown when joining a network that has a captive portal. Note that this option may not work with all vendors, depending on how the captive portal is implemented.</small>
Advertising:	<input type="checkbox"/> Enable Advertising Services content

Table 140: *Customize Guest Registration, Basic Properties*

Field	Description
Name	(Required) Enter a name for the page. This name is seen only by administrators in ClearPass Guest.
Description	Optional comments or notes about the page.
Enabled	Specifies whether the self-registration is enabled or disabled for use.
Register Page	(Required) Enter the guest registration page name (filename) that will appear in the URL-- for example, "register_page_name".

Table 140: Customize Guest Registration, Basic Properties(Continued)

Field	Description
Parent	To use the settings from a previously configured self-registration page, select an existing page name from the drop-down list. This is useful if you need to configure multiple registrations. You can override parent page values by editing field values yourself. To create a self-registration page with new values, select the Guest Self-Registration (guest_register) option from the Parent field drop-down menu.
HotSpot	If the standalone self -registration (No parent- standalone) option was selected in the Parent field, the Hotspot option is available. You can configure this setting so that registrants have to pay for access.
User Database	(Required) The service handler used to create the self-provisioned guest accounts.
Skin	(Required) Skin to use for the Web page. Options include: <ul style="list-style-type: none">● (Default)● Aruba ClearPass Skin● Blank Skin● ClearPass Guest Skin● Custom Skin 1● Custom Skin 2● Galleria Skin● Galleria Skin 2
Prevent CNA	Enables bypassing the Apple Captive Network Assistant (CNA). The CNA is the pop-up browser shown when joining a network that has a captive portal. This option might not work with all vendors; it is dependent on how the captive portal is implemented.
Advertising	To enable Advertising Services content on this registration page, select the check box in this row.

When you complete the **Basic Properties** area and click **Save and Continue**, the form expands to include the **Access Control** area, where you can specify access restrictions for the self-registration page.

Figure 262 *Customize Guest Registration, Access Control Area*

Access Control

Controls access to the registration page.

Authentication:	<input checked="" type="checkbox"/> Require operator credentials prior to registering the guest <small>If checked, access to this registration page will require operator credentials. The sponsor's operator profile must have the Guest Manager > Create New Guest Account privilege.</small>
Allowed Access:	<div style="border: 1px solid #ccc; height: 40px; width: 100%;"></div> <small>Enter the IP addresses and networks from which self-registration is permitted.</small>
Denied Access:	<div style="border: 1px solid #ccc; height: 40px; width: 100%;"></div> <small>Enter the IP addresses and networks that are denied self-registration access.</small>
* Deny Behavior:	<div style="border: 1px solid #ccc; padding: 2px;">Send HTTP 404 Not Found status ▾</div> <small>Select the response of the system to a request that is not permitted.</small>
Time Access:	<div style="border: 1px solid #ccc; height: 40px; width: 100%;"></div> <small>Enter a list of time ranges during which self-registration is enabled, one per line. For example, 'weekdays 7:00 to 19:00'. Leave blank to enable registration at all times.</small>

Save Changes
Save and Continue

Table 141: *Customize Guest Registration, Access Control*

Field	Description
Authentication	To require an operator to log in with their credentials before they can create a new guest account, select the Require operator credentials prior to registering guest check box in this row. The sponsor's operator profile must include the Guest Manager > Create New Guest Account privilege. If you choose this option, the authenticated page it produces for creating accounts is very simple, and does not include navigation or other links that would otherwise be available in the operator user interface.
Allowed Access	The IP addresses and networks from which access is allowed or denied (IPv4 and IPv6 are both supported). These access control lists determine whether a client is permitted to access this guest self-registration page. You can specify multiple IP addresses and networks, one per line, using the following syntax :
Denied Access	<ul style="list-style-type: none"> • 1.2.3.4 – IP address • 1.2.3.4/24 – IP address with network prefix length • 1.2.3.4/255.255.255.0 – IP address with explicit network mask

Table 141: *Customize Guest Registration, Access Control(Continued)*

Field	Description
Deny Behavior	(Required) The response shown to the user if their request is denied. Options in this drop-down list include: <ul style="list-style-type: none">• Send HTTP 404 Not Found status• Show Access Denied page• Show a blank page
Time Access	The Time Access field allows you to specify the days and times that self-registration is enabled. Times must be entered in 24-hour clock format. For example: <ul style="list-style-type: none">• Mondays, Wednesdays and Fridays, 8:00 to 17:00• Weekdays, 6:00 to 18:00• Weekends 10:00 to 22:00 and Thursday 11:00 to 13:00

Access Control Rules

The access control rules will be applied in order, from the most specific match to the least specific match.

Access control entries are more specific when they match fewer IP addresses. The most specific entry is a single IP address (for example, **1.2.3.4**), while the least specific entry is the match-all address of **0.0.0.0**.

As another example, the network address **192.168.2.0/24** is less specific than a smaller network such as **192.168.2.192/26**, which in turn is less specific than the IP address **192.168.2.201** (which may also be written as **192.168.2.201/32**).

To determine the result of the access control list, the most specific rule that matches the client's IP address is used. If the matching rule is in the **Denied Access** field, then the client will be denied access. If the matching rule is in the **Allowed Access** field, then the client will be permitted access.

If the **Allowed Access** field is empty, all access will be allowed, except to clients with an IP address that matches any of the entries in the **Denied Access** field. This behavior is equivalent to adding the entry **0.0.0.0** to the **Allowed Access** field.

If the **Denied Access** list is empty, only clients with an IP address that matches one of the entries in the **Allowed Access** list will be allowed access. This behavior is equivalent to adding the entry **0.0.0.0** to the Denied Access list.

Editing Registration Page Properties

To edit the properties of the registration page:

1. Go to **Configuration > Pages > Guest Self-Registration**.
2. Select an entry in the **Guest Self-Registration** list and click its **Edit** link. The **Customize Guest Registration** workflow diagram opens.
3. Click the **Register Page** link, or one of the **Title**, **Header**, or **Footer** fields for the **Register Page**. The **Register Page UI** area of the **Customize Guest Registration** form opens.

Figure 263 *The Customize Guest Registration Form, Register Page UI Area*

Customize Guest Registration

Register Page UI

Options controlling the appearance of the guest registration page.

Title:	<input style="width: 90%;" type="text" value="Guest Registration"/> <p style="font-size: x-small; color: #2e5496;">The title to display on the guest registration page.</p>
Header HTML:	<div style="border: 1px solid #ccc; padding: 5px; min-height: 60px;"> <pre style="font-family: monospace; font-size: x-small; margin: 0;"><p> Please complete the form below to gain access to the network. </p></pre> </div> <div style="text-align: right; margin-top: 5px;"> <input style="width: 100px;" type="button" value="Insert content item..."/> </div> <p style="font-size: x-small; color: #2e5496;">HTML template code displayed before the guest registration form.</p>
Footer HTML:	<div style="border: 1px solid #ccc; padding: 5px; min-height: 60px;"> <pre style="font-family: monospace; font-size: x-small; margin: 0;">{if \$gcsr_metadata.nas_login.enabled}<p> Already have an account? Sign In </p>{/if}</pre> </div> <div style="text-align: right; margin-top: 5px;"> <input style="width: 100px;" type="button" value="Insert content item..."/> </div> <p style="font-size: x-small; color: #2e5496;">HTML template code displayed after the guest registration form.</p>
Override Form:	<input type="checkbox"/> Do not include guest registration form contents <p style="font-size: x-small; color: #2e5496;">Select this option if you want to replace the HTML of the form.</p>

Save and Reload

Save Changes

Save and Continue

Table 142: *Customize Guest Registration Form, Register Page UI Area*

Field	Description
Title	Title to display on the guest registration page. Template code may be specified. See " Smarty Template Syntax " on page 700 for details on the template code that may be inserted.
Header HTML	HTML for the message that is displayed above the guest registration form. Template code may be specified. See " Smarty Template Syntax " on page 700 for details on the template code that may be inserted.
Footer HTML	HTML for the message that is displayed below the guest registration form. Template code may be specified. See " Smarty Template Syntax " on page 700 for details on the template code that may be inserted.
Override Form	If selected, lets you replace the HTML of the form and override the normal behavior of the registration page, which is to display the registration form between the header and footer templates.

Table 142: *Customize Guest Registration Form, Register Page UI Area(Continue)*

Field	Description
Save and Reload	Saves your changes, updates the self-registration page, and launches or refreshes a second browser window to show the effects of the changes.
Save Changes	Saves your changes and returns to the process diagram for self-registration.
Save and Continue	Saves your changes, updates the self-registration page, and continues to the next editor.

Editing the Default Self-Registration Form Settings

To edit the fields on the self-registration form, go to **Configuration > Pages > Guest Self-Registration**, click the registration page's row in the list, and then click its **Edit** link. On the **Customize Guest Registration** diagram, click the **Form** link for the **Register Page**. The **Customize Form Fields (guest_register)** list view opens.

Figure 264 *The Customize Form Fields List View*

Rank	Field	Type	Label	Description
10	sponsor_name	text	Sponsor's Name:	Name of the person sponsoring this account.
15	sponsor_email	text	Sponsor's Email:	Email of the person sponsoring this account.
20	visitor_name	text	Your Name:	Please enter your full name.
25	visitor_phone	text	Phone Number:	Please enter your contact phone number.
30	visitor_company	text	Company Name:	Please enter your company name.
40	email	text	Email Address:	Please enter your email address. This will become your username to log into the network.
50	start_time	datetime	Activation Time:	Scheduled date and time at which to enable the account. If blank, the account will be enabled immediately.
60	expire_after	hidden	Expires After:	Amount of time before this account will expire.
65	expire_time	datetime	Expiration Time:	Optional date and time at which the account will expire and be deleted. If blank, the account will not expire.
70	role_id	hidden	Account Role:	Role to assign to this account.
75	enabled	dropdown	Account Status:	Select an option for changing the status of this account.
80	random_password	static	Password:	
81	no_password	hidden	Password Change:	If set, prevents the user from changing their own password.
85	no_portal	hidden	Portal Login:	If set, prevents the user from logging into the guest service portal.
100	secret_question	text	Secret Question:	Enter your secret question. The answer will be required to reset your password.
101	secret_answer	text	Secret Answer:	Enter the answer to your secret question.
900	create_time	hidden	Created:	Time the account was created.
900	mac	hidden	MAC Address:	MAC address of the device.
901	remote_addr	hidden	Create Address:	This is your IP address.
902	http_user_agent	hidden	User Agent:	This is your browser's user agent string.
903	url			
904	ssid	hidden	ESSID:	
905	apname	hidden	AP Name:	
905	apgroup	hidden	AP Group:	
906	vcname	hidden	Virtual Controller:	
1000	auto_update_account	hidden		
99990	creator_accept_terms	checkbox	Confirm:	
99999	submit	submit	Register	

The default settings for this form are as follows:

- The **visitor_name** and **email** fields are enabled. The email address of the visitor will become their username for the network.
- The **expire_after** field is set to a value of 24 by default; this sets the default expiration time for a self-registered visitor account to be 1 day after it was created. This field is hidden by default on the register page.
- The **role_id** field is set to a value of 2 by default; this sets the default role for a self-registered visitor account to the built-in Guest role. This field is hidden by default on the register page.
- The **auto_update_account** field is set by default. This is to ensure that a visitor who registers again with the same email address has their existing account automatically updated.

Columns on the form editor:

Table 143: *Form Editor Columns*

Field	Description
Rank	Specifies the relative ordering of the fields when displaying the form. This list always shows the fields in order by rank.
Type	Controls what kind of user interface element is used to interact with the user.
Label	The label for this field as it is displayed on the form.
Description	The description for this field as it is displayed on the form.

To work with a form field, click its row in the list. The row expands to include configuration options:

Table 144: *Form Editor Options*

Field	Description
Edit	Make changes to an existing field. The Form Field Editor opens. Any changes made to the field using this editor will apply only to this field on this form.
Edit Base Field	Make changes to an existing field's definition. Any changes made to the field using this editor will apply to all forms that are using this field (except where the form field has already been modified to be different from the underlying field definition).
Remove	Removes the field from the form. To add a field back to the form after it has been removed, use the Insert Before or Insert After option and select it from the Field Name drop-down list in the Form Field Editor that opens.
Insert Before	Add a new field to the form. Clicking one of these links opens a blank form field editor and automatically sets the rank number of the new field.
Insert After	
Disable Field	Disables this field on the form. To enable it on the form again, click Enable Field .
Preview Form	Opens an example of the form so you can see what it looks like. This preview form can be submitted to test the field validation rules you have defined. If all fields are able to be validated, the form submit is successful and a summary of the values submitted is displayed. This allows you to verify any data conversion and formatting rules you have set up.

See also:

["Editing Self-Registration Pages" on page 347](#)

Editing Guest Receipt Page Properties

To edit the properties of the guest receipt page:

1. Go to **Configuration > Pages > Guest Self-Registration**
2. Select an entry in the **Guest Self-Registration** list and click its **Edit** link. The **Customize Guest Registration** workflow diagram opens.
3. Click the **Receipt Page** link or one of the **Title**, **Header**, or **Footer** fields for the **Receipt Page** to edit the properties of the receipt page. This page is shown to guests after their visitor account has been created.

Figure 265 *The Customize Guest Registration Form, Receipt Page UI Area*

Table 145: *Customize Guest Registration Form, Receipt Page UI Area*

Field	Description
Title	Title to display on the guest receipt page. Template code may be specified. See " Smarty Template Syntax " on page 700 for details on the template code that may be inserted.
Header HTML	HTML for the message that is displayed above the guest receipt. Template code may be specified. See " Smarty Template Syntax " on page 700 for details on the template code that may be inserted.
Footer HTML	HTML for the message that is displayed below the guest receipt. Template code may be specified. See " Smarty Template Syntax " on page 700 for details on the template code that may be inserted.

Table 145: *Customize Guest Registration Form, Receipt Page UI Area(Continue)*

Field	Description
Override Receipt	If selected, lets you replace the HTML of the guest receipt.
Save Changes	Saves your changes and returns to the process diagram for self-registration.
Save and Continue	Saves your changes, updates the self-registration page, and continues to the next editor (Receipt Actions).

Editing Receipt Actions

To edit the actions that are available after a visitor account has been created:


1. Go to **Configuration > Pages > Guest Self-Registration**.
2. Select an entry in the **Guest Self-Registration** list and click its **Edit** link. The **Customize Guest Registration** workflow diagram opens.
3. In the **Receipt Page** area of the diagram, click the  **Actions** link. The **Receipt Actions** part of the **Customize Guest Registration** form opens.

Figure 266 *The Actions Link on the Workflow Diagram*



Figure 267 The Customize Guest Registration Form, Receipt Actions Page, Download Area

Customize Guest Registration

Receipt Actions

Options for delivering a receipt to a self-registered guest.

Download

Enabled: Enable download of guest receipt

Rank: Rank ordering number for this receipt action.

Print Template: Print template to use to generate this receipt.

Filename: Template code to evaluate to generate the filename for the receipt.

Action Icon: Optional custom icon to use for this receipt action.

Action Text: Optional custom label to use for this receipt action.

Print

Enabled: Enable print window for guest receipts

Email Delivery

Enabled:

SMS Delivery

Enabled:

Sponsorship Confirmation

Enabled: Require sponsor confirmation prior to enabling the account

Download Pass

Options for downloading a guest receipt as a pass for use with Apple Passbook.

Not Available: Your pass configuration does not currently enable passes to be downloaded.
 Ensure that a valid Pass Certificate has been installed.

Editing Download Actions for Guest Receipt Delivery

The **Download** area on the **Receipt Actions** part of the **Customize Guest Registration** form lets you configure template and display options to deliver a receipt to the user as a downloadable file.

Table 146: Customize Guest Registration Form, Receipt Actions Page, Download Area

Field	Description
Enabled	If selected, enables download of guest receipts. The form expands to include configuration options for receipt downloads.
Rank	Specifies the relative ordering number for this receipt action.
Print	Specifies the print template to use to generate the receipt. Options include:

Table 146: *Customize Guest Registration Form, Receipt Actions Page, Download Area(Continued)*

Field	Description
Template	<ul style="list-style-type: none"> ● Account List ● Certificate Expiry ● Download Receipt ● Guest Account Expiry ● GuestManager Receipt ● One account per page ● SMS Receipt ● SMS Sponsor Confirmation Alert ● Sponsor Device Provisioning ● Sponsorship Confirmation ● Two-column scratch cards
Filename	The template code to evaluate to generate the filename for the receipt.
Action Icon	Specifies a custom icon to use for the download receipt action. Image files that have been uploaded to Content Manager will be included in this drop-down list.
Action Text	Label to use for the download receipt action.

Editing Print Actions for Guest Receipt Delivery

The **Print** area on the **Receipt Actions** part of the **Customize Guest Registration** form lets you configure options for displaying the receipt in a printable window in the visitor's browser.

Figure 268 *The Customize Guest Registration Form, Receipt Actions Page, Print Area*

The screenshot shows a configuration panel titled "Print" with a printer icon. It contains the following fields:

- Enabled:** A checkbox labeled "Enable print window for guest receipts" which is checked.
- Rank:** A text input field containing the number "20". Below it is the text "Rank ordering number for this receipt action."
- Print Template:** A dropdown menu showing "Download Receipt". Below it is the text "Print template to use to generate this receipt."
- Action Icon:** A dropdown menu showing "(Default)". Below it is the text "Optional custom icon to use for this receipt action."
- Action Text:** An empty text input field. Below it is the text "Optional custom label to use for this receipt action."

Table 147: *Customize Guest Registration Form, Receipt Actions Page, Print Area*

Field	Description
Enabled	If selected, enables the print window for guest receipts. The form expands to include configuration options for printer actions.
Rank	Specifies the relative ordering number for this receipt action.
Print Template	Specifies the print template to use to generate the receipt. Options include: <ul style="list-style-type: none"> ● Account List

Table 147: *Customize Guest Registration Form, Receipt Actions Page, Print Area(Continued)*

Field	Description
	<ul style="list-style-type: none"> • Certificate Expiry • Download Receipt • Guest Account Expiry • GuestManager Receipt • One account per page • SMS Receipt • SMS Sponsor Confirmation Alert • Sponsor Device Provisioning • Sponsorship Confirmation • Two-column scratch cards
Action Icon	Specifies a custom icon to use for the printer receipt action. Image files that have been uploaded to Content Manager will be included in this drop-down list.
Action Text	Label to use for the printer receipt action.

Editing Email Delivery of Guest Receipts

The **Email Delivery** options available for the receipt page actions allow you to specify the email subject line, the print template and email format, and other fields relevant to email delivery.

Figure 269 *The Customize Guest Registration Form, Receipt Actions Area, Email Delivery Options*

Email Delivery

Enabled:	<input type="text" value="Always auto-send guest receipts by email"/>
* Email Field:	<input type="text" value="(Use Default: email)"/> <small>The field containing the visitor account's email address.</small>
Subject Line:	<input type="text"/> <small>Template specifying the subject line for emailed visitor account receipts. Leave blank to use the default (Visitor account receipt for {\$email})</small>
* Email Receipt:	<input type="text" value="(Use Default: GuestManager Receipt)"/> <small>The plain text or HTML print template to use when generating an email receipt.</small>
* Email Skin:	<input type="text" value="(Use Default: Use the default skin)"/> <small>The format in which to send email receipts.</small>
* Send Copies:	<input type="text" value="(Use Default: Use 'Bcc:' if sending to a visitor)"/> <small>Specify when to send visitor account receipts to the recipients in the Copies To list.</small>
Copies To:	<input type="text" value="default"/> <small>An optional list of email addresses to which copies of visitor account receipts will be sent. Enter '_admin' to have the email sent to the sponsor's email address.</small>
Reply-To:	<input checked="" type="checkbox"/> Allow the reply-to address to be overridden <small>If checked, the reply-to address will be overridden by the sponsor_email field. Leave unchecked to use the global from address.</small>
Override From:	<input type="checkbox"/> Override the from address instead of using reply-to <small>If checked, the from address will be overridden in lieu of the reply-to value above. Note, this feature may require configuration on your mail server to allow the override.</small>

Table 148: *Customize Guest Registration Form, Receipt Actions Area, Email Delivery Options*

Field	Description
Enabled	<p>Specifies options for disabling or configuring the sending of guest receipts by email. Options include:</p> <ul style="list-style-type: none"> ● Disable sending guest receipts by email — Email receipts are never sent for a guest registration. ● Always auto-send guest receipts by email — An email receipt is always generated using the selected options, and will be sent to the visitor's email address. ● Auto-send guest receipts by email with a special field set — If the auto-send field available for this delivery option is set to a non-empty string or a non-zero value, an email receipt will be generated and sent to the visitor's email address. The auto-send field can be used to create an "opt-in" facility for guests. Use a check box for the auto_send_smtp field and add it to the create_user form, or a guest self-registration instance, and email receipts will be sent to the visitor only if the check box has been selected. ● Display a link enabling a guest receipt via email — A link is displayed on the receipt page; if the visitor clicks this link, an email receipt will be generated and sent to the visitor's email address. ● Send an email to a list of fixed addresses — An email receipt is always generated using the selected options, and will be sent only to the list of email addresses specified in the Copies To field.
Auto-Send Field	(Required) Specifies the field that, if it contains a non-empty string or non-zero value, will cause an account receipt email to be automatically sent upon creation of a visitor account.
Email Field	(Required) Specifies the field containing the visitor account's email address.
Subject Line	Template specifying the subject line for emailed visitor account receipts. To use the default (Visitor account receipt for {\$email}), leave this field empty.
Email Receipt	<p>(Required) Specifies the plain text or HTML print template to use when generating an email receipt. Options include:</p> <ul style="list-style-type: none"> ● (Use Default: GuestManager Receipt) ● Account List ● Certificate Expiry ● Download Receipt ● Guest Account Expiry ● GuestManager Receipt ● One account per page ● SMS Receipt ● SMS Sponsor Confirmation Alert ● Sponsor Device Provisioning ● Sponsorship Confirmation ● Two-column scratch cards
Email Skin	<p>(Required) Specifies the format in which to send email receipts. Options include:</p> <ul style="list-style-type: none"> ● (Use Default: Use the default skin) ● No skin — Plain text only ● No skin — HTML only ● No skin — Native receipt format ● Use the default skin ● Aruba ClearPass skin ● Blank skin ● ClearPass Guest skin ● Custom Skin 1

Table 148: *Customize Guest Registration Form, Receipt Actions Area, Email Delivery Options(Continued)*

Field	Description
	<ul style="list-style-type: none">● Custom Skin 2● Galleria Skin 1● Galleria Skin 2
Send Copies	(Required) Specifies when to send visitor account receipts to the recipients in the Copies To list. Options include; <ul style="list-style-type: none">● (Use Default: Use "Bcc:" if sending to a visitor)● Do not send copies● Always send using "cc:"● Always send using "Bcc:"● Use "cc:" if sending to a visitor● Use "Bcc:" if sending to a visitor
Copies To	List of email addresses to which copies of visitor account receipts will be sent. To have the email sent to the sponsor's email address, enter "_admin".
Reply-To	If selected, the reply-to address will be overridden by the sponsor_email field. To use the global From Address, leave this check box unselected.
Override From	If selected, the From Address will be overridden instead of using the reply-to value specified above. To allow this override, this feature might require configuration on your mail server.
Rank	Specifies the relative ordering number for this receipt action.
Action Icon	Specifies a custom icon to use for the email delivery receipt action. Image files that have been uploaded to Content Manager will be included in this drop-down list.
Action Text	Label to use for the email delivery receipt action.

Editing SMS Delivery of Guest Receipts

The **SMS Delivery** options available for the receipt page actions allow you to specify the field containing the visitor's phone number, the service provider, and the SMS receipt template.

Figure 270 *The Customize Guest Registration Form, Receipt Actions Area, SMS Delivery Options*

SMS Delivery	
Enabled:	Display a link enabling a guest receipt via SMS <input type="button" value="v"/>
Phone Number Field:	(Use Default) <input type="button" value="v"/> The field containing the visitor's phone number.
Service Provider:	(Use Default) <input type="button" value="v"/> The service provider to use when sending SMS messages.
SMS Receipt:	(Use Default) <input type="button" value="v"/> The plain-text format print template to use when generating an SMS receipt.
Rank:	40 Rank ordering number for this receipt action.
Action Icon:	(Default) <input type="button" value="v"/> Optional custom icon to use for this receipt action.
Action Text:	<input type="text"/> Optional custom label to use for this receipt action.

Table 149: *Customize Guest Registration Form, Receipt Actions Area, SMS Delivery Options*

Field	Description
Enabled	Specifies options for disabling or configuring SMS delivery. Options include: <ul style="list-style-type: none"> • Disable sending guest receipts by SMS — SMS receipts are never sent for a guest registration. • Always auto-send guest receipts by SMS — An SMS receipt is always generated using the selected options, and will be sent to the visitor's phone number. • Auto-send guest receipts by SMS with a special field set — If the Auto-Send Field is set to a non-empty string or a non-zero value, an SMS receipt will be generated and sent to the visitor's phone number. The auto-send field can be used to create an "opt-in" facility for guests. Use a check box for the auto_send_sms field and add it to the create_user form, or a guest self-registration instance, and SMS messages will be sent to the specified phone number only if the check box has been selected. • Display a link enabling a guest receipt via SMS — A link is displayed on the receipt page; if the visitor clicks this link, an SMS receipt will be generated and sent to the visitor's phone number. Only one SMS receipt per guest registration can be sent in this way.
Auto-Send Field	Specifies the field that, if it contains a non-empty string or non-zero value, will cause an account receipt SMS to be automatically sent upon creation of a visitor account.
Phone Number Field	Specifies the field to use for the visitor's phone number.
Service Provider	Specifies the service provider to use when sending SMS messages.
SMS Receipt	Specifies the plain text format print template to use when generating an SMS receipt. Options include: <ul style="list-style-type: none"> • (Use Default: SMS Receipt)

Table 149: *Customize Guest Registration Form, Receipt Actions Area, SMS Delivery Options(Continued)*

Field	Description
	<ul style="list-style-type: none">• Download Receipt• SMS Receipt• SMS Sponsor Confirmation Alert
Rank	Specifies the relative ordering number for this receipt action.
Action Icon	Specifies a custom icon to use for the SMS delivery receipt action. Image files that have been uploaded to Content Manager will be included in this drop-down list.
Action Text	Label to use for the SMS delivery receipt action.

Enabling Downloading Passes

The **Download Pass** area of the **Receipt Actions** form provides options for downloading a guest receipt as a pass to use with Apple Passbook.

- If a pass certificate is not installed, an error is displayed. For information on digital passes and installing pass certificates, see "[Digital Passes](#)" on page 420.
- If a pass certificate is installed, select the appropriate pass template.

When your changes are complete on the **Receipt Actions** part of the **Customize Guest Registration** form, click **Save Changes**.

Editing Sponsor Confirmation

You can allow the sponsor to choose the role for the guest account at the time the sponsor approves the self-registered account. When a guest submits the registration form, the sponsor receives an email notification. To confirm the guest's access and change the guest's role, the sponsor clicks a link in the email and is redirected to the **Guest Registration Confirmation** form.

To enable role selection by the sponsor and configure the email notification:

1. Go to **Configuration > Pages > Guest Self-Registrations**.
2. Select an entry in the **Guest Self-Registration** list and click its **Edit** link. The **Customize Guest Registration** workflow diagram opens.
3. In the **Receipt Page** area of the diagram, click the **Sponsor Confirmation** link. The **Sponsorship Confirmation** part of the **Customize Guest Registration** form opens.

Figure 271 *The Sponsor Confirmation Link on the Workflow Diagram*

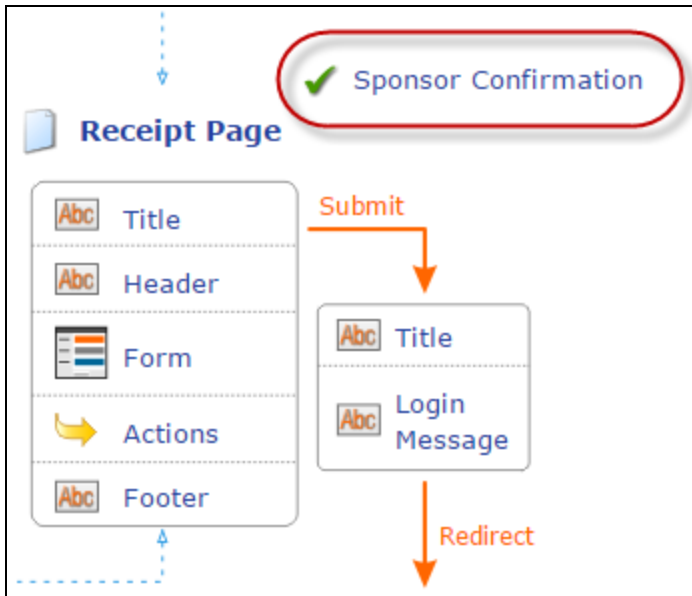


Figure 272 The Customize Guest Registration Form, Sponsorship Confirmation Page, Email Delivery Area

Customize Guest Registration	
Sponsorship Confirmation	
Enabled:	<input checked="" type="checkbox"/> Require sponsor confirmation prior to enabling the account
Authentication:	<input checked="" type="checkbox"/> Require sponsors to provide credentials prior to sponsoring If checked, the sponsor will need to successfully authenticate prior to approving the request. The sponsor's operator profile must have the Guest Manager > Remove Accounts privilege.
Email Delivery	
* Email Field:	(Use Default: sponsor_email) ▼ The field containing the sponsor's email address.
Email Confirmation:	Sponsorship Confirmation ▼ The plain text or HTML print template to send to the sponsor.
* Email Skin:	(Use Default: Use the default skin) ▼ The format in which to send email receipts.
* Send Copies:	Do not send copies ▼ Specify when to send visitor account receipts to the recipients in the Copies To list.
Reply-To:	<input type="checkbox"/> Allow the reply-to address to be overridden If checked, the reply-to address will be overridden by the guest's email field.
SMS Delivery	
SMS:	<input type="checkbox"/> Send an SMS to the sponsor notifying them of the request
UI Overrides	
UI Overrides:	<input type="checkbox"/> Display fields to override UI text and labels
Account Overrides	
Role Override:	(No override) ▼ Change the guest's role upon a successful confirmation from the sponsor. Note that this does not generate a change of authorization for any active session the guest has.
Extend Expiration:	<input type="text"/> Extend the account's expiration time. Leave blank to use the original expiration time. Enter a single value to automatically add the time. Enter a list of values, one per line, to display an option to the sponsor ("value Label"). Example values: +12h, +30d, or +1y.
<input type="button" value="Save Changes"/> <input type="button" value="Save and Continue"/>	

Editing Email Delivery Options for Sponsorship Confirmation

The **Email Delivery** area on the **Sponsorship Confirmation** part of the **Customize Guest Registration** form lets you configure options for the notification email that is sent to the sponsor, such as sponsor authentication and the print template and email format.

Table 150: Customize Guest Registration Form, Sponsorship Confirmation Page, Email Delivery Area

Field	Description
Enabled	If selected, sponsorship confirmation is required before the guest account can be enabled. The form expands to include configuration options for sponsorship confirmation.
Authentication	if selected, sponsors must provide credentials and be successfully authenticated before they can approve the guest account request. The sponsor's operator profile must include the Guest Manager > Remove Accounts privilege.
Email Field	(Required) Specifies the field to use for the sponsor's email address.
Email Confirmation	Specifies the print template to use to generate the email to the sponsor. Options include: <ul style="list-style-type: none">● Account List● Certificate Expiry● Download Receipt● Guest Account Expiry● GuestManager Receipt● One account per page● SMS Receipt● SMS Sponsor Confirmation Alert● Sponsor Device Provisioning● Sponsorship Confirmation● Two-column scratch cards
Email Skin	(Required) Specifies the format in which to send the email to the sponsor. Options include: <ul style="list-style-type: none">● (Use Default: Use the default skin)● No skin — Plain text only● No skin — HTML only● No skin — Native receipt format● Use the default skin● Aruba ClearPass skin● Blank skin● ClearPass Guest skin● Custom Skin 1● Custom Skin 2● Galleria Skin 1● Galleria Skin 2
Send Copies	(Required) Specifies when to send copies of the sponsorship email to the recipients in the Copies To list. Options include; <ul style="list-style-type: none">● Do not send copies● Always send using "cc:"● Always send using "Bcc:"
Copies To	List of email addresses to which copies of the sponsorship email will be sent. To have the email sent to the sponsor's email address, enter "_admin".
Reply-To	If selected, the reply-to address will be overridden by the guest's email field.
Override From	If selected, the From Address will be overridden instead of using the reply-to value specified above. To allow this override, this feature might require configuration on your mail server.

Editing SMS Delivery Options for Sponsorship Confirmation

The **SMS Delivery** options available for sponsorship confirmation allow you to specify the field containing the visitor's phone number, the service provider, and the SMS receipt template.

Figure 273 *The Customize Guest Registration Form, Sponsorship Confirmation Page, SMS Delivery Area*

SMS Delivery	
SMS:	<input checked="" type="checkbox"/> Send an SMS to the sponsor notifying them of the request
Phone Number Field:	(Use Default: sponsor_phone) ▼ The field containing the sponsor's phone number.
Service Provider:	(Use Default) ▼ The service provider to use when sending SMS messages.
SMS Receipt:	(Use Default: SMS Sponsor Confirmation Alert) ▼ The plain-text format print template to use when generating an SMS receipt.

Table 151: *Customize Guest Registration Form, Sponsorship Confirmation Page, SMS Delivery Area*

Field	Description
SMS	If selected, an SMS message will be sent to the sponsor notifying them of the guest account request. The form expands to include configuration options for SMS delivery.
Phone Number Field	Specifies the field to use for the sponsor's phone number.
Service Provider	Specifies the service provider to use when sending SMS messages.
SMS Receipt	Specifies the plain text format print template to use when generating an SMS receipt. Options include: <ul style="list-style-type: none"> • (Use Default: SMS Receipt) • Download Receipt • SMS Receipt • SMS Sponsor Confirmation Alert

Editing UI Override Options for Sponsorship Confirmation

The **UI Overrides** area on the **Sponsorship Confirmation** part of the **Customize Guest Registration** form lets you customize the user interface text and labels, overriding the default values.

Figure 274 *The Customize Guest Registration Form, Sponsorship Confirmation Page, UI Overrides Area*

UI Overrides

UI Overrides: Display fields to override UI text and labels

Subject Line:
 Template specifying the subject line for emailed visitor account receipts. Leave blank to use the default (Wireless access request from: {\$email})

Confirmation Title:
 Override the default page title (Guest Registration Confirmation).

Header HTML:

```
<p>
{if !$confirm_success}
A guest has requested your confirmation for guest access
{else}
{/if}
</p>
```


 HTML template code displayed before the login form.

Form Override: Override the form

Confirm Button:
 Override the default confirm button (Confirm).

Reject Button:
 Override the default reject button (Reject).

Footer HTML:

 HTML template code displayed after the confirmation form.

Registration Receipt:

```
{if $guest_receipt.deleted}
{nwa_icontext type="error"}Your registration request has
been rejected.{/nwa_icontext}
{elseif $user.register_token && !$user.enabled}<p>
{nwa_script src=core}
<script>
addLoadEvent(function()
{ldelim}Nwa_IdHide("guest_register_receipt_actions");
{rdelim});
</script>
Your account is currently awaiting confirmation. This page
will refresh every 30 seconds.
<meta http-equiv="refresh" content="30; url=
```


 HTML template code displayed on the guest receipt prior to confirmation.

Table 152: *Customize Guest Registration Form, Sponsorship Confirmation Page, UI Overrides Area*

Field	Description
UI Overrides	If selected, lets you customize the user interface text and labels. The form expands to include configuration options to override default values.
Subject Line	Template specifying the subject line for emailed guest account receipts. To use the default (Wireless access request from: {\$email}), leave this field empty.
Confirmation Title	Title for the confirmation page. To use the default title (Guest Registration Confirmation), leave this field empty.

Table 152: *Customize Guest Registration Form, Sponsorship Confirmation Page, UI Overrides Area(Continued)*

Field	Description
Header HTML	HTML for the message that is displayed before the login form. Template code may be specified. See " Smarty Template Syntax " on page 700 for details on the template code that may be inserted. You can use the drop-down list to add images or links.
Form Override	If selected, lets you override the form. The Confirm Button and Reject Button configuration options are removed from this form.
Confirm Button	Label for the Confirm button. To use the default (Confirm), leave this field empty.
Reject Button	Label for the Reject button. To use the default (Reject), leave this field empty.
Footer HTML	HTML for the message that is displayed after the confirmation form. Template code may be specified. See " Smarty Template Syntax " on page 700 for details on the template code that may be inserted. You can use the drop-down list to add images or links.
Registration Receipt	HTML for the message that is displayed on the guest receipt prior to confirmation. Template code may be specified. See " Smarty Template Syntax " on page 700 for details on the template code that may be inserted. You can use the drop-down list to add images or links.

Editing Account Override Options for Sponsorship Confirmation

The **Account Overrides** area on the **Sponsorship Confirmation** part of the **Customize Guest Registration** form provides options for changing the guest's role, account expiration, and account state.

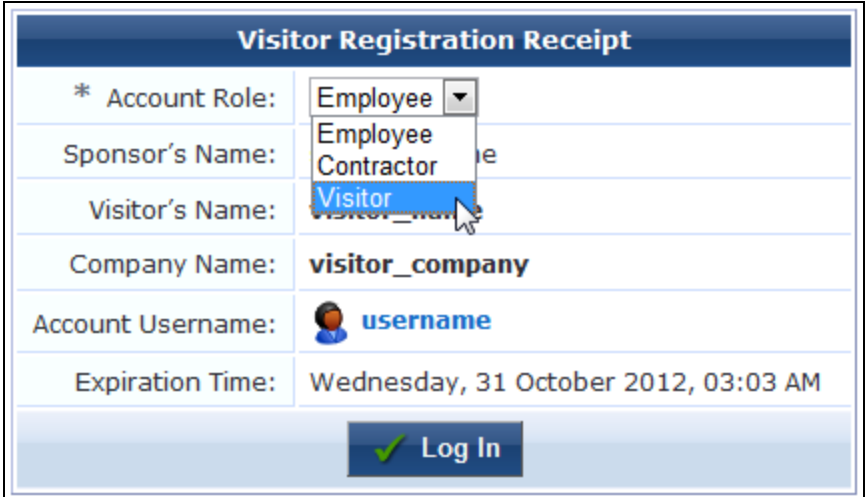
Figure 275 *The Customize Guest Registration Form, Sponsorship Confirmation Page, Account Overrides Area*

Account Overrides

Role Override:
 Change the guest's role upon a successful confirmation from the sponsor.
 An Enforcement Policy containing the role name must exist for sessions to be updated automatically.

Extend Expiration:
 Extend the account's expiration time. Leave blank to use the original expiration time.
 Enter a single value to automatically add the time.
 Enter a list of values, one per line, to display an option to the sponsor ("value | Label").
 Example values: +12h, +30d, or +1y.

Table 153: *Customize Guest Registration Form, Sponsorship Confirmation Page, Account Overrides Area*

Field	Description
Role Override	<p>Specifies the role assigned to the guest when the sponsor's confirmation is successful, or lets the sponsor assign the role during confirmation. Options include:</p> <ul style="list-style-type: none"> • (No override) • (Prompt) • [Contractor] • [Employee] • [Guest] <p>If "Prompt" is selected, the sponsor chooses the role for the guest from the Account Role drop-down list of the guest registration receipt.</p>  <p>The screenshot shows a form titled "Visitor Registration Receipt" with the following fields: <ul style="list-style-type: none"> * Account Role: A dropdown menu currently showing "Employee" with a list of options: "Employee", "Contractor", and "Visitor". Sponsor's Name: A text input field. Visitor's Name: A text input field. Company Name: A text input field containing "visitor_company". Account Username: A text input field containing "username" with a user icon. Expiration Time: A text input field containing "Wednesday, 31 October 2012, 03:03 AM". A "Log In" button with a green checkmark is at the bottom. </p> <p>For more information, see "Changing a Guest Account Role" on page 372.</p>
Extend Expiration	<p>To extend the guest account's expiration time, you may enter a value in this field. To use the original expiration time, leave this field empty.</p> <p>To automatically add time, enter a single value.</p> <p>To display an option to the sponsor, enter a list of values, one per line ("Value Label").</p> <p>Example values: +12h, +30d, or +1y.</p>
Account State	<p>Specifies the state to assign to the account upon confirmation. Options include:</p> <ul style="list-style-type: none"> • Enabled — Account will have network access prior to confirmation • Disabled — Account will remain disabled until confirmation
Save Changes	Saves your changes and returns to the process diagram for self-registration.
Save and Continue	Saves your changes, updates the self-registration page, and continues to the next editor (Login Page).

Changing a Guest Account Role

If you are changing a guest account's role, you must also configure change of authorization (CoA) requests to handle the change correctly. This ensures that the appropriate CoA requests are triggered for active sessions. The following steps are performed in ClearPass Policy Manager:

1. Go to **Policy Manager > Configuration > Enforcement > Profiles > Add**.
2. On the **Profile** tab, open the the **Template** drop-down list and select **RADIUS Change of Authorization (CoA)**.

3. In the **Name** field, the name you enter for the profile must include the exact role name in square brackets. For example, for the role “[Guest]”, the profile name might be “My Company [Guest] CoA”.
4. On the **Attributes** tab, open the **Select RADIUS CoA Template** drop-down list and select **Aruba - Change-User-Role**.
5. Click a row and add an attribute with the **Type** as **Radius:IETF**. For the **Value** enter the role name, but without the square brackets this time.

Editing Login Page Properties

The login page is displayed if automatic guest login is enabled and a guest clicks the **Submit** button from the receipt page to log in.

To edit the properties of the login page:

1. Go to **Configuration > Pages > Guest Self-Registrations**. Click to expand the registration page's row in the form, and then click its **Edit** link. The **Customize Guest Self-Registration** diagram opens.
2. Under the **Receipt Page > Submit** area of the diagram, click either the **Title** or **Login Message** link to edit the properties of the login page.

Figure 276 *The Login Page Links on the Workflow Diagram*

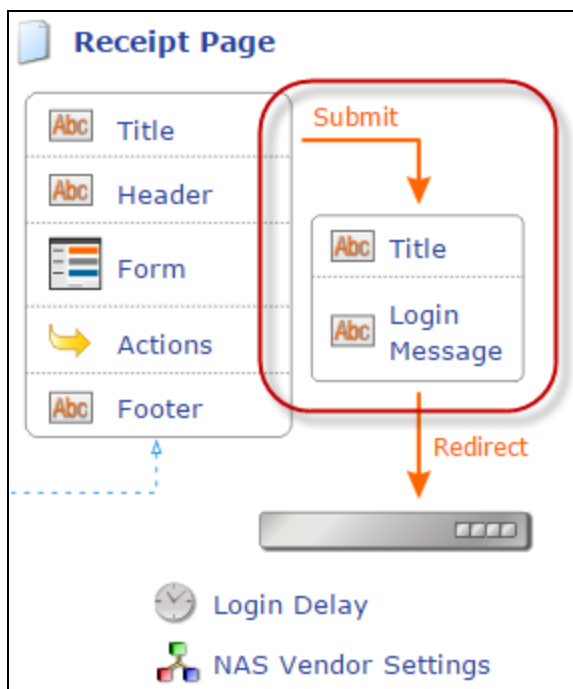


Figure 277 *The Customize Guest Registration Form, Login Form Page, Enabled/Disabled Area*

Customize Guest Registration					
Enabled:	Disabled				
Health Check:	<input type="checkbox"/> Require a successful OnGuard health check If selected, the guest will be required to pass a health check prior to accessing the network.				
Authentication Providers:	<div style="border: 1px solid #ccc; padding: 5px;"> <p> Add new authentication provider</p> <table border="1"> <thead> <tr> <th>Provider</th> <th>Client ID</th> </tr> </thead> <tbody> <tr> <td colspan="2" style="text-align: center;"> There are no authentication providers defined. </td> </tr> </tbody> </table> </div>	Provider	Client ID	There are no authentication providers defined.	
Provider	Client ID				
There are no authentication providers defined.					
<input type="button" value="Save Changes"/> <input type="button" value="Save and Continue"/>					

Table 154: *Customize Guest Registration Form, Login Form Page, Enabled/Disabled Area*

Field	Description
Enabled	Specifies the login or device enrollment method. Options include: <ul style="list-style-type: none">• Disabled• Enable guest login to a Network Access Server — Allows NAS login. The form expands to include configuration options. See "Configuring the Login Form Part of the Page" on page 374 and "Configuring the Login Message Part of the Page" on page 377.• Enable Onboard device enrollment — Allows simultaneous self-registration and Onboard device enrollment. The form expands to include configuration options. See "Configuring Self-Registration with Onboard Device Enrollment" on page 378
Health Check	If selected, the guest must pass a health check prior to accessing the network.
Authentication Providers	Specifies an authentication provider. All authentication providers that have been configured are included in this list. To add a new authentication provider, click the Add new authentication provider link. The row expands to include the Properties form, where you can select and configure a social network provider for authentication.
Save Changes	Saves your changes and returns to the process diagram for self-registration.
Save and Continue	Saves your changes, updates the self-registration page, and continues to the next editor (Self-Service Portal).

Configuring the Login Form Part of the Page

The login page is also a separate page that can be accessed by guests using the login page URL. The login page URL has the same base name as the registration page, but with **login** appended. To determine the login page URL for a guest self-registration page, first ensure that the **Enable guest login to a Network Access Server** option is checked, and then click the [Launch network login](#) link from the self-registration process diagram.

The login page consists of two separate parts: the login form page, and a login message page.

The options available under the **Login Form** heading may be used to customize the login page.

Login Form and Post-Authentication Areas

Figure 278 *The Customize Guest Registration Form, Login Form and Post-Authentication Areas*

Customize Guest Registration													
Enabled:	Enable guest login to a Network Access Server ▼												
Login Form Options controlling the appearance of the NAS login form.													
Custom Form:	<input type="checkbox"/> Provide a custom login form If selected, you must supply your own HTML login form in the Header or Footer HTML areas.												
Custom Labels:	<input type="checkbox"/> Override the default labels and error messages If selected, you will be able to alter labels and error messages for the current login form.												
Pre-Auth Check:	<input checked="" type="checkbox"/> Perform a local authentication check If checked, the username and password will be checked locally before proceeding to the NAS authentication. This option should not be selected if an external authentication server is in use.												
Username Authentication:	<input type="checkbox"/> Only require a username for authentication If set, the password field will not be displayed. Only accounts with the Username Authentication flag set on their account can login.												
Terms:	<input checked="" type="checkbox"/> Require a Terms and Conditions confirmation If checked, the user will be forced to accept a Terms and Conditions checkbox.												
Post-Authentication Actions to perform after a successful pre-authentication.													
Health Check:	<input type="checkbox"/> Require a successful OnGuard health check If selected, the guest will be required to pass a health check prior to accessing the network.												
Update Endpoint:	<input checked="" type="checkbox"/> Mark the user's MAC address as a known endpoint If selected, the endpoint's attributes will also be updated with other details from the user account.												
Advanced:	<input checked="" type="checkbox"/> Customize attributes stored with the endpoint												
Endpoint Attributes:	<table border="1"> <tbody> <tr><td>username</td><td> </td><td>Username</td></tr> <tr><td>visitor_name</td><td> </td><td>Visitor Name</td></tr> <tr><td>cn</td><td> </td><td>Visitor Name</td></tr> <tr><td>visitor_phone</td><td> </td><td>Visitor Phone</td></tr> </tbody> </table> <p>List of name value pairs to pass along. user_field Endpoint Attribute.</p>	username		Username	visitor_name		Visitor Name	cn		Visitor Name	visitor_phone		Visitor Phone
username		Username											
visitor_name		Visitor Name											
cn		Visitor Name											
visitor_phone		Visitor Phone											

Table 155: *The Customize Guest Self-Registration Form, Login Form and Post-Authentication*

Field	Description
Custom Form	Indicates you will provide a custom login form. If selected, you must supply your own HTML login form for the header or footer HTML areas.
Custom Labels	Enables altering the default labels and error messages.
Username Label	Label that appears on the form for the username field. Leave blank to use the default, (Username:).
Password Label	Label that appears on the form for the password field. Leave blank to use the default (Password:).
Pre-Auth Check	The username and password will be checked locally before proceeding to the NAS authentication. Do not select this option if an external authentication server is used.
Pre-Auth Error	Customized label text to display if username and password lookup fails. Leave blank to use the default (Invalid username or password).
Username Authentication	Allows the user to log in with only a username. The Password field will not be displayed. Only accounts with the Username Authentication flag set can log in.
Terms	Requires the user mark a check box to accept a Terms and Conditions agreement.

Field	Description
Terms Label	Label that appears on the form for the terms check box. Leave blank to use the default (Terms:).
Terms Text	Enter the HTML code containing your terms and conditions. Leave blank to use the default, (I accept the terms of use)
Terms Layout	Layout for the terms and conditions text—either above or below the Terms check box.
Terms Error	Text to display if the terms are not accepted. Leave blank to use the default (In order to log in, you must accept the terms and conditions.).
Log In Label	Label that appears on the form for the login button. Leave blank to use the default (Log In).
Health Check	Requires the visitor to pass a health check before they can access the network. The health check is done automatically through the OnGuard Dissolvable Agent.
Header HTML	The HTML content to display above the health check text. You can use the drop-down list to add images or other content items.
Footer HTML	The HTML content to display below the health check text. You can use the drop-down list to add images or other content items.
Update Endpoint	Marks the user's MAC address as a known endpoint, and updates the endpoint's attributes with other details from the user account (for example, the SSID, AP, and MAC address). If this check box is selected, the form expands to include the Advanced field.
Advanced	Lets you specify custom attributes to store in the endpoint. If this check box is selected, the form expands to include the Endpoint Attributes field.
Endpoint Attributes	Enter the list of name-value pairs to pass as custom attributes. Follow the format user_field Endpoint Attribute . Examples are shown.

Login UI Area

The login form page contains a form prompting for the guest's username and password. The title, header, and footer of this page can be customized. If the **Provide a custom login form** option is selected, then the form must also be provided in either the Header HTML or Footer HTML sections.

Figure 279 *The Customize Guest Registration Form, Login UI Area*

Login UI
Options controlling the appearance of the NAS login page.

Login Page Title:	<input style="width: 95%;" type="text" value="Network Login"/> <small>The page title to display on the login page.</small>
Header HTML:	<pre style="font-family: monospace; font-size: 0.9em;">{nwa_cookiecheck} {if \$errmsg}{nwa_icontext type=error}{\$errmsg escape} {/nwa_icontext}{/if} {nwa_text id=7980}<p> Please log in to the network using your username and password. </p>{/nwa_text}</pre> <div style="text-align: right; margin-top: 5px;"> <input style="width: 150px;" type="text" value="Insert content item..."/> </div> <small>HTML template code displayed before the login form.</small>
Footer HTML:	<pre style="font-family: monospace; font-size: 0.9em;"><p> Need an account? Click Here </p></pre> <div style="text-align: right; margin-top: 5px;"> <input style="width: 150px;" type="text" value="Insert content item..."/> </div> <small>HTML template code displayed after the login form.</small>

Table 156: *The Customize Guest Self-Registration Form, Login UI Section*

Field	Description
Login Page Title	The title that will be displayed on the NAS login page.
Header HTML	The HTML content to display above the NAS login form. You can use the drop-down lists to add images or other content items.
Footer HTML	The HTML content to display below the NAS login form. You can use the drop-down lists to add images or other content items.

Click the **Save Changes** button to return to the process diagram for self-registration.

Configuring the Login Message Part of the Page

The login message page is displayed after the login form has been submitted, while the guest is being redirected to the NAS for login. The title and message displayed on this page can be customized.

Figure 280 *The Customize Guest Registration Form, Login Page Area, Title and Login Message Fields*

Title:	<input style="width: 95%;" type="text" value="Network Login In Progress..."/> <small>The page title to display while logging into the NAS.</small>
Login Message:	<div style="border: 1px solid #ccc; padding: 5px; min-height: 40px;"> <pre style="font-family: monospace; font-size: 0.9em; margin: 0;">Please wait while you are logged into the network...</pre> </div> <div style="text-align: right; margin-top: 5px;"> <input style="width: 150px;" type="text" value="Insert content item..."/> </div> <small>HTML template code displayed while the login attempt is in progress.</small>

The login delay can be set. This is the time period, in seconds, for which the login message page is displayed.

Figure 281 *The Customize Guest Registration Form, Automatic Login Area, Login Delay Option*

Automatic Login
Options controlling automatically logging in from the receipt form.

* Login Delay: seconds
The time in seconds to delay while displaying the login message.

[Save Changes](#) [Save and Continue](#)

Click the **Save Changes** button to return to the process diagram for self-registration.

Configuring Self-Registration with Onboard Device Enrollment

To allow Onboard enrollment with self-registrations:

1. Go to **Configuration > Pages > Guest Self-Registrations**. Click to expand the registration page's row in the form, and then click its **Edit** link. The **Customize Guest Self-Registration** diagram opens.
2. Under the **Receipt Page > Submit** area of the diagram, click the **Login Message** link to edit the properties of the login page.

Figure 282 *The Login Message Link on the Workflow Diagram*

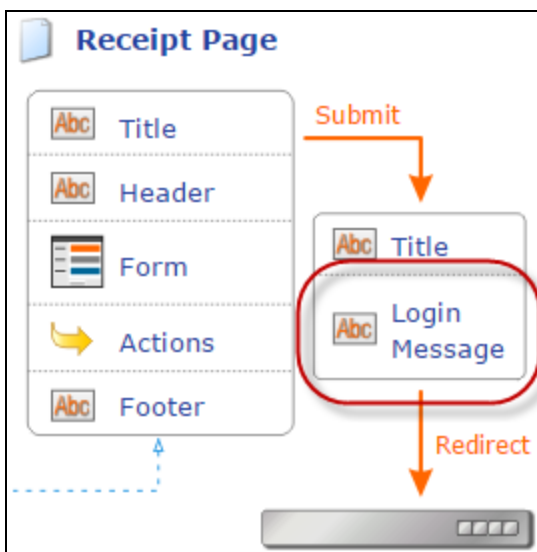


Figure 283 *The Customize Guest Self-Registration Page, Onboard Enrollment Options*

Table 157: *Customize Guest Registration, Onboard Enrollment*

Field	Description
Enabled	To allow simultaneous self-registration and Onboard device enrollment, select Enable Onboard device enrollment .
Provisioning Settings	Local Device Provisioning is the only option available in this field when Onboard device enrollment is selected.
Health Check	To require the device to pass a health check before access is granted, select the check box in this row.
Header HTML	Enter the HTML for the message that is displayed before the health check. You can use the drop-down lists to add images or links.
Footer HTML	Enter the HTML for the message that is displayed after the health check. You can use the drop-down lists to add images or links.

Click the **Save Changes** button to return to the process diagram for self-registration.

Editing Social Logins Properties

Options in the **Social Logins** area let you present guests with a variety of social login options.

To edit the social logins properties of the login page:

1. Go to **Configuration > Pages > Guest Self-Registrations**. Click to expand the registration page's row in the form, and then click its **Edit** link. The **Customize Guest Self-Registration** diagram opens.
2. Under the **Receipt Page > Submit** area of the diagram, click either the **Title** or **Login Message** link to edit the properties of the login page.
3. Scroll to the **Social Logins** area of the form.

Figure 284 The Customize Guest Registration Form, Login Form Page, Social Logins Area: Enabling Social Logins

Social Logins

Optionally present guests with various social login options.

Social Login: Enable login with social network credentials

Add new authentication provider

Use the form below to add an authentication provider to this login.

Properties

* Provider:	Facebook
Enabled:	Select...
* Client ID:	37Signals (Basecamp)
* Client Secret:	Amazon
Advanced:	Bitbucket
Endpoint Attributes:	Bitly
Provider Specific	Box
Email:	Buffer
Friends:	Clever
	Copy
	Dailymotion
	Discogs
	Disqus
	Dropbox
	Dropbox OAuth V2
	Etsy
	Eventful
	Facebook
	Facebook WiFi
	Fitbit
	Flickr

* required field

Add

⊘ Cancel

Provider	Client ID
<div style="display: flex; align-items: center; gap: 5px;"> i There are no authentication providers defined. </div>	

To display social network login buttons, add the following to the Header HTML or Footer HTML area.

Buttons: `{nwa_social_logins}`

Refer to the help for more details.

Debug: Log debugging data

Save Changes
Save and Continue

Table 158: Customize Guest Registration Form, Login Form Page, Social Logins Area: Enabling Social Logins

Field	Description
Social Login	If selected, enables the use of social network credentials to log in. The form expands to include Authentication Providers social login configuration options.
Authentication Providers	After you enable social logins, options in this area let you specify and configure the options for the social network provider.
Add new authentication provider	Opens the properties form for adding and configuring a social network provider.
Buttons	Shows the syntax for displaying social network login buttons on the page. You must add <code>{nwa_social_logins}</code> to either the HTML Header or HTML Footer area.
Debug	If selected, social logins debugging will be included in the application log.

Figure 285 The Customize Guest Registration Form, Login Form Page, Authentication Providers Area (Facebook selected as an example provider)

Social Logins

Optionally present guests with various social login options.

Social Login: Enable login with social network credentials

Add new authentication provider

Use the form below to add an authentication provider to this login.

Properties	
* Provider:	<input type="text" value="Facebook"/>
Enabled:	<input checked="" type="checkbox"/> Use this provider
* Client ID:	<input type="text"/> <small>The Client ID associated to your provider. They may use a different label.</small>
* Client Secret:	<input type="text"/> <small>The Client Secret associated to your provider. They may use a different label.</small>
Advanced:	<input checked="" type="checkbox"/> Show advanced properties
Destination:	<input type="text"/> <small>Guests authenticating with this provider will be redirected to this URL after login.</small>
Auto Redirect:	<input type="checkbox"/> Automatically redirect the guest to this provider <small>Checking this box will remove the ability to support local logins, or any other providers. We recommend also enabling "Custom Form:" in the "Web Login" itself.</small>
Endpoint Attributes:	<input type="text" value="Do not create additional attributes"/> <small>Creating attributes is only needed if you are creating specialized enforcement policies on them.</small>
Username Prefix:	<input type="text"/> <small>Prepend this text to all usernames. A prefix or suffix can be useful if you are providing a means to login using a variety of providers.</small>
Username Suffix:	<input type="text"/> <small>Append this text to all usernames.</small>
Icon Label:	<input type="text"/> <small>Override the default label on this provider's icon.</small>
Hostname:	<input type="text"/> <small>If specified, use this hostname when redirecting the user to authenticate. This is optional - leave blank if unsure.</small>
Notes:	<input type="text"/> <small>Enter comments or notes about this provider. This description is only shown to administrators.</small>
Provider Specific Options	
Email:	<input type="checkbox"/> Request access to the guest's email address <small>Access requires an additional permission for this provider.</small>
Friends:	<input type="checkbox"/> Retrieve the guest's friends <small>Access requires an additional permission for this provider.</small>
<input type="button" value="Add"/> <input type="button" value="Cancel"/>	
<small>* required field</small>	
Provider	Client ID
There are no authentication providers defined.	

Buttons:
Refer to the help for more details.

Debug: Log debugging data

Table 159: *Customize Guest Registration Form, Login Form Page, Authentication Providers Area*

Field	Description
Provider	(Required) Specifies the social network provider to use. All social network providers that have been configured are included in this list. The following options presented in the Authentication Providers area depend on the provider selected in this drop-down list.
Enabled	If this check box is selected, the specified provider can be used.
Admin SDK Refresh Token	(Required) (Google Apps) Valid Google API admin refresh token. To generate a new refresh token, clear this value. You will need to generate a new authorization code.
Advanced	If selected, displays additional options on this form.
Allow Guests	(Google Apps) If selected, allows Google accounts that are not part of your domain to log in as guests. The <code>social_vip</code> flag will be set to false for these users.
Authorization Code	(Required) (Google Apps) When you generate a new code, it is automatically entered in this field, and you can close the redirect window.
Auto Redirect	If selected, local logins and other providers will not be supported. If this option is selected, we recommend you also enable Custom Form in the Login Form area.
Client ID	(Required) Client ID to use with this provider. The provider might use a different label.
Client Secret	(Required) Client secret to use with this provider. The provider might use a different label.
Delete	Removes the provider from the list and deletes its configuration. You will be asked to confirm the deletion.
Destination	URL to which guests authenticating with this provider will be redirected after logging in.
Disable	Disables the provider. To enable it again, click the Enable link.
Disconnect Action	(Facebook WiFi) For the Facebook Wi-Fi provider, specifies the action to take when a disconnect is requested by Facebook. Options include: <ul style="list-style-type: none">• Terminate Session• Cisco - Disable Host-Port• Cisco - Bounce-Host-Port• Cisco - Reauthenticate Session
District ID	(Clever) Identifier for the school district. During authentication, this ID is compared to the ID returned by a Clever Instant Login. If no value is entered in this field, Clever's District Picker will handle the details.
Edit	Opens the Properties form. You can edit any of the configuration options for the provider.
Email	If selected, allows access to the guest's email address. Access requires additional permission for the provider.
Endpoint Attributes	Specifies whether to create endpoint attributes, and how they will be handled. Options include: <ul style="list-style-type: none">• Do not create additional attributes• Create Endpoint attributes converting any arrays to JSON• Create Endpoint attributes flattening the entire data set If one of the Create options is selected, an endpoint attribute is created for every attribute

Field	Description
	returned by the user. This is only needed if you are creating specialized enforcement policies on them.
Flatten Prefix	If Endpoint Attributes was selected, you may enter text to prepend to all keys when flattening. This stores a normalized version of all the returned attributes in the endpoint. If nothing is entered in this field, the default "social" will be used.
Friends	(Facebook) If selected, allows a list of the guest's friends to be retrieved, if permission is granted by the guest. The list is limited to only those friends who also use your application ID.
Generate Code	To generate a new authorization code, click the link in this field. You will be redirected to a new window to generate an authorization code.
Google Apps VIP	Name of the user record attribute to apply to the <code>social_vip</code> flag. For more information, refer to the Google Directory API for retrieving users.
Google Groups	(Google Apps) If selected, all groups associated with the account will be retrieved and stored as a list of group names and a list of matching email addresses. The Admin SDK Refresh Token and Authorization Code must also be regenerated.
Google Plus	(Google) if selected, allows access to the guest's Google Plus profile. Access requires additional permission for the provider.
Group Membership	(Microsoft Azure) If selected, all groups associated with the account will be retrieved and stored as a list of group names and a list of matching email addresses.
Hostname	If specified, overrides the hostname guests are redirected to for authentication. This field is optional; leave it empty if you are unsure.
Icon Label	Overrides the default label on the provider's icon.
LinkedIn VIP	(LinkedIn) Enter a LinkedIn Distance value (0 - 3). If the guest is within this distance, the <code>social_vip</code> flag will be enabled for them.
Move Up Move Down	Moves the provider up or down in the list.
Notes	You may enter additional notes or comments about the provider. This description is only seen by administrators.
Twitter VIP	(Twitter) Name of a Twitter account. If the guest follows this account, they will have the "social_vip" flag enabled.
Username Prefix	Text to prepend to all usernames. A prefix can be useful if you are providing a way to log in using a variety of providers.
Username Suffix	Text to append to all usernames. A suffix can be useful if you are providing a way to log in using a variety of providers.
VIP Attribute	(Google Apps; Microsoft Azure) Name of the user record attribute to apply to the <code>social_vip</code> flag. For more information, refer to the Microsoft Graph API for retrieving users.
Add	When your entries are complete on the Properties, form, click this button. The Properties form closes and the provider is included in the Authentication Providers list.

Enabling and Editing NAS Login Properties

If automatic guest login is not enabled, the submit button on the receipt page will not be displayed, and automatic Network Access Server (NAS) login will not be performed.

To enable and edit the properties for automatic NAS login:

1. Go to **Configuration > Pages > Guest Self-Registrations**. Click to expand the **Guest Self-Registration** row in the form, and then click its **Edit** link. The **Customize Guest Self-Registration** diagram opens.
2. In the lower-right corner of the diagram, click the image of the **NAS** box or click the **NAS Vendor Settings** link. The **Login** form opens.

Figure 286 The NAS Vendor Settings Area of the Diagram

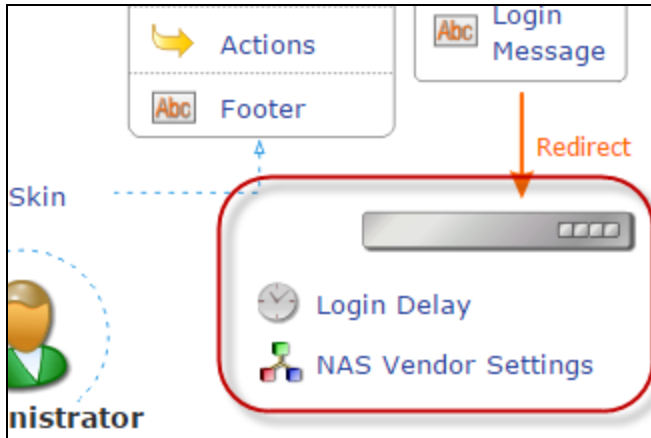


Figure 287 The Customize Guest Registration Form, NAS Login Area

Customize Guest Registration	
Login Options controlling logging in for self-registered guests.	
Enabled:	<input type="checkbox"/> Enable guest login to a Network Access Server
* Vendor Settings:	<input type="text" value="Aruba Networks"/> Select a predefined group of settings suitable for standard network configurations.
Login Method:	<input type="text" value="Controller-initiated — Guest browser performs HTTP form submit"/> Select how the user's network login will be handled. Server-initiated logins require the user's MAC address to be available, usually from the captive portal redirection process.
* IP Address:	<input type="text" value="securelogin.arubanetworks.com"/> Enter the IP address or hostname of the vendor's product here.
Secure Login:	<input type="text" value="Use vendor default"/> Select a security option to apply to the web login process.
Dynamic Address:	<input type="checkbox"/> The controller will send the IP to submit credentials In multi-controller deployments, it is often required to post credentials to different addresses made available as part of the original redirection. The address above will be used whenever the parameter is not available or fails the requirements below.
Security Hash:	<input type="text" value="Do not check – login will always be permitted"/> Select the level of checking to apply to URL parameters passed to the web login page. Use this option to detect when URL parameters have been modified by the user, for example their MAC address.
Default Destination Options for controlling the destination clients will redirect to after login.	
* Default URL:	<input type="text"/> Enter the default URL to redirect clients. Please ensure you prepend "http://" for any external domain.
Override Destination:	<input type="checkbox"/> Force default destination for all clients If selected, the client's default destination will be overridden regardless of its value.
<input type="button" value="Save Changes"/> <input type="button" value="Save and Continue"/>	

Table 160: *Customize Guest Registration Form, NAS Login Area*


Field	Description
Enabled	Specifies the NAS login method. Options include: <ul style="list-style-type: none"> • Disabled • Enable guest login to a Network Access Server • Enable Onboard device enrollment
Provisioning Settings	(Required) For Onboard device enrollment, specifies the provisioning settings to use when enrolling self-registered devices.
Vendor Settings	(Required) Specifies the vendor or other settings to use for standard network configurations. Options include: <ul style="list-style-type: none"> • A list of Vendors • Custom Settings —The form includes options for configuring your custom settings. • Captive Portal with ClearPass Web Auth —The form includes the options for configuring this vendor setting. • Single Sign-On — SAML Identity Provider — If this option is selected, an appropriate service must be created in ClearPass using the ClearPass IDP service template. The external service provider must then be configured to use the SAML Web login page as the IdP. • Single Sign-On — Authorize Only
Login Method	Specifies how the user's network login will be handled. Options include: <ul style="list-style-type: none"> • Controller-initiated — Guest browser performs HTTP form submit • Server-initiated — Change of authorization (RFC 3576) sent to the controller Server-initiated logins require the user's MAC address to be available, usually from the captive portal redirect process.
IP Address	(Required) IP address or hostname of the vendor's product.
Secure Login	Specifies the security option to apply to the Web login process. Options include: <ul style="list-style-type: none"> • Use vendor default • Secure login using HTTPS • Send cleartext passwords over HTTP
Dynamic Address	If selected, the controller will send the IP address to submit credentials. The address entered in the IP Address field above will be used if the parameter is not available or fails the Denied Dynamic and Allowed Dynamic requirements.
Denied Dynamic	IP addresses and networks from which dynamic addresses are denied.
Allowed Dynamic	IP addresses and networks from which dynamic addresses are permitted.
Security Hash	Specifies the level of checking to apply to URL parameters that are passed to the Web login page. You can select one of these options to detect when URL parameters have been modified by the user (for example, their MAC address). Options include: <ul style="list-style-type: none"> • Do not check — login will always be permitted • Deny login on validation error — login will not be permitted
URL Hash Key	(Required) Key that will be used to hash the Redirect URL.
Confirm Key	

Table 160: *Customize Guest Registration Form, NAS Login Area(Continued)*

Field	Description
Submit URL	(Required) URL of the NAS device's login form.
Submit Method	(Required) Method to use when logging in to the NAS. Options include: <ul style="list-style-type: none"> • POST • GET
Username Field	(Required) Name of the username field for the NAS device's login form.
Password Field	(Required) Name of the password field for the NAS device's login form.
Password Encryption	(Required) Specifies the type of password encryption to use when logging in to the NAS. Options include: <ul style="list-style-type: none"> • No encryption (plaintext password) • UAM basic • UAM with shared secret
Extra Fields	You may enter additional field names and values to send to the NAS device as name=value pairs, one per line.
Username Suffix	You may enter a suffix to automatically append to the username before logging in to the NAS.
UAM Secret	Shared secret between the NAS device and the Web login form.
URL Field	Name of the destination field required by the NAS.
Default URL	(Required) Default URL to which to redirect clients.
Override Destination	If selected, the default destination will be forced for all clients, and the client's default destination will be overridden regardless of its value.
Save Changes	Saves your changes and returns to the process diagram for self-registration.
Save and Continue	Saves your changes, updates the self-registration page, and continues to the next editor (Self-Service Portal).

Self-Service Portal Properties

The self-service portal offers guests the ability to log in with their account details, view their account details, or change their password. Additionally, the **Reset Password** link provides a method that allows guests to recover a forgotten account password.

When the self-service portal is enabled, a  **Go To Portal** link is displayed on the list of guest self-registration pages, and may be used to determine the URL that guests should use to access the portal.

The self-service portal is accessed through a separate link that must be published to guests. The page name for the portal is derived from the registration page name by appending “_portal”.

To edit the properties of the self-service portal:

1. Go to **Configuration > Pages > Guest Self-Registrations**. Click to expand the **Guest Self-Registration** row in the form, and then click its **Edit** link. The **Customize Guest Self-Registration** diagram opens.

2. In the **Self-Service Portal** area, click either the **Self-Service Portal** link or click one of the links below it: **Login Page**, **Summary Page**, **Change Password**, or **Reset Password** . The **Self-Service Portal** area of the **Customize Guest Registration** form opens.

Figure 288 *The Self-Service Portal Page Links on the Workflow Diagram*

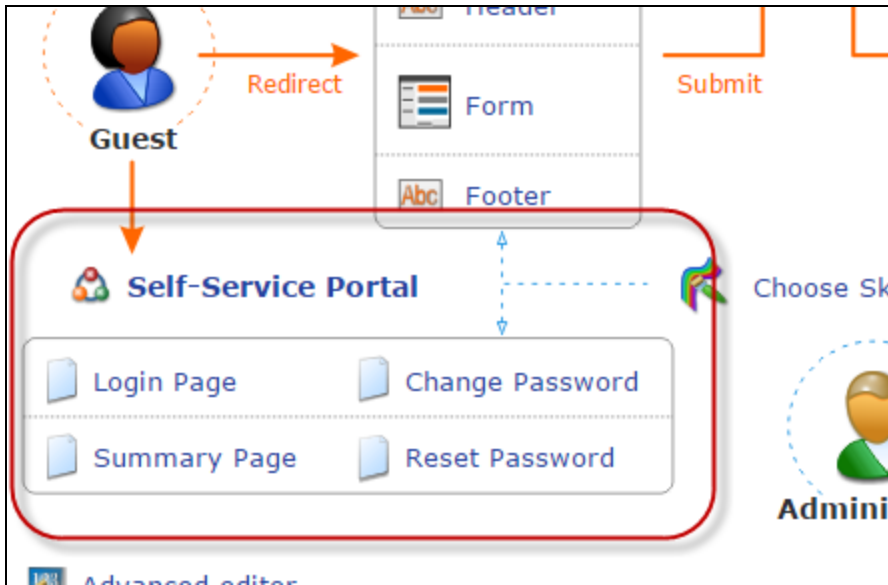


Figure 289 *The Customize Guest Registration Form, Self-Service Portal*

Customize Guest Registration	
Self-Service Portal	
Options controlling details and actions a visitor has to their own account.	
Enabled:	<input checked="" type="checkbox"/> Enable self-service portal
Disabled Users:	<input checked="" type="checkbox"/> Prohibit disabled users from accessing the service portal
Silent Login:	<input type="checkbox"/> Auto login by IP address If set, and the user has an active accounting session, they will be logged in automatically.
Login Page	
UI Overrides:	<input type="checkbox"/> Display fields to override UI text and labels
Summary Page	
UI Overrides:	<input type="checkbox"/> Display fields to override UI text and labels
Change Password	
Change Password:	<input type="checkbox"/> Disable the ability to change passwords
UI Overrides:	<input type="checkbox"/> Display fields to override UI text and labels
Reset Password	
Reset Password:	<input type="checkbox"/> Disable the ability to reset passwords
* Required Field:	(Secret Question) <input type="text"/> The field containing a value the visitor must match prior to resetting their password.
* Password Generation:	Passwords will be randomly generated <input type="text"/> Select the policy for reset password generation.
UI Overrides:	<input type="checkbox"/> Display fields to override UI text and labels
<input type="button" value="Save and Reload"/> <input type="button" value="Save Changes"/>	

The fields at the top of the form let you configure basic properties for the self-service portal.

Table 161: *The Customize Guest Registration Form, Self-Service Portal Area, Basic Properties*

Field	Description
Enabled	If selected, enables the self-service portal for guest access. If this check box is not selected, access to the portal is disabled and a “disabled” message is displayed to the user.
Disabled Message	The message to display to the user if the self-service portal is not enabled. To use the default value, leave this field empty.
Disabled Users	If selected, users whose accounts are disabled cannot log in to the self-service portal.
Silent Login	If selected, a user will be logged in automatically if their client IP address matches the IP address of an active RADIUS accounting session (that is, the guest’s HTTP client address is the same as the RADIUS Framed-IP-Address attribute for an active session).

Figure 290 The Customize Guest Registration Form, Self-Service Portal Page, Login Page Area

Login Page	
UI Overrides:	<input checked="" type="checkbox"/> Display fields to override UI text and labels
Create Account:	<input type="checkbox"/> Remove the Create Account link
Page Title:	<input type="text"/> Override the default page title.
Header HTML:	<pre>{nwa_cookiecheck} <p> Please log in to the Self Service area to access the details about your account. </p></pre> <input type="text" value="Insert..."/> HTML template code displayed before the login form.
Login Form Override:	<input type="checkbox"/> Override the login form
Form Title:	<input type="text"/> Override the default form title.
Username Label:	<input type="text"/> Override the default username label.
Password Label:	<input type="text"/> Override the default password label.
Login Button:	<input type="text"/> Override the default login button.
Footer HTML:	<pre>{if !\$gsr_metadata.service_portal.disable_reset_password}<p> {nwa_iconlink icon="images/icon-reset-password22.png" text=6746 NwaText:"I've forgotten my password"}guest_service_reset.php{/nwa_iconlink} </p>{/if} {if !\$gsr_metadata.service_portal.disable_create_account}<p> {nwa_iconlink icon="images/icon-create-user22.png" text=6745 NwaText:"I don't have an account"} {\$gsr_metadata.id}.php{/nwa_iconlink} </p>{/if}</pre> <input type="text" value="Insert..."/> HTML template code displayed after the login form.

The **Login Page** area of the form lets you configure the self-service portal's login page.

Table 162: Customize Guest Registration Form, Self-Service Portal Page, Login Page Area

Field	Description
UI Overrides	If selected, lets you customize the self-service portal's login form's text and HTML. The form expands to include configuration options.
Create Account	If selected, removes the "Create Account" link from the self-service portal's login page.
Page Title	Title to display on the self-service portal's login page. To use the default value, leave this field empty.

Table 162: *Customize Guest Registration Form, Self-Service Portal Page, Login Page Area(Continued)*

Field	Description
Header HTML	The HTML content to display before the login form. You can use the drop-down list to add images or other content items.
Login Form Override	If selected, overrides the login form.
Form Title	Title to display on the login form. To use the default value, leave this field empty.
Username Label	Label to display on the username field. To use the default value, leave this field empty.
Password Label	Label to display on the password field. To use the default value, leave this field empty.
Login Button	Label to display on the login button. To use the default value, leave this field empty.
Footer HTML	The HTML content to display after the login form. You can use the drop-down list to add images or other content items.

Figure 291 *The Customize Guest Registration Form, Self-Service Portal Page, Summary Page Area*

Summary Page

UI Overrides: Display fields to override UI text and labels

Page Title:
[Override the default page title.](#)

Header HTML:

```
<h2>
    ClearPass
</h2>
<p>
    Welcome to the visitor portal{if
$guest_user.visitor_name}, {$guest_user.visitor_name}{/if}.
</p>
```


[HTML template code displayed before the summary.](#)

Footer HTML:

[HTML template code displayed after the summary.](#)

The **Summary Page** area of the form lets you configure the self-service portal's summary page.

Table 163: *Customize Guest Registration Form, Self-Service Portal Page, Summary Page Area*

Field	Description
UI Overrides	If selected, lets you customize the self-service portal's summary page's text and HTML. The form expands to include configuration options.
Page Title	Title to display on the self-service portal's summary page. To use the default value, leave this field empty.
Header HTML	The HTML content to display before the summary. You can use the drop-down list to add images or other content items.
Footer HTML	The HTML content to display after the summary. You can use the drop-down list to add images or other content items.

Figure 292 *The Customize Guest Registration Form, Self-Service Portal Page, Change Password Area*

Change Password

Change Password:	<input type="checkbox"/> Disable the ability to change passwords
UI Overrides:	<input checked="" type="checkbox"/> Display fields to override UI text and labels
Page Title:	<input type="text"/> <small>Override the default page title.</small>
Header HTML:	<div style="border: 1px solid #ccc; padding: 5px; min-height: 100px;"> <pre><p> To change your password, please complete the form below. </p></pre> </div> <div style="text-align: right; margin-top: 5px;"> <input type="button" value="Insert..."/> </div> <small>HTML template code displayed before the password form.</small>
Form Title:	<input type="text"/> <small>Override the default form title.</small>
Old Password Label:	<input type="text"/> <small>Override the default old password label.</small>
Old Password Description:	<input type="text"/> <small>Override the default old password description.</small>
New Password Label:	<input type="text"/> <small>Override the default new password label.</small>
New Password Description:	<input type="text"/> <small>Override the default new password description.</small>
Confirm Password Label:	<input type="text"/> <small>Override the default confirm password label.</small>
Confirm Password Description:	<input type="text"/> <small>Override the default confirm password description.</small>
Change Password Button:	<input type="text"/> <small>Override the default change password button.</small>
Footer HTML:	<div style="border: 1px solid #ccc; padding: 5px; min-height: 100px;"> <pre><p> {nwa_iconlink icon="images/icon-swirl22.png" text=7040 NwaText:"Back to Customer Service"}guest_service.php{/nwa_iconlink} </p></pre> </div> <div style="text-align: right; margin-top: 5px;"> <input type="button" value="Insert..."/> </div> <small>HTML template code displayed after the password form.</small>

The **Change Password** area of the form lets you configure the self-service portal's password fields.

Table 164: *Customize Guest Registration Form, Self-Service Portal Page, Change Password Area*

Field	Description
Change Password	If selected, guests cannot use the self-service portal to change their passwords.
Extend Expiration	Amount of time to extend an account's expiration window whenever the password is changed. If a value is entered, the account's lifetime will be automatically renewed in cases where it would otherwise expire before the next required password change. To use the original expiration time, leave this field empty.
UI Overrides	If selected, lets you customize the self-service portal's password fields. The form expands to include configuration options.
Page Title	Title to display on the self-service portal's password form. To use the default value, leave this field empty.
Header HTML	The HTML content to display before the password form. You can use the drop-down list to add images or other content items.
Form Title	Title to display on the password form. To use the default value, leave this field empty.
Old Password Label	Label to display on the old password field. To use the default value, leave this field empty.
Old Password Description	Label to display on the old password description field. To use the default value, leave this field empty.
New Password Label	Label to display on the new password field. To use the default value, leave this field empty.
New Password Description	Label to display on the new password description field. To use the default value, leave this field empty.
Confirm Password Label	Label to display on the confirm password field. To use the default value, leave this field empty.
Confirm Password Description	Label to display on the confirm password description field. To use the default value, leave this field empty.
Change Password Button	Label to display on the change password button. To use the default value, leave this field empty.
Footer HTML	The HTML content to display after the password form. You can use the drop-down list to add images or other content items.

Figure 293 *The Customize Guest Registration Form, Self-Service Portal Page, Reset Password Area*

Reset Password	
Reset Password:	<input type="checkbox"/> Disable the ability to reset passwords
* Required Field:	(Secret Question) The field containing a value the visitor must match prior to resetting their password.
Match:	<input type="checkbox"/> Perform a case-insensitive match on the required field
* Password Generation:	Passwords will be randomly generated Select the policy for reset password generation.
UI Overrides:	<input checked="" type="checkbox"/> Display fields to override UI text and labels
Page Title:	<input type="text"/> Override the default page title.
Header HTML:	<input type="text"/> Insert... HTML template code displayed before the reset form.
Reset Form Override:	<input type="checkbox"/> Override the reset form
Form Title:	<input type="text"/> Override the default form title.
Footer HTML:	<input type="text"/> T Insert... HTML template code displayed after the reset form.
<input type="button" value="Save and Reload"/> <input type="button" value="Save Changes"/>	

The **Reset Password** area of the form lets you configure the self-service portal's password reset fields. For more information, see "Resetting Passwords with the Self-Service Portal" on page 394.

Table 165: *Customize Guest Registration Form, Self-Service Portal Page, Reset Password Area*

Field	Description
Reset Password	If selected, guests cannot use the self-service portal to reset a forgotten password.
Required Field	Specifies the field to use for a value the guest must match in order to confirm their identity before they can reset their password.
Match	If selected, a case-insensitive match is performed on the value the user enters in the required field.
Password Generation	Specifies the password reset method to use in the self-service portal. Options include: <ul style="list-style-type: none"> Passwords will be randomly generated Manually enter passwords
UI Overrides	If selected, lets you customize the self-service portal's password reset fields. The form expands to include configuration options.
Page Title	Title to display on the self-service portal's reset password form. To use the default value, leave this field empty.
Header HTML	The HTML content to display before the reset password form. You can use the drop-down list to add images or other content items.

Table 165: *Customize Guest Registration Form, Self-Service Portal Page, Reset Password Area(Continued)*

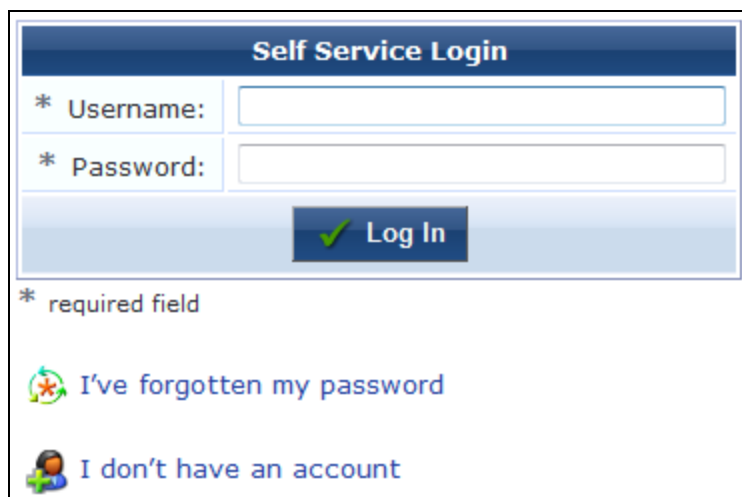
Field	Description
Reset Form Override	If selected, overrides the reset password form.
Form Title	Title to display on the reset password form. To use the default value, leave this field empty.
Footer HTML	The HTML content to display after the reset password form. You can use the drop-down list to add images or other content items.
Save and Reload	Saves your changes on this form and stays on this page.
Save Changes	Saves your changes and returns to the process diagram for self-registration.

Resetting Passwords with the Self-Service Portal

The self-service portal includes the ability to reset a guest account's password.

The default user interface for the self-service portal is shown below:

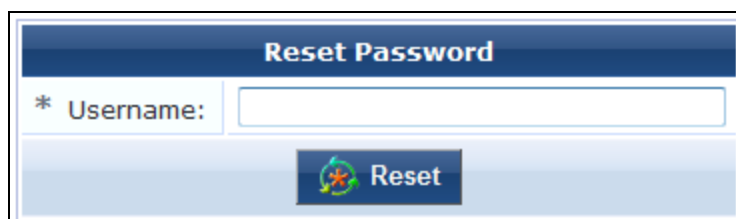
Figure 294 *The Self-Service Login Form*



The screenshot shows a web form titled "Self Service Login". It contains two input fields: "* Username:" and "* Password:". Below the fields is a "Log In" button with a green checkmark icon. Underneath the button, there is a note "* required field". At the bottom of the form, there are two links: "I've forgotten my password" with a key icon and "I don't have an account" with a person icon.

When the user clicks the  **I've forgotten my password** link, it displays a form where the user can reset their password:

Figure 295 *The Reset Password Form*



The screenshot shows a web form titled "Reset Password". It contains one input field: "* Username:". Below the field is a "Reset" button with a key icon.

If the user enters a valid username, the password for that user account is reset, and the receipt page showing the new password and a login option (if NAS login has been enabled) is displayed.

This feature allows the password to be reset for any guest account on the system, which might pose a security risk. It is strongly recommended that when this feature of the self-service portal is enabled, guest registrations should also store a secret question/secret answer field.

To enable a more secure password reset operation, use the **Reset Password** fields described in "Self-Service Portal Properties" on page 386 to perform the following steps.

First, enable the **secret_question** and **secret_answer** fields to the registration form. The default appearance of these fields on the registration form is shown below:

Figure 296 *The Visitor Registration Form*

The screenshot shows a registration form titled "Visitor Registration". It contains the following fields and instructions:

* Your Name:	<input type="text"/> Please enter your full name.
* Email Address:	<input type="text"/> Please enter your email address. This will become your username to log into the network.
Secret Question:	<input type="text"/> Enter your secret question. The answer will be required to reset your password.
* Secret Answer:	<input type="text"/> Enter the answer to your secret question.
* Confirm:	<input type="checkbox"/> I accept the terms of use Flag indicating that the creator has accepted the terms and conditions of use.

At the bottom of the form is a blue button with a green checkmark and the text "Register".

Next, enable the **Required Field** option in the **Self-Service Portal** properties. Setting this to **(Secret Question)** will ask the guest the **secret_question** and will only permit the password to be reset if the guest supplies the correct **secret_answer** value.

With these settings, the user interface for resetting the password now includes a question and answer prompt after the username has been determined:

Figure 297 *The Reset Password Form*

The screenshot shows a "Reset Password" form. It contains the following fields and instructions:

Username:	demo@example.com
Secret Question:	What is my favorite color?
* Secret Answer:	<input type="text"/> Enter the answer to your secret question.

At the bottom of the form is a button with a circular arrow icon and the text "Reset".

Selecting a different value for the **Required Field** allows other fields of the visitor account to be checked. These fields should be part of the registration form. For example, selecting the **visitor_name** field as the required field results in a **Reset Password** form like this:

Figure 298 *The Reset Password Form with Visitor Name as the Required Field*

Managing Web Logins



The **Web Logins** page lists all the Web login pages you have created, and lets you edit and test them and create new Web login pages.

To view the list of your Web login pages and work with them, go to **Configuration > Pages > Web Logins**. The **Web Logins** list view opens. All Web login pages you have created are included in the list. Information shown for each page includes its name for internal identification, title as displayed in the user interface, filename, and the skin assigned to it.

Figure 299 *The Web Logins List View*

Name	Page Title	Page Name	Page Skin
Copy of test	Login	test_weblogin_1	(Default)
<div style="display: flex; justify-content: space-between; align-items: center;"> Edit Duplicate Delete Test </div>			
test	Login	test_weblogin	(Default)
2 web logins Reload			Show all rows

You can click a page's row in the list for additional options:

Table 166: *The Web Logins List View*

Field	Description
Edit	Edit any of a Web login page's attributes. The Web Login Editor form opens. For more information, see "Creating and Editing Web Login Pages" on page 397.
Duplicate	Create a copy of a Web login page to use as a basis for a new page. A progress bar is shown while the page settings are duplicated. When it is complete, the new page is displayed in the list with "Copy of" prepended to its name. The copy has all attributes prepopulated from the original page. You can click the copy's row in the list to open the editor and edit any of its attributes.
Delete	Delete the page. You will be asked to confirm the deletion.

Field	Description
Test	<p>View and test a Web login page. The page opens in a new tab as it would appear to a user:</p> <div data-bbox="623 277 1484 743" style="border: 1px solid black; padding: 10px;"> <p>Please login to the network using your ClearPass username and password.</p> <div data-bbox="639 399 1149 596" style="border: 1px solid #ccc; padding: 5px;"> <div style="background-color: #003366; color: white; text-align: center; padding: 2px;">Login</div> <p>* Username: <input style="width: 100%;" type="text"/></p> <p>* Password: <input style="width: 100%;" type="password"/></p> <div style="text-align: center; margin-top: 5px;"><input type="button" value="Log In"/></div> </div> <p>* required field</p> <p>Contact a staff member if you are experiencing difficulty logging in.</p> </div>
Create new Web login page	<p>Create a new Web login page. For more information, see "Creating and Editing Web Login Pages" on page 397.</p>

Creating and Editing Web Login Pages



Onboard device provisioning pages are now managed from the **Web Login** tab in **Onboard > Provisioning Settings**.

Onboard creates a default Web login page that is used to start the device provisioning process.

To create a new Web login page, go to **Configuration > Pages > Web Logins** and click the **Create new Web login page** link in the upper-right corner. The **Web Login Editor** form opens.

General Properties Area

Figure 300 *The Web Login Editor Form, General Properties Area*

Web Login Editor	
* Name:	Example Web Logins Page <small>Enter a name for this web login page.</small>
Page Name:	My Example Page <small>Enter a page name for this web login. The web login will be accessible from "/guest/page_name.php".</small>
Description:	 <small>Comments or descriptive text about the web login.</small>
* Vendor Settings:	Aruba Networks <small>Select a predefined group of settings suitable for standard network configurations.</small>
Login Method:	Controller-initiated — Guest browser performs HTTP form submit <small>Select how the user's network login will be handled. Server-initiated logins require the user's MAC address to be available, usually from the captive portal redirection process.</small>
Address:	securelogin.arubanetworks.com <small>Enter the IP address or hostname of the vendor's product here.</small>
Secure Login:	Use vendor default <small>Select a security option to apply to the web login process.</small>
Dynamic Address:	<input checked="" type="checkbox"/> The controller will send the IP to submit credentials <small>In multi-controller deployments, it is often required to post credentials to different addresses made available as part of the original redirection. The address above will be used whenever the parameter is not available or fails the requirements below.</small>
Allowed Dynamic:	 <small>Enter the IP addresses and networks from which dynamic addresses are permitted.</small>
Denied Dynamic:	 <small>Enter the IP addresses and networks from which dynamic addresses are denied.</small>
Security Hash:	Do not check – login will always be permitted <small>Select the level of checking to apply to URL parameters passed to the web login page. Use this option to detect when URL parameters have been modified by the user, for example their MAC address.</small>

Table 167: *Web Login Editor, General Properties*

Field	Description
Name	(Required) Name for the page.
Page Name	Identifier page name that will appear in the URL -- for example, "/guest/page_name.php".
Description	Additional information or comments about the page.
Vendor Settings	(Required) Specifies vendor-specific settings for network configuration. This drop-down list includes a list of Vendors you can select from, and a list of Other settings: <ul style="list-style-type: none"> ● Custom Settings—The form includes options for configuring your custom settings. ● Captive portal with ClearPass Web Auth—The form includes the options for configuring this vendor setting.

Field	Description
	<ul style="list-style-type: none"> ● Single Sign-On - SAML Identity Provider—Complete the configuration options for this vendor setting. An appropriate service must also be created in ClearPass using the ClearPass IDP service template. The external service provider must then be configured to use the SAML Web login page as the IdP. ● Single Sign-On - Authorize Only—Allows the server to be configured as an IdP, and a login form is not displayed. If the AppAuth request to validate the SAML SP request is successful, the user is logged in through the normal SAML IdP flow. If the AppAuth request is not successful, a SAML Failure response is returned to the service provider. This vendor setting is useful if you have configured Aruba Auto SignOn (ASO) with third-party Identity providers.
Login Method	<p>Specifies how the user's network login should be handled. Options include:</p> <ul style="list-style-type: none"> ● Controller-initiated—Guest browser performs HTTP form submit ● Server-initiated—Change of authorization (RFC 3576) sent to controller—Server-initiated logins require the user's MAC address to be available. This is usually acquired through the captive portal redirect. If you are setting up Multi-Factor Authentication (MFA) with username-only authentication, choose this option. ● Policy Initiated—An enforcement policy will control a change of authorization—This option should be selected if a Policy Manager policy that includes a "bounce client" will be run as part of the page's actions. This option should be selected if you are using OnGuard health checks.
Address	(Required) IP address or hostname of the vendor's product.
Secure Login	<p>Specifies the security option to use for the Web login process. Options include:</p> <ul style="list-style-type: none"> ● Use vendor default ● Secure login using HTTPS ● Send cleartext passwords over HTTP.
Dynamic Address	For multi-controller deployments, if selected, enables sending the IP to submit credentials. The Allowed Dynamic and Denied Dynamic fields are added to the form.
Allowed Dynamic	IP addresses and networks that will be allowed.
Denied Dynamic	IP addresses and networks that will be denied.
Security Hash	<p>Specifies the level of checking to apply to URL parameters passed to the Web login page. Detects when URL parameters have been modified by the user (for example, their MAC address). To prevent the user from tampering with parameters passed in the redirect URL (for example, their MAC address), select one of the validation error options. Options include:</p> <ul style="list-style-type: none"> ● Do not check —login will always be permitted ● Deny login on validation error — login will not be permitted If one of the validation error options is selected, the form expands to include the URL Hash Key fields.
URL Hash Key	(Required) The shared secret (64 characters) used by ClearPass and the NAD for the hash key to validate the redirect URL. This must be entered twice in order to verify the key.
Confirm Key	

Login Form Area

Options in the **Login Form** area specify the behavior and content of the login form. The options available in this area depend on the selection you made in the **Vendor Settings** field.

Figure 301 *The Web Login Editor Form, Login Form Area*

Login Form	
Options for specifying the behaviour and content of the login form.	
Authentication:	Anonymous – Do not require a username or password ▼ Select the authentication requirement. Access Code requires a single code (username) to be entered. Anonymous allows a blank form requiring just the terms or a Log In button. A pre-existing account is required. Auto is similar to anonymous but the page is automatically submitted. Access Code and Anonymous require the account to have the Username Authentication field set.
Auto-Generate:	<input type="checkbox"/> Create a new anonymous account The account will be created without a session limit or expiration time, and with the Guest role (ID 2). Enter a value for 'Anonymous User' to use a specific username, or leave blank to randomly generate a username.
* Anonymous User:	<input type="text"/> The account to use for anonymous authentication. The password will be visible within the HTML. It is recommended to increase the account Session Limit to the number of guests you wish to support.
Prevent CNA:	<input type="checkbox"/> Enable bypassing the Apple Captive Network Assistant The Apple Captive Network Assistant (CNA) is the pop-up browser shown when joining a network that has a captive portal. Note that this option may not work with all vendors, depending on how the captive portal is implemented.
Custom Form:	<input type="checkbox"/> Provide a custom login form If selected, you must supply your own HTML login form in the Header or Footer HTML areas.
Custom Labels:	<input type="checkbox"/> Override the default labels and error messages If selected, you will be able to alter labels and error messages for the current login form.
* Pre-Auth Check:	App Auth — check using Aruba Application Authentication ▼ Select how the username and password should be checked before proceeding to the NAS authentication.
Terms:	<input type="checkbox"/> Require a Terms and Conditions confirmation If checked, the user will be forced to accept a Terms and Conditions checkbox.

Table 168: *Web Login Editor, Login Form Properties*

Field	Description
Submit URL	URL of the NAS device's login form.
Submit Method	Method to use when submitting the login form to the NAS. Options include: <ul style="list-style-type: none"> • POST • GET
Authentication	Specifies the authentication requirement method to use. Options include: <ul style="list-style-type: none"> • Credentials — Require a username and password • Access Code — Only require a username for authentication—This option does not require a password. If you are setting up Multi-Factor Authentication (MFA) with username-only authentication, choose this option. • Anonymous — Do not require a username or password—This option adds the Auto-Generate and Anonymous User fields to the form. It allows a blank form with only the terms or a Log In button. A pre-existing account is required. • Auto — Do not require a username or password and automatically submit the page—This option can be used if no authentication or prompting is needed. A pre-existing local anonymous account is required. This option should be selected if you are using OnGuard health checks.
Auto-Generate	If selected, auto-generates the anonymous account. The account is created without a session limit or expiration time, and with the Guest role (ID 2).

Field	Description
Anonymous User	(Required) Account to use for anonymous authentication. The password will be visible in the HTML. The account Session Limit should be increased to the number of guests to be supported. To use a specific username, enter it in this field. To randomly generate a user name, leave this field blank.
Client Certificate	If Single Sign-On - SAML Identity Provider was selected in Vendor Settings , you can specify whether the user should select a client certificate when authenticating. Options include: <ul style="list-style-type: none"> • None — Do not request a client certificate from the user • Optional — Request a client certificate from the user, but allow none • Required — Require a client certificate from the user
Prevent CNA	If selected, enables bypassing the Apple Captive Network Assistant (CNA). The CNA is the pop-up browser shown when joining a network that has a captive portal. This option might not work with all vendors; it is dependent on how the captive portal is implemented.
Custom Form	If selected, indicates you will provide a custom login form. You must supply your own HTML login form for the header or footer HTML areas.
Custom Labels	If selected, enables altering the default labels and error messages. This option adds the Pre-Auth Error field to the form.
Username Field	Name of the username field for the login form. This value is passed to the NAS device when the form is submitted.
Username Suffix	Suffix automatically appended to the username before submitting the login form to the NAS.
Username Label	Label that appears on the form for the username field. Leave blank to use the default, (Username:).
Password Field	Name of the password field for the login form. This value is passed to the NAS device when the form is submitted.
Password Encryption	Type of password encryption to use when submitting the login form. Options include: <ul style="list-style-type: none"> • No Encryption (plaintext password) • UAM basic • UAM with shared secret
Password Label	Label that appears on the form for the password field. Leave blank to use the default (Password:).
UAM Secret	Shared secret between the NAS device and the Web login form.
Pre-Auth Check	Specifies how the username and password should be checked before authentication. Options include: <ul style="list-style-type: none"> • None - no extra checks will be made — If you are setting up Multi-Factor Authentication (MFA) with username-only authentication, choose this option. • App Authentication - check using Aruba Application Authentication — When this option is selected, if the user is denied access, an error message attribute is returned from the policy evaluation. A more detailed error message is then displayed to the user, instead of the default "Invalid username or password". This gives the user more information about why access was rejected — for example, it might indicate they are using the service outside of permitted hours, or the account is in the wrong group, or that an external authentication source has a denied message.

Field	Description
	<ul style="list-style-type: none"> • App Authorization – check using Aruba Application Authorization • Local – match a local account • RADIUS – check using a RADIUS request • Single Sign-On – enable SSO for this Web login — When this option is selected, guests are redirected to the Identity Provider (IdP) configured in ClearPass, where they authenticate themselves. They are redirected back to ClearPass, which verifies the login was successful and uses the same credentials to redirect to the actual Web login flow. (SSO support is enabled at Policy Manager > Configuration > Identity > Single Sign-On)
Pre-Auth Error	Customized label text to display if username and password lookup fails. Leave blank to use the default (Invalid username or password).
Terms	If selected, requires the user to mark a check box to accept a Terms and Conditions agreement.
Extra Fields	You may specify any additional field names and values to send to the NAS device. Enter these as <code>name=value</code> pairs, one per line.
Terms Label	Label that appears on the form for the terms check box. Leave blank to use the default (Terms:).
Terms Text	HTML code containing your terms and conditions. Leave blank to use the default, (I accept the <code>terms of use</code>)
Terms Layout	Layout for the terms and conditions text—either above or below the Terms check box.
Terms Error	Text to display if the terms are not accepted. Leave blank to use the default (In order to log in, you must accept the terms and conditions.).
Log In Label	Label that appears on the form for the login button. Leave blank to use the default (Log In).
Title	Title to display on the Web login page. To use the default (Login), leave this field blank.
Login Message	HTML template code for the text to display while the login is in progress.
Login Delay	Specifies the number of seconds to delay while displaying the login message. The default content is shown, and can be modified. You can also use the drop-down list to add images or other content items.

Default Destination Area

Options in the **Default Destination** area control the destination page users are redirected to after login.

Figure 302 *The Web Login Editor Form, Default Destination Area*

Default Destination	
Options for controlling the destination clients will redirect to after login.	
* Default URL:	<input type="text"/> Enter the default URL to redirect clients. Please ensure you prepend "http://" for any external domain.
Override Destination:	<input checked="" type="checkbox"/> Force default destination for all clients If selected, the client's default destination will be overridden regardless of its value.

Table 169: Web Login Editor, Default Destination Properties

Field	Description
Default URL	(Required) Default URL for the redirect page. For external domains, this must include the http:// prefix.
Override Destination	If selected, forces the default destination for all clients, overriding any default value already set on the client.

Login Page Area

Options in the **Login Page** area control the look and feel of the login page.

Figure 303 The Web Login Editor Form, Login Page Area

Login Page
Options for controlling the look and feel of the login page.

* Skin:	<input type="text" value="(Default)"/> Choose the skin to use when this web login page is displayed.
Title:	<input type="text"/> The title to display on the web login page. Leave blank to use the default (Login).
Header HTML:	<pre>{nwa_cookiecheck} {if \$errmsg}{nwaicontext type=error}{\$errmsg escape} {/nwaicontext}{/if} {nwa_text id=7980}<p> Please login to the network using your username and password. </p>{/nwa_text}</pre> <div style="display: flex; justify-content: space-between; margin-top: 5px;"> <input type="text" value="Insert content item..."/> <input type="text" value="Insert self-registration link..."/> </div> HTML template code displayed before the login form.
Footer HTML:	<pre>{nwa_text id=7979}<p> Contact a staff member if you are experiencing difficulty logging in. </p>{/nwa_text}</pre> <div style="display: flex; justify-content: space-between; margin-top: 5px;"> <input type="text" value="Insert content item..."/> <input type="text" value="Insert self-registration link..."/> </div> HTML template code displayed after the login form.
Login Message:	<pre>{nwa_text id=7978}<p> Logging in, please wait... </p>{/nwa_text}</pre> <div style="display: flex; justify-content: flex-end; margin-top: 5px;"> <input type="text" value="Insert content item..."/> </div> HTML template code displayed while the login attempt is in progress.
* Login Delay:	<input type="text" value="0"/> The time in seconds to delay while displaying the login message.

Table 170: *Web Login Editor, Login Page Properties*

Field	Description
Skin	(Required) Specifies the skin to use for the login page. Options include: <ul style="list-style-type: none">• (Default)• Aruba ClearPass Skin• Blank Skin• ClearPass Guest Skin• Custom Skin 1• Custom Skin 2• Galleria Skin• Galleria Skin 2
Title	Title that will be displayed on the page.
Header HTML	HTML content to display above the login form. The default content is shown, and can be modified. You can also use the drop-down lists to add images or other content items, or to insert a self-registration link. To appear in this list, content items must first be uploaded to the Content Manager .
Footer HTML	HTML content to display below the login form. The default content is shown, and can be modified. You can also use the drop-down lists to add images or other content items, or to insert a self-registration link. To appear in this list, content items must first be uploaded to the Content Manager .
Login Message	HTML template code for the text to display while the login attempt is in progress. The default content is shown, and can be modified. You can also use the drop-down list to add images or other content items. To appear in this list, content items must first be uploaded to the Content Manager .
Login Delay	(Required) Specifies the number of seconds to delay while displaying the login message.

Advertising Services Area

The check box in the **Advertising Services** area lets you selectively enable Advertising Services for each Web login page on which you want to display advertising.

Figure 304 *The Web Login Editor Form, Advertising Services Area*

Advertising Services
Enable advertising content on the login page.

Advertising: Enable Advertising Services content

Social Logins Area


Options in the **Social Logins** area let you present guests with various social login options.

Figure 305 *The Web Login Editor Form, Social Logins Area: Enabling Social Logins*

Social Logins
Optionally present guests with various social login options.

Social Login: Enable login with social network credentials

Authentication Providers:


 Add new authentication provider

Use the form below to add an authentication provider to this login.

Properties	
* Provider:	Select... ▾
Enabled:	<input checked="" type="checkbox"/> Use this provider
* Client ID:	<input type="text"/> <small>The Client ID associated to your provider. They may use a different label.</small>
* Client Secret:	<input type="text"/> <small>The Client Secret associated to your provider. They may use a different label.</small>
Advanced:	<input type="checkbox"/> Show advanced properties
Endpoint Attributes:	Do not create additional attributes ▾ <small>Creating attributes is only needed if you are creating specialized enforcement policies on them.</small>

Read Only Access

* required field

Provider	Client ID
 There are no authentication providers defined.	

Buttons:
Refer to the help for more details.

Debug: Log debugging data

Table 171: *Web Login Editor Form, Social Logins Area: Enabling Social Logins*

Field	Description
Social Login	If selected, enables the use of social network credentials to log in. The form expands to include Authentication Providers social login configuration options.
Authentication Providers	After you enable social logins, options in this area let you specify and configure the options for the social network provider.
Add new authentication provider	Opens the properties form for adding and configuring a social network provider.
Buttons	Shows the syntax for displaying social network login buttons on the page. You must add {nwa_social_logins} to either the HTML Header or HTML Footer area.
Debug	If selected, social logins debugging will be included in the application log.

Figure 306 The Web Login Editor Form, Social Logins Area, Authentication Providers Area (Facebook selected as an example provider)

Authentication Providers:

Add new authentication provider

Use the form below to add an authentication provider to this login.

Properties

* Provider:	<input type="text" value="Facebook"/>
Enabled:	<input checked="" type="checkbox"/> Use this provider
* Client ID:	<input type="text"/> <small>The Client ID associated to your provider. They may use a different label.</small>
* Client Secret:	<input type="text"/> <small>The Client Secret associated to your provider. They may use a different label.</small>
Advanced:	<input checked="" type="checkbox"/> Show advanced properties
Destination:	<input type="text"/> <small>Guests authenticating with this provider will be redirected to this URL after login.</small>
Auto Redirect:	<input type="checkbox"/> Automatically redirect the guest to this provider <small>Checking this box will remove the ability to support local logins, or any other providers. We recommend also enabling "Custom Form:" in the "Web Login" itself.</small>
Endpoint Attributes:	<input type="text" value="Do not create additional attributes"/> <small>Creating attributes is only needed if you are creating specialized enforcement policies on them.</small>
Username Prefix:	<input type="text"/> <small>Prepend this text to all usernames. A prefix or suffix can be useful if you are providing a means to login using a variety of providers.</small>
Username Suffix:	<input type="text"/> <small>Append this text to all usernames.</small>
Icon Label:	<input type="text"/> <small>Override the default label on this provider's icon.</small>
Hostname:	<input type="text"/> <small>If specified, use this hostname when redirecting the user to authenticate. This is optional – leave blank if unsure.</small>
Notes:	<input type="text"/> <small>Enter comments or notes about this provider. This description is only shown to administrators.</small>

Provider Specific Options

Email:	<input type="checkbox"/> Request access to the guest's email address <small>Access requires an additional permission for this provider.</small>
Friends:	<input type="checkbox"/> Retrieve the guest's friends <small>Access requires an additional permission for this provider.</small>

* required field

Provider	Client ID
There are no authentication providers defined.	

Table 172: Web Login Editor Form, Social Logins Area, Authentication Providers Area

Field	Description
Provider	(Required) Specifies the social network provider to use. All social network providers that have been configured are included in this list. The following options presented in the Authentication Providers area depend on the provider selected in this drop-down list.
Enabled	If this check box is selected, the specified provider can be used.
Admin SDK Refresh Token	(Required) (Google Apps) Valid Google API admin refresh token. To generate a new refresh token, clear this value. You will need to generate a new authorization code.

Field	Description
Advanced	If selected, displays additional options on this form.
Allow Guests	(Google Apps) If selected, allows Google accounts that are not part of your domain to log in as guests. The <code>social_vip</code> flag will be set to false for these users.
Authorization Code	(Required) (Google Apps) When you generate a new code, it is automatically entered in this field, and you can close the redirect window.
Auto Redirect	If selected, local logins and other providers will not be supported. If this option is selected, we recommend you also enable Custom Form in the Login Form area.
Client ID	(Required) Client ID to use with this provider. The provider might use a different label.
Client Secret	(Required) Client secret to use with this provider. The provider might use a different label.
Delete	Removes the provider from the list and deletes its configuration. You will be asked to confirm the deletion.
Destination	URL to which guests authenticating with this provider will be redirected after logging in.
Disable	Disables the provider. To enable it again, click the Enable link.
Disconnect Action	(Facebook WiFi) For the Facebook Wi-Fi provider, specifies the action to take when a disconnect is requested by Facebook. Options include: <ul style="list-style-type: none"> • Terminate Session • Cisco - Disable Host-Port • Cisco - Bounce-Host-Port • Cisco - Reauthenticate Session
District ID	(Clever) Identifier for the school district. During authentication, this ID is compared to the ID returned by a Clever Instant Login. If no value is entered in this field, Clever's District Picker will handle the details.
Edit	Opens the Properties form. You can edit any of the configuration options for the provider.
Email	If selected, allows access to the guest's email address. Access requires additional permission for the provider.
Endpoint Attributes	Specifies whether to create endpoint attributes, and how they will be handled. Options include: <ul style="list-style-type: none"> • Do not create additional attributes • Create Endpoint attributes converting any arrays to JSON • Create Endpoint attributes flattening the entire data set If one of the Create options is selected, an endpoint attribute is created for every attribute returned by the user. This is only needed if you are creating specialized enforcement policies on them.
Flatten Prefix	If Endpoint Attributes was selected, you may enter text to prepend to all keys when flattening. This stores a normalized version of all the returned attributes in the endpoint. If nothing is entered in this field, the default "social" will be used.
Friends	(Facebook) If selected, allows a list of the guest's friends to be retrieved, if permission is granted by the guest. The list is limited to only those friends who also use your application ID.
Generate Code	To generate a new authorization code, click the link in this field. You will be redirected to a new window to generate an authorization code.

Field	Description
Google Apps VIP	Name of the user record attribute to apply to the <code>social_vip</code> flag. For more information, refer to the Google Directory API for retrieving users.
Google Groups	(Google Apps) If selected, all groups associated with the account will be retrieved and stored as a list of group names and a list of matching email addresses. The Admin SDK Refresh Token and Authorization Code must also be regenerated.
Google Plus	(Google) if selected, allows access to the guest's Google Plus profile. Access requires additional permission for the provider.
Group Membership	(Microsoft Azure) If selected, all groups associated with the account will be retrieved and stored as a list of group names and a list of matching email addresses.
Hostname	If specified, overrides the hostname guests are redirected to for authentication. This field is optional; leave it empty if you are unsure.
Icon Label	Overrides the default label on the provider's icon.
LinkedIn VIP	(LinkedIn) Enter a LinkedIn Distance value (0 - 3). If the guest is within this distance, the <code>social_vip</code> flag will be enabled for them.
Move Up Move Down	Moves the provider up or down in the list.
Notes	You may enter additional notes or comments about the provider. This description is only seen by administrators.
Twitter VIP	(Twitter) Name of a Twitter account. If the guest follows this account, they will have the "social_vip" flag enabled.
Username Prefix	Text to prepend to all usernames. A prefix can be useful if you are providing a way to log in using a variety of providers.
Username Suffix	Text to append to all usernames. A suffix can be useful if you are providing a way to log in using a variety of providers.
VIP Attribute	(Google Apps; Microsoft Azure) Name of the user record attribute to apply to the <code>social_vip</code> flag. For more information, refer to the Microsoft Graph API for retrieving users.
Add	When your entries are complete on the Properties, form, click this button. The Properties form closes and the provider is included in the Authentication Providers list.

Multi-Factor Authentication Area

Options in the **Multi-Factor Authentication** area let you require a secondary factor when authenticating. When the guest enters their username to log in, they are sent a code which they must successfully retrieve and enter to complete the login. For more information, see ["About Multi-Factor Authentication" on page 412](#).

Figure 307 *The Web Logins Editor Form, Multi-Factor Authentication Area*

Multi-Factor Authentication	
Require a secondary factor when authenticating.	
Provider:	Duo Security - Two Factor Authentication ▼
Authentication Order:	Credentials and then device ▼
* Duo AKEY:	<input type="text"/> <small>Your akey is a string that you should generate and keep secret from Duo. It should be at least 40 characters long. Reference the Duo website for tips on generating this key.</small>
* Duo Integration Key:	<input type="text"/>
* Duo Secret Key:	<input type="text"/>
* Duo API Hostname:	<input type="text"/>
Header HTML:	<input type="text"/> Insert... <small>HTML template code displayed before the provider's vendor-specific authentication area.</small>
Footer HTML:	<input type="text"/> Insert... <small>HTML template code displayed after the provider's vendor-specific authentication area.</small>

Table 173: *Web Logins Editor, Multi-Factor Authentication*

Field	Description
Provider	Specifies the multi-factor authentication provider. Options include: <ul style="list-style-type: none"> • No multi-factor authentication • Duo Security - Two Factor Authentication • Facial Networks - ZOOM Multi-Factor Authentication • Kasada - authenticator • Kasada - authenticator (legacy) • ImageWare Systems - GoMobile Interactive • SMS Verification Codes
App Name	(Required) App name to use with this provider.
Authentication Order	Specifies the authentication order. Options include: <ul style="list-style-type: none"> • Credentials and then device — If you are setting up Multi-Factor Authentication (MFA) with username-only authentication, choose this option. • Device and then credentials
Client ID	(Required) Client ID to use for this provider.
Duo AKEY	(Required) A string that you should generate and keep secret from Duo. The string should be at least 40 characters long. The Duo Web site provides tips for how to generate this key.
Duo API Hostname	(Required) The Duo API hostname.

Table 173: Web Logins Editor, Multi-Factor Authentication(Continued)

Field	Description
Duo Integration Key	(Required) The Duo ikey.
Duo Secret Key	(Required) The Duo skey.
Email	If selected, emails will be sent during application enrollment. If deselected, the user must scan the QR code.
Enroll	If selected, usernames will be automatically enrolled with the provider.
Factors	The number of factors to require. For some providers, options are included to specify types of factor, such as: <ul style="list-style-type: none"> • photolock - The Photo • fingerprint - The Fingerprint • gridlock - The Pattern • onetap - The Onetap • password - The Password
Footer HTML	HTML template code displayed after the provider’s vendor-specific authentication area. This is the login “wait” page displayed to the user while the authentication code is sent to and submitted by them. You can also use the drop-down lists to add images or other content items, or to insert a self-registration link. To appear in this list, content items must first be uploaded to the Content Manager .
Grace Period	Specifies the number of hours between multi-factor authentication checks. If the user logs in again before this interval expires, they can skip the secondary check if the device name and username have not changed. To require full authentication every time, leave this field empty. The default interval is 24 hours.
Header HTML	HTML template code to display before the provider’s vendor-specific authentication area. This is the login “wait” page displayed to the user while the authentication code is sent to and submitted by them. You can also use the drop-down lists to add images or other content items, or to insert a self-registration link. To appear in this list, content items must first be uploaded to the Content Manager .
Hostname	(Required) Hostname of the ImageWare server.
Password	(Required) Password to use with this provider.
Phone Attribute	(Required) For SMS Verification Codes, the attribute name containing mobile numbers. Names should be entered as a comma-separated list. The order of the list determines the lookup priority.
Role	Your role ID.
Secret Key	(Required) The Facial Networks client secret.
Service Provider	Service provider to use when sending SMS messages.

Table 173: *Web Logins Editor, Multi-Factor Authentication(Continued)*

Field	Description
Tenant Name	(Required) Tenant name to use with this provider. A tenant is a company or other entity that has created a tenant account with ImageWare in order to use the GoMobile server for security.
Username	(Required) Username to use with this provider.
Verify Template	The full URL of the verification template.

Network Login Access Area

Options in the **Network Login Access** area control access to the login page.

Figure 308 *The Web Login Editor Form, Network Login Access Area*

Network Login Access
Controls access to the login page.

Allowed Access:	<input style="width: 100%; height: 40px;" type="text"/> <small>Enter the IP addresses and networks from which logins are permitted.</small>
Denied Access:	<input style="width: 100%; height: 40px;" type="text"/> <small>Enter the IP addresses and networks that are denied login access.</small>
* Deny Behavior:	<input style="width: 100%; height: 20px;" type="text" value="Send HTTP 404 Not Found status"/> <small>Select the response of the system to a request that is not permitted.</small>

Table 174: *Web Login Editor, Network Login Access Properties*

Field	Description
Allowed Access	IP addresses and networks from which logins will be allowed. (IPv4 and IPv6 are both supported)
Denied Access	IP addresses and networks from which logins will be denied. (IPv4 and IPv6 are both supported)
Deny Behavior	<p>(Required) Response shown to the user if their login request is denied. Options in this drop-down list include:</p> <ul style="list-style-type: none"> ● Send HTTP 404 Not Found status ● Show Access Denied page ● Show a blank page

Post-Authentication Area

Options in the **Post-Authentication** area control the actions to perform after a successful pre-authentication.

Figure 309 *The Web Login Editor Form, Post-Authentication Area*

Post-Authentication
Actions to perform after a successful pre-authentication.

Health Check:	<input checked="" type="checkbox"/> Require a successful OnGuard health check <small>If selected, the guest will be required to pass a health check prior to accessing the network.</small>
Header HTML:	<div style="border: 1px solid #ccc; padding: 2px; min-height: 20px;"></div> <div style="text-align: right; margin-top: 5px;"> <input type="text" value="Insert content item..."/> </div> <small>HTML template code displayed before the health check text.</small>
Footer HTML:	<div style="border: 1px solid #ccc; padding: 2px; min-height: 20px;"></div> <div style="text-align: right; margin-top: 5px;"> <input type="text" value="Insert content item..."/> </div> <small>HTML template code displayed after the health check text.</small>
Update Endpoint:	<input checked="" type="checkbox"/> Mark the user's MAC address as a known endpoint <small>If selected, the endpoint's attributes will also be updated with other details from the user account.</small>
Advanced:	<input checked="" type="checkbox"/> Customize attributes stored with the endpoint
Endpoint Attributes:	<div style="border: 1px solid #ccc; padding: 2px; min-height: 40px;"> <pre>username Username visitor_name Visitor Name cn Visitor Name visitor_phone Visitor Phone</pre> </div> <small>List of name value pairs to pass along. user_field Endpoint Attribute.</small>

Table 175: *Web Login Editor, Post-Authentication Properties*

Field	Description
Health Check	If selected, requires the visitor to pass a health check before they can access the network. The health check is done automatically through the OnGuard Dissolvable Agent.
Header HTML	HTML content to display above the health check text. The default content is shown, and can be modified. You can also use the drop-down list to add images or other content items.
Footer HTML	HTML content to display below the health check text. The default content is shown, and can be modified. You can also use the drop-down list to add images or other content items.
Update Endpoint	If selected, marks the user's MAC address as a known endpoint, and updates the endpoint's attributes with other details from the user account. If this check box is selected, the form expands to include the Advanced field.
Advanced	If selected, lets you specify custom attributes to store in the endpoint. The form expands to include the Endpoint Attributes field.
Endpoint Attributes	List of name-value pairs to pass as custom attributes. Follow the format user_field Endpoint Attribute . Examples are shown in this text box.

About Multi-Factor Authentication

Multi-factor authentication (MFA) lets you require multiple factors, or proofs of identity, when authenticating a user. Usually at least two of the following categories are required:

- Knowledge: A secret the user knows, such as their password or PIN.

- Possession: Something the user has, such as a security token generator or a certificate. This requirement can also be met by having the user answer a registered phone number or email address to retrieve a temporary code.
- Inherence: A physical characteristic of the user, such as their voice, face, or fingerprint.

Policy configurations can define how often multi-factor authentication will be required, or conditions that will trigger it:

- Time-based policy: Policy might require MFA on a daily or weekly basis, or if the user has not logged in from the device for a certain number of days, or if the device was unhealthy in the past 30 days.
- Posture-based policy: Policy might require MFA if the device's posture changes to unhealthy, or if the posture of any of the user's other devices changes to unhealthy, or if a company alert or security check is issued.
- Policy based on other conditions: Policy might require MFA if the user has never logged in from the location before, or has failed authentication three times, or if a third-party application or system triggers MFA.

Configuring Multi-Factor Authentication

To configure multi-factor authentication in ClearPass, you first create an account with an MFA provider and create the users for the guest account. Next, you set up either a captive portal login or an Onboard login.

To set up the MFA provider and the users:

1. Collect any required elements from the selected MFA provider's account. These might include such things as a secret key, integration key, hostname, tenant name, app name, client ID, or special username and password.
2. Create a user account in ClearPass Guest with the same name that is configured in the MFA provider.

To set up a captive portal login:

1. Configure ClearPass for regular guest services.
2. Go to **ClearPass Guest > Configuration > Pages > Web Logins** and either create a new Web login page or edit an existing one. Scroll to the **Multi-Factor Authentication** area and provide the following information:
 - a. In the **Provider** drop-down list, select the appropriate MFA provider.
 - b. Complete all the required fields for the provider.
 - c. Select one of the options in the **Authentication Order** drop-down list. Options include **Credentials and then device** or **Device and then credentials**.
 - d. Complete the rest of the form. For more information, see "[Creating and Editing Web Login Pages](#)" on [page 397](#).
3. Redirect the captive portal to this Web login page.
4. Connect a device. You will be prompted for a username twice. Depending on the authentication order you specified the **Web Login Editor**, the user will be authenticated by the provider either first or second.
5. Approve the authentication request of the provider through the authorized device for the account.

To set up an Onboard login:

1. Configure ClearPass for regular Onboard services.
2. Go to **ClearPass Guest > Onboard > Deployment and Provisioning > Provisioning Settings** and either create a new provisioning setting or edit an existing one. On the **Web Login** tab, scroll to the **Multi-Factor Authentication** area and provide the following information:
 - a. In the **Provider** drop-down list, select the appropriate MFA provider.

- b. Complete all the required fields for the provider.
 - c. Select one of the options in the **Authentication Order** drop-down list. Options include **Credentials and then device** or **Device and then credentials**.
 - d. Complete the rest of the form. For more information, see "[Configuring Provisioning Settings for the Web Login Page](#)" on page 229.
3. Redirect the captive portal to the Onboard page.
 4. Connect a device. You will be prompted for a username twice. Depending on the authentication order you specified the **Web Login Editor**, the user will be authenticated by the provider either first or second.
 5. Approve the authentication request of the provider through the authorized device for the account. The rest of the onboarding process will be the same as usual.

Managing Web Pages



Simple Web pages provide additional information to guests -- for example, advising them that the device does not meet security requirements, service is unavailable, their browser is unsupported, the device is jailbroken, or to provide "terms and conditions" information.

The **Web Pages** view lists all the Web pages you have created, and lets you edit and preview them and create new Web pages. It also includes templates for new Web pages. Each template may be used as it is or can be used as the basis for a page you design. For more information, see "[The Web Page Templates](#)" on page 415.

To view the list of your Web pages and work with them, go to **Configuration > Pages > Web Pages**. The **Web Pages** list view opens. The templates and all Web pages you have created are included in the list. Information shown for each page includes its name as displayed to administrators in ClearPass Guest, the page title that is displayed to guests, the page's filename used in the URL, and the skin currently assigned to it.

Figure 310 *The Web Pages List View*

Name	Page Title	Page Name	Page Skin
Browser Unsupported This page can be used to show a 'Browser Not Supported' page.	Browser Unsupported!	browser_unsupported	(Default)
Jailbroken Device This page can be used to show a 'Jailbroken Device' page.	Jailbroken Device!	jailbroken_device	(Default)
Posture Check This page can be used to show a 'Posture Check' page.	Posture Check!	posture_check	(Default)
Service Unavailable This page can be used to show a 'Service Unavailable' page.	Service Unavailable!	service_unavailable	(Default)
Terms and Conditions This page can be used to show a 'Terms' page.	Terms of Use	terms	(Default)
Edit Copy Launch Page			
Refresh		1	
			Showing 1 - 5 of 5 10 rows per page ▼

You can click a Web page's row in the list for additional options:

Table 176: *The Web Pages List View*

Field	Description
Edit	Edit any of a Web page's attributes. The Edit Web Page form opens. For more information, see "Creating and Editing Simple Web Pages" on page 417.
Copy	Create a copy of a Web page to use as a basis for a new page. The Copy Web Page form opens, where you can edit any of the page's attributes. For more information, see "Creating and Editing Simple Web Pages" on page 417.
Launch Page	View the page. The page opens in a new tab as it would appear to the guest.
Delete	Delete the page. You will be asked to confirm the deletion.
Create a new Web page	Create a new Web login page. For more information, see "Creating and Editing Simple Web Pages" on page 417.

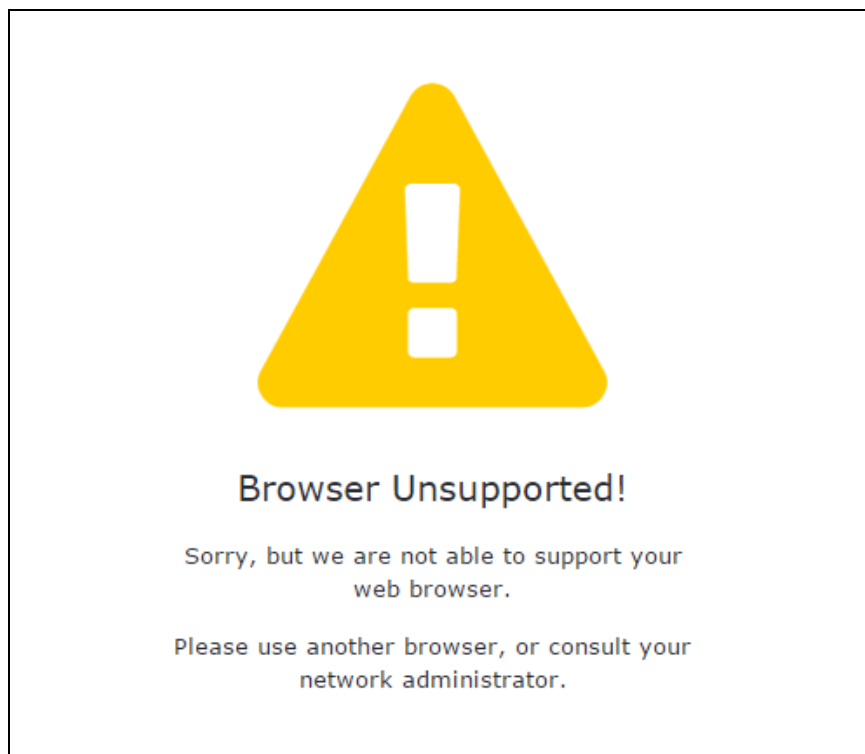
The Web Page Templates

ClearPass Guest provides the following templates for simple Web pages. You can use these templates as they are, or edit any of their properties to suit your needs, or copy them to use as a basis for new Web pages. These templates are available at **Configuration > Pages > Web Pages**.

Browser Unsupported Page Template

The **Browser Unsupported** template can be used to show a message advising the guest that their browser is not supported.

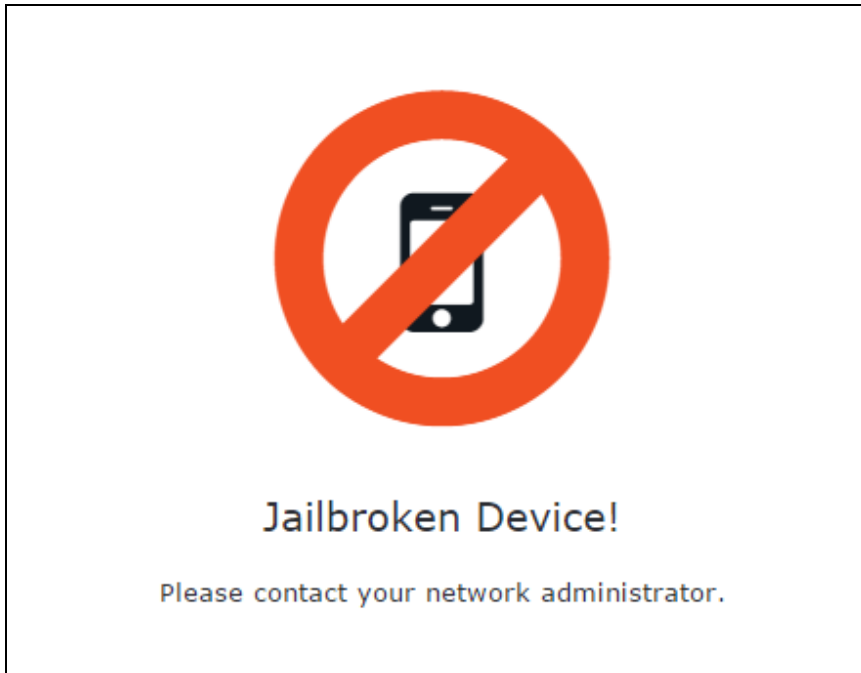
Figure 311 *The Page Displayed by the Browser Unsupported Template*



Jailbroken Device Page Template

The **Jailbroken Device** template can be used to show a message advising the guest that the iOS device has been modified, or jailbroken.

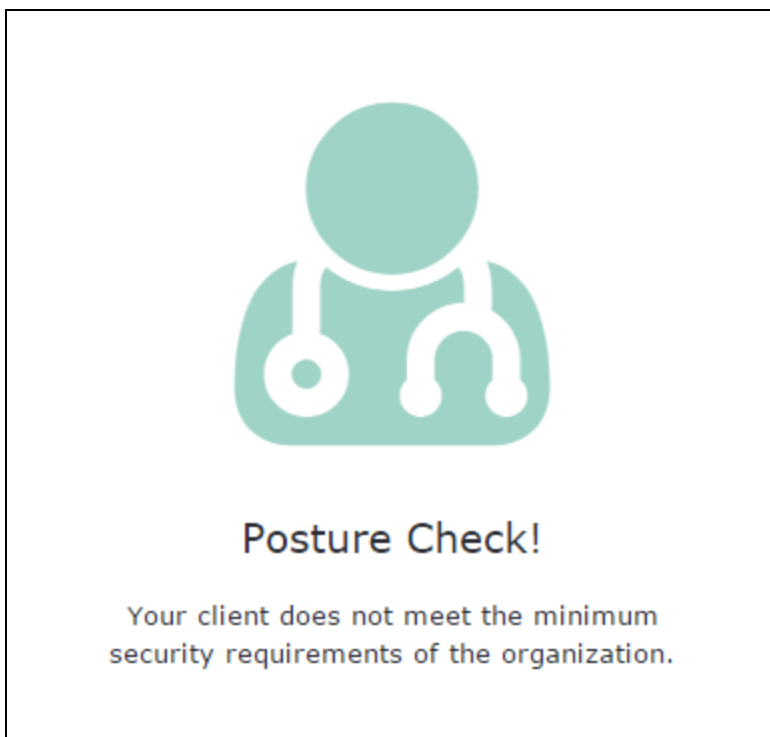
Figure 312 *The Page Displayed by the Jailbroken Device Template*



Posture Check Page Template

The **Posture Check** template can be used to show a message advising the guest that the device does not meet the organization's minimum security requirements (detected by OnGuard).

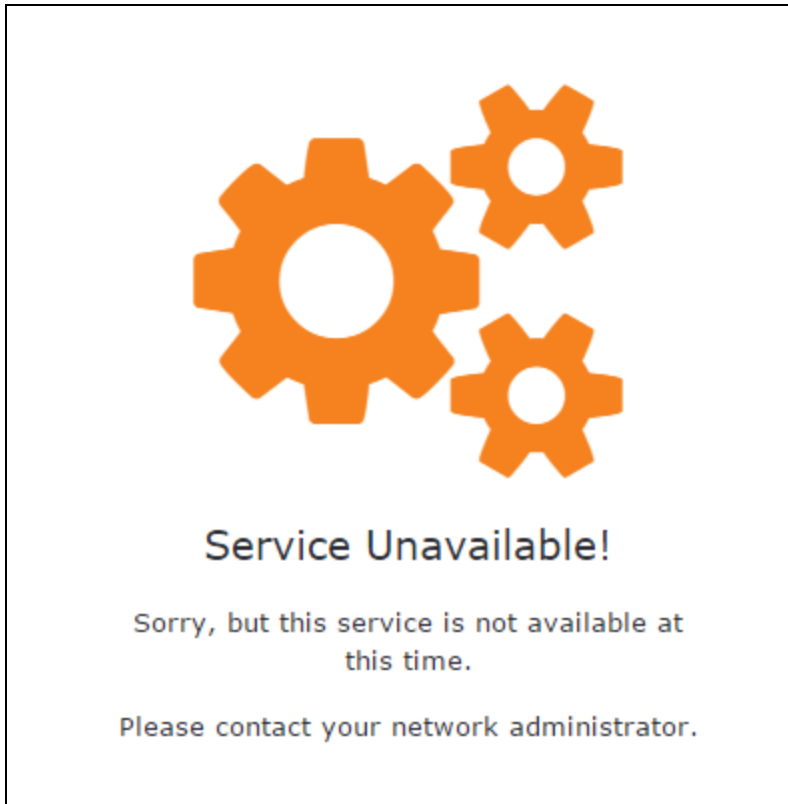
Figure 313 *The Page Displayed by the Posture Check Template*



Service Unavailable Page Template

The **Service Unavailable** template can be used to show a message advising the guest that service is temporarily unavailable.

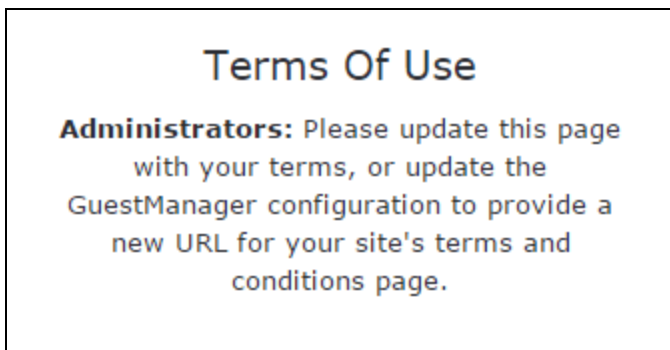
Figure 314 *The Page Displayed by the Service Unavailable Template*



Terms and Conditions Template

The Terms and Conditions template can be used to provide information to the user about the terms and conditions of use.

Figure 315 *The Page Displayed by the Terms and Conditions Template*



Creating and Editing Simple Web Pages

The **Web Page Settings** form lets you create a new simple Web page, edit an existing page, or copy a template or existing page to use as a basis for a new page. To perform these tasks, go to **Configuration > Pages > Web Pages**, and then:

- To create a new simple Web page, click the **Create a new Web page** link in the upper-right corner.

- To edit an existing simple Web page, click the **Edit** link for a page in the list.
- To make a copy of a template or existing page to use as a basis for a new page, click the **Copy** link for a template or page in the list.

The **Web Page Settings** form opens.

Figure 316 *The Web Page Settings Editor, General Settings*

The screenshot shows the 'Web Page Settings' form with the following fields and options:

- * Name:** Text input field. Description: Enter a name for the web page. This name is only shown to administrators.
- * Page Name:** Text input field. Description: Enter a page name for this web page. The web page will be accessible from "/>

Figure 317 *The Web Page Settings Editor, Advanced Settings*

The screenshot shows the 'Advanced Settings' section of the form with the following options and fields:

- Show advanced settings
- Prevent CNA:** Enable bypassing the Apple Captive Network Assistant. Description: The Apple Captive Network Assistant (CNA) is the pop-up browser shown when joining a network that has a captive portal. Note that this option may not work with all vendors, depending on how the captive portal is implemented.
- Access Control**
 - Allowed Access:** Text input field. Description: Enter the IP addresses and networks from which access is permitted.
 - Denied Access:** Text input field. Description: Enter the IP addresses and networks that are denied access.
 - * Deny Behavior:** Dropdown menu set to 'Send HTTP 404 Not Found status'. Description: Select the response of the system to a request that is not permitted.

Table 177: *Web Page Editor, General Properties*

Field	Description
Name	(Required) Name for the page. This name is seen only by administrators in ClearPass Guest.
Page Name	Page name (filename) that will appear in the URL-- for example, "page_name".
Enabled	If selected, enables the page for use.
Description	Optional comments or notes about the page.
Skin	Specifies the skin to use for the Web page. Options include: <ul style="list-style-type: none">● (Default)● Aruba ClearPass Skin● Blank Skin● ClearPass Guest Skin● Custom Skin 1● Custom Skin 2● Galleria Skin● Galleria Skin 2
Title	Title to display on the Web page. To not use a title, leave this field blank.
HTML	HTML content for the page. If you are editing a template or copy of another page, that page's content is shown and can be modified. You can also use the drop-down list to add images or links.
Advanced Settings	If selected, adds advanced configuration options to the form.
Prevent CNA	If selected, enables bypassing the Apple Captive Network Assistant (CNA). The CNA is the pop-up browser shown when joining a network that has a captive portal. This option might not work with all vendors; it is dependent on how the captive portal is implemented.
Allowed Access	IP addresses and networks from which access is allowed. (IPv4 and IPv6 are both supported)
Denied Access	IP addresses and networks that are denied access. (IPv4 and IPv6 are both supported)
Deny Behavior	(Required) Specifies the response shown to the user if their request is denied. Options in this drop-down list include: <ul style="list-style-type: none">● Send HTTP 404 Not Found status● Show Access Denied page● Show a blank page

Receipts



The Receipts area of the user interface lets you customize the receipts that are available to guests and sponsors. To work with receipts configuration, go to **Configuration > Receipts > Start Here**.

This section includes:

- ["Digital Passes" on page 420](#)

- ["Email Receipts and SMTP Services" on page 435](#)
- ["Customizing SMS Receipt" on page 442](#)
- ["Customizing Print Templates " on page 444](#)

Digital Passes



Digital passes are cryptographically signed files containing fields and images that are used as boarding passes, event tickets, coupons, store passes, or other scannable items.

In ClearPass Guest, you can upload and install digital pass certificates, create new templates for digital passes, and use the passes for guest receipts.

To work with digital passes, go to **Configuration > Receipts > Digital Pass Templates**.

This section includes:

- ["About Digital Passes" on page 420](#)
- ["Viewing Digital Pass Certificates" on page 424](#)
- ["Installing Digital Pass Certificates" on page 425](#)
- ["Managing Digital Passes" on page 426](#)
- ["Creating and Editing a Digital Pass Template" on page 427](#)
- ["Example Template Code Variables" on page 433](#)
- ["Images in Digital Passes" on page 434](#)

About Digital Passes

A digital pass is a cryptographically signed file that contains fields and images. When viewed by a user, a pass looks like a simple card, with a front side and a back side. Passes are issued to users as boarding passes, event tickets, coupons, store passes, or other scannable items (for example, a membership pass).

Figure 318 Example Digital Pass: A Boarding Pass



Passes can be organized in Apple Passbook on the user's device. Good visual design practices ensure that each pass can be quickly recognized when displayed amongst other passes. (Apple Passbook is available on Apple iOS 6+ devices.)

Figure 319 Example Apple Passbook



To use a pass such as a membership card or store card, the user selects it from the passbook and displays it so the barcode can be scanned. To use a pass such as a boarding pass or event ticket where date relevance or location relevance was configured, it can be accessed when it becomes active on the lock screen at the relevant time or place.

Passes for Guest Receipts in ClearPass Guest

In ClearPass Guest, you can use passes to provide a guest receipt to a user who has registered using a guest self-registration page. ClearPass Guest supports the pass format specified for the Apple Passbook application.

The front of a guest receipt pass typically shows the site SSID, the username, password, and account expiration time. The back of the pass provides instructions for connecting to the network. It also contains logos and icons, typically those of the organization providing the guest receipt. The exact details of what is written into the guest receipt pass are determined by a pass template.

When the guest has registered and the guest receipt page is displayed, they can click the **Add to Passbook** link. This generates the new guest receipt pass, using fields from the registered guest account such as the username, password, and expiration time. The fields included in the pass, as well as where they are placed and how they are formatted, are determined by the pass template that was selected for the guest self registration. The pass is also cryptographically signed using a Pass Certificate. The generated pass is provided as a download, and the user can add the downloaded pass to their passbook.

Pass Templates

The pass template defines what is written into the pass. You can create, edit, copy, and delete pass templates. For more information, see ["Managing Digital Passes"](#) on page 426 and ["Creating and Editing a Digital Pass"](#)

[Template" on page 427.](#)

Pass templates define:

- Name and a description: Used to identify the template in ClearPass administrative forms and views.
- Style: Boarding Pass, Event ticket, Coupon, Store Pass, or Generic.
- Colors: Foreground, background, and label. If no alternate colors are specified, then default colors will be used. If there are alternate colors specified, then they will be used instead of the default colors.
- Summary: Short description for a voice-over.
- Icon: Displayed on the lock screen. A shine effect is automatically applied to the icon. To select an icon image, it must first be uploaded to the Public Files area of the content manager.
- Logo: Displayed in the top left corner of the front of the pass. To select a logo image, it must first be uploaded to the Public Files area of the content manager.
- Fields: For the front and back of the pass. The information shown on the pass is broken up into fields. Each field is defined by a dictionary which gives it a value and label (which are displayed to the user), a unique key, and optional information about how its value should be formatted.
- Relevant locations (GPS coordinates) and relevant date: Used by Apple Passbook to show a message on the Lock screen where and when the pass becomes relevant.

Many settings for a pass template accept standard template code. This is the same template code that is supported for print templates. This allows an administrator to specify either simple direct values or more complex values based upon the evaluation of template code. All template code is evaluated at the time that the pass is generated from the pass template, using values from the guest receipt as inputs to the pass template.

A pass can contain both a low-resolution version (i.e. for non-Retina displays) and a high-resolution version (i.e. for Retina displays) of each image. If uploaded to the content manager, the high-resolution version of an image is also automatically included in the pass. The high-resolution version must be named with a @2x suffix placed just before the file extension—for example:

Company_Logo.png (low-resolution file name)

Company_Logo@2x.png (high-resolution file name)

Apple Passbook Certificates



You must have a Pass Certificate issued by Apple to be able to generate Apple Passbook passes.

As part of the generation process, the pass is cryptographically signed using a Pass Certificate. A Pass Certificate is a special type of X.509 certificate issued by Apple through the Apple Developer portal. You need a Pass Certificate to cryptographically sign the passes when they are generated and downloaded. This cryptographic signature is verified by Passbook when adding a pass. Passbook will only accept a pass that has been signed by a valid Pass Certificate issued by Apple. To obtain a pass certificate, you must have an Apple developer account. You may register for a developer account at developer.apple.com.

For more information, see ["Viewing Digital Pass Certificates" on page 424](#) and ["Installing Digital Pass Certificates" on page 425](#).

Digital Passes Process Overview

To obtain and install an Apple Passbook certificate:

1. Log in to the Apple Developer portal at developer.apple.com.

2. Register a Pass Type ID for your pass.
3. Create a certificate for your Pass Type ID.
4. Follow the portal's instructions to create a certificate signing request using Keychain Access (a standard Mac OS X application) and submit it to the portal.
5. Download the Pass Type ID certificate.

You also need to provide the private key for the pass certificate. If you created the certificate signing request using Keychain Access:

1. In Keychain Access, locate the private key for the certificate signing request.
2. Export this private key to a Personal Information Exchange (.p12) file.

To install the pass certificate and the associated private key in ClearPass Guest, go to **Configuration > Receipts > Digital Pass Templates** and click the **Install Pass Certificate** link. For more information, see ["Installing Digital Pass Certificates" on page 425](#).

To enable pass downloads:

1. Go to **Configuration > Pages > Guest Self-Registration**, click an enabled guest self registration's row, and then click its **Edit** link.
2. In the diagram, click the **Actions** link for the **Receipt Page**.
3. Scroll down to the **Download Pass** area and set the **Enabled** field to **Display a link enabling download of a guest receipt pass**.
4. Select the template to use (there should be at least one default template available for selection).






Viewing Digital Pass Certificates



You must have a pass certificate in order to generate and download passes. A Pass Certificate is a special type of X.509 certificate issued by Apple through the Apple Developer portal. You need a Pass Certificate to cryptographically sign the passes when they are generated and downloaded. This cryptographic signature is verified by Passbook when adding a pass. Passbook will only accept a pass that has been signed by a valid Pass Certificate issued by Apple.

To view the certificate that will be used to sign Apple Passbook digital passes, go to **Configuration > Receipts > Digital Pass Templates** and click the **View pass certificate** link. If a pass certificate has been installed, this page displays the certificate details.

Figure 320 *The Pass Certificate View*

Pass Certificate	
Certificate Details <i>Details about the certificate and its owner.</i>	
Issued To:	 Pass Type ID: pass.com.arubanetworks.clearpassguest.qa
Valid From:	 Wednesday, 02 October 2013, 1:37 PM
Valid To:	 Thursday, 02 October 2014, 1:37 PM
Subject:	UID pass.com.arubanetworks.clearpassguest.qa Common Name Pass Type ID: pass.com.arubanetworks.clearpassguest.qa Org.Unit 32L6AAH9M5 Organization Aruba Networks, Inc. Country US
Issuer Details <i>Details about the certificate authority that issued the certificate.</i>	
Issued By:	 Apple Worldwide Developer Relations Certification Authority
Issuer:	Country US Organization Apple Inc. Org.Unit Apple Worldwide Developer Relations Common Name Apple Worldwide Developer Relations Certification Authority
Advanced <i>Technical information about the certificate.</i>	
Fingerprint:	0473 99e6 3866 33fa ad45 d996 1753 fd3c 1386 7b18 <i>This is the SHA-1 "fingerprint" or "thumbprint" of the certificate.</i>
Details:	 Show

If no pass certificate is installed yet, no details are displayed. Click the **Upload pass certificate** link to obtain and install a certificate. See "Installing Digital Pass Certificates" on page 425.

Installing Digital Pass Certificates

You must have a valid Pass Certificate issued by Apple in order to generate and download passes. To obtain a pass certificate, you first need an Apple developer account. Developer accounts are free; to register for an account, go to developer.apple.com and click the register link at the bottom of the page.

To obtain the Apple Passbook certificate that will be used to sign digital passes:

1. Log in to the Apple Developer portal at **developer.apple.com**.
2. Register a Pass Type ID for your pass.
3. Create a certificate for your Pass Type ID.
4. Follow the portal's instructions to create a certificate signing request using Keychain Access (a standard Mac OS X application) and submit it to the portal.
5. Download the Pass Type ID certificate.

You also need to provide the private key for the pass certificate. If you created the certificate signing request using Keychain Access:

1. In **Keychain Access**, locate the private key for the certificate signing request.
2. Export this private key to a Personal Information Exchange (.p12) file.

To install the certificate, go to **Configuration > Receipts > Digital Pass Templates** and click the **Install Pass Certificate** link. Step 1 of the **Install Pass Certificate** form opens.

Figure 321 *The Install Pass Certificate Form*

Table 178: *Install Pass Certificate*

Field	Description
Format	Specifies whether you will upload the certificate as a file or paste in the certificate text. The form expands to include the Step 2 options.
Certificate	(Required) For certificates pasted as text, copy and paste the digital certificate's text. This is a block of encoded text and should include the "BEGIN CERTIFICATE" and "END CERTIFICATE" lines. For uploaded certificate files, browse to the certificate to upload. This should be one of the following: PEM encoded X.509 file containing the certificate (*.pem) PKCS#12 encoded file containing both the certificate and the private key (*.p12)
Private Key	(Required) For private keys pasted as text, copy and paste the private key's text. This is a block of encoded text and should include the "BEGIN PRIVATE KEY" and "END PRIVATE KEY" lines. For uploaded private key files, if the certificate file does not include the private key, browse to the private key to upload. The private key should be either a PEM-encoded or a Personal Information Exchange (.p12) file.
Passphrase	Passphrase that was used to encrypt the file containing the private key. If the private key is not encrypted, leave this field blank.
Confirm Passphrase	
Upload Certificate	The certificate is uploaded and the details are displayed on the Pass Certificate page. See Viewing the Digital Pass Certificate.

Managing Digital Passes

Pass properties are defined in pass templates. These properties include name and a description, style (type of pass), colors, summary, icon, logo, fields, relevant locations, relevant date, and associated apps.

To view or work with your list of digital pass templates, go to **Configuration > Receipts > Digital Pass Templates**. The **Pass Templates** list view opens.

Figure 322 *The Digital Pass Templates List View*

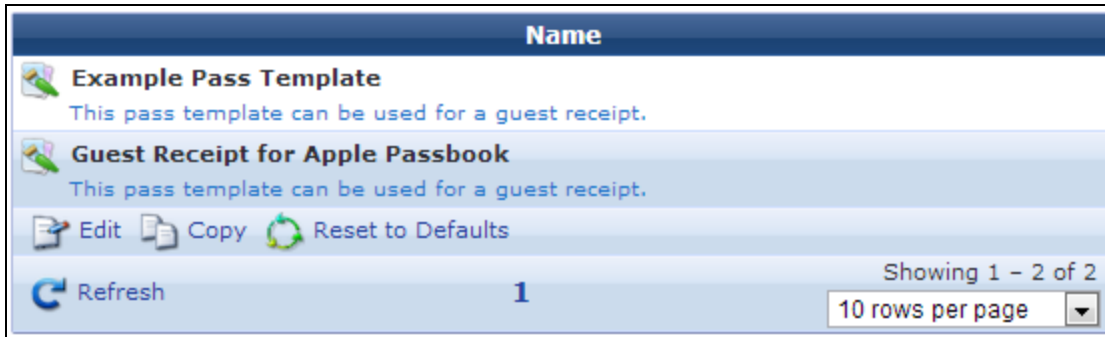


Table 179: *Pass Templates*

Field	Description
Edit	Edit any of the template's properties.
Copy	Make a copy of the template to use as a basis for a new template.
Reset to Defaults	Resets the default template to its original settings if changes were made. (Only available for the default template)
Delete	Deletes the pass template. (The default Guest Receipt template cannot be deleted)
Create a new template	Create a new template.

Creating and Editing a Digital Pass Template

To create or edit a digital pass template, go to **Configuration > Receipts > Digital Pass Templates**, and then click the **Create a new template** link in the upper right corner, or click the **Edit** link for a template in the list. The **Pass Template Settings** form opens.

Defining Basic Properties

Figure 323 *The Pass Template Settings Form, Basic Properties*

Table 180: *Basic Properties, Pass Template Settings*

Field	Description
Name	(Required) Short name that identifies the template clearly. Digital pass template names can include spaces. You may highlight this name and replace it with a new name.
Description	Comments or notes about the template. This description is only seen by administrators.

Defining Pass Properties

Figure 324 The Pass Template Settings Form, Pass Properties Area

Pass Properties	
Background Color:	<input type="text"/> The background color is used for the background of the front and back of the pass. Leave this field blank to use the default background color.
Foreground Color:	<input type="text"/> The foreground color is used for the 'values' of fields shown on the front of the pass. Leave this field blank to use the default foreground color.
Label Color:	<input type="text"/> The label color is used for the 'labels' of fields shown on the front of the pass. Leave this field blank to use the default label color.
* Summary:	<p>i The summary lets VoiceOver make your pass accessible to blind and low vision users.</p> <input type="text" value="{nwa_text id=15601 1=\${site_ssid}WiFi Account for #1{/nwa_text}"/> Enter a short summary for the pass. This text typically contains standard 'template code' that will be evaluated when the pass is generated. Any template code here must produce a summary for a pass to be valid.
* Pass Style:	<p>Generic — a general purpose pass <input type="button" value="v"/> Choose what type of pass you want to generate.</p>
Icon Image:	<p>i This icon will be shown on the lock screen and in notifications and in emails where the pass is attached. It is recommend that the low-resolution version of this image be 29x29 pixels and the '@2x' high-resolution version be 58x58 pixels.</p> <input type="text" value="(Use the default icon)"/> Start typing to select an icon, or leave blank to use the default icon. If available, the '@2x' high-resolution version will also be added to the pass (see the note above).
Logo Image:	<p>i This logo will be shown on the front of the pass, in the top-left corner. It is recommend that the low-resolution version of this image be 50x50 pixels and the '@2x' high-resolution version be 100x100 pixels.</p> <input type="text" value="(Use the default logo)"/> Start typing to select a logo, or leave blank to use the default logo. If available, the '@2x' high-resolution version will also be added to the pass (see the note above).
Logo Text:	<p>i This text is shown alongside the logo at the top of the pass.</p> <input type="text" value="{nwa_text id=15601 1=\${site_ssid}WiFi Account for #1{/nwa_text}"/> Enter the logo text or leave blank for no text. This text typically contains standard 'template code' that will be evaluated when the pass is generated.
Thumbnail Image:	<p>i This image is shown to the right of the primary field. The thumbnail is only shown on an event ticket or a generic pass.</p> <input type="text" value="(Do not include a thumbnail image)"/> Start typing to select a thumbnail image, or leave blank to not include a thumbnail image. If available, the '@2x' high-resolution version will also be added to the pass (see the note above).

For examples of variables that can be used in the **Summary** and **Logo Text** fields described in the following table, click the **Example 'template code' replacements** link above the form, or see "Example Template Code Variables" on page 433.

For a list of image fields supported by each of the different pass styles, click the **A note regarding images and icons** link above the form, or see "Images in Digital Passes" on page 434.

Table 181: Pass Properties, Pass Template Settings

Field	Description
Background Color	Color used for the background of both the front and back of the pass. To use the default color, leave this field blank.
Foreground Color	Color used for the "values" field on the front of the pass. To use the default foreground color, leave this field blank.
Label Color	Color used for the labels of fields shown on the front of the pass. To use the default label color, leave this field blank.
Summary	(Required) Short summary for the pass. This lets VoiceOver make the pass accessible to blind and low-vision users. Summary text typically contains standard template code that is evaluated when the pass is generated. Template code entered here must produce a summary for the pass to be valid.
Pass Style	(Required) Specifies the style of pass to generate. Options include: <ul style="list-style-type: none"> ● Generic — a general purpose pass ● Boarding Pass (e.g., airline, boat, bus, train) ● Coupon (e.g., coupon, special offer, discount) ● Event Ticket (e.g., conference, sporting event, concert, movie) ● Store Card (e.g., loyalty, discount, points, gift)
Icon Image	Icon shown on the lock screen and in notifications and emails where the pass is attached. To use the default icon, leave this field blank. The low-resolution version of the icon image should be 29 x 29 pixels. If an "@2x" high-resolution version is available, it will also be added to the pass. The "@2x" high-resolution version should be 58 x 58 pixels.
Logo Image	Logo shown at the top-left corner of the front of the pass. To use the default logo, leave this field blank. The low-resolution version of the logo image should be 50 x 50 pixels. If an "@2x" high-resolution version is available, it will also be added to the pass. The "@2x" high-resolution version should be 100 x 100 pixels.
Logo Text	Text shown next to the logo at the top of the pass. To have no text next to the logo, leave this field blank. Logo text typically contains standard template code that is evaluated when the pass is generated.
Thumbnail Image	Image shown to the right of the primary field. To have no thumbnail image, leave this field blank. The thumbnail image is only shown on the Event Ticket or Generic pass styles. If an "@2x" high-resolution version is available, it will also be added to the pass.
Transit Type	Transport type for a Boarding Pass style of pass. Options include Air, Boat, Bus, Generic, or Train . The icon corresponding to the selected type of transit will be shown on the front of the pass between the first two primary fields.

Field	Description
Footer Image	Image shown below all of the fields on the front of a Boarding Pass style of pass. To have no footer image, leave this field blank. If an "@2x" high-resolution version is available, it will also be added to the pass.
Strip Image	Image shown behind the primary field on the front of the pass. To have no strip image, leave this field blank. The strip image is only used on the Coupon, Event Ticket, or Store Card pass styles. The low-resolution version of the strip image should be 312 x 84 pixels for Event Tickets, and 312 x 123 for Store Card and Coupon pass styles. If an "@2x" high-resolution version is available, it will also be added to the pass. The "@2x" high-resolution version of the strip image should be double the width and height of the low-resolution version for each pass style.
Background Image	Image shown as a background on the front of an Event Ticket. If a background image is specified, any background color that was specified will be ignored. To have no background image, leave this field blank. The background image is only shown on the Event Ticket pass style. If an "@2x" high-resolution version is available, it will also be added to the pass.

Defining Pass Fields

Figure 325 *The Pass Template Settings Form, Pass Fields Area*

Pass Fields					
Add new field					
	Field	Value	Mode	Type	Location
	site_ssid This field will show the SSID of the network that the user should connect to.	{site_ssid}	Optional	Default	Primary
	username This field will show the user's username.	{\$.username}	Optional	Default	Secondary
Edit Disable Move Up Move Down Delete					
	password This field will show the user's password.	{\$.password}	Optional	Default	Secondary
	expire_time This field will show the relative time at which the user's account will expire. If the account will not expire, this field will be removed from the pass.	{\$.expire_time}	Optional	Date	Auxiliary
* Fields	welcome_detail This field will provide the user with a welcome message.	{nwa_text id=15598 1=\$.username}Welcome %1, your account ha...	Optional	Default	Back
	network_detail This field shows the SSID, and if applicable, the associated WPA key.	{if site_ssid}{site_ssid}{if site_wpa_key}{nwa_text id=...	Optional	Default	Back
	instructions This field will provide the user with more detailed instructions on how to connect to the network.	{nwa_text id=15594 1=site_ssid 2=\$.username 3=\$.password}...	Optional	Default	Back
	expire_detail This field will show the absolute time at which the user's account will expire. If the account will not expire, this field will be removed from the pass.	{\$.expire_time}	Optional	Date	Back
	self_service_url This field will provide the self-service portal URL. If the portal is not enabled, this field will be removed from the pass.	{self_service_url}	Optional	Default	Back

Table 182: *Pass Fields, Pass Template Settings*

Field	Description
Fields	(Required) List of fields currently included in this pass template, with descriptions. You can click a field's row for configuration options.
Edit	Opens the Field Properties editor, where you can enable the field and modify its placement, content, and presentation properties.
Disable	Disables the field for the pass. To enable it again, click its Enable link.

Field	Description
Move Up	Fields are shown in this list in their rank order. You can use the Move Up and Move Down links to modify the order.
Move Down	
Delete	Deletes a field from this pass template. You will be asked to confirm the deletion.
Add new field	Lets you add and configure a new field. The row expands to include the Field Properties form.

Defining Relevant Locations

When a relevant location is configured and enabled, the pass can be displayed on the user's lock screen when they arrive within a radius of the specified coordinates — for example, a Boarding Pass can be displayed when the user arrives at a station or airport. The size of the location's radius is determined by the pass style.

Figure 326 *The Pass Template Settings Form, Relevant Locations Area*

Relevant Locations

Relevant Locations: Add 'relevant locations' to the pass
Check this box to show the pass on the user's lock screen when near a given location. Passbook determines the appropriate distance around the locations that the pass will appear on the lock screen.

Location Limit: **10**
A pass may only contain 10 (ten) locations. Each location below will be evaluated, but only the first 10 valid locations will be included in the pass.

* Locations:

Name	Latitude	Longitude	Altitude	Message	Status	Mode
There are no locations defined.						

Add, edit or remove locations from the template.

Table 183: *Relevant Locations, Pass Template Settings*

Field	Description
Relevant Locations	If selected, shows the digital pass on the user's lock screen when near a given location. Passbook determines the appropriate distance around the location for the pass to be displayed on the lock screen.
Location Limit	A pass template may only contain 10 locations. More may be added here, but only the first 10 valid locations will be included in the pass.
Locations	(Required) Lists the locations that have been defined for this pass template.
Add new location	Lets you add and configure a new location. The row expands to include the Location Properties form.

Defining Relevant Dates

When a relevant date is configured and enabled, the pass can be displayed on the user's lock screen during an appropriate window of time—for example, an Event Ticket pass would be displayed within the time window for entry to the event. The length of the time window is determined by the pass style.

If the result of processing a 'date' field is a number, then that number will be interpreted as a UNIX timestamp (i.e. the number of seconds since the UNIX epoch of 1st January 1970 00:00:00 GMT). A UNIX timestamp of 0 (zero) or less will be treated the same as an empty value.

If the result of processing a 'date' field is textual (i.e. not a number and not empty), then the text will be converted to a valid date and time value. If conversion fails, or if the date is on or prior to the 1st January 1970 00:00:00 GMT (i.e. a UNIX timestamp of 0 or less), then the field will be treated as though it were empty.

If you set a relevant date for a Generic pass template, it must also include a relevant location.

For examples of variables that can be used in the **Date** field described in the following table, click the **Example 'template code' replacements** link above the form, or see "Example Template Code Variables" on page 433.

Figure 327 *The Pass Template Settings Form, Relevant Date Area*

Relevant Date	
Relevant Date:	<input checked="" type="checkbox"/> Add a 'relevant date' to the pass Check this box to show the pass on the user's lock screen near to a given date. Passbook determines the appropriate duration of time around the date that the pass will appear on the lock screen. Alternatively, or additionally, you may also configure any 'date' pass field above as a 'relevant date'.
Date and Location:	<input type="checkbox"/> A generic pass must also contain relevant locations for a relevant date to have effect. See the note above, regarding the relevant date and relevant locations.
* Date Mode:	<input type="text" value="Required — the pass will not be generated if the value is empty"/> Choose whether a date for this field is required or optional.
Date Rank:	<input type="text" value="1"/> If there are multiple fields that provide a 'relevant date', they will be processed by rank in ascending order. The first field that, when processed, yields a valid date will be selected as the 'relevant date' for the pass.
Date:	<input type="text"/> Enter the 'relevant date' text or leave blank for no value. This text typically contains standard 'template code' that will be evaluated when the pass is generated.
Date Fields:	<input type="checkbox"/> If the result of processing a 'date' field is a number, then that number will be interpreted as a UNIX timestamp (i.e. the number of seconds since the UNIX epoch of 1st January 1970 00:00:00 GMT). A UNIX timestamp of 0 (zero) or less will be treated the same as an empty value. <input type="checkbox"/> If the result of processing a 'date' field is textual (i.e. not a number and not empty), then the text will be converted to a valid date and time value. If conversion fails, or if the date is on or prior to the 1st January 1970 00:00:00 GMT (i.e. a UNIX timestamp of 0 or less), then the field will be treated as though it were empty.

Table 184: *Relevant Dates, Pass Template Settings*

Field	Description
Relevant Date	If selected, shows the digital pass on the user's lock screen when near a given date. Passbook determines the appropriate span of time around the date for the pass to be displayed on the lock screen. You can also edit a date type field in the Pass Fields area of the form to be a relevant date.
Date and Location	If the template is a Generic pass style, a relevant location must also be included in order for a relevant date to take effect.
Date Mode	(Required) Specifies whether a date for this field is required or optional. Options include: <ul style="list-style-type: none"> • Optional — The pass can still be generated even if no value is supplied for the date field • Required — The pass will not be generated if the value for the date field is empty
Date Rank	Rank order for processing the date field defined here. If multiple relevant date fields are included in the template, they are processed in ascending order, and the first field that has a valid date will be the relevant date for the pass.
Date	Text for the relevant date. For no value, leave this field empty. Date text typically contains standard template code that is evaluated when the pass is generated.
Date Fields	If the result of processing a date field is a number, the number is interpreted as a UNIX timestamp. If the result of processing a date field is textual (not a number and not empty), the text is converted to a valid date and time value.

Defining Associated Apps

Multiple associated apps can be added. An Apple ID must be provided for each app. Although multiple associated apps may be referenced by a pass, a link is displayed on the back of the pass only for the first app

that is compatible with the device. If the app is installed on the device, the link displayed on the pass opens the app. If the app is not installed on the device, the link opens the App Store at that app.

Figure 328 *The Pass Template Settings Form, Associated Apps Area*

Table 185: *Associated Apps, Pass Template Settings*

Field	Description
Associated Apps	If selected, shows an associated application on the back of the pass. Passbook determines the appropriate distance around the location for the pass to be displayed on the lock screen.
First Compatible App	Multiple associate apps can be referenced by a pass, but only the first app that is compatible with the current device will have a link shown on the back of the pass. If the app is installed on the device, that link will open the app. If the app is not installed, the link will open the app store and show the app.
Apps	(Required) Lists the associated apps that are referenced by this pass template.
Add new app	Lets you add and configure a new app. The row expands to include the App Properties form.

When you have completed your entries on this page, click **Save Changes**. The new service is created and displayed in the **IP Phone Services** list.

Example Template Code Variables

When you create or edit a digital pass template, many of the settings accept standard template code. This is the same code that is supported for print templates. This allows you to specify either simple direct values or more complex values based upon the evaluation of template code. All template code is evaluated when the pass is generated from the pass template, using values from the guest receipt as inputs to the pass template.

The illustration below shows some of the special variables that can be used in the pass template fields that accept template code. This variables list is also available when you go to **Configuration > Receipts > Digital Pass Templates**, click the **Edit** or **Create** link, and then click the **Example 'template code' replacements** link. Variables are available for user fields and certificate fields.

Figure 329 *Template Code Variables Available for Digital Passes*

Variable	Description	Example
User Fields		
{\$.username}	User account name	12345678
{\$.password}	User account password	87654321
{\$.enabled}	Non-zero if the guest account is enabled	1
{\$.role_name}	Role assigned to guest account	Guest
{\$.start_time}	Time at which the guest account will become active	1155772123
{\$.expire_time}	Time at which the guest account will expire	1155858523
{\$.expire_postlogin}	Lifetime of the guest account login in minutes after login	120
{\$.visitor_name}	User's name	Susan Guest
{\$.visitor_company}	User's company name	Acme Sprockets
{\$.sponsor_name}	Sponsor's name	John Sponsor
{\$.custom_field}	Custom fields attached to the account	
{\$.action}	Action taken on account (create, delete or edit)	create
{\$.source}	Source of account action (create_user, reset_password, etc.)	create_user
{\$.result.error}	Non-zero if an error occurred while creating the guest account	0
{\$.result.message}	Message related to the account creation	
{\$.timestamp}	Time at which the receipt was generated	1155752000
{\$.site_ssid}	SSID of the wireless LAN	
{\$.site_wpa_key}	WPA key for the wireless LAN	
Certificate Fields		
{\$.c.username}	Username stored in the certificate	user0
{\$.c.device_type}	Device type stored in the certificate	iOS
{\$.c.device_udid}	Device UDID stored in the certificate	123456789abcdef0123456789abcdef0123456789a
{\$.c.device_imei}	Device IMEI stored in certificate	1123456789012345
{\$.c.device_iccid}	Device ICCID stored in the certificate	1234567890123456789
{\$.c.mac_address}	MAC address stored in the certificate	01:23:45:67:89:ab
{\$.c.product_name}	Product name stored in the certificate	iPad2,1
{\$.c.product_version}	Product version stored in the certificate	10B329
{\$.c.custom_field}	Custom field(s) stored in the certificate	field1=a,field2=b
{\$.c.email_address}	Email address stored in the certificate	test@example.com
{\$.c.valid_from}	Time at which the certificate becomes valid	1155772123
{\$.c.valid_to}	Time at which the certificate expires	1155858523
{\$.c.page_name}	Name of the page at which a new certificate can be provisioned	device_provisioning

Images in Digital Passes

To make images available for selection, they must first be uploaded to the **Public Files** area in **Content Manager**.

The images supported by each style of pass are shown below. This images list is also available when you go to **Configuration > Receipts > Digital Pass Templates**, click the **Edit** or **Create** link, and then click the **A note regarding images and icons** link.

Figure 330 Images Supported by Each Style of Pass

	Icon	Logo	Background	Thumbnail	Strip	Footer
Boarding Pass	✓	✓	✗	✗	✗	✓
Coupon	✓	✓	✗	✗	✓	✗
Event Ticket (without strip image)	✓	✓	✓	✓	✗	✗
Event Ticket (with strip image)	✓	✓	✗	✗	✓	✗
Generic Pass	✓	✓	✗	✓	✗	✗
Store Card	✓	✓	✗	✗	✓	✗

Only PNG image files (*.png) are supported by passes.

A pass can contain both a low-resolution version (i.e. for non-Retina displays) and a high-resolution version (i.e. for Retina displays) of each image. If it has been uploaded to the content manager, the high-resolution version of an image is also automatically included in the pass. The high-resolution version must be named with the suffix **@2x** at the end of the filename, just before the file extension—for example:

- Company_Logo.png (low-resolution filename)
- Company_Logo@2x.png (high-resolution filename)

Email Receipts and SMTP Services



With SMTP Services, you can configure ClearPass Guest to send customized guest account receipts to visitors and sponsors by email. Email receipts may be sent in plain text or HTML format. You may also send email receipts using any of the installed skins to provide a look and feel.

To use the email sending features, you must have the **SMTP Services Plugin** installed.


This section includes:

- ["About Email Receipts" on page 435](#)
- ["Configuring Email Receipts " on page 438](#)
- ["Email Receipt Options" on page 438](#)
- ["About Customizing SMTP Email Receipt Fields" on page 440](#)

About Email Receipts



You can send email receipts for guest accounts that are created using either sponsored guest access or self-provisioned guest access. This is convenient in situations where the visitor may not be physically present to receive a printed receipt.

ClearPass Guest may be configured to automatically send email receipts to visitors, or to send receipts only on demand. Email receipts may be sent manually from the guest account receipt page by clicking the  **Send email receipt** link displayed there.

When using guest self-registration, the email delivery options available for the receipt page actions allow you to specify the email subject line, the print template and email format, and other fields relevant to email delivery.


To configure these email delivery options:

1. Go to **Configuration > Pages > Guest Self-Registrations**. Click to expand the **Guest Self-Registration** row in the form, and then click its **Edit** link. The **Customize Guest Self-Registration** diagram opens.
2. In the **Receipt Page** area, click the **Actions** link. The **Receipt Actions** form opens.
3. Scroll to the **Email Delivery** section of the form and choose one of the options from the **Enabled** drop-down list. The form expands to include configuration options for email delivery.

Figure 331 *The Actions Link on the Workflow Diagram*



Figure 332 *The Customize Guest Registration Form, Email Delivery Area*

 Email Delivery	
Enabled:	Always auto-send guest receipts by email ▼
* Email Field:	(Use Default: email) ▼ The field containing the visitor account's email address.
Subject Line:	<input type="text"/> Template specifying the subject line for emailed visitor account receipts. Leave blank to use the default (Visitor account receipt for {\$email})
* Email Receipt:	(Use Default: GuestManager Receipt) ▼ The plain text or HTML print template to use when generating an email receipt.
* Email Skin:	(Use Default: Use the default skin) ▼ The format in which to send email receipts.
* Send Copies:	(Use Default: Use 'Bcc:' if sending to a visitor) ▼ Specify when to send visitor account receipts to the recipients in the Copies To list.
Copies To:	default An optional list of email addresses to which copies of visitor account receipts will be sent. Enter '_admin' to have the email sent to the sponsor's email address.
Reply-To:	<input checked="" type="checkbox"/> Allow the reply-to address to be overridden If checked, the reply-to address will be overridden by the sponsor_email field. Leave unchecked to use the global from address.
Override From:	<input type="checkbox"/> Override the from address instead of using reply-to If checked, the from address will be overridden in lieu of the reply-to value above. Note, this feature may require configuration on your mail server to allow the override.

The options shown in [Table 186](#) are available in the **Enabled** drop-down list to control email delivery. For more information on configuring these options, see "Editing Receipt Actions" on page 358.

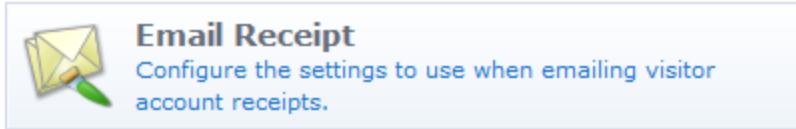
Table 186: *Email Delivery Options, Customize Guest Self-Registration*

Field	Description
Disable sending guest receipts by email	Email receipts are never sent for a guest registration.
Always auto-send guest receipts by email	An email receipt is always generated using the selected options, and is sent to the visitor's email address.
Auto-send guest receipts by email with a special field set	If the Auto-Send Field is set to a non-empty string or a non-zero value, an email receipt is generated and sent to the visitor's email address. The auto-send field can be used to create an "opt-in" facility for guests. Use a check box for the auto_send_sms field and add it to the create_user form, or a guest self-registration instance, and SMS messages are sent to the specified phone number only if the check box has been selected.
Display a link enabling a guest receipt via email	A link is displayed on the receipt page; if the visitor clicks this link, an email receipt is generated and sent to the visitor's email address.
Send an email to a list of fixed addresses	An email receipt is always generated using the selected options, and is sent only to the list of email addresses specified in the "Copies To" field.

Configuring Email Receipts



You can configure the default settings used when generating an email receipt by going to **Configuration > Receipts > Email Receipt**.



See "Email Receipt Options" on page 438 for details about the email receipt options.

Email Receipt Options

The **Customize Email Receipt** form may be used to set default options for visitor account email receipts. To configure email receipt options, go to **Configuration > Receipts > Email Receipt**. The **Customize Email Receipt** form opens.

Figure 333 *The Customize Email Receipt Form*

Customize Email Receipt	
Receipt Options Select options for the email receipt.	
Subject Line:	<input type="text" value="Visitor account receipt for {Email}"/> Template specifying the subject line for visitor account receipts sent by email.
* Email Receipt:	<input type="text" value="GuestManager Receipt"/> The plain text or HTML print template to use when generating an email receipt.
* Skin:	<input type="text" value="Use the default skin"/> The format in which to send email receipts.
Copies To:	<input type="text"/> An optional list of email addresses to which copies of visitor account receipts will be sent. Enter '_admin' to have the email sent to the sponsor's email.
* Send Copies:	<input type="text" value="Use 'Bcc:' if sending to a visitor"/> Specify when to send visitor account receipts to the recipients in the Copies To list.
Reply-To:	<input type="checkbox"/> Allow the reply-to address to be overridden per operator If checked, the reply-to address will be overridden by the sponsor_email field of a user, or the admin's email. Leave unchecked to use the global from address.
Fields Select the visitor account fields related to the email receipt.	
* Email Field:	<input type="text" value="email"/> The field containing the visitor account's email address.
* Auto-Send Field:	<input type="text" value="auto_send_smtp"/> The field which, if it contains a non-empty string or non-zero value, will cause an account receipt email to be automatically sent upon creation of a visitor account.
Test Mail Settings Send a test mail message.	
To:	<input type="text"/> To send a test message, enter the recipient's address.
<input type="button" value="Send Test Message"/> <input type="button" value="Save and Close"/>	

Table 187: The Customize Email Receipt Form

Field	Description
Subject Line	May contain template code, including references to guest account fields. The default value, Visitor account receipt for { \$email } , uses the value of the email field. See " Smarty Template Syntax " on page 700 for more information on template syntax.
Email Receipt	(Required) Specifies the plain text or HTML template to use for the email receipt.
Skin	<p>(Required) Specifies the skin to use to provide the basic appearance of the email. Options include:</p> <ul style="list-style-type: none"> ● No skin – Plain text only – A skin is not used, and the email will be sent in plain text format. Use this option to remove all formatting from the email. ● No skin – HTML only – A skin is not used, but the email will be sent in HTML format. Use this option to provide a basic level of formatting in the email. ● No skin – Native receipt format – A skin is not used. The email will be sent in either plain text or HTML format, depending on the type of print template that was selected. ● Use the default skin – The skin currently marked as the default skin is used. ● Aruba ClearPass Skin ● Blank Skin ● ClearPass Guest Skin ● Custom Skin 1 ● Custom Skin 2 ● Galleria Skin ● Galleria Skin 2 <p>When sending an email message using HTML formatting, the images and other resources required to display the page will be included in the message.</p>
Copies To	Creates a list of additional email addresses that are designated to receive copies of the generated email receipts. To have the email receipt sent to the sponsor's email address, enter the keyword _admin in this field. In this case the email receipt will be sent to the current operator.
Send Copies	<p>(Required) Specifies how copies of the email receipts will be sent to the additional email addresses listed in the Copies To field:</p> <ul style="list-style-type: none"> ● Do not send copies – The Copies To list is ignored and email is not copied. ● Always send using 'cc:' – The Copies To list is always sent a copy of any guest account receipt (even if no guest account email address is available). ● Always send using 'bcc:' – The Copies To list is always sent a blind copy of any guest account receipt (even if no guest account email address is available). ● Use 'cc:' if sending to a visitor – If a guest account email address is available, the email addresses in the Copies To list will be copied. ● Use 'bcc:' if sending to a visitor – If a guest account email address is available, the email addresses in the Copies To list will be blind copied.
Reply-To	If selected, the Reply-To address will be overridden by the sponsor_email field of the user, or by the admin's email. When you select this check box, the

Field	Description
	Override From field is added to the form. To use the global From Address, do <i>not</i> select the check box in this field.
Override From	If selected, overrides the From Address instead of using the Reply-To value.
Email Field	(Required) Specifies the field that will contain the visitor's email address.
Auto-Send Field	(Required) Specifies the field that will cause an account receipt email to be automatically sent when a visitor account is created. The email receipt will only be sent if the field selected here contains a non-empty string of non-zero value.
Test Mail Settings	To preview and verify the appearance of the email receipt, you can send yourself or another person a test message. Enter the test message recipient's email address, then click Send Test Message . The test message is sent immediately.

Figure 334 Example of Email Receipt Test Message Content

Welcome **Test Receipt**, your account has been created and is now ready to use.



WiFi Network: Aruba

Visitor Account and Wi-Fi Instructions:

- 1 Make sure your wireless adapter is set to dynamically obtain an IP address
- 2 Connect to the wireless network: **Aruba**
- 3 Enter credentials:
 - Username: *test@example.com*
 - Password: **password**
- 4 Account expires: Friday, December 7, 2012 12:32

Copyright © 2012 Aruba Networks, Inc. All rights reserved.

About Customizing SMTP Email Receipt Fields

The behavior of email receipt operations can be customized with certain guest account fields. You do this on a per-user basis.

Table 188: SMTP Email Receipt Fields

Field	Description
smtp_enabled	May be set to a non-zero value to enable sending an email receipt. If unset, the default value from the email receipt configuration is used. The special values “_Auto” (Always auto-send guest receipts by email), “_AutoField” (Auto-send guest receipts by email with a special field set), “_Click” (Display a link enabling a guest receipt via email), and “_Cc” (Send an email to a list of fixed addresses) may also be used.
smtp_subject	Specifies the subject line for the email message. Template variables appearing in the value will be expanded. If the value is “default”, the default subject line from the email receipt configuration is used.
smtp_template_id	Specifies the print template ID to use for the email receipt. If blank or unset, the default value from the email receipt configuration is used.
smtp_receipt_format	Specifies the email format to use for the receipt. It may be one of “plaintext” (No skin – plain text only), “html_embedded” (No skin – HTML only), “receipt” (No skin – Native receipt format), “default” (Use the default skin), or the plugin ID of a skin plugin to specify that skin. If blank or unset, the default value from the email receipt configuration is used.
smtp_email_field	Specifies the name of the field that contains the visitor’s email address. If blank or unset, the default value from the email receipt configuration is used. Additionally, the special value “_None” indicates that the visitor should not be sent any email.
smtp_auto_send_field	Specifies the name of the field that contains the auto-send flag. If blank or unset, the default value from the email receipt configuration is used. Additionally, the special values “_Disabled” and “_Enabled” may be used to never send email or always send email, respectively.
smtp_cc_list	Specifies a list of additional email addresses that will receive a copy of the visitor account receipt. If the value is “default”, the default carbon-copy list from the email receipt configuration is used.
smtp_cc_action	Specifies how to send copies of email receipts. It may be one of “never”, “always_cc”, “always_bcc”, “conditional_cc”, or “conditional_bcc”. If blank or unset, the default value from the email receipt configuration is used.

Logic for Sending Email Receipts

The logic used to send an email receipt is:

- If email receipts are disabled, take no action.
- Otherwise, check the auto-send field.
 - If it is “_Disabled” then no receipt is sent.
 - If it is “_Enabled” then continue processing.
 - If it is any other value, assume the **auto-send** field is the name of another guest account field. Check the value of that field, and if it is zero or the empty string then no receipt is sent.
- Determine the email recipients:
 - Address the email to the value specified by the **email** field in the visitor account. If the **email** field is “_None” then do not send an email directly to the visitor.
 - Depending on the value of the Send Copies setting, add the email addresses from the Copies To: list to the email’s “Cc:” or “Bcc:” list.

- If there are any “To:”, “Cc:” or “Bcc:” recipients, generate an email message using the specified print template and send it to the specified recipient list.
- Additional options and considerations are described in the following table:

Table 189: *Logic for Email Receipts: Additional Options*

Field	Description
smtp_warn_before_subject	This field overrides what is specified in the subject line under Logout Warnings on the email receipt. If the value is “default”, the default subject line under the Logout Warnings section on the email receipt configuration is used.
smtp_warn_before_template_id	This field overrides the print template ID specified under Logout Warnings on the email receipt. If the value is “default”, the default template ID under the Logout Warnings section on the email receipt configuration is used.
smtp_warn_before_receipt_format	This field overrides the email format under Logout Warnings to use for the receipt. It may be one of “plaintext” (No skin – plain text only), “html_embedded” (No skin – HTML only), “receipt” (No skin – Native receipt format), “default” (Use the default skin), or the plugin ID of a skin plugin to specify that skin. If blank or unset, the default value in the Email Field under the Logout Warnings on the email receipt configuration is used.
smtp_warn_before_cc_list	This overrides the list of additional email addresses that receive a copy of the visitor account receipt under Logout Warnings on the email receipt. If the value is “default”, the default carbon-copy list under Logout Warnings from the email receipt configuration is used.
smtp_warn_before_cc_action	This field overrides how copies are sent as indicated under Logout Warnings on the email receipt. to send copies of email receipts. It may be one of “never”, “always_cc”, “always_bcc”, “conditional_cc”, or “conditional_bcc”. If blank or unset, the default value from the email receipt configuration is used.
warn_before_from_sponsor	This field overrides the Reply To field (that is, the sponsor_email field of a user, or the admin’s email) under the Logout Warnings on the email receipt. If the value is “default”, the Reply To field under Logout Warnings from the email receipt configuration is used.
warn_before_from	This field overrides the Override From field under the Logout Warnings on the email receipt. If the value is “default”, the Override From field under Logout Warnings from the email receipt configuration is used.

Customizing SMS Receipt

To configure SMS receipt options, go to **Configuration > Receipts > SMS Receipt**. The **Customize SMS Receipt** page opens.

The fields described below are for the SMS plugin configuration page. Use the SMS receipt page for further customization. For information on standard SMS services, see ["SMS Services" on page 453](#).

Figure 335 *The Customize SMS Receipt Form*

Table 190: *Customize SMS Receipt Form*

Field	Description
SMS Receipt	Specifies the plain text format print template to use when generating an SMS receipt. Options include: <ul style="list-style-type: none"> • Download Receipt • SMS Receipt • SMS Sponsor Confirmation Alert
Phone Number Field	Specifies the field that contains the guest's phone number.
Auto-Send Field	Specifies the field that, if it contains a non-empty string or a null value, will cause an account receipt SMS to be automatically sent when the guest account is created.
Save Configuration	Saves your changes on this form and returns you to the Start Here page of the Configuration module.

SMS Receipt Fields

The behavior of SMS receipt operations can be customized with certain guest account fields. You can override global settings by setting these fields.

- **sms_enabled** – This field may be set to a non-zero value to enable sending an SMS receipt. If unset, the default value is true.
- **sms_handler_id** – This field specifies the handler ID for the SMS service provider. If blank or unset, the default value from the SMS plugin configuration is used.
- **sms_template_id** – This field specifies the print template ID for the SMS receipt. If blank or unset, the default value from the SMS plugin configuration is used.
- **sms_phone_field** – This field specifies the name of the field that contains the visitor's phone number. If blank or unset, the default value from the SMS plugin configuration is used.

- **sms_auto_send_field** – This field specifies the name of the field that contains the auto-send flag. If blank or unset, the default value from the SMS plugin configuration is used. Additionally, the special values “_Disabled” and “_Enabled” may be used to never send an SMS or always send an SMS, respectively.

The logic used to send an SMS receipt is:

- If SMS receipts are disabled, take no action.
- Otherwise, check the auto-send field.
 - If it is “_Disabled” then no receipt is sent.
 - If it is “_Enabled” then continue processing.
 - If it is any other value, assume the **auto-send** field is the name of another guest account field. Check the value of that field, and if it is zero or the empty string then no receipt is sent.
- Determine the phone number – if the **phone number** field is set and the value of this field is at least 7 characters in length, then use the value of this field as the phone number. Otherwise, if the value of **the auto-send** field is at least 7 characters in length, then use the value of this field as the phone number.
- If the phone number is at least 7 characters long, generate a receipt using the specified plain-text print template and send it to the specified phone number.



ClearPass Guest 3.9 and earlier used www.amigopod.com for a number of actions, including updates, SMS, and network diagnostics. The address used now is clearpass.arubanetworks.com. If you have opened host-specific openings in your firewall for the ClearPass appliance, please update them to the new name.

Customizing Print Templates

Print templates are used to define the format and appearance of a guest account receipt. To work with print templates, go to **Configuration > Receipts > Templates**. The **Guest Manager Print Templates** list view opens. All print templates you have created are included in the list. Information shown for each template includes its name for internal identification, format, and status.

Figure 336 *The Guest Manager Print Templates List View*

△ Name	Format	Status
Account List	List	Enabled
Certificate Expiry	Page	Enabled
Download Receipt	Plain Text	Enabled
GuestManager Receipt	Page	Enabled
One account per page	Page	Enabled
SMS Receipt	Plain Text	Enabled
Sponsorship Confirmation	Page	Enabled
Two-column scratch cards	2-column list	Enabled

8 print templates Reload Show all rows ▾

You can click a print template's row in the list for additional options:

Table 191: *Guest Manager Print Templates List View*

Field	Description
Edit	Edit the print template. The Edit Print Template page opens. See " Creating New Print Templates " on page 445.
Duplicate	Creates a copy of the print template that you can use as the basis of a new template.
Delete	Deletes the print template. You will be asked to confirm the deletion.
Preview	The template's row expands to display a preview of the print template as the user would see it.
Show Usage	The template's row expands to show a list of the receipts that currently use the template. You can click an item in the list to edit it.
Permissions	The Edit Print Template Permissions form opens, where you can modify which operator profiles and other users have access to the print template.
Edit code	This option is available if a print template was created using the wizard but has since been modified. See " Modifying Wizard-Generated Templates " on page 451 for further information.
Create new print template using wizard	Create a new template using the wizard. The Print Template Wizard (new) page opens. See " Print Template Wizard " on page 448.
Create new print template	Create a new print template. The Create Print Template page opens. See " Creating New Print Templates " on page 445.

Options to show where a print template is being used, and to control individual permissions for a print template, are also available when selecting a print template. See "[Setting Print Template Permissions](#)" on page 451.

Plain text print templates may be used with SMS services to send guest account receipts; see "[About SMS Guest Account Receipts](#)" on page 461 for details. Because SMS has a 160 character limit, the number of characters used in the plain text template will be displayed below the preview. If you are including a guest account's email address in the SMS, remember to allow for lengthy email addresses (up to 50 characters is a useful rule of thumb).

Creating New Print Templates

To define a new print template, go to **Configuration > Receipts > Templates** and click the  **Create new print template** link in the upper-right corner. The **Create Print Template** page opens. This page has two parts.

The first part provides a list of the variables that can be used in the template together with their meaning and an example of each. User and certificate fields are available for print templates.

Figure 337 *Template Code Variables Available for Print Templates*

Variable	Description	Example
User Fields		
{ \$u.username }	User account name	12345678
{ \$u.password }	User account password	87654321
{ \$u.enabled }	Non-zero if the guest account is enabled	1
{ \$u.role_name }	Role assigned to guest account	Guest
{ \$u.start_time }	Time at which the guest account will become active	1155772123
{ \$u.expire_time }	Time at which the guest account will expire	1155858523
{ \$u.expire_postlogin }	Lifetime of the guest account login in minutes after login	120
{ \$u.visitor_name }	User's name	Susan Guest
{ \$u.visitor_company }	User's company name	Acme Sprockets
{ \$u.sponsor_name }	Sponsor's name	John Sponsor
{ \$u.custom_field }	Custom fields attached to the account	
{ \$action }	Action taken on account (create, delete or edit)	create
{ \$source }	Source of account action (create_user, reset_password, etc.)	create_user
{ \$result.error }	Non-zero if an error occurred while creating the guest account	0
{ \$result.message }	Message related to the account creation	
{ \$timestamp }	Time at which the receipt was generated	1155752000
{ \$site_ssid }	SSID of the wireless LAN	Aruba
{ \$site_wpa_key }	WPA key for the wireless LAN	
Certificate Fields		
{ \$c.username }	Username stored in the certificate	user0
{ \$c.device_type }	Device type stored in the certificate	iOS
{ \$c.device_udid }	Device UDID stored in the certificate	123456789abcdef0123456789abcdef0123456789a
{ \$c.device_imei }	Device IMEI stored in certificate	1123456789012345
{ \$c.device_iccid }	Device ICCID stored in the certificate	1234567890123456789
{ \$c.mac_address }	MAC address stored in the certificate	01:23:45:67:89:ab
{ \$c.product_name }	Product name stored in the certificate	iPad2,1
{ \$c.product_version }	Product version stored in the certificate	10B329
{ \$c.custom_field }	Custom field(s) stored in the certificate	field1=a,field2=b
{ \$c.email_address }	Email address stored in the certificate	test@example.com
{ \$c.valid_from }	Time at which the certificate becomes valid	1155772123
{ \$c.valid_to }	Time at which the certificate expires	1155858523
{ \$c.page_name }	Name of the page at which a new certificate can be provisioned	device_provisioning

This section is followed by the **Create Print Template** form used to configure the sections of the template: the body, the header and the footer. Each section must be written in HTML. You can use the drop-down list in each section to add images or other content items.

Figure 338 *The Create Print Template Form*

Table 192: *Create Print Template Form*

Field	Description
Name	(Required) Name for the print template. The name is used to select which template to use when printing a list of accounts.
Enabled	If selected, enables this print template for use.
Layout	(Required) Specifies how the guest account list will be printed when this template is used. Options include: <ul style="list-style-type: none"> ● Plain text format ● One account per page ● 1-column list ● 2-column list ● 3-column list ● 4-column list ● 5-column list
User Account HTML	HTML template code used to generate a single account receipt. This template is used once for each guest account in the document. You can use the drop-down list to add images or links.
Document Header HTML	HTML template code used at the beginning of the document. This template is used only once, before the account receipts are generated. You can use the drop-down list to add images or links.
Document Footer HTML	HTML template code used at the end of the document. This template is used only once, after the account receipts are generated. You can use the drop-down list to add images or links.
Create Template	Saves the new template and returns to the list at Configuration > Receipts > Templates .
Create and Reload	Saves the new template and stays on this Create Print Template page.

You can add Smarty template functions and blocks to your code. These act as placeholders to be substituted when the template is actually used.

See ["Smarty Template Syntax" on page 700](#) for further information on Smarty template syntax.

You can use an **{if}** statement to define a single print template that caters to multiple situations. For example, if you want to customize the print template to display different content depending on the action that has been taken, the following code could be used:

```
{if $action == "create"}
<p>
  Your guest account has been created and is now ready to use!
</p>
<ul>
{if $site_ssid}
  <li>Connect to the wireless network named: <b>{$site_ssid}</b></li>
{/if}
  <li>Make sure your network adapter is set to 'DHCP - Obtain an IP address
Automatically'.</li>
  <li>Open your Web browser.</li>
  <li>Enter your username and password in the spaces provided.</li>
</ul>
{elseif $action == "edit"}
<p>
  Your guest account has been updated.
</p>
{elseif $action == "delete"}
{/if}
<table {$stable_class_content} width="500">
  <tbody>
{if $u.guest_name}
  <tr>
  <th class="nwaLeft">guest name</th>
  <td class="nwaBody">{$u.guest_name}</td>
  </tr>
{/if}
</table>
```

If this code is placed in the User Account HTML section, it will cater to the create, edit, and delete options.

Print Template Wizard

The **Print Template Wizard** provides a simplified way to create print templates. You can select a basic style and provide a logo image, title, and content text, and select the guest account fields to include.

Each of the basic styles provides support for a logo image, title area, subtitle area, notes area, and footer text. These items can be customized by typing in an appropriate value in the Print Template Wizard. A real-time preview allows changes made to the design to be viewed immediately.




Because the print template is an HTML template, it is possible to use HTML syntax as well as Smarty template code in these areas. See the ["Reference" on page 697](#) chapter for reference material about HTML and Smarty template code.

To use the **Print Template Wizard**, go to **Configuration > Receipts > Templates** and click the **Create new print template using wizard** link in the upper-right corner. The **Print Template Wizard** page opens.


Figure 339 The Print Template Wizard

Print Template Wizard


*** Style:**




Table



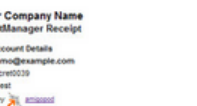
Simple



Centered



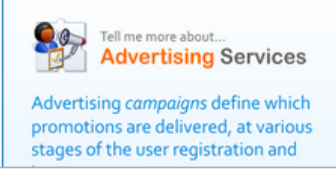
Label Printer
62 x 54mm



Label Printer
70 x 54mm

Select the style of print template to use.

Logo Image:



Tell me more about...
Advertising Services

Advertising campaigns define which promotions are delivered, at various stages of the user registration and

Select an image to use on the print template. New images can be uploaded using the Content Manager.

Title:
Enter a title to display on the print template, e.g. your organization's name.

Subtitle:
Enter a subtitle to display on the print template.

Field Header:
Enter a field header for the details displayed on the print template.

Fields:

Field
<input type="text" value="username"/>
<input type="text" value="password"/>
<input type="text" value="role_name"/>

Select the visitor account fields to display on the print template.

Notes:

```

<p>
  Your guest account has been created and is now ready to
  use!
</p>
<ul>
  {if $site_ssid}
  <li>Connect to the wireless network named: <b>{$site_ssid}</b>
  </li>
  {if $site_wpa_key}
  <li>Use the encryption key: <b>{$site_wpa_key}</b>
  {/if}
  </li>
  <li>Make sure your network adapter is set to
  "DHCP - Obtain an IP address Automatically".
  </li>
  <li>Open your web browser.
  </li>
  </ul>
  
```

Insert...

Enter the notes to display on the print template, e.g. a welcome message or usage instructions.

Footer:
Enter the footer text to display on the print template.

Print Template Preview
A preview of your print template is shown below.

Preview: i Select a style of print template.

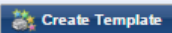


Table 193: Print Template Wizard

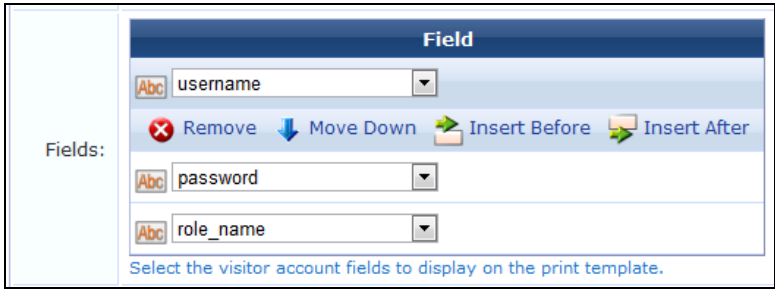

Field	Description
Style	<p>(Required) Specifies the style of print template to use. Small thumbnail images are shown to indicate the basic layout of each style. Options include:</p> <ul style="list-style-type: none"> ● Table – Best for square or nearly square logo images, and well suited for use with “scratch card” guest accounts. ● Simple – Best for wide or tall logo images and for situations where an operator will print a page with guest account details. ● Centered – Best for wide logo images; less formal design. ● Label Printer – Three sizes are provided. These print template styles are designed for small thermal printers in various widths. On-screen assistance is provided when printing to ensure that a consistent result can be obtained.
Preview at right	<p>After a style is selected, you can click one of these links to display the real-time preview of the print template at either the right side or the bottom of the Print Template Wizard.</p>
Preview at bottom	
Logo Image	<p>Specifies the logo image to use on the print template. All images that have been uploaded to the Content Manager are displayed in this field. To select an image, click to highlight it in this field.</p>
Title	<p>Title to display on the print template.</p>
Subtitle	<p>Subtitle to display on the print template.</p>
Field Header	<p>Field header for the details that are displayed on the print template.</p>
Fields	<p>Specifies the visitor account fields to display on the print template. Use a drop-down list to choose a field name. By default, the wizard sets up the template with the username, password and role_name fields, but these may be customized. You can add fields, remove fields, or change the order of fields. Your changes are shown in the preview. To expand the row to display configuration options, either click the drop-down list, or click the icon at the left of the drop-down list. Options include:</p> <ul style="list-style-type: none"> ● Remove — Removes the field from this form and from the print template. ● Move Up — Moves this field to appear above the previous field in the list. ● Move Down — Moves the field to appear below the next field in the list. ● Insert Before — Adds a new drop-down list above the active row so you can add a new field to the print template. ● Insert After — Adds a new drop-down list below the active row so you can add a new field to the print template. 
Notes	<p>Notes to display in the print template — for example, a welcome message or usage instructions.</p>

Table 193: Print Template Wizard(Continued)

Field	Description
Footer	Footer text to display on the print template.
Print Template Preview	Real-time preview of the print template as a guest would see it. Shows the changes you make in the wizard. Use the links above the wizard to change the position of the preview.
Create Template	Saves the new print template and returns to the Guest Manager Print Templates list view.

Modifying Wizard-Generated Templates

After you create a print template using the **Print Template Wizard**, you can return to the wizard to modify it.

Click the  **Edit print template code (Advanced)** link to use the standard print template editor. See "Creating New Print Templates" on page 445 for a description.



If you use the wizard to edit a print template after changes have been made to it outside the wizard, those outside changes will be lost. This is indicated with the warning message "The print template code has been modified. Making changes using the wizard will destroy any changes made outside of the wizard."

Setting Print Template Permissions

On the **Guest Manager Print Templates** list view, the **Permissions** link for a template can be used to control access to an individual print template at the level of an operator profile. The **Permissions** link is only displayed for a template if the current operator has the Object Permissions privilege. The Object Permissions privilege is located in the Administrator group of privileges.

To view and work with permissions for a print template:

1. Go to **Configuration > Receipts > Templates**. The **Guest Manager Print Templates** list view opens.
2. Click the template's row in the list, and then click its **Permissions** link. The **Edit Print Template Permissions** form opens.

Figure 340 *The Edit Print Template Permissions Form*

















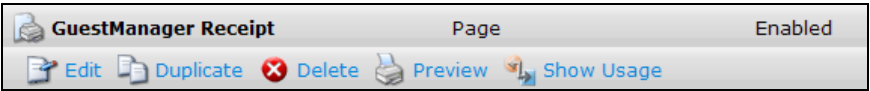
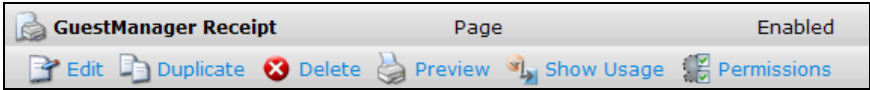
Edit Print Template Permissions							
Object:	 GuestManager Receipt						
Owner Profile:	 IT Administrators <i>Operators in this profile will always be granted full access to this object.</i>						
Access:	<table border="1"> <thead> <tr> <th>Entity</th> <th>Permissions</th> </tr> </thead> <tbody> <tr> <td> Authenticated operators</td> <td> Full access (ownership)</td> </tr> <tr> <td> Guests</td> <td> Full access (ownership)</td> </tr> </tbody> </table>	Entity	Permissions	 Authenticated operators	 Full access (ownership)	 Guests	 Full access (ownership)
	Entity	Permissions					
 Authenticated operators	 Full access (ownership)						
 Guests	 Full access (ownership)						
<i>Select the permissions for this object.</i>							
<div style="display: flex; justify-content: space-around;">  Save Changes  Save and Reload </div>							

Table 194: *Edit Print Template Permissions Form*

Field	Description
Object	Name of the selected print template. The name cannot be edited.
Owner Profile	Name of the operator profile that will always have full access to the print template.
Access	Specifies who has access to this print template, and the level of permissions they have for it. Use the Entity and Permissions drop-down lists in this row to set permissions.
Entity	<p>Specifies the operator profiles or other entities that can have access to this print template. Options include:</p> <ul style="list-style-type: none"> Operator Profiles: — Any of the following specific operator profiles may be selected. The corresponding permissions will apply to all operators with that operator profile. <ul style="list-style-type: none"> Null Profile Operations and Marketing Receptionist Network Administrator Help Desk Read-only Administrator Device Registration BYOD Operator API Guest Operator Other Entities: <ul style="list-style-type: none"> Authenticated Operators — The permissions for all operators (other than the owner profile) may be set using this item. Permissions for an individual operator profile will take precedence over this item. Guests — The permissions for guests may be set using this item.
Permissions	<p>Specifies the permissions for the user type selected in the corresponding Entity list. Options include:</p> <ul style="list-style-type: none"> No access — The print template is not visible in the list, and cannot be used, edited, duplicated, or deleted. Visible-only access — The print template is visible in the list, but cannot be edited, duplicated, or deleted. <div data-bbox="461 1306 1328 1396" data-label="Image"> </div> Read-only access — The print template is visible in the list, and the settings for it may be viewed. The print template cannot be edited or deleted. <div data-bbox="461 1480 1328 1570" data-label="Image"> </div> Update access — The print template is visible in the list, and may be edited. The print template cannot be deleted and the permissions for the print template cannot be modified. <div data-bbox="461 1654 1328 1745" data-label="Image"> </div> Update and delete access — The print template is visible in the list, and may be edited or deleted. The permissions for the print template cannot be modified.

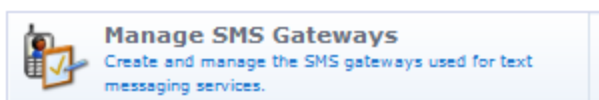
Table 194: *Edit Print Template Permissions Form(Continued)*

Field	Description
	 <ul style="list-style-type: none"> • Full access (ownership) — The print template is visible in the list, and may be edited or deleted. The permissions for the print template can be modified, if the operator has the Object Permissions privilege. 
Delete	To remove an entity from the list in the Access field, click anywhere in the entity's row. A Delete link is displayed for that row. Click the Delete link to remove the entity's row from the list. You will be asked to confirm the deletion.
Add	To add an entity to the list in the Access field, click anywhere in an entity's row. An Add link is displayed for that row. Click the Add link to add a new pair of Entity and Permissions fields.
Save Changes	Saves your changes on this form and returns to the Guest Manager Print Templates list view.
Save and Reload	Saves your changes on this form and stays on this form.

SMS Services



With SMS Services, you can configure ClearPass Guest to send SMS messages to guests. You can use SMS to send a customized guest account receipt to your guest's mobile phone. You can also use SMS Services to send an SMS from your Web browser. To use the SMS features, you must have the **SMS Services** plugin installed.



This section describes:

- "Viewing SMS Gateways" on page 454
- "Creating or Editing an SMS Gateway" on page 454
- "Sending an SMS " on page 460
- "About SMS Credits" on page 460
- "About SMS Guest Account Receipts " on page 461
- "About SMS Receipt Options" on page 462
- "Working with the Mobile Carriers List" on page 462



ClearPass Guest 3.9 and earlier used www.amigopod.com for a number of actions, including updates, SMS, and network diagnostics. The address used now is clearpass.arubanetworks.com. If you have host-specific openings in your firewall for the ClearPass appliance, please update them to the new address.

Viewing SMS Gateways



A ClearPass Guest SMS service is automatically added when a subscription ID is configured in ClearPass. You can also add one, and work with existing gateways.

To view and work with the list of SMS gateways, go to **Configuration > SMS Services > Gateways**. The **SMS Gateways** list view opens.

Figure 341 *The SMS Gateways List View*

Name	Service Name	Credits
SMS Gateway	ClearPass Guest SMS Service	204

1 gateway Reload 20 rows per page

All SMS gateways that have been defined are included in the list, and their names and available credits are displayed. You can click a gateway's row in the list or use the links provided on the page for additional options:

Table 195: *SMS Gateways List*

Field	Description
Edit	Edit a gateway's properties. See " Creating or Editing an SMS Gateway " on page 454.
Duplicate	Creates a copy of the gateway to use as a base for a new gateway. A new gateway will be added to the list with the name "Copy of <original gateway>".
Delete	Deletes the gateway from the list. You are asked to confirm the deletion. Click OK at the prompt to delete the gateway.
Make Default	Makes this gateway the default gateway for SMS messages.
Send SMS	Lets you send an SMS message via this gateway. The row expands to include the New SMS Message form, where you can enter the recipient's mobile phone number and the message text, then send the message.
Create new SMS gateway	To add a carrier to the list, click this link in the upper-right corner. The Create SMS Gateway opens. See " Creating or Editing an SMS Gateway " on page 454.

Creating or Editing an SMS Gateway

An SMS gateway is automatically created and added to the SMS Gateways list when you enter your subscription ID in ClearPass Policy Manager at **Administration > Agents and Software Updates > Software Updates**. You can also use ClearPass Guest to create a new SMS gateway.

The **SMS Gateway Configuration** form is used to create and to edit an SMS gateway.

To create a new SMS gateway through ClearPass Guest:

1. Go to **Configuration > SMS Services > Gateways**. The **SMS Gateways** list view opens.
2. Click the **Create new SMS gateway** link in the upper right corner. The **SMS Gateway Configuration** form opens.

To edit an existing SMS gateway:

1. Go to **Configuration > SMS Services > Gateways**. The **SMS Gateways** list view opens.

- Click the gateway's row in the list, and then click its **Edit** link. The **SMS Gateway Configuration** form opens.

Figure 342 *The SMS Gateway Configuration Form, Service Settings Area (Custom HTTP Handler selected as the gateway)*

Service Settings	
Display Name:	<input type="text"/> The name for this service handler. This will be displayed to operators using the system.
* Service URL:	<input type="text"/> The URL template to use when sending a message. The following substitutions are available: @USERNAME@ - Service Username @PASSWORD@ - Service Password @API_ID@ - API ID @FROM@ - SMS Source Address @TO@ - Recipient @MESSAGE@ - Message @MESSAGE_ENC@ - Message that has already been URL encoded e.g. https://sms.acme.co/send?username=@USERNAME@&password=@PASSWORD@&mobile=@TO@&msg=@MESSAGE@
* Service Method:	<input checked="" type="radio"/> GET <input type="radio"/> POST The HTTP method used to access the gateway.
* Authentication Method:	<input checked="" type="radio"/> Substituted parameters <input type="radio"/> HTTP Basic Authentication How the username and password will be passed to the gateway.
Service Username:	<input type="text"/> Your authorization username for the SMS service provider. Note, if you are using ClearPass Guest SMS Service and have entered your ClearPass Subscription ID, the username and password fields should be left blank
Service Password:	<input type="text"/> Your authorization password for the SMS service provider.
Confirm Password:	<input type="text"/> Your authorization password for the SMS service provider.
API ID:	<input type="text"/> An optional API ID, if required by the SMS provider.
SSL Certificate:	<input type="text"/> Path of the uploaded SSL certificate (public/cert.pem). Must be in pem format.
SSL Passphrase:	<input type="text"/> Passphrase of the above certificate. Leave blank if there is no passphrase.
Confirm Passphrase:	<input type="text"/> Passphrase of the above certificate. Leave blank if there is no passphrase.
SMS Source Address:	<input type="text"/> Set the originator address of sent SMS messages. This may be a phone number or short string, depending on the provider.
Message Format:	<input type="checkbox"/> Convert text to hex-encoded UTF-16 If selected, the message will be converted to hex-encoded UTF-16. Refer to your service provider's documentation if this is necessary.

The first part of the SMS Gateway Configuration form includes the **Service Settings** options:

Table 196: *SMS Gateway Configuration Form, Gateway and Service Settings Areas*

Field	Description
SMS Gateway	<p>(Required) If you are creating a new gateway, specifies the SMS gateway service to use. If you are editing an existing gateway, this field cannot be edited. Options include:</p> <ul style="list-style-type: none"> • ClearPass Guest SMS Service • Custom HTTP Handler • SMS over SMTP • SMPP v3.4 • External Providers <p>The following options presented in the Service Settings area depend on the gateway selected here.</p>
Address	(Required) If a fixed email address was specified, enter the email address to which all SMS messages will be sent.
Address Template	(Required) If a template to determine the address was specified, enter an example address that will be used as the pattern for the address format.
API ID	Optional API ID, if required by the SMS provider.
Authentication Method	<p>(Required) Specifies how the username and password will be passed to the gateway. Options include:</p> <ul style="list-style-type: none"> • Substituted parameters • HTTP Basic Authentication
Carrier Selection	<p>Specifies how the carrier will be determined. Options include:</p> <ul style="list-style-type: none"> • Registration form will have the visitor_carrier field—The visitor will supply the carrier information when they register. The Mobile Carrier field will be included in the visitor's registration form, and added to the Test SMS Settings area of the forms. • Select a carrier—The form expands to include the Mobile Carrier field. Choose the carrier from the Mobile Carrier drop-down list. • Configure Carrier Settings—The form expands to include configuration options for the carrier.
Display Name	Name for this gateway service handler. The name entered here is the one that will be displayed to operators using the system.
HTTP Headers	<p>If the POST option was selected in the Service Method field for a custom HTTP handler gateway, you can use this text field to override the HTTP header. For example:</p> <pre>Content-Type: text/xml</pre>
HTTP Post	(Required) If the POST option was selected in the Service Method field for a custom HTTP handler gateway, you can use this text field to enter the text to post. See the service URL field for available substitutions.
Message Encoding	Message encoding to use when sending messages to the SMPP provider.
Message Format	If selected, specifies that the message format should be converted to hex-encoded UTF-16 (Unicode). This is not needed for all custom SMS handlers; refer to your service provider's documentation.
Mobile Carrier	(Required) Specifies the carrier to use.

Field	Description
Null Terminate Strings	If selected, C-Octet strings on SMPP SMS servers will be null-terminated.
Number Format	Specifies the country code requirement of the carrier. Options include: <ul style="list-style-type: none"> ● Use the visitor's value ● Always include the country code ● Never include the country code
Port Number	The port number used to reach the server. To use the default, leave this field empty.
Service Method	(Required) If Custom HTTP Handler was selected in the SMS Gateway field, select the HTTP method to use. Options include: <ul style="list-style-type: none"> ● GET ● POST
Service Password	Your password for your SMS service provider.
Confirm Password	If you are using ClearPass Guest SMS Service and have entered your ClearPass subscription ID in the Software Updates page of ClearPass Policy Manager's Administration module, leave this field blank. The subscription ID is automatically used as the password for the ClearPass SMS Service.
Service URL	(Required) The URL template to use when sending a message. Use the following items in the template: <ul style="list-style-type: none"> ● @USERNAME@ – Service Username ● @PASSWORD@ – Service Password ● @API_ID@ – API ID ● @FROM@ – SMS Source Address ● @TO@ – Recipient ● @MESSAGE@ – Message ● @MESSAGE_ENC@ – Message that has already been URL encoded
Service Username	Your authorization username for your SMS service provider. If you are using ClearPass Guest SMS Service and have entered your ClearPass subscription ID in the Software Updates page of ClearPass Policy Manager's Administration module, leave this field blank. The subscription ID is automatically used as the username for the ClearPass SMS Service.
SMPP Server Address	IP address or DNS name of the SMPP server.
SMPP System Type	(Required) The registered SMPP System Type.
SMS Address	Specifies how the email address will be determined. Options Include: <ul style="list-style-type: none"> ● Use a template to determine the email address ● Use a fixed email address
SMS Source Address	Originator address of sent SMS messages. Depending on the provider, this may be either a phone number or a short string.
Source Address NPI	Numbering plan identification (NPI) type of the source address. Options include: <ul style="list-style-type: none"> ● NPI_UNKNOWN

Field	Description
	<ul style="list-style-type: none"> ● NPI_E164 ● NPI_DATA ● NPI_TELEX ● NPI_E212 ● NPI_NATIONAL ● NPI_PRIVATE ● NPI_ERMES ● NPI_INTERNET ● NPI_WAPCLIENT
SSL Certificate	Path of the uploaded SSL certificate (public/cert.pem). This must be in .pem format.
SSL Passphrase	Passphrase for the certificate specified in the SSL Certificate field. If there is no passphrase, leave this field blank.
Confirm Passphrase	
Subject Line	Text for the message's subject line. This field supports Smarty template syntax. For a Smarty template syntax description, See " Smarty Template Syntax " on page 700.

The **Mobile Number Settings** area of the **SMS Gateway Configuration** form includes options for defining the mobile phone number settings:

Figure 343 *The SMS Gateway Configuration Form, Mobile Number Settings Area*

Mobile Number Settings	
Country Code:	<input type="text"/> <small>The default country code to use for mobile telephone numbers that start with the national prefix.</small>
Default Length:	<input type="text"/> <small>Most SMS providers require the number sent with the country code. If your country has a default length, enter it here and the country code above will be automatically added where necessary. For example, North American numbers have a default length of 10, and country code 1.</small>
Auto Plus Length:	<input type="text"/> <small>If your SMS provider requires a "+" for international numbers, enter the minimum length of international numbers. Any number entered whose length is greater than or equal to this value, will automatically have the "+" prepended. For example, North American numbers have a default length of 10, and country code 1, so the Auto Plus Length would be 11.</small>
National Prefix:	<input type="text" value="0"/> <small>Optional national dialing prefix to recognize.</small>

Table 197: *SMS Gateway Configuration -- Mobile Number Settings Options*

Field	Description
Country Code	Default country code to use for mobile telephone numbers that start with the national prefix. Most SMS providers require that the number be sent with the country code.
Default Length	If your country has a default length, enter it here. The country code entered in the previous field will be automatically added if it is required. For example, North American numbers have a default length of 10, and country code 1.
Auto Plus Length	If your SMS provider requires a "+" for international numbers, enter the minimum length for international numbers. If a phone number is entered whose length is greater than or equal to this value, the "+" will automatically be prepended. For example, North American numbers have a default length of 10 and a country code of 1, so the Auto

Field	Description
	Plus Length would be 11.
National Prefix	If your country uses a national dialing prefix such as "0", you may enter it here. When sending an SMS to a number that starts with the national dialing prefix, the prefix is removed and replaced with the country code instead.

The lower part of the **SMS Gateway Configuration** form includes the **Connection Settings**, **Debug**, and **Test SMS Settings** areas:

Figure 344 The SMS Gateway Configuration Form, Connection Settings, Debug, and Test SMS Settings Areas

The screenshot shows a web form with three main sections: **Connection Settings**, **Debug**, and **Test SMS Settings**.
Connection Settings: Includes two required fields: *** Connect Timeout:** (15 seconds) and *** HTTP Timeout:** (60 seconds).
Debug: Includes a checkbox for **Enable Debug:** (Log detailed information to the application log).
Test SMS Settings: Includes a text area for *** Message:** (160 characters left) and a text field for *** Recipient:** (mobile telephone number).
 At the bottom, there are two buttons: **Send Test Message** and **Save and Close**.

Table 198: SMS Gateway Configuration -- Connection Settings, Debug, and Test SMS Settings Options

Field	Description
Connection Timeout	(Required) The connection timeout for this SMS service, in seconds.
HTTP Timeout	(Required) The timeout for the HTTP transfer to complete, in seconds.
Enable Debug	If selected, debug messages will be generated for each stage of the HTTP transaction and the detailed information will be included in the application log.
Message	(Required) The message to send to verify the configuration.
Recipient	(Required) The test recipient's mobile phone number for verifying the configuration.
Send Test Message	To verify the configuration, after you enter the test message and the test recipient's mobile number, click this button. The test recipient should receive the message and confirm the results.

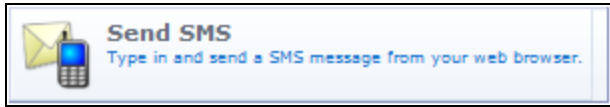
When you have completed your changes on this form, click **Save and Close**. The new configuration settings take effect immediately.

When you save your entries for the SMS over SMTP option, a new screen, **Mobile Carriers**, is added to the left navigation. For more information, see "Working with the Mobile Carriers List" on page 462.

Sending an SMS



You can send an SMS message if the system has been configured to allow this.



To send an SMS message:

1. Go to **Configuration > SMS Services > Send SMS**. The **New SMS Message** form opens.

Figure 345 The New SMS Message Form

Table 199: New SMS Message Form

Field	Description
Service	Service that will be used to send the message. If multiple services are available, you may specify the service to use.
Recipient	(Required) Mobile number of the recipient, in international format.
Message	(Required) Message to send. The maximum message length is 160 characters.
Send Message	Sends the SMS message.

About SMS Credits

Most SMS providers use a system of credits for sending messages. In ClearPass Guest SMS Services, one credit is used for each sent message. The credit is used when the message is sent, regardless of whether the recipient actually receives the message. Please review your provider's details and pricing.

To determine the number of remaining SMS credits for a service, go to the **Configuration > SMS Services > Gateways** list, and find the service's row in the list. The **Credits Available** column indicates the number of

remaining SMS credits for your account. This value is determined when the first message is sent, and is updated when each message is sent.

When credits are running low, a warning message is emailed to the administrator group. The email address is determined by looking up all local operators with the special IT Administrators operator profile, and using any configured email address for those operators.

Up to three messages will be sent:

- A low-credit warning is sent when the "Credits Available" value reaches the warning threshold (the default value is 50).
- A second low-credit warning is sent when the "Credits Available" value reaches half the warning threshold.
- A final message is sent when the "Credits Available" value reaches zero.



To adjust the warning threshold, set the **Credit Warning** value in the configuration for the SMS Services Plugin. See ["Configuring the SMS Services Plugin" on page 654](#).

About SMS Guest Account Receipts



You can send SMS receipts for guest accounts that are created using either sponsored guest access or self-provisioned guest access. This is convenient in situations where the visitor may not be physically present to receive a printed receipt.

ClearPass Guest may be configured to automatically send SMS receipts to visitors, or to send receipts only on demand.

To manually send an SMS receipt:

1. Go to the **Guest > Manage Accounts** and click to expand the row of the guest to whom you want to send a receipt.
2. Click **Print** to display the **Updated Account Details** view, and then click the **Send SMS receipt** link. The **SMS Receipt** form opens.
3. Use the fields on the **SMS Receipt** form to enter the service to use, the recipient's mobile phone number, and the message text.

Figure 346 *The SMS Receipt Form*

SMS Receipt

* Service:
Select the service to use when sending the message.

Recipient:
Enter the mobile telephone number of the recipient in international format.

Message:
Visitor Access
Username: SHA@SH
Password:
--
Powered by Aruba
96 characters left
This is the message that will be sent.

Send Message

When using guest self-registration, SMS Delivery options are available for the receipt page actions. See ["Editing Receipt Actions"](#) on page 358 for full details. For more information on SMS services, see ["SMS Services"](#) on page 453.

About SMS Receipt Options



SMS receipt configuration options are available in the Configuration module (see ["Customizing SMS Receipt"](#) on page 442). Advanced configuration options for the SMS Services, including receipt options, are also available in the plugin configuration (see ["Configuring Plugins"](#) on page 636).

Working with the Mobile Carriers List



If you have included SMS over SMTP gateways in your SMS gateways list, you can manage the list of SMTP carriers that are included in the **Mobile Carrier** drop-down list on the **Configuration > SMS Services > Gateways > Edit SMS Gateway** form.

To include the **Mobile Carrier** field in the visitor's registration form, when you create or edit a gateway you must choose **Registration form will have the visitor_carrier field** in the **Carrier Selection** drop-down list. The **Mobile Carrier** field will be included in the visitor's registration form, and added to the **Test SMS Settings** area of the forms. See [Creating or Editing an SMS Gateway](#).

To view or work with the mobile carriers list, go to **Configuration > SMS Services > Mobile Carriers**. The **Mobile Carrier List** view opens. The carriers in this list are the ones that are included in the **Mobile Carrier** drop-down list on the **SMS Services > Gateways > Edit SMS Gateway** form.

Figure 347 *The Mobile Carrier List View*

Name	Enabled	Country	SMS	MMS
7-11 Speakout(GSM)	No	USA	number@cingularme.com	
AT&T Enterprise Paging	No	USA	number@page.att.net	
AT&T Wireless	No	USA	number@txt.att.net	number@mms.att.net
Airtel (Andhra Pradesh, India)	No	Andhra Pradesh, India	number@airtelap.com	
Airtel (Karnataka, India)	No	Karnataka, India	number@airtelkk.com	
Airtel Wireless	No	Montana, USA	number@sms.airtelmontana.com	
Alaska Communications Systems	No	USA	number@msg.acsalaska.com	
Alltel Wireless	No		number@message.alltel.com	
BPL Mobile	No	Mumbai, India	number@bplmobile.com	
Bell Mobility & Solo Mobile	No	Canada	number@txt.bell.ca	

Table 200: *Mobile Carrier List View*

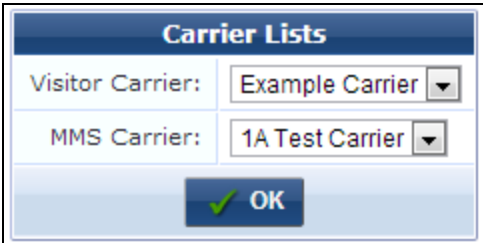
Field	Description
Quick Help	Displays some information about the SMS SMTP carrier list and about how to use the Mobile Carrier List view.
Display Lists	Lets you filter the list. The form expands to include the Carrier Lists form. Use the drop-down lists on this form to specify the SMS carrier or the MMS carrier, and then click OK . To be available in the drop-down lists on this Carrier Lists form, a carrier must first be enabled. 
Create	Add a carrier to the list. The Mobile Carrier List view expands to include the Mobile Carrier Editor form. See "The Mobile Carrier Editor Form" on page 464, below.

Table 200: *Mobile Carrier List View(Continued)*

Field	Description
Edit	Edit the carrier. The row expands to include the Mobile Carrier Editor form for that carrier. See "The Mobile Carrier Editor Form " on page 464, below.
Enable	To enable a carrier, click the Enable link in its row and then refresh the screen. The carrier will then be available to work with and will be included in the drop-down lists when you click the Display Lists link.
Delete	Deletes the carrier, You will be asked to confirm the deletion.

Figure 348 *The Mobile Carrier Editor Form*

The procedures for adding and for editing a carrier are the same. To open the **Mobile Carrier Editor** form, click either the **Create** link or an **Edit** link on the **Mobile Carrier List**. The list view expands to include the **Mobile Carrier Editor** form.

Table 201: *Mobile Carrier Editor Form*

Field	Description
Name	(Required) Name of the carrier. If there is more than one format of the carrier company's name, use the format the public most readily identifies with the carrier service.
Enable	(Required) If selected, the carrier is included in the list of available choices for users.
Country	Country where the carrier's service is offered. If appropriate, you may also indicate an area within the country, such as a city, county, state, or province.
SMS Address	Specifies how the email address will be determined. Options include: <ul style="list-style-type: none"> ● Use a template to determine the email address— When this option is chosen, the next field's name becomes SMS Template. ● Use a fixed email address—Use this option if all SMS messages are to be sent to the same address. When this option is chosen, the next field's name becomes Address.

Table 201: Mobile Carrier Editor Form(Continued)

Field	Description
SMS Template	(Required) Example email address for SMS messages. This provides the pattern for the address format. The default is to substitute the number for all characters preceding the @ sign, producing the pattern number@address . Use the keyword "NUMBER" where appropriate, otherwise everything after the @ sign will be used. Some carriers require additional characters before or after the phone number. In this case, use the keyword string NUMBER in the pattern to limit the substitution to just the phone number portion of the address—for example, NUMBER.msg@carrier.example.com, or username+NUMBER@mymail.com
Address	(Required) Email address to which all SMS messages will be sent.
MMS	(Required) If selected, the SMS template will also be used for all MMS messages, and the MMS Template row is removed from the form. To use an MMS template for MMS messages, leave this check box unmarked.
MMS Template	Example email address for MMS messages. This provides the pattern for the address format. Use the keyword "NUMBER" where appropriate, otherwise everything after the @ sign will be used.
Number Format	Specifies the country code requirement of the carrier. Options include: <ul style="list-style-type: none"> ● Use the visitor's value ● Always include the country code ● Never include the country code
Subject Line	Text for the message's subject line. This field supports Smarty template syntax, and the number is available as {\$number}. For example: Sent to: {\$number} in the year {'Y' date} ...would produce: Sent to: 15555551234 in the year 2012 For a Smarty template syntax description, See " Smarty Template Syntax " on page 700.
Create Carrier	Creates the new carrier and adds it to the Mobile Carrier List.
Save Changes	Saves your changes to the existing carrier and updates the Mobile Carrier List.

About Translations



Translation services let you configure the language that will be displayed to guests in the ClearPass Guest interface. You can set a default language, enable auto-detection based on the user's browser settings, enable various language packs, and allow the user to select the language. Language packs are editable, letting you customize label and message text and numerous other settings. You can use the Plugin Manager to enable the translation assistant features, and to configure ClearPass Guest's language settings for your own use.




- To view and manage your list of enabled translation packs, see "[Translation Packs](#)" on page 466.
- To edit basic information for a translation pack, see "[Creating and Editing Translation Packs](#)" on page 467.

- To set the default language, show IDs for labels and messages, and provide a language selector on each page of the user interface, see ["Translation Assistant" on page 468](#).
- To customize a translation pack's labels and messages, see ["Customizing Translated User Interface Text" on page 469](#).
- To view the Translation Plugin settings, see ["Configuring the Translations Plugin" on page 659](#) in the Administration module.

Translation Packs

To work with individual translation packs, go to **Configuration > Translations > Translation Packs**. The **Language Packs** list view opens.

Figure 349 *The Language Packs List View*

△ Name	Enabled	Code	Display	Locale	RTL	Parent
 Arabic Translations	Enabled	ar	العربية	ar.UTF-8, arabic, ar	Yes	Base
 Chinese Translations	Enabled	zh	中文	zh_CN.UTF-8, zh.UTF-8, chinese, zh	No	Base
 Danish Translations	Enabled	da	Dansk	da_DK.UTF-8, da.UTF-8, danish, da	No	Base
 Dutch Translations	Enabled	nl	Nederlands	nl_NL.UTF-8, nl.UTF-8, dutch, nl	No	Base
 English Translations	Enabled	en	English	en_US.UTF-8, en.UTF-8, english, en	No	Base
 French Translations	Enabled	fr	Français	fr_FR.UTF-8, fr.UTF-8, french, fr	No	Base
 German Translations	Enabled	de	Deutsch	de_DE.UTF-8, de_DE, de.UTF-8, de	No	Base
 Japanese Translations	Enabled	ja	日本語	ja_JP.UTF-8, ja.UTF-8, japanese, ja	No	Base
 Korean Translations	Enabled	ko	한국말	ko_KR.UTF-8, ko.UTF-8, korean, ko	No	Base
 Spanish Translations	Enabled	es	Español	es_ES.UTF-8, es.UTF-8, spanish, es	No	Base

 Edit
  Override Translations
  Export
  Duplicate
  Use
  Make Default

10 translation packs  Reload Show all rows ▾

All translation packs that have been enabled are included in the list. You can click a translation pack's row in the list for additional options:

Table 202: *Translation Packs List View Options*

Field	Description
Edit	Enable or disable the translation pack and edit its name, display name, language code, flag image, and list of locale identifiers. For more information, see "Creating and Editing Translation Packs" on page 467 .
Override Translations	Specify and edit the translated wording of the application's labels and messages. For more information, see "Customizing Translated User Interface Text" on page 469 .
Export	Download your customized translations to a file and send them to your ClearPass Support team. Your feedback helps us enhance the default translations.
Duplicate	Create a new translation pack. You can give the copy of the translation pack a new name, enable it, and edit its display name, language code, flag image, and locales list. For more information, see "Creating and Editing Translation Packs" on page 467 .
Use	Applies this language pack. Labels in ClearPass Guest are displayed in the language. To revert, click the Use link for a different language in the list.
Make Default	Use a translation pack as the new default language for the application. You can also reset the default language from the Translation Assistant form.

Creating and Editing Translation Packs

To create or edit a translation pack:

Go to **Configuration > Translations > Translation Packs**, then click the **Edit** or **Duplicate** link for a translation pack in the list. The **Translation Pack Configuration Form** form opens.

Figure 350 *The Translation Pack Configuration Form*

Translation Pack Configuration	
Parent:	English Translations
Name:	<input type="text"/> <small>The name for this translation pack.</small>
Enabled:	<input checked="" type="checkbox"/> Enable this translation pack <small>Note only one pack can be enabled per language code.</small>
Display Name:	<input type="text" value="English"/> <small>The display name for this translation pack. This will be displayed anywhere languages can be selected.</small>
Language Code:	<input type="text"/> <small>The unique language code for this translation.</small>
Flag:	<input type="text" value="flag-uk"/> <small>The flag to include in the language selection list. Icon should be 24x24 pixels.</small>
Locales:	<input type="text" value="en_US.UTF-8, en.UTF-8, english, en"/> <small>Enter a comma-delimited list of locale identifiers.</small>
RTL:	<input type="checkbox"/> This language writes text right-to-left
<input type="button" value="Save Changes"/>	

Table 203: *Translation Pack Configuration*

Field	Description
Parent	Name of the translation pack you used as a basis. This field only appears if you are duplicating a translation pack, and cannot be edited.
Name	Name of this translation pack. This identifying name is different from the display name, and is only seen by application administrators.
Enabled	If selected, enables this translation pack. To create the translation pack but not enable it yet, leave this check box unselected. Each language code can have only one corresponding translation pack enabled at a time.
Display Name	Name to display in the language selection options in the user interface.
Language Code	Unique ISO 639-1 language code that corresponds to this translation pack. Only one translation pack at a time can be enabled for each language code.
Flag	Specifies the filename of the flag image to use for this translation pack. Image files should have been previously uploaded to the Content Manager. In the user interface's language selection options, a small image of a flag is shown next to each language.

Field	Description
Locales	Comma-separated list of locale identifiers for this language pack. Locale identifiers let you customize translation packs for regional differences.
RTL	If selected, specifies that this language displays text right-to-left.
Save Changes	Saves your changes and returns to the Translation Packs list view.

Translation Assistant

To configure some basic user assistance features for the user interface's language settings, go to **Configuration > Translations > Translation Assistant**. The **Translation Assistant** form opens.

Figure 351 *The Translation Assistant Form*

The screenshot shows the 'Translation Assistant' form. It has a dark blue header with the title 'Translation Assistant'. Below the header, there are two main sections: 'Server Settings' and 'Translation Assistant'. The 'Server Settings' section includes a 'Default Language' dropdown menu set to '(English)' and an 'Auto-Detection' checkbox that is unchecked. The 'Translation Assistant' section includes a 'Text IDs' checkbox that is unchecked and a 'Language Selector' checkbox that is checked. At the bottom of the form is a 'Save Changes' button.

Figure 352 *The Translation Assistant Form with Text IDs Showing*

This screenshot shows the same 'Translation Assistant' form but with text IDs visible. The header is '[#3607 Translation Assistant]'. The 'Server Settings' section is labeled '[#12261 Server Settings]' and includes a 'Default Language' dropdown set to '[#12262 (English)]'. The 'Auto-Detection' checkbox is labeled '[#12266 Disable language auto-detection]'. The 'Translation Assistant' section is labeled '[#3607 Translation Assistant]' and includes a 'Text IDs' checkbox labeled '[#12272 Show Text IDs with text]' which is checked, and a 'Language Selector' checkbox labeled '[#12269 Enable the language selector on each page]' which is unchecked. The 'Save Changes' button is labeled '[#518 Save Changes]'.

Table 204: Translation Assistant Configuration

Field	Description
Default Language	Specifies the default language pack for the user's application.
Auto-Detection	If selected, disables automatic browser-based language detection and enforces the default translation pack instead. The default behavior is to use the language the user's browser has detected as preferred, instead of using the default translation pack.
Text IDs	If selected, the text IDs are displayed on all headings and field names in the ClearPass Guest user interface, and an Override all translations generated for this page link is displayed at the bottom of each page. Displaying the text IDs lets translators easily identify the fields on each page in order to customize translations. For more information, see " Customizing Translated User Interface Text " on page 469.
Language Selector	If selected, provides language selection options on each page of the user interface. A row of language links with flags is displayed at the bottom of each page. If this check box is not selected, the language selection options are only displayed on the login page.
Save Changes	Saves your changes on this form.

Customizing Translated User Interface Text

You can override the default translations provided for labels and messages in the user interface, customizing these items in each translation pack.

To customize label and message text for a translation pack, do one of the following:

- Go to **Configuration > Translations > Translation Packs**, and then click the **Override Translations** link for a translation pack in the list. The **Translation Pack Configuration** form opens. Text IDs for any items that already have custom overrides are listed in the **Translations** area of the form. To edit a different field, you can enter its text ID and refresh the form. A row will be added for the field.

Figure 353 The Translation Pack Configuration Form

Translation Pack Configuration

Name: English Translations

Enabled: Enable this translation pack

Display Name: English

Language Code: en

Locales: en_US.UTF-8, en.UTF-8, english, en

Translations

Text IDs: Enter a comma-separated list of IDs to edit. Click Refresh below to update the view. Leave blank to display the current overrides. id1,id2,id3-id14,id25-id46

Common IDs: [Login Errors](#) | [Login Pages](#) | [Health checks](#) | [Operator Login](#) | [Onboarding](#) | [Registration Errors](#) | [Sponsorship Confirmation](#) | [Navigation](#)
Click a link to view common ID sets.

- Go to **Configuration > Translations > Translation Assistant**. Select the language, select the check box in the **Text IDs** field, and save your changes. Text IDs are shown with every label, and an **Override all translations generated for this page** link is now displayed at the bottom of every page in ClearPass Guest. To customize translations for a certain page or group of pages, go to the page you want to translate and click its **Override all translations generated for this page** link. The Edit Translations form opens. Text IDs for that page and the set of pages it belongs to (for example, all pages related to Web Logins) are

listed in the Translations area of the form. The form includes a row for each text ID, where you can provide a custom translation.

Figure 354 *The Translation Pack Configuration Form with Text IDs Showing*

[#12291 Translation Pack Configuration]

[#338 Name:] English Translations

[#552 Enabled:] [#12303 Enable this translation pack]

[#5262 Display Name:] English

[#12300 Language Code:] en

[#12294 Locales:] en_US.UTF-8, en.UTF-8, english, en

[#12228 Translations]

[#12273 Text IDs:] 367,1247,9105,10545,11461-11462
[#12311 Enter a comma-separated list of IDs to edit. Click Refresh below to update the view. Leave blank to display the current overrides. id1,id2,id3-id14,id25-id46]

[#12310 Common IDs:] Login Errors | Login Pages | Health checks | Operator Login | Onboarding | Registration Errors | Sponsorship Confirmation | Navigation
[#12309 Click a link to view common ID sets.]

367: Back to main

1247: License not found: %1

9105: Back to support

10545: Windows 7 (NT @CLEAN_VERSION@)

11461: Security Token:

11462: Security Warning: Invalid security token submitted.
This may indicate another website is attempting to forge a request using your login credentials.

[#6140 Refresh] [#4014 Save and Reload] [#518 Save Changes]

Table 205: *The Translation Pack Configuration Form*

Field	Description
Name	These fields show the information for this translation pack and cannot be edited on this form.
Display Name	
Language Code	
Locales	
Enabled	If selected, enables this translation pack. If this translation pack should not be enabled at this time, leave this check box unselected. Each language code can have only one corresponding translation pack enabled at a time.
Text IDs	Comma-separated list of text IDs for labels and messages in the ClearPass Guest user interface. <ul style="list-style-type: none"> If you accessed this form from the Override Translations link on the Translation Packs

Field	Description
	<p>list view, this field is empty. If you know the text IDs of fields you want to edit, enter them here, separated by commas, and then click Refresh. To view or edit just the items that already have custom overrides, you can leave this field blank.</p> <ul style="list-style-type: none"> If you accessed this form from the Override all translations generated for this page link at the bottom of any page in ClearPass Guest, this field contains a list of all the text IDs for that page and related pages and messages.
Common IDs	<p>Each link in this field corresponds to a group of related pages and messages. Click a link to display the text IDs for all labels and messages in that group. The text IDs are listed in the Text IDs field, and a row is added to the form for each text ID.</p>
(text ID numbers)	<p>These rows appear if text IDs were specified in the Text IDs field. The default text for the field is shown below the text box. For each item you want to override, enter the new text in the text box.</p>
Refresh	<p>If you entered items in the Text IDs field, click this button to add their rows to the form so you can edit them.</p>
Save and Reload	<p>Saves your changes and reloads this form.</p>
Save Changes	<p>Saves your changes and returns to the Translation Packs list view.</p>



Advertising Services lets you deliver marketing promotions and advertisements to your users on a variety of Guest Management registration, receipt, and login pages.

To work with ClearPass Guest Advertising Services, go to **Configuration > Advertising > Start Here**.

This section includes:

- ["About Advertising Services" on page 473](#)
- ["About the Tutorial" on page 474](#)
- ["Advertising Pages" on page 476](#)
- ["Advertising Spaces" on page 484](#)
- ["Advertising Campaigns" on page 492](#)
- ["Advertising Promotions" on page 496](#)
- ["Advertising Materials" on page 502](#)

About Advertising Services

This section describes the main elements you work with to configure Advertising Services to deliver marketing promotions and advertisements through ClearPass Guest: materials, promotions, campaigns, spaces, and pages.

Materials

A material is the individual advertisement you deliver — the ad the user sees. You can deliver ads through Web browsers, email, and SMS. The "type" of an advertising material can be a text, image, Flash, raw HTML, YouTube, or SMS text advertisement. Materials can also be assigned any number of labels, which can be used by promotions to create labeled promotions and to provide intelligent delivery.

Promotions

Most of the rules for how and when advertisements are delivered and what materials should be included are defined in a promotion. These rules are applied to all of the advertising materials that the promotion includes, whether those materials are included directly or indirectly.

A promotion can include both materials and/or other promotions. You can use this feature to build simple groupings of materials with simple rules or more complex groupings of materials and promotions with more complex rules.

Promotions can be enabled and disabled, and have a start date and an end date. They can also be assigned any number of labels. Promotions can include materials and/or other promotions using a fixed, rotating, weighted, or labeled content selection type.

Promotions can also be configured to use intelligent delivery, which uses labels to match relevant advertising to users.

Materials and promotions are then organized into advertising campaigns that run over a specified date range and with a specified priority (rank and weight).

Campaigns

An advertising campaign is the strategy by which you organize the presentation of your ads. It defines which promotions and materials to deliver, and when they should be delivered. You can rank and weight a campaign to balance it against other campaigns. A campaign can also be configured for presentation between a specified start date and end date.

Spaces

Spaces are the areas of a page that are defined for advertising content. Spaces use simple rules to select advertisements with the appropriate size, number, and format of materials. The space determines what types of materials can be shown (images, text ads, SMS ads) and, in the case of images, any size constraints on the size of the ad. For example, size constraints on a 'top' space would normally ensure that only wide but short images are displayed, whereas the constraints on a 'right' space would often allow any type of ad but require that the ad be narrower (e.g. 320 pixels wide).

Pages

Finally, for each ClearPass Guest page or group of pages, you can specify the advertising spaces you want to make active and the campaigns and materials to present on them. Advertising can be placed on login, registration, receipt, and self-service pages, and email and SMS receipts.

Advertising Services Process Overview

To use advertising services:

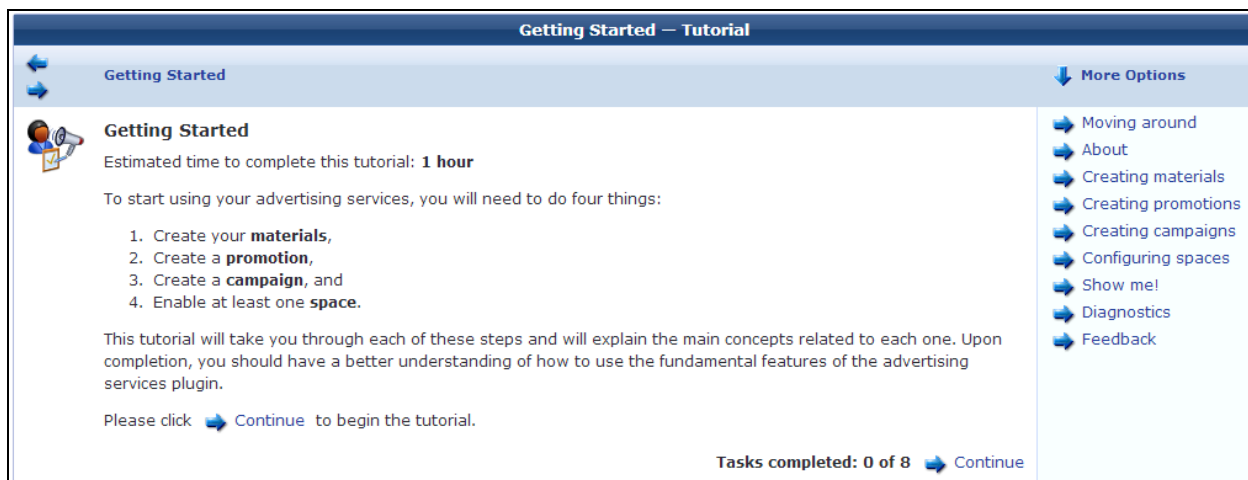
1. Enable the **Advertising Services** option for each Web login or guest self-registration page that is to display advertising. This option is enabled in either **Web Logins** or **Guest Self-Registration** configuration.
2. Add fields for gathering demographic information to Guest self-registration forms.
3. Create the materials and upload them to ClearPass Guest.
4. Create a promotion.
5. Create a campaign.
6. Enable at least one space.
7. For each page or group of pages, specify which campaigns and spaces can be presented.
8. Fine-tune campaign delivery to ensure the best user experience.

About the Tutorial

ClearPass Guest provides a Getting Started tutorial to help you become familiar with Advertising Services concepts and procedures. You can refer to the tutorial at any time.

To view the tutorial, go to **Configuration > Advertising > Start Here** and click the **Getting Started** link. The first page of the tutorial window opens.

Figure 355 *The Advertising Services Getting Started Tutorial*



Topics in the tutorial cover how to create materials, promotions, and campaigns and configure spaces. You can view the finished product of the practice exercises. Tips are provided on how to troubleshoot the different stages of the process.

Navigating the Tutorial

Table 206: *Tutorial Navigation Elements*

To Do This:	Use These Controls:
Move through the tutorial sequentially	Click the Continue link in the bottom right corner next to the count of completed tasks.
Move one page forward or backward	Use the right and left arrows in the top left corner.
Jump to any section of the tutorial	Use the navigation links on the right side.
See additional navigation options	Click the More Options link in the upper right corner. The navigation menu expands to include the Getting Started , Restart Tutorial , and Quit Tutorial links.
Go back to the beginning	Click the More Options link in the upper right corner, and then click the Restart Tutorial link. You will be asked to confirm, and are returned to the Getting Started page.
Exit the tutorial at any time	Click the More Options link in the upper right corner, and then click the Quit Tutorial link.

After you open the tutorial window, it remains open on your screen as you navigate through the application. This lets you refer to it and to related areas of the application at the same time. To close the tutorial window, click the **Quit Tutorial** link.






Advertising Pages



The **Advertising Pages** form lists the Guest Manager areas whose pages can be used for advertising, and provides access to advertising configuration for them. In ClearPass Guest, these pages include login, registration, receipt and self-service pages, and email and SMS receipts.

To work with the advertising settings for a Guest Manager page group or page, go to **Configuration > Advertising > Pages**. The **Advertising Pages** list view opens.

Figure 356 *The Advertising Pages List View*

Page Group	Type	# Child Pages
 Guest Management Advertising settings for guest management pages used by operators and administrators.	Guest Management	4
 Guest Self-Registration Default settings for visitor self-registration.	Guest Self-Registration	8
 Edit  Go To  Launch		

Columns show the page group, the type of page, and the number of child pages in that group. For example, the Guest Management page group has four child pages and the Guest Self-Registration page group has eight child pages, as shown in the following table.

Table 207: *Page Groups and Child Pages*

Page Group	Child Pages
Guest Management	Web Receipts Download Receipt Email Receipts SMS Receipts
Guest Self-Registration	Registration Page Receipt Page Receipt Download Receipt Email Login Page Login Message Receipt SMS Self-Service :Portal

You can click a page group in the **Advertising Pages** list for additional options:

Table 208: Advertising Pages List

Field	Description
Edit	Edit the advertising settings for any of the pages in the Guest Management or Self-Registration page groups. See "Editing Advertising Pages" on page 477.
Go To	Opens the corresponding area of the ClearPass Guest application: <ul style="list-style-type: none"> For Guest Management, opens the Start page of the Guest Manager module. For Guest Self-Registration, opens the Customize Guest Registration edit diagram.
Launch	For Guest Self-Registration, opens the visitor self-registration login page in a new tab.

Editing Advertising Pages

In ClearPass Guest, advertising can be placed on registration pages, receipt and self-service pages, and email and SMS receipts. For each of these pages, you can specify whether or not advertising will be delivered, the advertising spaces that will be used, and the campaigns to present on the page. These settings can be applied to all pages in a page group, or can be overridden for single pages in the group.



Advertising Services must be enabled for each Web login or guest self-registration page that is to display advertising. To enable this option, go to either **Configuration > Pages > Web Logins** or **Configuration > Pages > Guest Self-Registration > Master Enable** and select the **Advertising Services** check box.

To edit advertising settings for a page group or page, go to **Configuration > Advertising > Pages**, then click the **Edit** link for a page group. The **Edit Page** form opens.

Figure 357 The Edit Page Form

Edit Page

General Properties

Page:	Guest Management
Parent Page:	Guest Management does not have a parent page.
Child Pages:	<p>The following pages are children of this page. ↑ Hide children (4 in total)</p> <ul style="list-style-type: none"> Guest Management (Web Receipts) Page advertising settings Guest Management (Download Receipt) Page advertising settings Guest Management (E-mail Receipts) Page advertising settings Guest Management (SMS Receipts) Page advertising settings
Advertising Enabled:	<input type="text" value="Use default setting (Enable advertising on this page)"/> <small>Select whether or not advertising should be delivered on this page.</small>
Description:	<div style="border: 1px solid #ccc; height: 40px; width: 100%;"></div> <small>Enter comments or notes about this page.</small>

In the **General Properties** area of the form, select either the page group or page and configure the basic properties.



If you leave the **Edit Page** form set to the parent page, your edits will apply to the parent page of the group and to all the child pages in the group. To override these settings for a child page, you must click **Show Children**, and then click the **Page advertising settings** link for the child page.

Table 209: *General Properties, Edit Page*

Field	Description
Page	The page group being edited. The page group name is a link to the corresponding area of the application: <ul style="list-style-type: none"> • The Guest Management link opens the Start page of the Guest Manager module. • The Guest Self-Registration link opens the Customize Guest Registration edit diagram.
Parent Page	Indicates the page's parent page, if there is one. This field only contains links when you are editing a child page: <ul style="list-style-type: none"> • Launch page — Opens the parent page. • Page advertising settings — Lets you configure advertising for the parent page.
Child Pages	Indicates the page's child pages, if there are any. This field only contains links when you are editing a parent page. <ul style="list-style-type: none"> • Show Children — Displays the list of child pages. • Page advertising settings — Lets you configure advertising services for a specific child page. • You can click a child page's name to go to the Customize Guest Registration form for that child page.
Advertising Enabled	Specifies whether the page is enabled or disabled for advertising. <ul style="list-style-type: none"> • Use default setting (Enable advertising on this page) – Enables advertising on this page and on its child pages. Available for page group only. • Use parent setting – Ensures that advertising on this child page is only enabled if advertising is enabled for the parent page. Available for child pages only. Default setting for a child page. • Disable advertising on this page – Disables advertising on this page. If this is a parent page, disables advertising for all child pages that are configured to "Use parent setting". • Enable advertising on this page – Enables advertising on this page. If this is a parent page, enables advertising for all child pages that are configured to "Use parent setting".
Description	Optional comments or notes about the page.

Figure 358 *The Edit Page Form, Space Options Area*

Space Options
These options control which spaces can be used for advertising on this page.

Allowed Spaces Policy:	<input type="text" value="Use parent spaces, but also allow advertising in..."/> <small>Select whether to use the same spaces as this page's parent, additional spaces, or all spaces.</small>
Allowed Spaces:	<div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <p style="text-align: center; margin: 0;">Allowed Space</p> <p style="margin: 0;"><input type="text" value="Mobile Page Interstitial (built-in)"/></p> <p style="margin: 0;"> ✖ Remove ➡ Insert Before ➡ Insert After </p> </div> <small>To allow advertising on this page to be placed in a 'space', add the space to this list. Note that a space must also be enabled for it to show an advertisement.</small>
Denied Spaces Policy:	<input type="text" value="No change"/> <small>Select whether or not to deny advertising in any spaces.</small>
Preview:	<p>i No enabled spaces are allowed, therefore no advertising will be shown for this page.</p> <small>Save and reload to update the preview.</small>

In the **Space Options** area of the form, set the options that control which advertising spaces can be shown on this page. The final set of advertising spaces that is used is determined by first applying the **Allowed Spaces** policy, and then applying the **Denied Spaces** policy.

Table 210: *Space Options, Edit Page*

Field	Description
Allowed Spaces Policy	<p>Specifies which spaces to use. Options include:</p> <ul style="list-style-type: none"> • Use default setting (Allow advertising in all spaces) – Allows advertising in all enabled and applicable advertising spaces. Available for page group only. • Allow advertising in... – The form expands to include the Allowed Spaces row. Available for page group only. • Use parent spaces – Allows advertising in the list of spaces defined by the parent page's space options (determined by applying the Allowed Spaces Policy followed by the Denied Spaces Policy). Available for child pages only. • Use parent spaces, but also allow advertising in... – The form expands to include the Allowed Spaces row. Additional spaces you select are added to the list of spaces defined by the parent page's space options (determined by applying the Allowed Spaces Policy followed by the Denied Spaces Policy). Available for child pages only. • Allow advertising in all spaces – Allows advertising in all enabled and applicable spaces. <p>The Denied Spaces Policy is applied after this field, so the final list of spaces that is used might be less than what is allowed here.</p>
Allowed Spaces	<p>If Use parent spaces, but also allow advertising in is selected in the Allowed Spaces Policy, use the controls in this field to add and sort spaces. Any advertising space you specify in this field will be added to the list of spaces used to deliver advertisements. (To be displayed, spaces must also be enabled)</p> <p>Suggestion: You can use this field at the page group level to specify a small number of allowed spaces, and then at the child page level to add extra spaces as needed,</p>
Denied Spaces Policy	<p>Specifies whether to deny advertising in any spaces. Options include:</p> <ul style="list-style-type: none"> • No change – Leaves the list of spaces allowed by the Allowed Spaces Policy unchanged. • Deny advertising in... – The form expands to include the Denied Spaces row. • Deny advertising in all spaces – Denies advertising in all spaces for this page.
Denied Spaces	<p>Specifies the denied spaces.</p> <p>Suggestion: You can also use this field to specify an exception to an "Allow advertising in all spaces" setting.</p>
Preview	<p>Displays a preview of the form showing your changes. To review the chosen set of advertising spaces, click the Save and Reload button and then expand this Preview list.</p>

Figure 359 The Edit Page Form, Campaign Options Area

Campaign Options These options control which campaigns can deliver advertising on this page.	
Allowed Campaigns Policy:	<input type="text" value="Use parent campaigns, but also allow advertising from..."/> Select whether to use the same campaigns as this page's parent, additional campaigns, or all campaigns.
Allowed Campaigns:	<div style="border: 1px solid #ccc; padding: 5px;"><p style="text-align: center;">Allowed Campaign</p><p>Example Campaign </p><p> Remove Insert Before Insert After</p></div> <p>To allow advertising on this page to be provided by a 'campaign', add the campaign to this list. Note that a campaign must also be enabled for it to deliver an advertisement.</p>
Denied Campaigns Policy:	<input type="text" value="Deny advertising from..."/> Select whether or not to deny advertising from any campaigns.
Denied Campaigns:	<div style="border: 1px solid #ccc; padding: 5px;"><p style="text-align: center;">Denied Campaign</p><p>Example Campaign </p><p> Remove Insert Before Insert After</p></div> <p>To deny advertising on this page from being provided by a 'campaign', add the campaign to this list.</p>
Preview:	<p>The following campaigns will be allowed to deliver advertisements for this page. Hide selected campaigns (3 in total)</p> <ul style="list-style-type: none"> Example Campaign Rewards September Back-to-School <p>Save and reload to update the preview.</p>
<div style="display: flex; justify-content: space-around;"> Save Changes Save and Reload</div>	

In the **Campaign Options** area of the form, set the options that control which campaigns can deliver advertising on this page. The final set of advertising campaigns that is used is determined by first applying the **Allowed Campaigns Policy**, and then applying the **Denied Campaigns Policy**.

Table 211: Campaign Options, Edit Page

Field	Description
Allowed Campaigns Policy	<p>Specifies which campaigns to use. Options include:</p> <ul style="list-style-type: none"> • Use default setting (Allow advertising from all campaigns) – Allows advertising from all enabled and applicable campaigns. Available for page group only. • Allow advertising from... – The form expands to include the Allowed Campaigns row. Available for page group only. • Allow advertising from all campaigns – Allows advertising from all enabled and applicable advertising campaigns. • Use parent campaigns – Allows advertising from the list of campaigns defined by the parent page's campaign options (determined by applying the Allowed Campaigns Policy followed by the Denied Campaigns Policy). Available for child pages only. • Use parent campaigns, but also allow advertising from... – The form expands to include the Allowed Campaigns row. Additional campaigns you select are added to the list of campaigns defined by the parent page's campaign options (determined by applying the Allowed Campaigns Policy followed by the Denied Campaigns Policy). Available for child pages only. <p>The Denied Campaigns Policy is applied after this field, so the final list of campaigns that is used might be less than what is allowed here.</p>
Allowed Campaigns	<p>If Use parent campaigns, but also allow advertising from... is selected, use the controls in this field to add and sort campaigns. (To display ads, campaigns must also be enabled)</p> <p>Suggestion: You can use this field at the page group level to specify a small number of allowed campaigns, and then at the child page level to add extra campaigns as needed,</p>
Denied Campaigns Policy	<p>Specifies whether to deny advertising in any campaigns. Options include:</p> <ul style="list-style-type: none"> • No change – Leaves the list of campaigns allowed by the Allowed Campaigns Policy unchanged. • Deny advertising from... – The form expands to include the Denied Campaigns row. • Deny advertising from all campaigns – Denies advertising from all campaigns for this page. <p>Suggestion: You can also use this field to specify an exception to an "Allow advertising from all campaigns" setting.</p>
Denied Campaigns	<p>If Deny advertising from... is selected, use the controls in this field to specify the denied campaigns.</p>
Preview	<p>Displays a preview of the form showing your changes. To review the chosen set of advertising campaigns, click the Save and Reload button and then expand this Preview list.</p>

The nwa_adspace Smarty Template Tag

For details about Smarty Template syntax and HTML, see "[Smarty Template Syntax](#)" on page 700 of the Reference chapter.



The nwa_adspace Smarty Template tag is for advanced users. You need to understand HTML and Smarty Templates in order to use it correctly.

The nwa_adspace tag can be placed into HTML fields that:

- Support Smarty Template evaluation
- Belong to pages that support advertising

The `nwa_adspace` tag supports the following parameters:

- `location`
- `name`
- `media`
- `stage`
- `container`
- `style`

location

The value of the Location field that must be set for an advertising space to be matched by location. The **Location** field and the **Other Location** field are configured on the **Edit Space** form (see ["Creating and Editing Advertising Spaces" on page 486](#)).



You must specify either a `location` or a `name`. The `nwa_adspace` tag will give an error if you do not specify at least one of these parameters.

If a `location` parameter is specified, then the value of the `location` parameter will be compared to the **Location** field of each advertising space. If the values match, then advertisements will be delivered at the point in the HTML where the `nwa_adspace` tag is defined, and according to any constraints defined by the advertising space.



To see which Location value a space uses, review the **Location** column in the **Advertising Spaces** list view (["Advertising Spaces" on page 484](#)).

Advertising spaces support a number of preset location options as well as custom locations via the **Other Location** field. The following parameters are supported for the location parameter:

Table 212: *Values for the location Parameter*

Value	Description
N/A	None—for manually-positioned spaces
<code>web_top</code>	Page Top—above content
<code>web_left</code>	Page Left—to the left of content
<code>web_bottom</code>	Page Bottom—below content
<code>web_right</code>	Page Right—to the right of content
<code>web_interstitial</code>	Page Interstitial—briefly replaces content

Value	Description
sms_top	SMS Top—above content
sms_bottom	SMS Bottom—below content
Use Other Location	Other—for user-defined locations

name

The value of the **Name** field that must be set for an advertising space to be matched by name.



You must specify either a `location` or a `name`. The `nwa_adspace` tag will give an error if you do not specify at least one of these parameters.

if a `name` parameter is specified, then the value of the `name` parameter will be compared to the **Name** field of each advertising space. If the values match, then advertisements will be delivered at the point in the HTML where the `nwa_adspace` tag is defined, and according to any constraints defined by the advertising space.

media

The type of media that advertisements are being delivered to.



You must specify a `media` value. The `nwa_adspace` tag will give an error if you do not specify this parameter.

The `media` parameter must be set correctly for the context in which the `nwa_adspace` tag will be processed. The following values are supported for the `media` parameter:

Table 213: Values for the `media` Parameter

Value	Description
sms	Specify this value to deliver SMS advertisements only.
web	Specify this value to deliver Web and Email advertisements only.

stage

The value of the **Stage** field that must be set for an advertising campaign to be matched.



You must specify a `stage` value. The `nwa_adspace` tag will be unable to match any advertising campaigns if you do not specify this parameter.

The `stage` parameter is used when processing advertising campaigns. Only the promotions or materials specified at the corresponding stage of the advertising campaign will be delivered. The following values are supported for the `stage` parameter:

Table 214: Values for the *stage* Parameter

Value	Description
web_login	Specify this value to deliver advertising on a login page (landing page).
web_registration	Specify this value to deliver advertising on a guest self-registration page.
web_receipt	Specify this value to deliver advertising on a receipt page.
web_self_service	Specify this value to deliver advertising on a guest self-service page.
web_after_login	Specify this value to deliver advertising on a login message page (post-login page).
sms_receipt	Specify this value to deliver advertising on an SMS receipt.

container

The name of the HTML element tag in which advertisements will be placed.



The `nwa_adspace` Smarty Template tag is for advanced users. You need to understand HTML and Smarty Templates in order to use it correctly.

When advertisements are to be delivered to a Web page or an email, they can be grouped and their layout controlled more effectively by placing them in a container. Typically, a DIV container would be used, but other valid HTML tags can be specified.

If the container parameter is not specified, then advertisements are delivered to the Web page or email without any extra grouping.

style

The style attribute of the HTML container element.



This parameter is only relevant when the `media` parameter is set to `web` and an HTML tag name has been specified for the `container` parameter.

If you specify a container, you can use the `style` parameter to specify style attributes for the container. The `style` parameter is optional.

Advertising Spaces



Spaces are the areas of a page that are defined for advertising content. The **Advertising Spaces** list shows and describes the spaces that are currently defined on each type of page, differentiated by device. Descriptions

include typical uses of the space. Several built-in spaces are available. You can also create new custom advertising spaces.

To work with the settings for advertising spaces, go to **Configuration > Advertising > Spaces**. The **Advertising Spaces** list view opens.

Figure 360 *The Advertising Spaces List View*

Space Name	Location
Mobile Page Bottom (built-in) A built-in advertising space for a mobile device that is located at the bottom of a page. This space is typically used for up to three text advertisements.	Page Bottom (web_bottom)
Edit Enable Copy	
Mobile Page Interstitial (built-in) A built-in advertising space for a mobile device that briefly replaces the page content. This space is typically used for a single video advertisement (e.g. 300 pixels wide, by 240 pixels high).	Page Interstitial (web_interstitial)
Mobile Page Top (built-in) A built-in advertising space for a mobile device that is located at the top of a page. This space is typically used for short but wide banner images (e.g. 300 pixels wide, by 100 pixels high).	Page Top (web_top)
Page Bottom (built-in) A built-in advertising space that is located at the bottom of a page. This space is typically used for up to three text advertisements.	Page Bottom (web_bottom)
Page Interstitial (built-in) A built-in advertising space that briefly replaces the page content. This space is typically used for a single large video advertisement (e.g. 480 pixels wide, by 360 pixels high).	Page Interstitial (web_interstitial)
Page Left (built-in) A built-in advertising space that is located on the left of a page. This space is typically used for up to three narrow Flash and image advertisements (e.g. 300 pixels wide, by 200 pixels high) and/or text advertisements.	Page Left (web_left)

All advertising spaces that have been created are included in this list. You can click a space's row in the list for additional options.

Table 215: *Advertising Spaces List*

Field	Description
Edit	Edit any of the space's properties. See "Creating and Editing Advertising Spaces" on page 486.
Delete	Deletes a custom space. You will be asked to confirm the deletion. Not available for built-in spaces.
Enable	Enable the space so advertising will be displayed in it. Before advertising will be delivered in an enabled space on a specific page, the page's settings also need to allow advertising in the space.

Field	Description
Disable	To make advertising inactive again for an enabled space, click the Disable link.
Copy	Make a copy of the space configuration to use as a basis for a new configuration. Suggestion: If you want to have multiple advertising spaces in the same location—for example, one for images and one just for text—creating a copy of a space and making slight changes to it might be the simplest way.
Create new advertising space	Create a new custom advertising space.

Creating and Editing Advertising Spaces

Spaces define the areas of a page that can display advertising content. Spaces use simple rules to select advertisements with the appropriate size, number, and format of materials. The space determines what types of materials can be shown (images, text ads, SMS ads) and, in the case of images, any size constraints on the size of the ad. For example, size constraints on a 'top' space would normally ensure that only wide but short images are displayed, whereas the constraints on a 'right' space would often allow any type of ad but require that the ad be narrower (e.g. 320 pixels wide).

Each space is configured to deliver advertisements in a particular location on a page, such as the top, bottom, left, or right. There is also what is called an "interstitial location": Instead of being displayed in an area of a page, interstitial ads replace the main content of a page for a brief time. For example, after a user logs in, an interstitial ad might be displayed for a moment before the main page content is displayed.

Each space is also given a rank. A rank of 1 is given higher preference than a rank of 2. The relative ranks you assign to spaces ensure they are displayed in the order you want. For example, if you have two spaces defined to be in the same location, the space you give a rank of 1 will be placed above the space that has a rank of 2.

The built-in advertising spaces are created automatically by the **Advertising Services** plugin. Most properties of a built-in space can be edited. You can also create new custom advertising spaces.

- To edit advertising settings for either a built-in or custom space, go to **Configuration > Advertising > Spaces**, and then click the **Edit** link for a space. The **Edit Space** form opens.
- To create a new custom advertising space, click the **Create new advertising space** link in the upper-right corner. The **Create Space** form opens.

The **Edit Space** and **Create Space** forms are identical, and are described below.

Figure 361 The Edit Space Form, General Properties Area

Edit Space	
General Properties	
* Name:	Mobile Page Bottom (built-in)
Enabled:	<input type="checkbox"/> Use this space Check this box to allow promotions to be shown in this space.
* Rank:	10 <input type="text"/> Use the rank to place one space before another. A rank of 1 (one) is higher than a rank of 2.
Description:	A built-in advertising space for a mobile device that is located at the bottom of a page. This space is typically used for up to three text advertisements. <small>Enter comments or notes about this space.</small>
Location:	Page Bottom — below content

In the **General Properties** area of the form, set the basic properties for the space:

Table 216: General Properties, Edit Space

Field	Description
Name	(Required) Name that clearly identifies this space. For a built-in space, this cannot be edited.
Enabled	If selected, allows advertising to be shown in this space. If this check box is not selected, the space will not show any advertisements. Before advertising will be delivered in an enabled space on a specific page, the page's settings also need to allow advertising in the space.
Rank	(Required) Applies a relative rank to the space. A rank of 1 is given higher preference than a rank of 2.

Field	Description
Description	Optional comments or notes about this advertising space.
Location	<p>Describes position of the space on the page. For a built-in space, this cannot be edited. For custom spaces, options include:</p> <ul style="list-style-type: none"> • None - for manually positioned spaces – Select this option if you will use the <code>nwa_adspace</code> Smarty Template tag, and to only specify the <code>name</code> parameter, not the <code>location</code> parameter. For more information, see "The nwa_adspace Smarty Template Tag" on page 481. • Page Top - above content – The space will deliver advertisements above the main content of a Web page. • Page Left - to the left of content – The space will deliver advertisements to the left of the main content of a Web page. • Page Bottom - below content – The space will deliver advertisements below the main content of a Web page. • Page Right - to the right of content – The space will deliver advertisements to the right of the main content of a Web page. • Page Interstitial - briefly replaces content – The space will deliver advertisements that will briefly replace the main content of a Web page. • SMS Top - above content – The space will deliver advertisements above the main content of an SMS message. • SMS Bottom - below content – The space will deliver advertisements below the main content of an SMS message. • Other - for user defined locations – Select this option if you will use the <code>nwa_adspace</code> Smarty Template tag to define a custom location by specifying the <code>location</code> parameter, not the <code>name</code> parameter. For more information, see "The nwa_adspace Smarty Template Tag" on page 481. If you select this option, the Other Location field is added to the form.
Other Location	If you selected Other - for user-defined locations in the Location field, use this field to define a name for a custom location. The custom location can then be referenced in any Smarty Template by using the <code>nwa-adspace</code> Smarty Template tag.

"Other Location" Example

If you wanted to add a custom advertising space that is positioned on the far-right edge of the registration page, you could do it as shown in the following example:

1. Choose **Other - for user defined locations** in the **Location** field.
2. In the **Other Location** field, create the name **custom_right**.
3. In a guest self-registration page, edit the **Footer HTML** to include an `nwa_adspace` Smarty Template tag as follows:

```
{nwa_adspace media="web"
  location="custom_right"
  stage="web_registration"
  container="div"
  style="position:absolute; left:839px; top:92px; width:320px; margin:20px 0 0 20px;"}
```

For more information, see ["The nwa_adspace Smarty Template Tag" on page 481](#).

Figure 362 *The Edit Space Form, Geometry Area*

Geometry	
These options control the geometry (width and height) of the advertising space.	
Screen Types:	<input type="text" value="Small Screens — show on small screens only (phones, mobile devices)"/>
	Limit what types of screen will show this advertising space. This setting is only applicable for web advertising.
Minimum Width:	<input type="text" value="220"/>
	Enter a minimum width (in pixels) for this space.
Maximum Width:	<input type="text" value="320"/>
	Enter a maximum width (in pixels) for this space.
Width:	Minimum: <input type="text" value="220"/> Maximum: <input type="text" value="320"/>
	Enter a minimum and/or maximum width (in pixels) for this space.
Minimum Height:	<input type="text"/>
	Enter a minimum height (in pixels) for this space.
Maximum Height:	<input type="text" value="360"/>
	Enter a maximum height (in pixels) for this space.
Height:	Minimum: <input type="text"/> Maximum: <input type="text" value="360"/>
	Enter a minimum and/or maximum height (in pixels) for this space.
Maximum Rows:	<input type="text" value="3"/>
	Enter a maximum number of rows.
Maximum Columns:	<input type="text" value="1"/>
	Enter a maximum number of columns.

In the **Geometry** area of the form, set the options that control the width and height of the space.

Some devices, such as desktop computers and laptops, have a large screen. Other devices, such as smart phones, have a small screen. Although it is possible to deliver large advertisements to small screens, it does not provide the best user experience. Geometry constraints let you configure an advertising space to be only displayed on a large screen or only displayed on a small screen. Typically, the width and height constraints would also be set to values that are appropriate for the selected screen type.



The screen type is detected by looking at the browser's User Agent value. Laptops, desktops, and devices like the iPad are treated as large-screen devices. Smart phones and other mobile devices are treated as small-screen devices.



While we endeavor to correctly detect the screen type for as many devices as possible, we are unable to test every possible device, so we do not claim detection to be correct for all devices.

Table 217: Geometry Options, Edit Space

Field	Description
Screen Types	Limits the types of screen that will show this space. This setting only applies to Web advertising. Options include: <ul style="list-style-type: none"> ● All Screens — show on both small and large screens – Ignores the detected screen type. ● Small Screens — show on small screens only (phones; mobile devices) – This space will only be shown if the user's device is detected to be a small-screen device. ● Large Screens — show on large screens only (laptops, desktops) – This space will only be shown if the user's device is detected to be a large-screen device.
Minimum Width	Optimum minimum width in pixels for advertising materials shown in this space. If an advertisement has a size (for example, a Flash or YouTube ad), the width of that advertisement must be at least as large as this minimum width if it is to be shown in this space. If you do not want to have a minimum width constraint, leave this field blank.
Maximum Width	Optimum maximum width in pixels for advertising materials shown in this space. If an advertisement has a size (for example, a Flash or YouTube ad), the width of that advertisement must be no larger than this maximum width if it is to be shown in this space. If you do not want to have a maximum width constraint, leave this field blank. Best Practice: Because an advertising space also has padding, it is best to set the maximum width constraint to be 20 pixels wider than the widest image that will be displayed in this space.
Width	Minimum and/or maximum width in pixels for this space.
Minimum Height	Optimum minimum height in pixels for advertising materials shown in this space. If an advertisement has a size (for example, a Flash or YouTube ad), the height of that advertisement must be at least as large as this minimum height if it is to be shown in this space. If you do not want to have a minimum height constraint, leave this field blank.
Maximum Height	Optimum maximum height in pixels for advertising materials shown in this space. If an advertisement has a size (for example, a Flash or YouTube ad), the height of that advertisement must be no larger than this maximum height if it is to be shown in this space. If you do not want to have a maximum height constraint, leave this field blank. Best Practice: Because an advertising space also has padding, it is best to set the maximum height constraint to be 20 pixels wider than the tallest image that will be displayed in this space.
Height	Minimum and/or maximum height in pixels for this space.
Maximum Rows	Maximum number of rows of advertisements to show in this space. A space can show multiple rows of ads, up to the maximum number of rows specified here. However, if a maximum height was specified, the system will only output as many rows as will fit within the maximum height constraint for the space.
Maximum Columns	Maximum number of columns of advertisements to show in this space. A space can show multiple columns of ads, up to the maximum number of columns specified (there is always at least one column). However, if a maximum width was specified, the system will only output as many columns as will fit within the maximum width constraint for the space.

"Maximum Height" Example

If a maximum height was specified, the system will only output as many rows as will fit within the maximum height constraint for the space. For example, with a maximum height constraint of 100 and a maximum rows constraint of 3, the system could output any of the following:

- Three rows with heights 40, 40, and 20

- Three rows with heights 30, 30, and 30
- Two rows with heights 60 and 40
- Two rows with heights 50 and 50
- One row of height 80
- One row of height 100

"Maximum Width" Example

If a maximum width was specified, the system will only output as many columns as will fit within the maximum width constraint for the space. For example, with a maximum width constraint of 100 and a maximum columns constraint of 3, the system could output any of the following:

- Three columns with widths 40, 40, and 20
- Three columns with widths 30, 30, and 30
- Two columns with widths 60 and 40
- Two columns with widths 50 and 50
- One columns of widths 80
- One columns of widths 100

Figure 363 *The Edit Space Form, Promotional Material Constraints Area*

In the **Promotional Material Constraints** area of the form, set the options that control what can and cannot be shown in the advertising space:

Table 218: *Promotional Material Constraints, Edit Space*

Field	Description
Allowed Material	<p>The types of promotional material that should be allowed in this space. Types included are:</p> <ul style="list-style-type: none"> • Flash advertisement [Web] • HTML code (advanced) [Web] • Image advertisement [Web] • Text advertisement [Web] • YouTube video advertisement [Web] • Text advertisement [SMS]

When you have completed your entries on this form:

- If you are creating a new space, click **Create** to create the new space and return to the **Advertising Spaces** list, or click **Create and Reload** to create the new space and reload the **Edit Space** form.
- If you are editing an existing space, click **Save** to save your changes and return to the **Advertising Spaces** list, or click **Save and Reload** to save your changes and reload the **Edit Space** form.

Advertising Campaigns



An advertising campaign is the strategy by which you organize the presentation of your ads. It defines which promotions and materials to deliver, and when they should be delivered.



The system requires at least one advertising campaign to be configured and enabled for any advertisements to be delivered.

To create and work with advertising campaigns, go to **Configuration > Advertising > Campaigns**. The **Advertising Campaigns** list view opens.

Figure 364 *The Advertising Campaigns List View*

Campaign Name	Start Date	End Date
Example Campaign An example campaign.		
Edit Delete Disable Copy		
Rewards An example campaign.		
September Back-to-School An example campaign.		

All advertising campaigns that have been created are included in this list. You can click a campaign's row in the list for additional options.

Table 219: *Advertising Campaigns List*

Field	Description
Edit	Edit any of the campaign's properties. See "Creating and Editing Advertising Campaigns" on page 493.
Delete	Delete the campaign from the system. You will be asked to confirm the deletion.
Enable	Enable the advertising campaign so it will provide advertisements. Before advertising will be delivered from an enabled campaign on a specific page, the page's settings also need to allow advertising from the campaign.

Field	Description
Disable	Disable the campaign. To make the campaign active again, click the Enable link.
Copy	Make a copy of the campaign's settings to use as a basis for a new campaign.
Create new advertising campaign	Create a new advertising campaign.

Creating and Editing Advertising Campaigns

An advertising campaign is the strategy by which you organize the presentation of your ads. It defines which promotions and materials to deliver, and at which stages they should be delivered. You can rank and weight a campaign to balance it against other campaigns. A campaign can also be configured for presentation between a specified start date and end date.

Campaigns can be delivered at the following stages:

- On the login page
- On the registration page
- On the registration receipt
- On the self-service portal pages
- Immediately after login
- On the SMS registration receipt

You can edit advertising campaigns, and you can create new advertising campaigns.

- To edit an advertising campaign, go to **Configuration > Advertising > Campaigns**, and then click the **Edit** link for a campaign in the list. The **Edit Campaign** form opens.
- To create a new advertising campaign, click the **Create new advertising campaign** link in the upper-right corner. The **Create Campaign** form opens.

The **Edit Campaign** and **Create Campaign** forms are identical, and are described below.

Figure 365 *The Edit Campaign Form, General Properties Area*

Edit Campaign	
General Properties	
* Name:	<input type="text" value="Example Campaign"/> <small>Enter a name for this campaign.</small>
Enabled:	<input checked="" type="checkbox"/> Use this campaign <small>Check this box to allow promotions from this campaign to be delivered.</small>
Start Date:	<input type="text"/> <input type="button" value="..."/> <small>The campaign will not take effect until this date.</small>
End Date:	<input type="text"/> <input type="button" value="..."/> <small>The campaign is ignored from this date.</small>
* Rank:	<input type="text" value="10"/> <input type="button" value="▲"/> <small>Use the rank to always choose one campaign before another. A rank of 1 (one) is higher than a rank of 2.</small>
* Weight:	<input type="text" value="1"/> <input type="button" value="▲"/> <small>When campaigns are of equal rank, the weight is used to give more (or less) exposure to this campaign compared to the others.</small>
Description:	<input type="text" value="An example campaign."/> <small>Enter comments or notes about this campaign.</small>

In the **General Properties** area of the form, set the basic properties for the campaign:

Table 220: *General Properties, Edit Campaign*

Field	Description
Name	(Required) Name that clearly identifies this campaign.
Enabled	If selected, allows promotions from this campaign to be delivered. If this check box is not selected, no ads will be provided from this campaign. Before advertising will be delivered from a campaign to a specific page, the page's settings also need to allow advertising from the campaign.
Start Date	(Optional) Date and time on which this campaign will begin. To start delivering this campaign immediately, leave this field blank. Click the button to open the calendar picker. In the calendar, use the arrows to select the year and month, click the numbers in the Time fields to increment the hours and minutes, then click a day to select the date.
End Date	(Optional) Date and time after which the campaign will no longer be delivered. To deliver this campaign indefinitely, leave this field blank. Click the button to open the calendar picker. In the calendar, use the arrows to select the year and month, click the numbers in the Time fields to increment the hours and minutes, then click a day to select the date.
Rank	(Required) Applies a relative rank to the campaign, which defines the order in which campaigns are processed when delivering ads. A rank of 1 is higher than a rank of 2. For information about campaign ranks, see " Campaign Rank and Weight " on page 496.
Weight	(Required) Applies a weight to a campaign. If two campaigns have equal rank, one with a greater weight will be displayed more than the other. For information about campaign weights, see " Campaign Rank and Weight " on page 496.
Description	Optional comments or notes about the campaign.

At the time ads are delivered on your pages, the system processes the information in the **General Properties** area in the following order:

1. Verifies which campaigns are enabled and ignores ones that are not.
2. Checks for start dates that are less than or equal to "now" and ignores campaigns that are not scheduled to start yet.
3. Checks for end dates that are greater than "now" and ignores campaigns whose end date is past.
4. Checks the rank of each remaining campaign. Includes only the highest ranked campaign, or multiple campaigns that have the same highest rank.
5. If there are multiple campaigns, checks the weight of each remaining campaign.

Figure 366 *The Edit Campaign Form, Web Promotions Delivery and SMS Promotions Delivery Areas*

Web Promotions Delivery
Configure when the campaign's web promotions are to be delivered.

With login:	<input type="text" value="Example Promotion"/> <small>Select the promotion to deliver on the landing page (login page).</small>
With registration:	<input type="text" value="Example Promotion"/> <small>Select the promotion to deliver on the registration page.</small>
With receipt:	<input type="text" value="Example Promotion"/> <small>Select the promotion to deliver on the registration receipt.</small>
With self-service:	<input type="text" value="— None —"/> <small>Select the promotion to deliver on the 'self-service portal' pages.</small>
After login:	<input type="text" value="Example Promotion"/> <small>Select the promotion to deliver when the user has logged in.</small>

SMS Promotions Delivery
Configure when the campaign's SMS promotions are to be delivered.

With receipt:	<input type="text" value="— None —"/> <small>Select the promotion to deliver on the SMS registration receipt.</small>
---------------	--

In the **Web Promotions Delivery** area of the form, set the options that define when the campaign's Web promotions are delivered. Use the **SMS Promotions Delivery** area to set when the campaign's SMS promotions are delivered.

The drop-down lists in the **Web Promotions** area also allow you to select a material instead of a promotion. This usage is rare, though, as it would display only a single static item.

Table 221: *Web Promotions Delivery, Edit Campaign*

Field	Description
With Login	Specifies the promotion to deliver on the landing page (login page). To not display ads at this stage, select None .
With Registration	Specifies the promotion to deliver on the registration page. To not display ads at this stage, select None .
With Receipt	Specifies the promotion to deliver on the registration receipt. To not display ads at this stage, select None .

Field	Description
With Self-Service	Specifies the promotion to deliver on the self-service portal pages. To not display ads at this stage, select None .
After Login	Specifies the promotion to deliver when the user has logged in. To not display ads at this stage, select None .
With Receipt	Specifies the promotion to deliver on the SMS registration receipt. To not display ads at this stage, select None .

Campaign Rank and Weight

Each advertising campaign must be assigned a rank and weight. These numbers let you balance how campaigns are chosen relative to each other.

- **Rank**—This number determines which of the available campaigns will be used. A lower number has a higher rank or priority, so a rank of 1 takes priority over a rank of 2. When the available campaigns are compared, the campaign with the highest rank (for example, rank = 1) is used and the other campaigns are ignored. To use multiple campaigns at the same time, they must have the same rank; they will be dropped if they have a lower rank.
- **Weight**—When multiple campaigns of equal rank are used, the weight determines how often each campaign's ads should be displayed relative to ads from the other campaigns.

Suppose you have multiple advertising campaigns that are defined to provide ads at the same time and stage. You can modify the *rank* to ensure that ads are displayed from the campaigns in the order you want. You can modify the *weight* to ensure that, on average, more ads are displayed from campaigns with higher weight. The frequency of display is determined by the ratio of each weight to the total weights.

- Example: Assume two campaigns of equal rank. If campaign A has a weight of 10, and campaign B has a weight of 5, campaign A's ads will be shown twice as often as campaign B's ads. To look at this another way, $10 + 5 = 15$, and campaign A's ads will be shown, on average, 10 out of every 15 times.
- Example: Assume three campaigns of equal rank. Campaign A has a weight of 2, campaign B has a weight of 3, and campaign C has a weight of 5. These numbers add up to 10, so on average, campaign A will be shown 2 out of every 10 times, campaign B would be shown 3 out of every 10 times, and campaign C would be shown 5 out of every 10 times.

Ranks and weights are assigned to campaigns when they are created or edited. See "[Creating and Editing Advertising Campaigns](#)" on page 493.

Advertising Promotions



Promotions define rules for how and when advertisements are delivered and what materials should be included. Promotions can also be configured to use intelligent delivery, presenting relevant advertising to users.

To create and work with advertising promotions, go to **Configuration > Advertising > Promotions**. The **Advertising Promotions** list view opens.

Figure 367 *The Advertising Promotions List View*

Promotion Name	Start Date	End Date
Example Promotion An example promotion with rotating content.		
Edit Delete Disable Copy		
Instant Rewards An example promotion with rotating content.		
In-Store Coupon November An example promotion with rotating content.		
Web Special An example promotion with rotating content.		

All advertising promotions that have been created are included in this list. You can click a promotion's row in the list for additional options.

Table 222: *Advertising Promotions List*

Field	Description
Edit	Lets you edit any of the promotion's properties. See " Creating and Editing Advertising Promotions " on page 497.
Delete	Deletes the promotion from the system. You will be asked to confirm the deletion.
Enable	Enables the promotion so it will provide advertisements.
Disable	Disables the promotion. To make the promotion active again, click the Enable link.
Copy	Makes a copy of the promotion's settings to use as a basis for a new promotion.
Create new advertising promotion	Lets you create a new advertising promotion.

Creating and Editing Advertising Promotions

Most of the rules for how and when advertisements are delivered and what materials should be included are defined in a promotion. These rules are applied to all of the advertising materials that the promotion includes, whether those materials are included directly or indirectly.

A promotion can include both materials and/or other promotions. You can use this feature to build simple groupings of materials with simple rules, or more complex groupings of materials and promotions with more complex rules.

Promotions can be enabled and disabled, and have a start date and an end date. They can also be assigned any number of labels. Promotions can include materials and/or other promotions using a fixed, rotating, weighted, or labeled content selection type. Promotions can also be configured to use intelligent delivery, which uses labels to match relevant advertising to users.

To edit an advertising promotion, go to **Configuration > Advertising > Promotions**, then click the **Edit** link for a promotion. The **Edit Promotion** form opens.

Figure 368 *The Edit Promotion Form, General Properties Area*

Edit Promotion	
General Properties	
* Name:	<input type="text" value="Example Promotion"/> <small>Enter a name for this promotion.</small>
Enabled:	<input checked="" type="checkbox"/> Use this promotion <small>Check this box to allow this promotional material to be delivered.</small>
Start Date:	<input type="text"/> <input type="button" value="..."/> <small>Ensure that the promotional material is not delivered until this time.</small>
End Date:	<input type="text"/> <input type="button" value="..."/> <small>Ensure that the promotional material is not delivered after this time.</small>
Description:	<input type="text" value="An example promotion with rotating content."/> <small>Enter comments or notes about this promotional material.</small>
Labels:	<input type="text"/> <small>Enter labels for this promotion, separated by commas or newlines. Other promotions can then automatically detect this promotion as 'labelled content'.</small>
* Type:	<input type="text" value="Rotating content"/> <input type="button" value="v"/> <small>Select the type of content.</small>

In the **General Properties** area of the form, set the basic properties for the promotion:

Table 223: *General Properties, Edit Promotion*

Field	Description
Name	(Required) Name that clearly identifies this promotion.
Enabled	If selected, allows this promotional to deliver ads. If this check box is not selected, no ads will be provided by this promotion.
Start Date	Date and time when the promotion can start providing ads. To have this promotion start providing ads immediately, leave this field blank. Click the button to open the calendar picker. In the calendar, use the arrows to select the year and month, click the numbers in the Time fields to increment the hours and minutes, then click a day to select the date.
End Date	Date and time after which the promotion will no longer provide ads. To have this promotion deliver ads indefinitely, leave this field blank. Click the button to open the calendar picker. In the calendar, use the arrows to select the year and month, click the numbers in the Time fields to increment the hours and minutes, then click a day to select the date.

Field	Description
Description	Optional comments or notes about this promotional material.
Labels	<p>To apply labels to this promotion, enter the labels in this field. To create new labels, enter the new label names separated by commas or new lines. The system creates each new label as a "tag". If some labels were already created, clicking in this field displays a list of the existing label tags to choose from.</p> <p>If you include labels here, other promotions will detect this promotion as labeled content.</p> <p>Labels are used to include or exclude this promotion when creating another higher-level labeled-content promotion. When processing intelligent delivery rules, labels are applied to all materials that are included, either directly or indirectly, by this promotion. For more information, see "Using Labels in Advertising Services" on page 501.</p>
Type	<p>(Required) The type of content. Options include:</p> <ul style="list-style-type: none"> ● Rotating content ● Fixed content ● Weighted content ● Labeled content <p>When you make a selection here, the name of the next area of the form changes to match and includes the appropriate options.</p>

Figure 369 *The Edit Promotions Form, Rotating Content Area*

Rotating Content
These options control the rotating content of the promotion.

* Content Items:	<table style="width: 100%; border-collapse: collapse;"> <thead> <tr style="background-color: #1a3d4d; color: white;"> <th style="text-align: center; padding: 2px;">Content</th> </tr> </thead> <tbody> <tr><td style="padding: 2px;">Example Banner (blue, 728x90) ▼</td></tr> <tr><td style="padding: 2px;">Example Banner (orange, 728x90) ▼</td></tr> <tr><td style="padding: 2px;">Example Banner (steel, 728x90) ▼</td></tr> <tr><td style="padding: 2px;">Example Image (blue, 300x200) ▼</td></tr> <tr><td style="padding: 2px;">Example Image (orange, 300x200) ▼</td></tr> <tr><td style="padding: 2px;">Example Image (orange, 300x200) ▼</td></tr> <tr><td style="padding: 2px;">Example Text ▼</td></tr> </tbody> </table>	Content	Example Banner (blue, 728x90) ▼	Example Banner (orange, 728x90) ▼	Example Banner (steel, 728x90) ▼	Example Image (blue, 300x200) ▼	Example Image (orange, 300x200) ▼	Example Image (orange, 300x200) ▼	Example Text ▼
Content									
Example Banner (blue, 728x90) ▼									
Example Banner (orange, 728x90) ▼									
Example Banner (steel, 728x90) ▼									
Example Image (blue, 300x200) ▼									
Example Image (orange, 300x200) ▼									
Example Image (orange, 300x200) ▼									
Example Text ▼									
Selected Content:	<p style="margin: 0;">↓ show selected items (7 total).</p> <p style="margin: 0;">Save and reload to update the preview.</p>								

Depending on the selection in the **Type** field, the next area of the form will be either **Rotating Content**, **Weighted Content**, **Fixed Content**, or **Labeled Content**. In this area, set the options that control the content of the promotion.

Table 224: *Rotating, Fixed, Weighted, or Labeled Content, Edit Promotion*

Field	Description
Content	For fixed content, select a single content item for the promotion.
Content Items	(Required) For rotating or weighted content, all items in this list are initially selected. Click an item's row to access controls for removing items or changing their order.
Content Types	(Labeled content) Types of content to include in this promotion. Options include: <ul style="list-style-type: none">• All content types• Materials only• Promotions only
Inclusion Mode	(Labeled content) How the list of inclusive labels is matched to the available content. Options include: <ul style="list-style-type: none">• All of the "inclusive labels" must match• At least one of the "inclusive labels" must match
Inclusive Labels	(Labeled content) Enter inclusive labels, separated by commas or new lines. Content must match these labels to be included in the promotion. (Refer to the Defined Labels field in the Intelligence area of the form)
Exclusion Mode	(Labeled content) How the list of exclusive labels is matched to the available content. Options include: <ul style="list-style-type: none">• All of the "exclusive labels" must match• At least one of the "exclusive labels" must match
Exclusive Labels	(Labeled content) Enter exclusive labels, separated by commas or new lines. Content is excluded from the promotion if it matches these labels. (Refer to the Defined Labels field in the Intelligence area of the form)
Selected Content	List of the content selected on this form. After making changes to the content selection, click the Save and Reload button to refresh this list.

Figure 370 The Edit Promotions Form, Intelligence Area

Intelligence
These options control the intelligent delivery of content for the promotion.

Enabled: Enable intelligent delivery.
Check this box to enable a more selective delivery by matching user labels to material labels.
Note that a material will also 'inherit' the labels from the promotions that include it (either directly or indirectly).

Requirement Levels:

Labels	Requirement Level
<p>i No labels have been added to the list.</p> <p> Add a label</p>	

Edit how often particular labels should be matched.
These settings override the 'default level' below.

Default Level: — Requirement —

Edit how often all 'other' labels should be matched.
This setting is applied to labels not listed above at 'requirement levels'.

Defined Labels:

Labels	Defined User Labels
<p>airgroup_device_type</p> <p>— Type</p>	<p>airgroup_device_type (Other), airtgroup_device_type Apple TV, airgroup_device_type Apple iPad, airtgroup_device_type Apple iPhone, airgroup_device_type Apple iPod, airtgroup_device_type Blu-Ray Player, airgroup_device_type PlayStation 3, airtgroup_device_type Printer, airgroup_device_type Xbox 360</p>

Above are the currently defined user labels.
You can copy some of them to materials or promotions to support intelligent delivery.

Save Changes
 Save and Reload

In the **Intelligence** area of the form, set the options that control intelligent delivery of content for the promotion:

Table 225: Intelligence Options, Edit Promotion

Field	Description
Enabled	If selected, allows a more selective delivery by matching user labels to material labels. (Material also inherits labels from the promotions that include it)
Requirement Levels	How often the specified labels should be matched. These settings override the Default Level in the next field. Use the controls to select label groups and a requirement level for each one.
Default Level	How often all other labels should be matched (applies to labels not selected in the Requirement Levels field).
Defined Labels	List of currently-defined user labels.

Using Labels in Advertising Services

A *label* identifies a user attribute or category. In Advertising Services, you can add intelligent delivery to your campaigns by creating labels and applying them to your promotions and materials:

1. Configure your pages to include fields for collecting user information such as gender, age, hobbies, or product preferences. When a user completes these fields, the attributes are stored in ClearPass (see "Creating a Custom Field " on page 295).

2. In the **Edit Promotion** form, use the **Labels** field to apply or easily create labels that correspond to the information-gathering fields you added to your pages (see "[Creating and Editing Advertising Promotions](#)" on page 497).
3. Configure the promotion to use labeled content (promotions, materials, or both), and specify which labels to include or exclude.
4. Also on the **Edit Promotion** form, enable the promotion for intelligent delivery. Indicate the percentage of ads that should match the labels. (For reference, this form provides a list of the labels that have already been defined in the system.)
5. On the **Edit Materials** form, you can also use the **Labels** field to apply existing labels or create new ones (see "[Creating and Editing Advertising Materials](#)" on page 503).
6. After the promotions and materials that include the labels and intelligent delivery configuration are complete, include them in a campaign (see "[Creating and Editing Advertising Campaigns](#)" on page 493).
7. When a user visits the pages while the campaign is running, Advertising Services displays ads with the labeled content that matches the user's attributes.

When you create labels in the Edit Promotion or Edit Materials forms, they are created as "tags" in the system. Clicking in a Labels field provides an auto-suggested list of existing tags to choose from. To see a list of Label tags that have already been created for your advertising campaigns, go to **Administration > Plugin Manager** and click the **Configuration** link for the **Advertising Services** plugin:

Figure 371 *The Advertising Services Plugin Configuration Form*





Advertising Materials



A material is the individual advertisement you deliver — the ad the user sees.

To create and work with advertising materials, go to **Configuration > Advertising > Materials**. The **Advertising Materials** list view opens.

Figure 372 *The Advertising Materials List View*

Material Name	Start Date	End Date
 Example Banner (blue,728x90) An example advertising banner.		
 Edit  Delete  Disable  Copy  Preview		
 Example Banner (orange,728x90) An example advertising banner.		
 Example Banner (steel,728x90) An example advertising banner.		
 Example Image (blue,300x200) An example advertising banner.		
 Example Image (orange,300x200) An example advertising banner.		
 Example Image (steel,300x200) An example advertising banner.		
 Example Text An example text advertisement.		

All advertising materials that have been created are included in this list. You can click a material's row in the list for additional options.

Table 226: *Advertising Materials List*

Field	Description
Edit	Lets you edit any of the material's properties. See " Creating and Editing Advertising Materials " on page 503.
Delete	Deletes the material from the system. You will be asked to confirm the deletion.
Disable	Disables the material. To make the material active again, click the Enable link.
Copy	Makes a copy of the material's settings to use as a basis for a new material.
Create new advertising promotion	Lets you create a new advertising material.

Creating and Editing Advertising Materials

An advertising material is the individual advertisement you deliver — the ad the user sees. You can deliver ads through Web browsers, email, and SMS. The medium of an advertising material can be a text, image, Flash, raw HTML, YouTube, or SMS text advertisement. Materials can also be assigned any number of labels, which can be used by promotions to create labeled promotions and to provide intelligent delivery.

To edit settings for an advertising material, go to **Configuration > Advertising > Materials**, then click the **Edit** link for a material. The **Edit Promotional Material** form opens.

Figure 373 The Edit Promotional Material Form, General Properties Area

Edit Promotional Material	
General Properties	
* Name:	Example Banner (orange, 728x90) <small>Enter a name for this material.</small>
Enabled:	<input checked="" type="checkbox"/> Use this material <small>Check this box to allow this promotional material to be delivered.</small>
Start Date:	<input type="text"/> <small>...</small> <small>Ensure that the promotional material is not delivered until this time.</small>
End Date:	<input type="text"/> <small>...</small> <small>Ensure that the promotional material is not delivered after this time.</small>
Description:	An example advertising banner. <small>Enter comments or notes about this promotional material.</small>
Labels:	<small>Enter labels for this material, separated by commas or newlines. Promotions can then automatically detect this material as 'labelled content'.</small>
* Type:	Web browser content <small>▼</small> <small>Select the type of material.</small>

In the **General Properties** area of the form, set the basic properties for the material:

Table 227: General Properties, Edit Promotional Material

Field	Description
Name	(Required) Name for this material.
Enabled	If selected, allows this material to be delivered.
Start Date	Date and time on which this campaign will begin. To start delivering this material immediately, leave this field blank.
End Date	Date and time after which the material will no longer be delivered. To deliver this material indefinitely, leave this field blank.
Description	Optional comments or notes about the material.
Labels	To apply labels to this material, enter the labels in this field. To create new labels, enter the new label names separated by commas or new lines. The system creates each new label as a "tag". If some labels were already created, clicking in this field displays a list of the existing label tags to choose from. If you include labels here, promotions will detect this material as labeled content. Labels are used to include or exclude material for a labeled content promotion. Labels are matched when processing intelligent delivery rules of a promotion that includes this material.
Type	(Required) The type of content. Options include: <ul style="list-style-type: none"> • Web browser content • SMS content When you make a selection here, the name of the next area of the form changes to match and includes the appropriate options.

Figure 374 The Edit Promotional Materials Form, Web Content Area

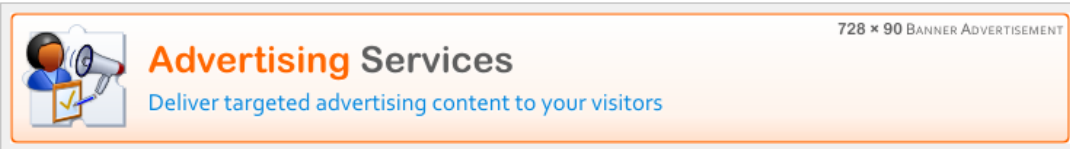
Web Content
These options control the content and formatting of web promotions.

* **Format:**
Select the format of the promotional material.

Hyperlink:
The URL to which the advertisement is linked.

Image:
Select an image file for the advertisement.

Title:
Title of the image. This will be displayed as the alternative text for the advertisement.

Preview: 

Depending on the selection in the **Type** field, the next area of the form will be either **SMS Content** or **Web Content**. In this area, set the options that control either the content of the SMS text messages promotion, or the content and formatting of the Web promotion.

Table 228: SMS Content or Web Content, Edit Material

Field	Description
Text	(SMS content) Enter the message text. To keep messages short, use 80 characters or fewer.
Format	(Web content) (Required) If Web browser content is selected in the Type field, use this field to select the format of the Web content material. Options include: <ul style="list-style-type: none"> ● Flash advertisement ● HTML code (advanced) ● Image advertisement ● Text advertisement ● YouTube video advertisement When you make a selection here, the rest of the form includes the appropriate options.
Flash	(Flash) The Flash animation file (.swf) of the material. Either select a file that is already uploaded to Content Manager, or upload a new file. Maximum file upload size is 15.0 MB.
Template Code	(HTML code) To code your own advertisement using raw HTML, enter the HTML code to display. Smarty template functions can be used. You can also use the drop-down list to add images or other content items.
Preview	(HTML code) Preview of the HTML. The preview is updated when you modify the contents of the Template Code field.
Hyperlink	(Image advertisement; Text advertisement) The destination page URL to which the advertisement is linked. To not associate a destination URL with the advertisement, leave this field blank.

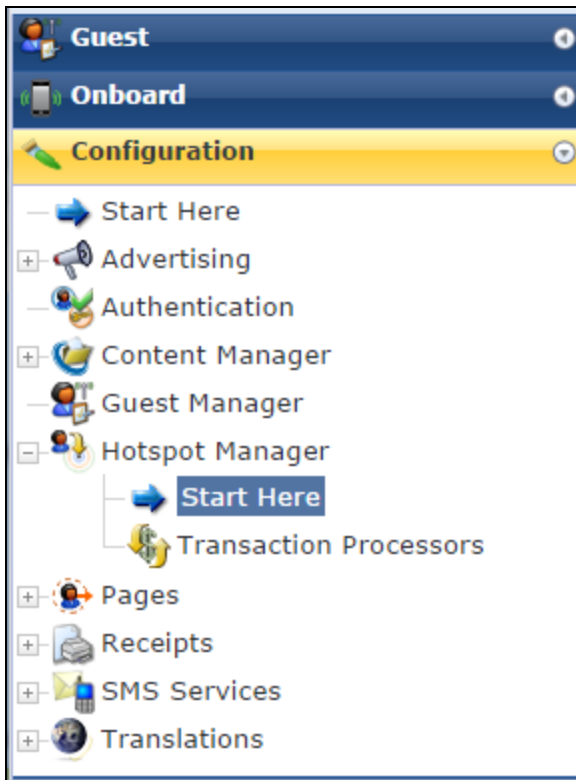
Field	Description
Image	(Image advertisement) The image file for the advertisement. Either select a file that is already uploaded to Content Manager, or upload a new file. Maximum file upload size is 15.0 MB.
Title	(Image advertisement; Text advertisement) Specify alternative text for the image. For a text advertisement, the title is shown as the first line of the ad; if a hyperlink is also specified, the title is clickable.
Preview	(Image advertisement) Preview of the selected advertisement. The preview is updated as you modify the properties of the advertisement.
Body	(Text advertisement) Content for the text advertisement.
Footer	(Text advertisement) The last line of a text advertisement. If a hyperlink is also specified, the footer is clickable
Video ID	(YouTube video advertisement) (Required) The YouTube video identifier for the video to display. This is a unique identifier for a video that has already been uploaded to YouTube.
Width	(YouTube video advertisement) (Required) The desired width in pixels for the video.
Height	(YouTube video advertisement) (Required) The desired height in pixels for the video.
Edit Global Settings	(YouTube video advertisement) Select this option to configure global settings that will apply to all advertising materials.
Experimental YouTube API	(YouTube video advertisement) Specifies whether the experimental API is enabled for all devices. Options include: <ul style="list-style-type: none"> • All devices –Use the experimental API for all devices • Disabled –Use the standard YouTube API (recommended) • Select Devices – Use the experimental API for specific devices
IFrame API Devices	(YouTube video advertisement) If selected, the experimental YouTube IFrame API is used only for iOS devices.



The Hotspot Manager controls self-provisioned guest or visitor accounts. This is where the customer is able to create his or her own guest account on your network for access to the Internet. This can save you time and resources when dealing with individual accounts.

Accessing Hotspot Manager

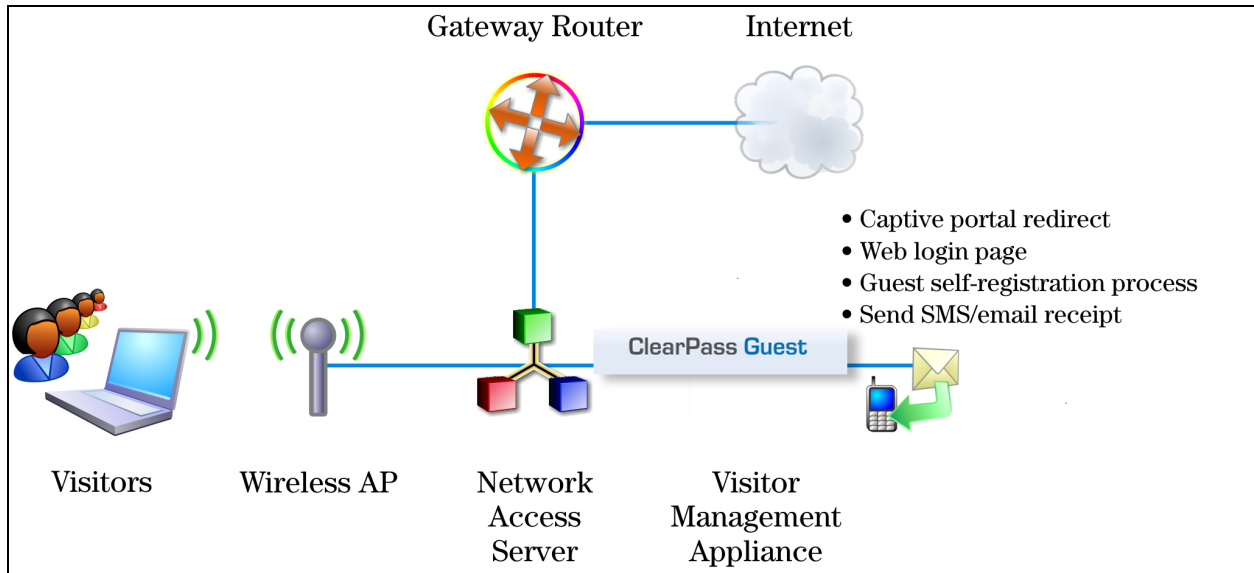
To access ClearPass Guest's hotspot management features, go to **Configuration > Hotspot Manager**.



About Hotspot Management

The following diagram shows how the process of customer self provisioning works.

Figure 375 Guest Self-Provisioning

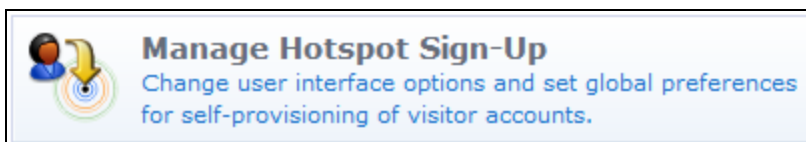


1. Your customer associates to a local access point and is redirected by a captive portal to the login page.
2. Existing customers may log in with their Hotspot username and password to start browsing.
New customers click the **Hotspot Sign-up** link.
3. On page 1, the customer selects one of the Hotspot plans you have created.
4. On page 2, the customer enters their personal details, including credit card information if purchasing access.
5. The customer's transaction is processed, and, if approved, their visitor account is created according to the appropriate Hotspot plan.
6. On page 3, the customer receives an invoice containing confirmation of their transaction and the details of their newly created visitor account.
7. The customer is automatically logged in with their username and password, providing instant Hotspot access.

Managing the Hotspot Sign-up Interface



To enable visitor access self provisioning, go to **Configuration > Hotspot Manager > Start Here** and select the **Manage Hotspot Sign-up** command.



The **Hotspot Preferences** form opens. This form allows you to change user interface options and set global preferences for the self-provisioning of visitor accounts.

Figure 376 *The Hotspot Preferences Form*

Hotspot Preferences	
General Hotspot Preferences Global options for self-provisioned visitor access.	
On/Off Switch:	<input checked="" type="checkbox"/> Enable visitor access self-provisioning
Require HTTPS:	<input checked="" type="checkbox"/> Always use HTTPS for customer connections Require HTTPS connections for customers creating Hotspot accounts. This is recommended to ensure the privacy of sensitive information such as credit card details.
* User Database:	ClearPass Policy Manager Self provisioned visitor accounts are created using this service handler.
* Transaction Processing:	vc Hotspot transactions are processed using this service handler.
* Service Not Available Title:	Temporarily Unavailable Title of the page displayed if self-provisioning has been disabled.
Service Not Available Message:	<pre><h2> Visitor Registration Temporarily Unavailable </h2> {nwaicontext icon="images/icon-schedule22.png"} We're sorry, but the system is currently unavailable due to maintenance. Please try again later. {/nwaicontext}</pre> <div style="text-align: right;"> <input type="button" value="Insert content item..."/> </div> <p>Enter HTML message to display to visitors if self-provisioning has been disabled.</p>
Captive Portal These options control the overall look and feel of the self provisioning visitor pages.	
Hotspot Sign-Up URL:	https://10.100.9.87/guest/hotspot_plan.php This is the URL that starts the self-provisioning process. For external captive portals, redirect visitors to this URL to start the Sign-Up process.
Look and Feel These options control the overall look and feel of the self provisioning visitor pages.	
Skin:	(Default) <input type="button" value="v"/> Choose the skin for the Hotspot visitor access pages.
SMS Services Override the default SMS settings.	
SMS Receipt:	(Use Default: Download Receipt) <input type="button" value="v"/> The plain-text format print template to use when generating an SMS receipt.
Phone Number Field:	(Use Default: visitor_phone) <input type="button" value="v"/> The field containing the visitor's phone number.
Auto-Send Field:	auto_send_sms <input type="button" value="v"/> The field which, if it contains a non-empty string or non-zero value, will cause an account receipt SMS to be automatically sent upon creation of a visitor account.
<input type="button" value="Save Changes"/>	

Table 229: Hotspot Preferences

Field	Description
On/Off Switch	If selected, enables self-provisioning for guest access.
Require HTTPS	If selected, requires an HTTPS connection for guests creating hotspot accounts, providing greater security. The guest is redirected to the HTTPS connection.
User Database	(Required) Service handler used to create self-provisioned guest accounts.
Transaction Processing	(Required) Service handler used to process hotspot transactions. If no transaction processor exists yet, click the Create a new transaction processor link. The Edit Transaction Processor opens. For more information, see " Creating a New Transaction Processor " on page 520.
Service Not Available Title	(Required) Title of the page that is displayed if self-provisioning is disabled.
Service Not Available Message	HTML for the message that is displayed to visitors if self-provisioning is disabled. For details about the template syntax you can use to format this message, see " Smarty Template Syntax " on page 700 in the <i>Reference</i> chapter. You can also use the drop-down list below this field to add images or links.
Hotspot Sign-Up URL	URL that starts the self-provisioning process. For external captive portals, redirect guests to this URL to start the sign-up process. For more information, see " Captive Portal Integration " on page 511.
Skin	Specifies the skin to use for the hotspot guest access pages. Options include: <ul style="list-style-type: none"> ● Default — The default skin is the one that is enabled in Plugin Manager. ● Aruba ClearPass Skin ● Blank Skin ● ClearPass Guest Skin ● Custom Skin 1 ● Custom Skin 2 ● Galleria Skin ● Galleria Skin 2
SMS Receipt	Specifies the plain-text format print template to use when generating an SMS receipt. Options include: <ul style="list-style-type: none"> ● Use Default: SMS Receipt ● Download Receipt ● SMS Receipt ● SMS Sponsor Confirmation Alert
Phone Number Field	Specifies the Guest Manager field containing the guest's phone number. The default is visitor_phone .
Auto-Send Field	Specifies the Guest Manager field that, if it contains a non-empty string or non-zero value, will cause an account receipt to be automatically sent when the guest account is created. The default is visitor_phone .
Save Changes	Saves your changes on this form.

Captive Portal Integration

To start the visitor self-provisioning process, new visitor registration is performed by redirecting the visitor to the URL specified on the **Hotspot Preferences** page; for example: https://guest.example.com/hotspot_plan.php. The **Hotspot Sign-Up** page opens to the first page of the wizard, **Choose Plan**.

The `hotspot_plan.php` page accepts two parameters:

- The **source** parameter is the IP address of the customer.
- The **destination** parameter is the original URL the customer was attempting to access (that is, the customer's home page). This is used to automatically redirect the customer on successful completion of the sign-up process.

For browsers without JavaScript, you may use the **<noscript>** tag to allow customers to sign up:

```
<noscript>
  <a href="https://guest.example.com/hotspot_plan.php">Hotspot Sign-Up</a>
</noscript>
```

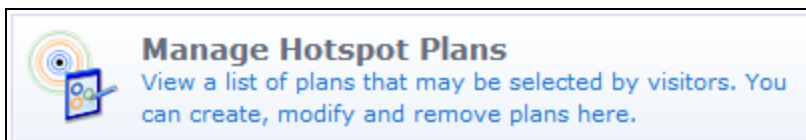
However, in this situation the MAC address of the customer will not be available, and no automatic redirection to the customer's home page will be made. You may want to recommend to your customers that JavaScript be enabled for best results.

Managing Hotspot Plans



Your Hotspot plans determine how a customer is to pay for Internet access when connected through ClearPass Guest. You also have the option to allow free access.

To view the list of hotspot plans your visitors can select and to access plan management, go to **Configuration > Hotspot Manager > Start Here** and click the **Manage Hotspot Plans** link.





The **Manage Hotspot Plans** list view opens, showing the list of default plans. Plans that are enabled have their name in **bold** and their icon in color: . Plans that are not enabled have their icon in gray: .

Figure 377 *The Manage Hotspot Plans List View*

Plan Name	Description	Actions
 Free Access	Free basic wireless access. Limited to 64 kbit, Web browsing traffic only, and a maximum of one hour.	 Edit  Delete
 Hourly Access	Wireless access charged at \$2.95 per hour. Offers full Internet access at 128 kbit/sec.	 Edit  Delete
 Daily Access	Wireless access charged at \$24.95 per day (24 hours). Offers full Internet access at 256 kbit/sec.	 Edit  Delete
 Weekly Access	Wireless access charged at \$54.95 per week (7 days). Offers full Internet access at 256 kbit/sec.	 Edit  Delete



Table 230: *Manage Hotspot Plans List View*

Field	Description
Edit	Let you edit an existing plan. See "Editing or Creating a Hotspot Plan" on page 512.
Delete	Lets you delete an existing plan. You are asked to confirm the deletion. When a plan is deleted you cannot undo the deletion.
Create Hotspot plan	Lets you create a new plan. See "Editing or Creating a Hotspot Plan" on page 512.

Editing or Creating a Hotspot Plan

When you create or edit a hotspot plan, you can customize which plans are available for selection, and any of the plan's details, such as its description, cost to purchase, allocated role, and the format of the customer's generated username and password.

To create or edit a plan, first go to **Configuration > Hotspot Manager > Start Here**, click the **Manage Hotspot Plans** link, and then:

- To create a new plan, click the  **Create Hotspot plan** link in the upper-right corner. The **Create Hotspot Plan** form opens.
- To edit a plan, click the  **Edit** link in the plan's row. The **Edit Hotspot Plan** form opens.

The procedures are the same for both the **Create Hotspot Plan** and the **Edit Hotspot Plan** forms.

Figure 378 *The Edit Hotspot Plan Form, Plan Details Area*

Edit Hotspot Plan	
Plan Details Describe your Hotspot plan.	
* Plan Name:	Free Access <small>The name of the plan. Hotspot customers choose a plan based on its name.</small>
Description:	Free basic wireless access. Limited to 64 kbit, Web browsing traffic only, and <small>Description of the plan. This will be displayed with the Hotspot plan's name.</small>
Invoice Description:	Basic wireless access <small>A brief description of the plan. This will be displayed on the customer's invoice along with the Hotspot plan's name.</small>
Enabled:	<input checked="" type="checkbox"/> Hotspot plan enabled <small>Enabled plans are shown to customers and may be selected for purchase.</small>

The **Plan Details** area of the form lets you configure items that are displayed to the user in the user interface and customer invoice.

Table 231: *Edit Hotspot Plan Form, Plan Details Area*

Field	Description
Plan Name	Name for this plan. Users select a hotspot plan on the strength of the name, so choose a name that helps the user clearly identify your service. Avoid names that might be difficult for the user to identify and trust.
Description	Description of the hotspot plan that is displayed with the plan's name.
Invoice Description	Description of the hotspot plan that is displayed on the customer's invoice along with the plan's name.
Enabled	If selected, enables this hotspot plan. If deselected, the disabled plan is not displayed to customers.

Figure 379 *The Edit Hotspot Plan Form, User Account Details Area*

User Account Details	
A user account is created for each Hotspot customer. Use these options to control how user accounts are created.	
* Generated Username:	##### <small>Format picture (see below) describing the usernames that will be created for customers. Leave blank to use the customer's email address as the username.</small>
Username Example:	36888419 Generate
Generated Password:	##### <small>Format picture (see below) describing the passwords that will be created for customers. Leave blank to use the password specified on the customer information form. This may require adding the 'password' field to the customer info form.</small>
Password Example:	01512971 Generate
Role:	[Guest] <small>The role to assign to accounts that will be created for this plan.</small>

In the **User Account Details** area, you can specify the usage of numbers, letters, and symbols in the generated username and password, and specify a role for accounts.

Table 232: *Edit Hotspot Plan Form, User Account Details Area*

Field	Description
Generated Username	<p>(Required) Lets you format the combination of numbers, letters, and symbols in the generated username.</p> <p>To use the customer's email address as the username, leave this field empty.</p> <p>To use only digits, leave the value set to #####. To indicate a different combination of numbers, letters, or symbols, use the following parameters:</p> <ul style="list-style-type: none"> • The number or hash symbol (#) is replaced with a random digit (0-9) • The dollar symbol (\$) is replaced with a random letter • The underscore symbol (_) is replaced with a random lowercase letter • The carat symbol (^) is replaced with a random uppercase letter • The asterisk symbol (*) is replaced with a random letter or digit • The "at" symbol (@) is replaced with a random letter or digit, excluding vowels • The exclamation symbol (!) is replaced with a random punctuation symbol • The ampersand symbol (&) is replaced with a random character (letter, digit, or punctuation symbol) • All other characters are used without modification. <p>For more information, see "Format Picture String Symbols" on page 736.</p>
Username Example	<p>This field shows a sample username generated according to the rules you specified by your entry in the Generated Username field. To view different examples, click the Generate link.</p>
Generated Password	<p>Lets you format the combination of letters, numbers, and symbols in the generated password.</p> <p>To use the password specified on the customer information form, leave this field empty. This might require adding the "password" field to the customer information form.</p> <p>To use only digits, leave the value set to #####. To indicate a different combination of numbers, letters, or symbols, use the following parameters:</p> <ul style="list-style-type: none"> • The number or hash symbol (#) is replaced with a random digit (0-9) • The dollar symbol (\$) is replaced with a random letter • The underscore symbol (_) is replaced with a random lowercase letter • The carat symbol (^) is replaced with a random uppercase letter • The asterisk symbol (*) is replaced with a random letter or digit • The "at" symbol (@) is replaced with a random letter or digit, excluding vowels • The exclamation symbol (!) is replaced with a random punctuation symbol • The ampersand symbol (&) is replaced with a random character (letter, digit, or punctuation symbol) • All other characters are used without modification. <p>For more information, see "Format Picture String Symbols" on page 736.</p>
Password Example	<p>This field shows a sample password generated according to the rules you specified by your entry in the Generated Password field. To view different examples, click the Generate link.</p>
Role	<p>Specifies the role to assign to accounts created for this plan.</p>

Figure 380 *The Edit Hotspot Plan Form, Time & Cost Details Area*

Time & Cost

Hotspot plans are purchased in units. Use these options to control the time and cost of each unit.

Time Tracking:	<input checked="" type="radio"/> Fixed date — Unit purchase is relative to the transaction time <input type="radio"/> Cumulative usage — Unit purchase is for total time spent online <input type="radio"/> Checkout date - Expiration will be midnight the day of checkout (Hotel PMS only) <input type="radio"/> Already paid - Select for other devices to share a paid plan (Hotel PMS only)
* Unit Cost:	<input style="width: 50px;" type="text" value="2.95"/> <small>The cost to purchase a single unit of this plan. Enter 0 to create a 'free access' plan.</small>
* Minimum Units:	<input style="width: 50px;" type="text" value="1"/> <small>Minimum number of units that may be purchased.</small>
* Maximum Units:	<input style="width: 50px;" type="text" value="24"/> <small>Maximum number of units that may be purchased. Enter the Minimum Units value to hide the quantity option.</small>
* Unit Time:	<input style="width: 50px;" type="text" value="3600"/> <small>Length of time, in seconds, corresponding to a single unit of this plan. 1 hour - 3600 1 day - 86400 1 week - 604800</small>
Unit Name:	<input style="width: 50px;" type="text" value="hour(s)"/> <small>The name used to describe one or more units of this plan.</small>

In the **Time & Cost** area, you can specify the time and cost of each unit. A unit is the amount of time purchased, as defined in the **Time Tracking** field.

Table 233: *Edit Hotspot Plan Form, Time & Cost Details Area*

Field	Description
Time Tracking	Specifies the amount or duration of time purchased. This defines the “unit”. Options include: <ul style="list-style-type: none"> ● Fixed date - Unit purchase is relative to the transaction time — The duration of the unit ends at a specified amount of time after the account is created. ● Cumulative usage - Unit purchase is for total time spent online — The duration of the unit is calculated as the cumulative time the user actually spends online. ● Checkout date - Expiration will be midnight the day of the checkout (Hotel PMS only) — The duration of the unit is begins when the account is created and ends at midnight of the day the user is scheduled to check out of the hotel. ● Already paid - Select for other devices to share a paid plan (Hotel PMS only) — Allows multiple devices to use a plan that is already created and paid for.
Unit Cost	(Required) Cost for a single unit of this plan. To create a free access plan, enter 0 .
Minimum Units	(Required) Minimum number of units that can be purchased.
Maximum Units	(Required) Maximum number of units that can be purchased. To hide the quantity option, enter the value you entered in the Minimum Units field.

Table 233: *Edit Hotspot Plan Form, Time & Cost Details Area(Continued)*

Field	Description
Unit Time	(Required) The length in time, in seconds, of a single unit of this plan. One hour = 3600 One day = 86400 ONE week = 604800
Unit Name	The name used to describe one or more units of this plan.
Update Plan	Saves the plan and opens the Manage Hotspot Plans list with the new plan displayed.

Managing Transaction Processors

Your hotspot plan must also identify the transaction processing gateway used to process credit card payments. ClearPass Guest supports plugins for the following transaction processing gateways:

- Credit Card Processors:
 - Authorize.Net AIM
 - CashNet
 - CyberSource
 - Demo — A Demo transaction processor that you can use to create hotspot forms and test hotspot transactions
 - eWAY
 - Netregistry
 - PayPal Express
 - PayPal PayFlow Pro
 - Wirecard Checkout
 - WorldPay
- Hotel Property Management Systems:
 - FIAS – Micros Opera / Protel / Silverbyte
 - HTNG – Agilisys

To view or work with transaction processor gateways, go to **Configuration > Hotspot Manager > Transaction Processors**. The **Hotspot Transaction Processors** list view opens. All transaction processors you have defined are included in the list.

Figure 381 *The Hotspot Transaction Processors List View*

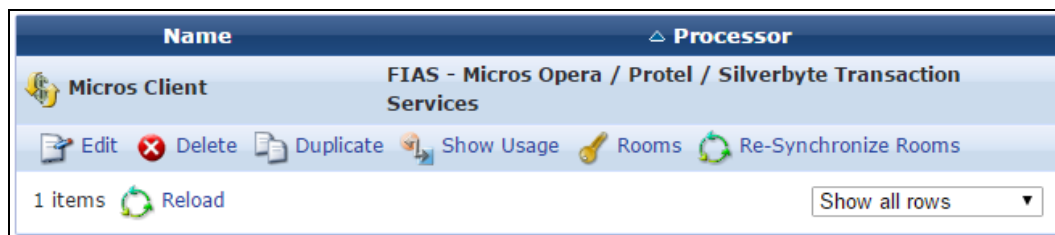


Table 234: *Hotspot Transaction Processors List View*

Field	Description
Edit	Lets you change the properties of the specified transaction processor. The Transaction Processor Configuration form opens. For more information, see " Creating a New Transaction Processor " on page 520.
Delete	Deletes the processor from the Hotspot Transaction Processors list. You will be asked to confirm the deletion.
Duplicate	Creates a copy of a transaction processor to use as a basis for a new processor.
Show Usage	The transaction processor's row expands to show a list of any hotspots associated with it. Each hotspot entry is a link to the Hotspot Preferences form, where you can change user interface options and set global preferences for the self-provisioning of visitor accounts. For more information, see " Managing the Hotspot Sign-up Interface " on page 508.
Rooms	Opens the Occupied Room List page, showing all current room reservation details. For more information, see " Occupied Room List " on page 518.
Re-Synchronize Rooms	Opens the Confirm Transaction Processor Sync form, where you can verify when the room data was last synchronized and update room details. For more information , see " Re-Synchronizing Rooms " on page 519.

Occupied Room List

To view all current room reservation details, click the **Rooms** link for a transaction processor at **Configuration > Hotspot Manager > Transaction Processors**. The **Occupied Room List** page opens. This view-only page displays information about transaction events for the selected processor, and all rooms that are currently reserved or transactions that are in progress are included in the list. All data is shown in real time.

Figure 382 *The Occupied Room List, Transaction Processors*

Room	First Name	Last Name	Reservation	Purchase	Date	Arrive	Depart
1		One	101	None		150904	160910
2		Two	102	None		150904	160910
3		Three	103	None		150904	160910
4		Four	104	None		150904	160910
5		Five	105	None		150904	160910
6		Six	106	None		150904	160910
7		Seven	107	None		150904	160910
8		Eight	108	None		150904	160910
9		Nine	109	None		150904	160910
201	Al	Bundy	201	None		150904	160910
202	Darth	Vader	202	None		150904	160910
203	Ralph	Kramden	203	None		150904	160910
402	Norman	Bates	402	None		150904	160910
403	Tony	Stark	403	None		150904	160910
404	Marty	McFly	404	None		150904	160910
405	Mary	Poppins	405	None		150904	160910
406	Hermione	Granger	406	None		150904	160910

35 rooms Reload Show all rows

Table 235: *Occupied Room List, Transaction Processors*

Field	Description
Current Status	Connection status between the transaction processor's database and ClearPass. If the status is shown as OK , ClearPass is connected to the transaction processor and all data shown on this page is current.
Last Recorded Event Stamps	List of the most recent connection commands and events, and the timestamps for when they occurred. Events include: <ul style="list-style-type: none"> • Last — The most recent event type • (LS) Link Start • (LC) Link Configuration • (LA) Link Active • (DE) Data Resync End • (GI) Guest In This list will also include any pending event and any items in the queue.
Room	The hotel room number.

Table 235: *Occupied Room List, Transaction Processors (Continued)*

Field	Description
First Name	The guest's first name.
Last Name	The guest's last name.
Reservation	The reservation number.
Purchase	The purchase status.
Date	The date of the transaction.
Arrive	The date the guest will arrive.
Depart	The date the guest will leave.

Re-Synchronizing Rooms

Room data is displayed in real time; however, if an error occurs when the transaction processor's database sends information to ClearPass, the data might become out of synch. To resynchronize room data between ClearPass and the transaction processor's database, click the **Re-Synchronize Rooms** link for a transaction processor at **Configuration > Hotspot Manager > Transaction Processors**. The row expands to include the **Confirm Transaction Processor Sync** form.

Figure 383 *The Confirm Transaction Processor Sync Form*

Confirm Transaction Processor Sync	
Last Data Sync Start:	2016-09-09 14:43:12
Last Data Sync End:	2016-09-09 14:43:12
Pending:	N/A
Clear:	<input checked="" type="radio"/> Re-Synchronize all room details <input type="radio"/> Clear the current pending command
Confirm:	Are you sure you want to sync the transaction processor ' Micros Client '? All existing transaction history will be lost.
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

Table 236: *Hotspot Transaction Processors, Confirm Transaction Processor Sync Form*

Field	Description
Last Data Sync Start	Date and time the last data synchronization began.
Last Data Sync End	Date and time the last data synchronization ended.
Pending	Displays any pending room transaction requests. If a transaction is triggered while one is already in progress, the new request is added to the pending queue and will not be sent to the transaction

Table 236: Hotspot Transaction Processors, Confirm Transaction Processor Sync Form (Continued)

Field	Description
	processor until the results of the previous request are received. If there are multiple transaction requests in the queue, each one must be processed in turn.
Clear	Clears the existing room data. Options include: Re-Synchronize all room details — Clears all current room data and any queued transactions. Clear the current pending command — Clears only the currently pending transaction. All past room data is retained, and other queued transaction requests can proceed.
Confirm	Consider carefully before re-synchronizing all room details, as this will delete all current room data and any pending payment requests.
OK	Commits the selected re-synchronization option.
Cancel	Cancels your entries and closes this form.

Creating a New Transaction Processor

The Transaction Processor Configuration form is used to create and to edit transaction processors.

To define a new transaction processor:


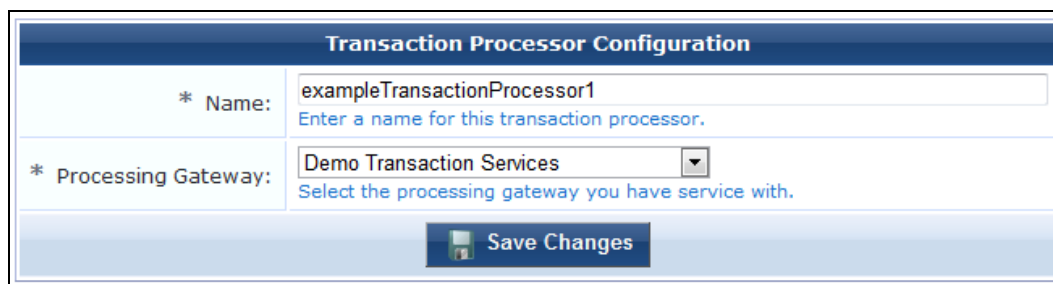
1. Go to **Configuration > Hotspot Manager > Transaction Processors** and click the  **Create new transaction processor** link in the upper-right corner. The **Transaction Processor Configuration** form opens.

Figure 384 The Transaction Processor Configuration Form



2. In the **Name** field, enter a name for the transaction processor.
3. In the **Processing Gateway** drop-down list, select the gateway with which you have a service account. The form expands to include additional configuration fields for that gateway type.

Each transaction processing gateway type requires unique merchant identification, password, and configuration information. Depending on the gateway provider, these configuration items will include some of the following:

Table 237: Transaction Processor Configuration

Field	Description
Allowed Access	IP addresses and networks from which callbacks are permitted. (IPv4 and IPv6 are both supported)
API Login	(Required) The Authorize.Net API account name.
API Password	(Required) The API password for this transaction processor.
Confirm Password	
API Username	(Required) The API username for this transaction processor.
Auto Email	If selected, passes along the flag to directly email the customer from Authorize.Net.
Beagle Anti-Fraud	if selected, enables Beagle GEO Anti-Fraud.
Business Center Login	URL for logging in to the business center.
Character Set	The character set this transaction processor's server is using when sending text.
Client ID	The PayPal app credentials pair client ID.
Client Secret	The PayPal app credentials pair secret.
Confirm Secret	
Confirmation Email	Email address to which all payment details will be sent. For more information, refer to https://integration.wirecard.at/doku.php/request_parameters#confirmmail .
Confirmation URL	URL that will capture and log all payment details, if you have one. For more information, refer to https://integration.wirecard.at/doku.php/request_parameters#confirmurl .
Country Code	(Required) Country code to use. Please refer to the PayPal country code guide for the appropriate value. For more information, refer to https://developer.paypal.com/docs/classic/api/country_codes/ This value will be overwritten if the form has the "country" field.
Currency Code	(Required) Country currency code to use. Please refer to the Wirecard currency code guide for the appropriate value. For more information, refer to https://integration.wirecard.at/doku.php/request_parameters#currency .
Customer ID	(Required) The customer's ID for this transaction processor.
Data Sync	(Required) Options include: <ul style="list-style-type: none"> ● Only sync the database the first time it is seen ● Sync the database whenever the local service restarts ● Sync the database whenever the server comes online ● Poll - Do not sync the data and poll for details

Table 237: Transaction Processor Configuration(Continued)

Field	Description
	<ul style="list-style-type: none"> • None - Do not sync the data
Denied Access	IP addresses and networks that are denied callbacks. (IPv4 and IPv6 are both supported)
Hostname	(Required) The server hostname or IP address.
Installation ID	The installation ID to use when starting a transaction with this transaction processor.
Item Code	(Required) The item code for the Wi-Fi service.
Keep Alive	Specifies whether and how to send periodic keepalive commands to the FIAS server. May be needed in scenarios where room updates are infrequent, or other networking devices such as switches or firewalls might drop connections. Options include: <ul style="list-style-type: none"> • None • Via Link Start (LS) — This option receives a response from the PMS software. • Via Link Alive (LA)
Keep Alive Repeat	If Keep Alive is configured, specifies the interval at which the periodic keepalive commands are sent to the FIAS server. Options include: <ul style="list-style-type: none"> • 5 minutes • 10 minutes • 20 minutes • 30 minutes • 1 hour
Logging	If selected, details are logged to cybs.log. Advised for debugging only.
Merchant ID	(Required) The merchant ID to use for this transaction processor when starting a transaction.
Mode	If selected, enables transaction processing in the production environment.
Name Match	(Required) Specifies how much of the last name must be matched. If the name is shorter than the required length, it will be matched in full. Matches are not case-sensitive. Options include: <ul style="list-style-type: none"> • Exact last name match • First 3 letters of the last name • First 4 letters of the last name • First 5 letters of the last name • First 6 letters of the last name • First 7 letters of the last name
No-Post Status	(Required) Options include: <ul style="list-style-type: none"> • Ignore the NP flag and allow access • Deny paid access to accounts with the NP flag • Deny all access to accounts with the NP flag
Payment ID	The payment ID as required by the PMS.
Payment Type	Specifies the payment method. Options include Select within Wirecard Payment Page , as well as a variety of other methods.

Table 237: Transaction Processor Configuration(Continued)

Field	Description
	For more information, refer to https://integration.wirecard.at/doku.php/request_parameters#paymenttype .
Port	(Required) The server TCP port. The port must not be in use by this appliance.
Production Environment URL	(Required) URL used for transactions when in production mode.
Requirements	(Required) Options include: <ul style="list-style-type: none"> ● Room number and last name ● Reservation number and last name
Resort ID	The resort ID as entered in the PMS system.
Revenue Center ID	The revenue center ID as required by the PMS.
Secret	(Required) The Wirecard secret.
Confirm Secret	
Service URL	The URL for this transaction processor's server.
Shared Secret	The MD5 shared secret to use for securing the transaction. Up to 16 characters are allowed. This must be the same as the "MD5 secret for transactions" that was configured in the transaction processor's administration interface.
Shop ID	The Wirecard shp ID, if you have one configured. For more information, refer to https://integration.wirecard.at/doku.php/request_parameters#shopid .
Signature	(Required) The API signature for this transaction processor.
Confirm Signature	
Test Environment URL	(Required) This URL is used for transactions when not in production mode.
Test WSDL	(Required) URL of the SOAP WSDL in non-production mode.
Time Zone	Specifies the time zone to use to override the system time zone if the hotel Property Management System (PMS) and ClearPass are in different time zones. By default, timestamps used in the FIAS protocol are relative to the ClearPass system's time.
Transaction Key	(Required) The SOAP transaction key.
Transaction Password	(Required) This transaction processor's API transaction password.
Confirm	

Table 237: Transaction Processor Configuration(Continued)

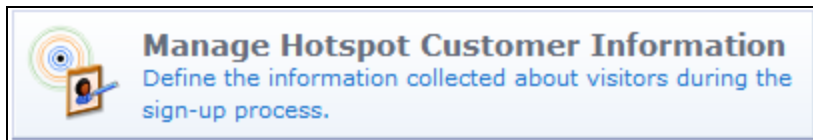
Field	Description
Password	
Transactions Timeout	(Required) Timeout, in seconds, of the transaction request.
WSDL	(Required) URL of the SOAP WSDL in production mode.
Your Logo URL	(Required) URL of your online shop where your online shop logo is located. For more information, refer to https://integration.wirecard.at/doku.php/request_parameters#imageurl .
Your Service URL	URL of an information page in your online shop that informs your consumer about different ways to contact you. Do not use this URL to link to the shopping basket of your consumer. For more information, refer to https://integration.wirecard.at/doku.php/request_parameters#serviceurl .

If your transaction processor requires visitors to enter their address, ClearPass Guest will automatically include address fields in the guest self-registration forms that use that transaction processor.

Managing Customer Information



You can customize the fields that the customer sees, the details of these fields, and the order in which they are presented. To customize the fields, go to **Configuration > Hotspot Manager > Start Here** and click the **Manage Hotspot Customer Information** link.



The **Customize Form Fields** view opens for the customer information form. See "[Customizing Forms and Views](#)" on page 305 for instructions for completing the form field editor.

Managing Hotspot Invoices



After the customer's transaction has been processed successfully, the customer receives an invoice containing confirmation of their transaction and the details of their newly created hotspot user account. You can customize the title shown on the invoice and how the invoice number is created. You can also customize the currency displayed on the invoice.

To customize the hotspot invoice, go to **Configuration > Hotspot Manager > Start Here** and then click the **Manage Hotspot Invoice** link. The **Manage Invoice** form opens.

Figure 385 *The Manage Invoice Form*


Manage Invoice	
* Invoice Title:	<pre>Your Company Name
 Your contact details</pre> <p>Enter the HTML template code to display as the title of the customer's invoice.</p>
* Invoice Numbering:	Specify format using template... Choose the way in which invoice numbers will be generated.
Invoice Number:	<pre>P-{nwa_makeid file="_site/HotspotInvoiceNumber.dat" output=1}</pre> <p>Insert content item...</p> <p>Enter an expression that describes the invoice number format.</p>
Preview:	P-3 This is a sample invoice number generated with the current settings.
* Currency Format:	\$1,000.00 The currency format to use when formatting a monetary amount for display.
Currency Code:	AUD The currency code to specify to the transaction service provider.
Login Code:	<pre><script type="text/javascript"><!--{literal} function browser_home() { if (typeof(window.home) == "function") { window.home(); } else { window.location = "about:home"; } } //--> {/literal} </script></pre> <p>Insert content item...</p> <p>The HTML template code to display in the bottom panel of the invoice.</p>
	

Table 238: Manage Invoice Form

Field	Description
Invoice Title	(Required) HTML template code used to display the title on the customer's invoice. For more information, see " Basic HTML Syntax " on page 697
Invoice Numbering	(Required) Specifies the method used to generate invoice numbers. Options include: <ul style="list-style-type: none">• Default numbered format• Sequential numbering from 1• Specify format using template
Invoice Number	Expression that describes the invoice number format.
Preview	This field shows an example of an invoice number generated using the current settings.
Currency Format	(Required) The currency format to use when formatting a monetary amount for display.
Currency Code	The currency code to specify to the transaction service provider.
Login Code	HTML template code to display in the bottom panel of the invoice.
Save Changes	Saves your changes to the invoice configuration.

You can use Smarty functions on this page. See "[Smarty Template Syntax](#)" on page 700 for further information on these. You can also insert content items such as logos or prepared text. See "[Customizing Guest Self-Registration](#)" on page 341 for details on how to do this.

Customizing the User Interface

Each aspect of the user interface your hotspot customers see can be customized.

This section includes:

- "[Customizing Visitor Sign-Up Page One](#)" on page 526 — Page One lets the guest select a plan.
- "[Customizing Visitor Sign-Up Page Two](#)" on page 529 — Page Two asks for the guest's personal information and payment method.
- "[Customizing Visitor Sign-Up Page Three](#)" on page 533 — Page Three is the customer's receipt.

Customizing Visitor Sign-Up Page One



Page one of the guest self-provisioning process asks the guest to select a plan. An example of the default "Choose Plan" page is shown below.

Figure 386 Example Choose Plan Page

Hotspot Sign-Up STEP 1

Welcome to the Hotspot Sign-Up. Get connected to the Internet without wires in just three easy steps.

To get started, select the type of wireless access you would like to purchase.

Choose Plan	
<input checked="" type="radio"/>	Free Access Free basic wireless access. Limited to 64 kbit, Web browsing traffic only, and a maximum of one hour.
<input type="radio"/>	Hourly Access Wireless access charged at \$2.95 per hour. Offers full Internet access at 128 kbit/sec. <input type="text" value="1"/> hour(s)
<input type="radio"/>	MyPlan test plan 1

Next >>

To customize how this page is displayed to the guest, go to **Configuration > Hotspot Manager > Start Here**, click the **Manage Hotspot Sign-Up** link, and then click the **Customize page 1 (Choose Plan)** link in the upper-right corner.

The **Edit Hotspot Plan Selection Page** form opens. You can use this form to edit the title, introductory text, and footer of the “Choose Plan” page. The introduction and the footer are HTML text that can use template syntax. For more information, see "[Smarty Template Syntax](#)" on page 700 in the *Reference* chapter.

Figure 387 *The Edit Page Form, Step 1: Choose Plan*

Edit Page

* Page Title:	Choose Plan <small>Title of this page.</small>
Introductory HTML:	<pre>{nwa_cookiecheck} <h2> Hotspot Sign-Up </h2> <p> Welcome to the Hotspot Sign-Up. Get connected to the Internet without wires in just three easy steps. </p> <p></pre> <small>This text is displayed at the top of the page, before the list of Hotspot plans.</small>
Footer HTML:	<div style="border: 1px solid #ccc; height: 30px; width: 100%;"></div> <small>This text is displayed at the bottom of the page, after the list of Hotspot plans.</small>
Options:	<input type="checkbox"/> Override standard form <small>If checked, the standard form on this page will not be included when the page is generated. Note: this option is recommended for advanced users only.</small>

Save Changes

Table 239: *Edit Page Form, Step One: Plan Selection Page*

Field	Description
Page Title	(Required) Title for the page where the guest selects a plan.
Introductory HTML	HTML code for the text to display at the top of the page, above the list of hotspot plans.
Footer HTML	HTML code for the text to display at the bottom of the page, below the list of hotspot plans.
Options	If selected, the standard form on this page will not be included when the page is generated. This option is recommended for advanced users only.
Save Changes	Saves your changes to the plan selection page.

Customizing Visitor Sign-Up Page Two



Page two of the guest self-provisioning process asks the guest to provide their personal details and payment method.

The example below shows the default “Your Details” page if the customer chooses to pay for the Hourly Access plan.

Figure 388 Example “Your Details” Page Shown to Customer, Hourly Plan

Your Details

Hotspot Sign-Up **STEP 2**

To create your wireless account, please enter your details below.

➔ You have selected: **Hourly Access** – 1 hour(s) (change)

Your Details	
Your Personal Details	
* First Name:	<input type="text"/> Your first name.
* Last Name:	<input type="text"/> Your last name.
* Company Name:	<input type="text"/> The name of your company.
Zip:	<input type="text"/>
Phone Number:	<input type="text"/> Your contact telephone number.
* Email Address:	<input type="text"/> Your email address.
Purchase Details	
* Card Number:	<input type="text"/> Your credit card number, without spaces.
* Card Expiry:	<input type="text"/> Your credit card expiration date.
* Card Name:	<input type="text"/> The name on the card, exactly as it is printed.
* Card Verification Code:	<input type="text"/> The 3 or 4 digit cardholder verification code printed on the card.
Purchase Amount:	\$2.95 This is the total amount of your purchase. Your credit card will not be charged until you click the Purchase button below.
* Confirm:	<input type="checkbox"/> I accept the terms of use
<input type="button" value="Purchase Access"/>	

Although it is not shown in this illustration, the default page also includes footer text providing information about privacy policies and security pertaining to the data collected by this page.

The example below shows the default “Your Details” page for a customer who chooses the Free Access plan.

Figure 389 Example “Your Details” Page Shown to Customer, Free Access Plan

Your Details

Hotspot Sign-Up **STEP 2**

To create your wireless account, please enter your details below.

➔ You have selected: **Free Access** (change)

Your Details	
Your Personal Details	
* First Name:	<input type="text"/> Your first name.
* Last Name:	<input type="text"/> Your last name.
* Company Name:	<input type="text"/> The name of your company.
Zip:	<input type="text"/>
Phone Number:	<input type="text"/> Your contact telephone number.
* Email Address:	<input type="text"/> Your email address.
* Confirm:	<input type="checkbox"/> I accept the terms of use
<input type="button" value="Create Account"/>	

To customize how the “Your Details” page is displayed to the guest, go to **Configuration > Hotspot Manager > Start Here**, click the **Manage Hotspot Sign-Up** link, and then click the **Customize page 2 (Customer Details)** link in the upper-right corner.

The **Edit Hotspot User Details Page** form opens. You can use this form to edit the content displayed when the customer enters their personal details, including credit card information if purchasing access. The progress of the user’s transaction is also shown on this page. For information about the template syntax you can use to format the content on this page, "[Smarty Template Syntax](#)" on page 700.

Figure 390 The Edit Page Form, Step 2: Customer Details

Edit Page	
* Page Title:	<input type="text" value="Your Details"/> <small>Title of this page.</small>
Introductory HTML:	<pre><h2> Hotspot Sign-Up </h2> <p> To create your wireless account, please enter your details below. </p></pre> <small>This text is displayed at the top of the page, before the form for the user's details.</small>
Footer HTML:	<pre><h2> Important Information </h2> (nwa_icontext type="info" class=" ") Note: We collect your personal information in order to provide you with wireless network service. Your personal details are kept strictly confidential at all times. (Read our privacy policy.)</pre> <small>This text is displayed at the bottom of the page, after the form for the user's details.</small>
Transaction Header HTML:	<pre><h2> Hotspot Sign-Up </h2> <p> Please wait while your transaction is being processed... </p></pre> <small>When a transaction is in progress, this text is displayed at the top of the page, before the progress notification area.</small>
Transaction Footer HTML:	<pre></pre> <small>When a transaction is in progress, this text is displayed at the bottom of the page, after the progress notification area.</small>
Options:	<input type="checkbox"/> Override standard form <small>If checked, the standard form on this page will not be included when the page is generated. Note: this option is recommended for advanced users only.</small>
<input type="button" value="Save Changes"/>	

Table 240: *Edit Page Form, Step Two: User Details and Payment Page*

Field	Description
Page Title	(Required) Title for the page where the guest enters their personal information and payment method.
Introductory HTML	HTML code for the text to display at the top of the page, above the guest's personal information.
Footer HTML	HTML code for the text to display at the bottom of the page, below the guest's personal information.
Transaction Header HTML	HTML code for the text to display while the transaction is in progress. This text is displayed at the top of the page, above the progress notification area.
Transaction Footer HTML	HTML code for the text to display while the transaction is in progress. This text is displayed at the bottom of the page, below the progress notification area.
Options	If selected, the standard form on this page will not be included when the page is generated. This option is recommended for advanced users only.
Save Changes	Saves your changes to the personal information and payment page.


Customizing Visitor Sign-Up Page Three



Page three of the guest self-provisioning process provides the customer an invoice containing confirmation of their transaction and the details of their newly created wireless account. An example of the default receipt page is shown below.

Figure 391 Example "Your Invoice" Page Shown to Customer

Your Receipt


Hotspot Sign-Up 

Your transaction was processed successfully. Welcome to the Hotspot!

Your wireless account is now ready to use. Just click the "Start Browsing" button below to automatically log in and continue to your Web browser's home page.

1 **Note:** If your computer is turned off, or goes out of range, you will need to log in to the Hotspot again. Make sure you have the username and password shown under "Account Details".

Please review the receipt below and save a copy for your records.

Your Invoice			
Your Company Name Your contact details	Date:	Tuesday, 04 December 2012, 12:36 AM	
	Invoice No:	P-8	
Purchase Details			
Description	Qty	Unit Price	Price
Free Access <small>Free basic wireless access. Limited to 64 kbit, Web browsing traffic only, and a maximum of one hour.</small>	1	0.00	\$0.00
			Total: \$0.00
Account Details			
Username:	✓ 16788743	Use this username to log in to the Hotspot.	
Password:	✓ 74066184	Use this password to log in to the Hotspot.	
Account Expires:	Account will expire at Tuesday, 04 December 2012, 01:36 AM Your account will stop working after this time.		
 Have you made a record of your username and password?			
Start Browsing >>			

To customize how the "Your Receipt" page is displayed to the guest, go to **Configuration > Hotspot Manager > Start Here**, click the **Manage Hotspot Sign-Up** link, and then click the **Customize page 3 (Invoice or Receipt)** link in the upper-right corner.

The **Edit Hotspot User Receipt Page** form opens. You can use this form to edit the title, introductory text, and footer text of the receipt page. For more information about the template syntax you can use to format the content of this page, see "[Smarty Template Syntax](#)" on page 700

Figure 392 *The Edit Page Form, Step 3: Invoice or Receipt*

Edit Page

* Page Title:	Your Receipt <small>Title of this page.</small>
Introductory Text:	<pre><h2> Hotspot Sign-Up </h2> <p> Your transaction was processed successfully. Welcome to the Hotspot! </p> <p> Your wireless account is now ready to use. Just click the "Start Browsing" </p></pre> <small>This text is displayed at the top of the page, before the user's invoice.</small>
Footer Text:	<small>This text is displayed at the bottom of the page, after the user's invoice.</small>
Options:	<input type="checkbox"/> Override standard format <small>If checked, the standard layout on this page will not be included when the page is generated. Note: this option is recommended for advanced users only.</small>

Save Changes

Table 241: *Edit Page Form, Step Three: Receipt Page*

Field	Description
Page Title	(Required) Title for the guest's receipt page.
Introductory Text	HTML code for the text to display at the top of the page, above the guest's invoice details.
Footer Text	HTML code for the text to display at the bottom of the page, below the guest's invoice details.
Options	If selected, the standard layout on this page will not be included when the page is generated. This option is recommended for advanced users only.
Save Changes	Saves your changes to the receipt page.

Viewing the Hotspot User Interface

ClearPass Guest lets you view and test the hotspot self-provisioning pages you create. To view the hotspot page:

1. Go to **Configuration > Pages > Guest Self-Registrations** and click **Create new self-registration page**. The **Customize Guest Registration** form opens.

2. Select the check box in the **Hotspot** row to enable hotspot registration for the self-registration page.
3. Complete the self-registration configuration. See "[Creating a Self-Registration Page](#)" on page 348.
4. Return to **Configuration > Pages > Guest Self-Registrations** and click the page's row in the list.
5. Click one of the following links:
 - The **Go to Portal** link opens an active preview of the self-service login page and form as the guest would see it. This is the form that lets the guest access their account information. You can test the behavior of the form.
 - The **Go to Login** link opens an active preview of the network login page and form as the guest would see it. This is the page the guest sees when they log in to the network. You may test the behavior of the form.

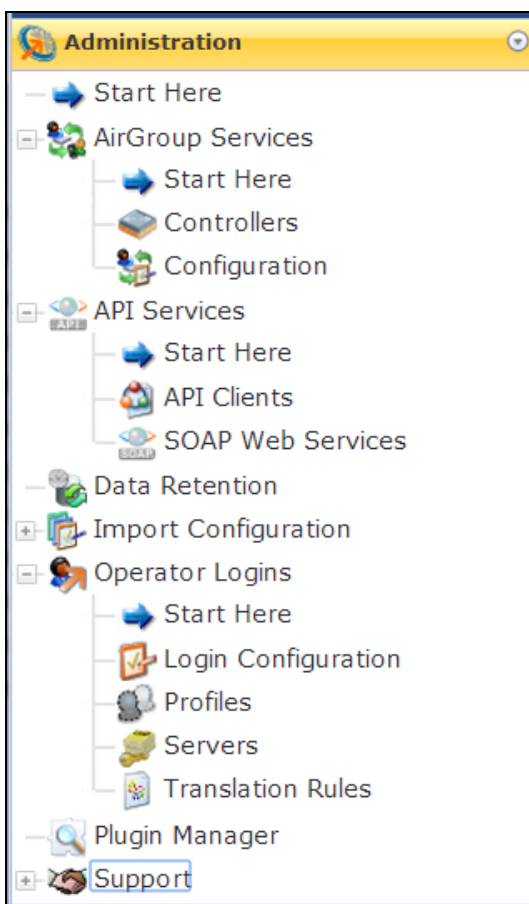


The Administration module provides tools used by a network administrator to perform both the initial configuration and ongoing maintenance of ClearPass Guest.

Accessing Administration

To access ClearPass Guest's administration features, click the **Administration** link in the left navigation.

Figure 393 *The Administration Module's Left Navigation*



AirGroup Services



This section describes creating and managing AirGroup controllers and configuring the AirGroup plugin, and provides links to other AirGroup steps performed in ClearPass Guest. For an overview of AirGroup functionality, see "[AirGroup Deployment Process](#)" on page 28. For complete AirGroup deployment information, refer to the AirGroup sections in the *ArubaOS User Guide* and the ClearPass Policy Manager documentation.

This section describes the following:

- "[AirGroup Controllers](#)" on page 538
- "[Creating and Editing AirGroup Controllers](#)" on page 540
- "[Configuring AirGroup Services](#)" on page 638
- "[AirGroup Diagnostics](#)" on page 543
- "[AirGroup Time-Based Sharing Syntax Examples](#)" on page 85
- "[Creating AirGroup Administrators](#)" on page 545
- "[Creating AirGroup Operators](#)" on page 545
- "[Authenticating AirGroup Users via LDAP](#)" on page 545
- "[Configuring LDAP User Search for AirGroup](#)" on page 545

AirGroup Controllers



You can create and manage multiple AirGroup controllers. You may configure each controller's remote access and other information, poll the current configuration, and view configuration details.

To work with your AirGroup controllers, go to **Administration > AirGroup Services > Controllers**. The **AirGroup Controllers** list view opens.

Figure 394 *The AirGroup Controllers List View*

Name	Hostname	Port	Config Status	APs	Groups	Roles
AirGroup Controller 1	192.0.2.3	5999	OK (101 minutes ago)	1	3	21
AirGroup Controller 2	192.0.2.11	3799	Not configured	0	0	0

All AirGroup controllers that have been created are included in the list. You can click an AirGroup controller's row in the list for additional options:

Table 242: *AirGroup List Options*

Field	Description
Show Details	Lets you view details for the AirGroup controller: Name, hostname or IP address and port number, configuration status, last polling time, currently defined roles and AP groups, and AP database details. See " AirGroup Controller Details " on page 539
Edit	Lets you edit the AirGroup controller's attributes. The Edit AirGroup Controller form opens. For more information, see " Creating and Editing AirGroup Controllers " on page 540 .
Disable	Disables the AirGroup controller. To enable it again at any time, click its Enable link.
Delete	Deletes the AirGroup controller. You are asked to confirm the deletion.
Read Configuration	Polls the AirGroup controller's current configuration. A progress bar is shown during the polling action. When the poll is complete, you can click Show Details to review the updated configuration details for the roles, AP groups, and AP database. For information on setting an automatic polling schedule, see " Configuring AirGroup Services " on page 638.
Create Controller	Lets you create a new AirGroup controller. The Create AirGroup Controller form opens. For more information, see " Creating and Editing AirGroup Controllers " on page 540.
AirGroup Diagnostics	Lets you perform AirGroup diagnostics. For more information, see " AirGroup Diagnostics " on page 543.

Figure 395 *AirGroup Controller Details*

AirGroup Controller																								
Controller:	AirGroup Controller 1																							
AirGroup RFC 3576:	192.0.2.3 : 5999																							
Configuration:	OK (5 minutes ago)																							
Last Checked:	Monday, 01 April 2013, 2:15 PM																							
Roles:	Number of roles: 21 <table border="0"> <tr> <td>ap-role</td> <td>default-via-role</td> <td>logon</td> </tr> <tr> <td>auth-guest-role</td> <td>default-vpn-role</td> <td>MAC-Guest</td> </tr> <tr> <td>authenticated</td> <td>denyall</td> <td>sdas-guest-logon-role</td> </tr> <tr> <td>BYOD-Provision</td> <td>Employee</td> <td>sham-BYOD-Provision</td> </tr> <tr> <td>cpbase</td> <td>guest</td> <td>sham-guest-logon-role</td> </tr> <tr> <td>cpg-qa-captiveportal</td> <td>guest-logon</td> <td>stateful-dot1x</td> </tr> <tr> <td>cpg-qa-logon</td> <td>guest-logon-role</td> <td>voice</td> </tr> </table> <p>Roles defined on the Aruba controller.</p>			ap-role	default-via-role	logon	auth-guest-role	default-vpn-role	MAC-Guest	authenticated	denyall	sdas-guest-logon-role	BYOD-Provision	Employee	sham-BYOD-Provision	cpbase	guest	sham-guest-logon-role	cpg-qa-captiveportal	guest-logon	stateful-dot1x	cpg-qa-logon	guest-logon-role	voice
ap-role	default-via-role	logon																						
auth-guest-role	default-vpn-role	MAC-Guest																						
authenticated	denyall	sdas-guest-logon-role																						
BYOD-Provision	Employee	sham-BYOD-Provision																						
cpbase	guest	sham-guest-logon-role																						
cpg-qa-captiveportal	guest-logon	stateful-dot1x																						
cpg-qa-logon	guest-logon-role	voice																						
AP Groups:	Number of AP groups: 3 <table border="0"> <tr> <td>cpg-qa-vap</td> <td>default</td> <td>qa-vap</td> </tr> </table> <p>AP group names defined on the Aruba controller.</p>			cpg-qa-vap	default	qa-vap																		
cpg-qa-vap	default	qa-vap																						
AP Database:	<table border="1"> <thead> <tr> <th>Name</th> <th>Details</th> <th>Serial</th> <th>Group</th> </tr> </thead> <tbody> <tr> <td> sdas-rap2 (RAP-2WG)</td> <td>MAC 1a:2b:3c:4a:5b:6c</td> <td>AH0012648</td> <td>qa-vap</td> </tr> <tr> <td>sdas-rap2.Floor 1.New Building.Main Campus</td> <td>IP 192.0.2.0</td> <td></td> <td></td> </tr> <tr> <td></td> <td>Switch 192.0.2.14</td> <td></td> <td></td> </tr> </tbody> </table>			Name	Details	Serial	Group	sdas-rap2 (RAP-2WG)	MAC 1a:2b:3c:4a:5b:6c	AH0012648	qa-vap	sdas-rap2.Floor 1.New Building.Main Campus	IP 192.0.2.0				Switch 192.0.2.14							
Name	Details	Serial	Group																					
sdas-rap2 (RAP-2WG)	MAC 1a:2b:3c:4a:5b:6c	AH0012648	qa-vap																					
sdas-rap2.Floor 1.New Building.Main Campus	IP 192.0.2.0																							
	Switch 192.0.2.14																							

Creating and Editing AirGroup Controllers

When you create a new AirGroup controller or edit an existing one, you may configure its name, description, notification status, its network connection and authentication settings, and SSH (Secure Shell) details for remote access.

To create a new AirGroup controller or edit an existing controller:

1. Go to **Administration > AirGroup Services > Controllers**, then either click **Create AirGroup controller** at the top of the form, or click a controller's **Edit** link. The **Create Controller** form opens.

Figure 396 *The Create Controller Form*

Create Controller	
General Settings <i>Common settings for the AirGroup controller.</i>	
* Name:	<input type="text" value="AirGroup Controller 2"/> <small>Enter a unique name for this controller.</small>
Description:	<input type="text"/> <small>Use this field to store comments or notes about this controller.</small>
Enabled:	<input checked="" type="checkbox"/> Send AirGroup notification events to this controller
Controller Settings <i>Configure settings for network connections and authentication.</i>	
* Hostname:	<input type="text" value="192.0.2.8"/> <small>Enter the hostname or IP address of the AirGroup controller.</small>
* RFC 3576 Port:	<input type="text" value="5999"/> <input type="button" value="↑"/> <input type="button" value="↓"/> <small>Enter the UDP port number for change of authorization (CoA) notifications.</small>
* Shared Secret:	<input type="password" value="*****"/> <small>Enter the shared secret for AirGroup dynamic notifications.</small>
Controller Configuration Access <i>Configure these settings to enable reading the controller's configuration.</i>	
SSH Username:	<input type="text" value="admin"/> <small>Enter the SSH username to access the controller.</small>
SSH Password:	<input type="password" value="*****"/> <small>Enter the SSH password to access the controller.</small>
Enable Password:	<input type="password" value="*****"/> <small>Enter the controller's enable password, if one is required.</small>
* SSH Timeout:	<input type="text" value="15"/> <input type="button" value="↑"/> <input type="button" value="↓"/> seconds <small>Enter the timeout in seconds for reading configuration.</small>
<input type="button" value="Create Controller"/> <input type="button" value="Cancel"/>	

Table 243: Create AirGroup Controller

Field	Description
Name	Short name that identifies the controller clearly. AirGroup controller names can include spaces.
Description	Additional useful information about the controller.
Enabled	Enables Policy Manager's AirGroup notification service for the controller. With this service enabled, the controller receives change of authorization (CoA) Requests for sharing events from associated MAC addresses and the events are logged.
Hostname	Hostname or IP address of the controller.
RFC 3576 Port	UDP port number for receiving CoA notifications. The default in ClearPass Guest is 5999 .
Shared secret	Shared secret for AirGroup dynamic notifications.
SSH Username	SSH username for accessing the controller.
SSH Password	SSH password for accessing the controller. The minimum password length is six characters.
Enable Password	The enable password for the controller.
SSH Timeout	Timeout limit in seconds for reading the configuration. The default is 15 seconds.

Configuring AirGroup Services

To enable support for dynamic notification of AirGroup events when new devices are added, each AirGroup-enabled controller must also be defined in ClearPass Guest. Configuration options include specifying roles to exclude from the user interface, and setting an automatic polling schedule, message parameters, and logging levels.

To configure AirGroup Services, go to **Administration > AirGroup Services > Configuration**. The **Configure AirGroup Services** form opens.

Figure 397 The Configure AirGroup Services Form

Configure AirGroup Services

AirGroup Controller Options
Options for collecting and using the configuration of AirGroup controllers.

Exclusions: denyall
List any role names, AP group names, or AP names that should be excluded from the AirGroup user interface, one per line. Items are matched case-insensitively. Comments may be entered on a line starting with '#'.

Polling: Automatically read configuration from AirGroup controllers on a schedule

Schedule: None -- Run task once
Select how frequently to run the task.

* Run At:
Select when the task should run.

Sharing Options
Options for different AirGroup sharing types.

Group Names:
List the user groups that are available in the 'Shared Groups' field. This list is automatically updated as new user group names are entered. Note that removing a group name from this list does not remove it from any shared group lists.

General Options
Network and logging options for AirGroup services.

* Network Interface: Automatic
AirGroup will use this network interface to send outbound notification messages. To enable using a virtual IP address, select the appropriate network interface. 'Automatic' uses the RFC-3576 Bind Address from Configuration » Authentication.

* Timeout: 5 seconds
Timeout for sending an AirGroup message.

* Attempts: 3
Maximum number of attempts to use when sending an AirGroup message.

* AirGroup Logging: Standard (Recommended) -- log basic information
Select an option for logging events related to AirGroup Services.

Table 244: Configure AirGroup Services

Field	Description
Exclusions	Role names, AP group names, or AP names that should not be displayed in the AirGroup user interface. Enter each item on a separate line. Entries are not case-sensitive. To add a comment, enter it on a separate line that begins with the "#" character.
Polling	If selected, schedules automatic polling of AirGroup controller configuration. The form expands to include scheduling options.
Schedule	Choose one of the following options from the drop-down list and complete the scheduling details: <ul style="list-style-type: none"> None -- Run task at once: In the Run At field, use the calendar picker to specify the month, day, and time to poll for configuration. Hourly: In the Minute field, enter the number of minutes past the hour to poll for configuration, or 00 to poll on the hour. If you do not need to poll every hour, you can use

Field	Description
	<p>the check boxes in the Hours field to specify which hours of the day the poll should run.</p> <ul style="list-style-type: none"> ● Daily: Use the text boxes in the Time of Day field to enter the hour and minute of the day the poll should run. ● Weekly: Use the check boxes in the Weekdays field to specify the day or days of the week the poll should run, then use the text boxes in the Time of Day field to enter the hour and minute of the day the poll should run. ● Monthly: Use the check boxes in the Months field to specify which month or months the poll should run, then use the text boxes in the Days field to specify the day or days of the month. Use the text boxes in the Time of Day field to enter the hour and minute of the day the poll should run. ● Yearly: In the Run On field, use the drop-down list to select a month, then enter the day and time in the text boxes. <p>When a poll is run, you may click Show Details in the Controllers list to view the updated configuration. For more information, see "AirGroup Controllers" on page 538. Automatic polling is run only on the publisher node.</p>
Group Names	<p>Enter names of shared groups that should be available in the Shared Groups field for users to choose from when they share a device. If additional user groups are also entered by users when they share a device, the list in the configuration is automatically updated to capture these fields. Removing a group name from this list does not remove it from other shared group lists.</p> <p>When you type a name for the group in the Group Names field, press the Enter key, and click Save, the group is created in the system and appears as a "tag". For more information, see "About AirGroup Time-Based Sharing" on page 89.</p> <p>Each group name may not exceed 64 characters. A maximum of 32 group names may be entered. The maximum character limit for the list is 320 characters (including comma separators).</p>
Network Interface	<p>Specifies the interface AirGroup will use to send outbound notification messages. To enable using a virtual IP address, select the appropriate interface. Options include:</p> <ul style="list-style-type: none"> ● Automatic — Automatically chooses the appropriate source IP address; either the management port or the data port, depending on the controller's IP address. ● Management port [MGMT] — Always uses the management port as the source address. ● Data/External port [DATA] — Always uses the data port as the source address.
Timeout	Number of seconds after which an attempt to send an AirGroup message will time out.
Attempts	Maximum number of times the system should attempt to send an AirGroup message.
AirGroup Logging	<p>Specifies the logging level. Options include:</p> <ul style="list-style-type: none"> ● Disabled—Do not log AirGroup related events ● Standard (Recommended)—Log basic information ● Extended—Log additional information ● Debug—Log debug information ● Trace—Log all debug information

AirGroup Diagnostics

The AirGroup Diagnostics form lets you perform several diagnostic actions. To access this form, go to **Administration > AirGroup Services > Configuration**, and then click the **AirGroup Diagnostics** link in the upper-right corner. The **AirGroup Diagnostics** form opens.

Figure 398 *The AirGroup Diagnostics Form*

AirGroup Diagnostics

* Diagnostic:

- Show information about a device
- Show information about a controller
- Associate a device with a controller
- Disassociate a device from a controller
- Show information about the AirGroup notification service
- Download AirGroup notification service log file

Submit

When you choose the diagnostic you want to run, the form expands to include fields for identifying information. When you enter the information and click **Submit**, the results of the query are displayed below the form. To run another diagnostic, click the **Reset Form** link before selecting the diagnostic.

Table 245: *AirGroup Diagnostics*

Field	Description
Show information about a device	Enter the device's MAC address. Information shown includes: <ul style="list-style-type: none"> • Device information (as entered on Guest > Create Device) • Controller IP address and AirGroup protocol version • Hostname of associated server, management IP address, and role • Times of AirGroup authorization requests along with controller IPs and enforcement profiles
Show information about a controller	Enter the controller's IP address or hostname. Information shown includes: <ul style="list-style-type: none"> • Times of AirGroup authorization requests along with MAC address, controller IPs, and enforcement profiles • MAC address, AirGroup state, time of last update, and expiration setting for devices associated with the controller
Associate a device with a controller	Links a MAC address to a controller as though the controller had issued an AirGroup authorization request for the device. Enter the device's MAC address and controller's IP address or hostname. Select the AirGroup protocol version. Two links are added below the form, one for viewing the device information, and one for viewing the controller information.
Disassociate a device from a controller	Removes the link between the MAC address and the controller as though the controller had reported the device no longer present on the network. Enter the device's MAC address and controller's IP address or hostname. Two links are added below the form, one for viewing the device information, and one for viewing the controller information.
Show information about the AirGroup notification service	Displays a list of statistics from the AirGroup notification service, showing values for various work items, CoA clients and requests, and RADIUS items.
Download AirGroup notification service log file	Downloads the log file to your system's Download folder.

See also:

- ["Configuring AirGroup Services" on page 638](#)
- ["AirGroup Controllers" on page 538](#)
- ["AirGroup Services " on page 538](#)

Creating AirGroup Administrators

AirGroup Administrators are users of ClearPass Guest who can define and manage their organization's shared devices. Devices can be shared globally, or shared with restrictions based on the username, role, or location of the user trying to access the device.

The AirGroup Administrator profile is automatically created in ClearPass Guest when the AirGroup Services plugin is installed. This profile is used to define the AirGroup Administrator role. To create an AirGroup Administrator, see ["Creating a New Operator" on page 680](#).

Creating AirGroup Operators

AirGroup Operators are users of ClearPass Guest who can provision a limited number of their own personal devices. Each device provisioned by an operator is automatically shared with all of that operator's provisioned devices. The operator can also define a group of other users who are allowed to share the operator's devices.

The AirGroup Operator profile is automatically created in ClearPass Guest when the AirGroup Services plugin is installed. This profile is used to define the AirGroup Operator role. To create an AirGroup Operator, see ["Creating a New Operator" on page 680](#).

Authenticating AirGroup Users via LDAP

ClearPass Guest supports LDAP authentication for administrators and operators. To provide AirGroup Services to LDAP-authenticated users:

1. Define the LDAP server for AirGroup. See ["External Operator Authentication" on page 680](#).
2. Define the appropriate translation rules to categorize the LDAP users. See ["Custom LDAP Translation Processing" on page 693](#).

Configuring LDAP User Search for AirGroup

On the AirGroup device registration portal, the **Shared Roles** and **Shared Locations** lists allow searching and selecting from the roles and locations defined in an AirGroup-enabled controller in order to specify the users with whom an AirGroup device should be shared. This section describes how to configure ClearPass Guest to enable interactive directory-based user search for these AirGroup fields.

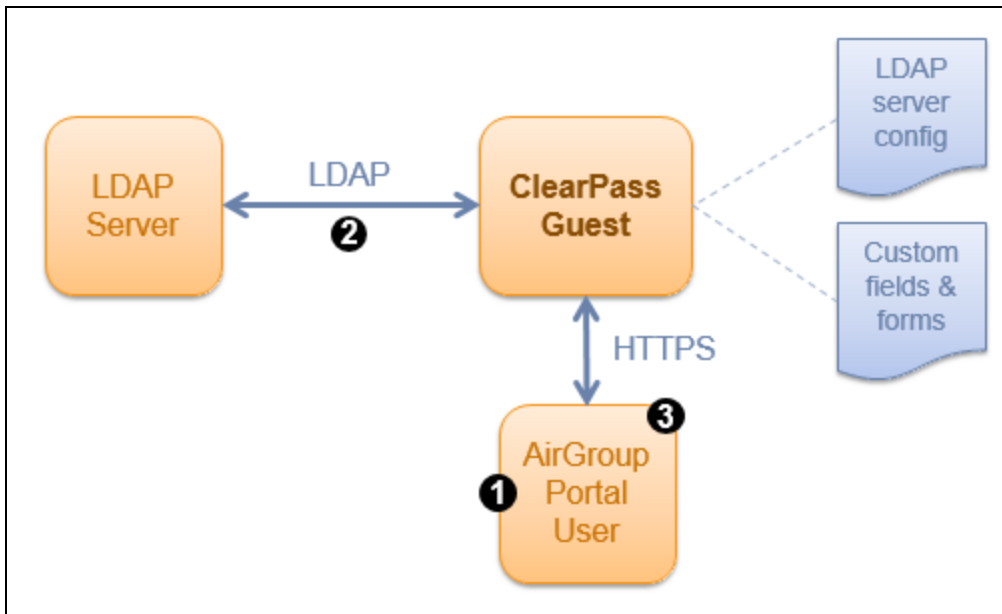
This section includes:

- ["LDAP User Search Architecture for AirGroup" on page 546](#)
- ["Configuration Summary for AirGroup" on page 546](#)
- ["Basic LDAP Server Settings for AirGroup" on page 546](#)
- [" User Search Settings for AirGroup" on page 548](#)
- ["Configuring the AirGroup Shared User Field" on page 549](#)
- ["Select2 Options Details" on page 551](#)
- ["Select2 Hook Details" on page 552](#)

LDAP User Search Architecture for AirGroup

The LDAP user search feature has several architectural components, as shown in the following diagram.

Figure 399 LDAP User Search Components



User Search Workflow for AirGroup

The workflow for a typical user search operation is:

1. The user of the AirGroup portal starts typing a username. This triggers a dynamic request to ClearPass Guest.
2. ClearPass Guest performs a search operation against the configured LDAP server.
3. Search results are returned to the portal user, who can then select from one of the matching item, or continue typing to further narrow the search.

Configuration Summary for AirGroup

To configure LDAP user search for AirGroup, you will:

1. Create a ClearPass Guest LDAP server
2. Enable user search for this server
3. Configure the user interface for the `airgroup_shared_user` field
4. Specify user search options for the user interface

Each of these steps is described in the following sections.

Basic LDAP Server Settings for AirGroup

In ClearPass Guest, go to **Administration > Operator Logins > Servers** and click the **Create new LDAP server** link. The **Server Configuration** form opens.

Figure 400 *The Server Configuration Form*

Server Configuration	
* Name:	<input type="text"/> Enter a name for this authentication server.
* Priority:	50 <input type="button" value="↑"/> <input type="button" value="↓"/> The priority rank of the service handler for authentication of local operators. Lower numbers represent higher priorities.
* Server Type:	Microsoft Active Directory <input type="button" value="v"/> Select the type of server you are connecting to.
* Server URL:	<input type="text"/> URL of the LDAP server, e.g. ldap://hostname/ or ldap://192.168.88.1/ou=IT-Services,ou=Departments,dc=amigopod,dc=com
Bind DN:	<input type="text"/> The Distinguished Name to use when binding to the LDAP server, or empty to perform anonymous bind.
Bind Username:	<input type="text"/> The username and domain to use when binding to the directory (username@domain, or domain\username format), or empty for an anonymous bind.
Bind Password:	<input type="password"/> The password to use when binding to the LDAP server, or empty for an anonymous bind.
Operator Logins	
Enabled:	<input checked="" type="checkbox"/> Use this server to authenticate operator logins
* Default Profile:	Null Profile <input type="button" value="v"/> Select the default operator profile to assign to operators authorized by this server.

In the basic properties and **Operator Logins** areas of the **Server Configuration** form:

Table 246: *Edit Authentication Server, Basic Properties*

Field	Description
Name	(Required) Name for the LDAP server.
Priority	(Required) Priority rank of the service handler for authentication of local operators. The lowest number has the highest priority.
Server Type	(Required) Specifies the type of server to connect to.
Server URL	(Required) The LDAP URL of the server. This would typically be in the form: ldap://ldap-server-hostname.example.com/<LDAP Base DN>
Bind DN	If your directory server requires authentication, provide suitable credentials. A typical base DN for Microsoft Active Directory might be DC=example,DC=com.
Bind Username	
Bind Password	
Enabled	Clear the Use this server to authenticate operator logins check box unless you also plan to configure LDAP operator logins with this server.

User Search Settings for AirGroup

Figure 401 The Server Configuration Form, User Search Area

User Search	
Enable <input type="checkbox"/> for users in the directory.	
Enabled:	<input checked="" type="checkbox"/> Use this server to search for matching users
* Filter:	Use the default LDAP filter <input type="button" value="v"/> The default filter looks for people based on their full name or their user ID.
* Display Attributes:	<pre>#sAMAccountName = id displayName = t # title = desc userPrincipalName = def the app.</pre> List the LDAP attributes to retrieve from the directory, and their type. Use the syntax 'attributeName = type', where type may be: 'id', 'text' or 'desc'.
Sort By:	displayName Name of the LDAP attribute on which the results should be sorted.
* Maximum Results:	30 <input type="button" value="v"/> Limit the number of results returned for each query.

In the **User Search** area of the **Edit Authentication Server** form:

Table 247: Edit Authentication Server, User Search

Field	Description
Enabled	If selected, the server will be used to search for matching users. The form expands to include additional options.
Filter	(Required) Filter methods. Options include: <ul style="list-style-type: none"> Use the default LDAP filter—Uses an LDAP filter suitable for an Active Directory search operation. <ul style="list-style-type: none"> The default filter matches user accounts based on any portion of the username (sAMAccountName attribute), or any portion of the user's full name (displayName attribute), and eliminates resources (display name starting with "*"), disabled accounts, and users without a userPrincipalName attribute. Specify a custom LDAP filter...—Allows you to enter a specific LDAP filter expression. <ul style="list-style-type: none"> This should be a valid LDAP filter expression per RFC 4515. The keyword @SEARCH@ is replaced with the user's actual search term when the filter is used.
Display Attributes *	(Required) Provide a list of LDAP attributes to retrieve when searching, and the treatment to apply to each attribute: <ul style="list-style-type: none"> id—Use the LDAP attribute as the value of a matching item. This value is used when a matching item is selected. This would normally be the case for the LDAP attribute that specifies the username. The directory should contain unique values in this attribute. text—Use the LDAP attribute as the text to display for a matching item. This would normally be the case for the LDAP attribute that specifies the user's common name (displayName in Microsoft Active Directory). Users will typically want to search on this attribute. desc—Use the LDAP attribute as additional descriptive text to display for a matching item. This is an optional item. <p>There must be exactly one attribute that is identified as an "id" attribute.</p> <p>Multiple LDAP attributes may be identified as "text" or "desc" attributes, in which case all the values are displayed together in the search results.</p> <p>If no LDAP attribute is identified as a "text" attribute, the "id" attribute will be used as the text.</p> <p>To use one attribute in different ways, provide a list of types. For example, specify sAMAccountName = id, desc to have the username act as both the ID and the description</p>

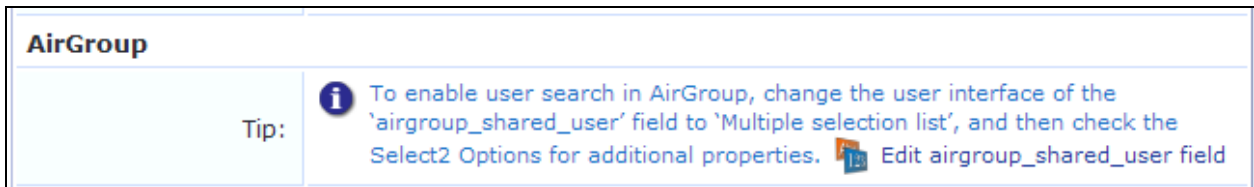
Field	Description
	text. Comments may be entered in this field by starting a line with the “#” character.
Sort By	Specify the name of an attribute on which to order the search results. Otherwise, the default value of displayName orders the results by the user's full name.
Maximum Results	(Required) Limits the total number of search results that can be displayed.

* In the **Display Attributes** field, the default value field provides the following behavior:

- **sAMAccountName = id**—The username is used as the value for a selected item.
- **displayName = text**—The user's full name is displayed as the label for a matching item.
- **# title = desc**—Commented out and not used by default. Enables the title of the user to be shown in the description.
- **userPrincipalName = desc**—The user's email address is displayed as descriptive text for a matching item.

Configuring the AirGroup Shared User Field

Figure 402 *The Server Configuration Form, AirGroup Field*



The **AirGroup** row of the **Edit Authentication Server** form is the starting point to enable the server for user search in AirGroup. This row provides a brief description of the process and a link to the **airgroup_shared_user** field's configuration form.

The **airgroup_shared_user** field stores a list of usernames with whom an AirGroup device should be shared. To enable user search, this field must be updated with new configuration options.

To configure the **airgroup_shared_user** field, do one of the following:

- From the **Administration > Operator Logins > Servers > Edit Authentication Server** form, click the **Edit airtgroup_shared_user field** link provided in the **Tip** in the **AirGroup** row.
- If you are not starting from the Edit Authentication Server form, go to **Configuration > Pages > Fields**, select the **airgroup_shared_user** field in the list, and then click **Edit**. The **Define Custom Field** form for that field opens.

Figure 403 *The Define Custom Field Form, Default Form Display Properties Area*

Default Form Display Properties

These properties control the default user interface displayed for this field.

User Interface:	<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">Multiple selection list ▼</div> <small style="color: #4F81BD;">The kind of user interface element to use when entering or editing this field.</small>
Searchable:	<input checked="" type="checkbox"/> Enable searching and advanced UI <small style="color: #4F81BD;">Select this option to use the 'select2' user interface. This provides search, autocomplete and better management for multiple selection lists.</small>
Label:	<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">Shared With:</div> <small style="color: #4F81BD;">Label for this field to display on the form.</small>
Description:	<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;"> Enter the usernames that will be able to use this device. Use a comma-separated list, e.g. </div> <small style="color: #4F81BD;">Descriptive text for this field, displayed with the user-interface element.</small>

Use the **Default Form Display Properties** area of the form to set the field type and enable search:

Table 248: *Default Form Display Properties, Relevant Fields*

Field	Description
User Interface	Type of user interface element to use for this field. Select Multiple selection list from this drop-down list.
Searchable	Select the Enable searching and advanced UI check box in this row. The Select2 Options and Select2 Hook fields are added to the form.

Figure 404 *The Define Custom Field Form, Select2 Options and Select2 Hook Fields*

Select2 Options:	<pre style="font-family: monospace; font-size: 0.9em;">multiple = 1 placeholder = (Select one or more users) minimumInputLength = 1 _advancedRender = 1 resultsCss.max-height = 400px ajax.dataType = sajax ajax.url = NwaLdapSponsorUserSearchAjax #ajax.args.server = <Name of server from Administration » Operator Logins » Servers> ajax.quietMillis = 500</pre> <small style="color: #4F81BD;">Optional list of additional properties for the enhanced 'select2' control.</small>
Select2 Hook:	<pre style="font-family: monospace; font-size: 0.9em;">function (args) { args.formatInputTooShort = function (text) { return "Start typing a user name."; }; };</pre> <small style="color: #4F81BD;">Optional JavaScript function to initialize the enhanced 'select2' control.</small>

In the **Advanced Properties** area of the form, you will customize the user interface for single and multiple-selection capabilities.

Table 249: Advanced Properties, Relevant Fields

Field	Description
Advanced	Select the Show advanced properties check box. Additional configuration options are added to the form.
Select2 Options	Used to customize the user interface for the “select2” control, which provides both single and multiple-selection capabilities. Default values are preconfigured for these fields. These defaults are intended for use with user search. However, the ajax.args.server parameter must be configured with the name of the LDAP server that should be searched.
Select2 Hook	
Save Changes	After the server name is specified in the ajax.args.server parameter in the Select2 Hook field, when you save your changes the AirGroup device registration portal includes the capability to search the directory based on username.

For details of the advanced options, functions, and additional parameters provided in the **Select2 Options** and **Select2 Hook** fields, see "[Select2 Options Details](#)" on page 551 and "[Select2 Hook Details](#)" on page 552. For in-depth technical information about these functions, refer to the Select2 programmer's documentation at <http://ivaynberg.github.com/select2/>.

Select2 Options Details

When configuring the `airgroup_shared_user` field for AirGroup user search, the advanced options provided in the **Select2 Options** field are shown in the following table:

Table 250: Details, Select2 Options Field

Option	Description
multiple = 1	Specifies that the field allows multiple selections. When this parameter is set, individual selections can be cleared by clicking an “x” delete icon displayed with each selection, or by using the Backspace key to erase a selected item.
placeholder = (Select one or more users)	Specifies the placeholder text that is displayed when the field is empty.
minimumInputLength = 1	Specifies that at least one character must be typed before a search operation is triggered. If the directory has a large number of user accounts in it, performing a single-character search is not likely to return any useful results, in which case this value should be increased.
_advancedRender = 1	Specifies that the list of matching items should be rendered in a way which includes an icon, text and description. If this parameter is not specified, only text is displayed in the matching items.
resultsCss.max-height = 400px	Specifies that the list of matching items should be up to 400 pixels in height. Additional CSS properties may be specified using the “resultsCss” value, if required.
ajax.dataType = sajax	Specifies that the field should use a dynamic query mechanism to look up a search term. This parameter should not be changed.

Option	Description
ajax.url = NwaAirGroupUserSearchAjax	Specifies that the field should perform a user search. This parameter should not be changed.
ajax.args.server = ...	Specifies the name of the LDAP server that should be searched. This parameter must match the name of the LDAP server that was created, or else the search operation will fail.
ajax.quietMillis = 500	Specifies that the user search operation should be performed after half a second (500 ms). This parameter is used to avoid performing searches while the user is still typing. To increase the responsiveness of the user interface, this parameter can be reduced, but doing so may increase the number of search operations performed against the LDAP server.

Additional parameters that may be specified in this field include:

Table 251: *Additional Parameters, Select2 Options Field*

Option	Description
width = 460px	Specifies the width of the field. A value in pixels may be specified, or another length unit supported by CSS. This parameter does not need to be specified if the CSS Style field is already used to specify a width.
maximumInputLength = <number>	Specifies the maximum number of characters that may be entered.
maximumSelectionSize = <number>	Specifies the maximum number of items that can be selected. After this number has been reached, the drop-down list will show a message returned by the formatSelectionTooBig function.
closeOnSelect = false	Specify this option to prevent the drop-down list from closing when a value is selected. This parameter is not recommended when dynamic search is enabled, as a dynamic list does not contain all possible items that may be selected.
containerCss.<style-name> = <style-value>	Specify CSS properties that will be applied to the containing element of the "select2" control.
dropdownCss.<style-name> = <style-value>	Specify CSS properties that will be applied to the drop-down list element of the "select2" control.

For in-depth technical information about these functions, refer to the Select2 programmer's documentation at <http://ivaynberg.github.com/select2/>. For information on configuring AirGroup for LDAP user search, see "Configuring LDAP User Search for AirGroup" on page 545.

Select2 Hook Details

The **Select2 Hook** field may be used to attach certain dynamic behaviors to the "select2" control.

This field must contain the definition of a JavaScript function that takes a single argument. The argument to this function specifies certain behavioral properties of the control. The function should return the argument, updated as necessary to specify the behavior that you want.

To change the behavior of the "select2" control, you need to attach a JavaScript function definition to one or more properties of the hook function's argument.

The hook function may also set or update any of the properties specified in the "Select2 Options".

A simple example is included as the default value with the `airgroup_shared_user` field:

```
function (args) {
  args.formatInputTooShort = function (text) {
    return "Start typing a user name.";
  };
  return args;
}
```

The functions that may be defined by the “Select2 Hook” function shown in the following table:

Table 252: *Select2 Hook Functions*

Function	Description
sortResults(results, container, query)	Used to sort the results list for searching right before it is displayed. Useful for sorting matches by relevance to the user’s search term.
formatNoMatches(term)	Function used to render the “No matches” message. Should return an HTML string.
formatSearching()	Function used to render the “Searching...” message that is displayed while a search is in progress. Should return an HTML string, or null to disable the message.
formatInputTooShort(term, minLength)	Function used to render the “Search input too short” message. Should return an HTML string.
formatSelectionTooBig(maxSize)	Function used to render the “You cannot select any more choices” message. Should return an HTML string.

For in-depth technical information about these functions, refer to the Select2 programmer’s documentation at <http://ivaynberg.github.com/select2/>. For information on configuring AirGroup for LDAP user search, see “Configuring LDAP User Search for AirGroup” on page 545.

MACTrac Services



MACTrac allows users to register their personal mobile devices on a local network. Each device registered by an operator is automatically shared with all of that operator’s registered devices. There is no limit to the number of device accounts an operator can create, and no expiration time is set on device accounts.

You use ClearPass Policy Manager to create MACTrac operators. MACTrac operators can then log in through ClearPass Guest to register and manage their devices.

For example, in a university setting, MACTrac provides a simple way for students to register their various devices on the network:

- The student is authenticated and can register as many devices as they wish.
- MACTrac automatically detects each device’s OS type, letting the network administrator easily build an inventory of the devices on the network and architect an appropriate network policy.
- There is no additional license fee for these devices: Although MACTrac is part of ClearPass Guest, MACTrac device registrations do not count against the ClearPass Guest license.

- As with other ClearPass Guest forms and views, the MACTrac user interface can be customized by adding a custom skin or options such as an "Add Another Device" button.

This section describes the following:

- "Creating MACTrac Operators" on page 554
- "Managing MACTrac Devices " on page 555
- "Registering MACTrac Devices " on page 557
- "Automatically Supplying the MACTrac Device Address" on page 559

Creating MACTrac Operators

MACTrac operators are users of ClearPass Guest who can register their personal devices on a local network. The MACTrac operator profile and translation rule are already available in ClearPass Guest, and the MACTrac role is available in ClearPass Policy Manager. No expiration time is set on MACTrac operator accounts.

To create a MACTrac operator, in **ClearPass Policy Manager**, go to **Configuration > Identity > Local Users** and click **Add**. The **Add Local User** form opens.

Figure 405 The Add Local User Form in Policy Manager

Add Local User	
User ID	<input type="text" value="mactracUser2"/>
Name	<input type="text" value="Setari MacTracker"/>
Password	<input type="password" value="....."/>
Verify Password	<input type="password" value="....."/>
Enable User	<input checked="" type="checkbox"/> (Check to enable local user)
Role	<input type="text" value="[MACTrac Operator]"/>
Attributes	
Attribute	Value
1. Email	= setMacTrac@mynetwork.org
2. Click to add...	
<input type="button" value="Add"/> <input type="button" value="Cancel"/>	

Table 253: Add Local User Form in Policy Manager

Field	Description
User ID	The MACTrac operator's username.
Name	The MACTrac operator's name.
Password	Password for the MACTrac user. The minimum password length is six characters.
Verify Password	
Enable User	If selected, enables this MACTrac operator. The new operator is enabled by default. If the operator is not to be activated until a later time, you may deselect this check box.
Role	Specifies the operator's role. Select the MACTrac Operator option.
Attribute	Lets you add attributes for additional information such as Phone, Email, Sponsor, Title, Department, or Designation , and provide values for these attributes.
Cancel	Cancels your entries on this form.
Add	Adds the new MACTrac operator to the Local Users list view.

Managing MACTrac Devices

The MACTrac operators you create can log in to ClearPass Guest to register their devices on their local network. Their view of the Guest user interface only includes the MACTrac features.



MACTrac operators can create and manage multiple device accounts. Options include editing, printing details, disabling, and deleting accounts.

To work with MACTrac devices, log in to ClearPass Guest as a MACTrac operator and go to **Guest > Manage Devices**. The **MACTrac Devices** list view opens.

Figure 406 *The MACTrac Devices List View*


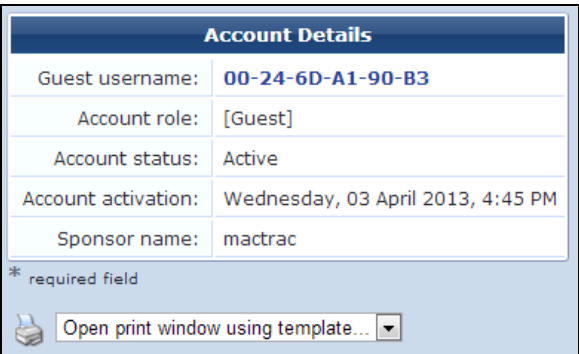
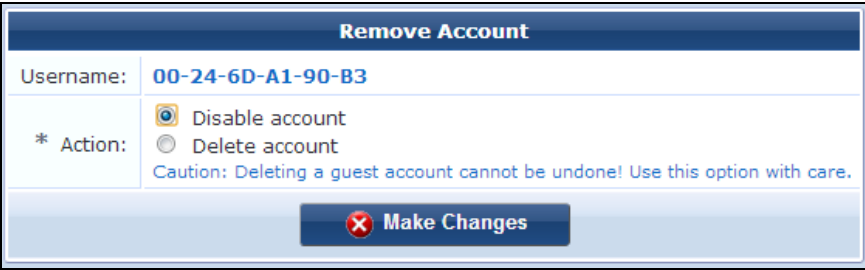
MAC Address	Device Type	Platform	Web Browser
G1:H2:I3:J4:K5:L6	Windows		Google Chrome
11:22:33:ab:cd:ef	Windows		Google Chrome
a1:b2:c3:d4:e5:f6	Windows		Google Chrome

Remove Edit Print

Refresh 1 Showing 1 - 3 of 3 20 rows per page

All MACTrac devices that have been registered are included in the list. You can click a device account's row in the list for additional options:

Table 254: MACTrac Devices List View

Field	Description
<p>Edit</p>	<p>Lets you edit any of a device account's attributes. The Edit MACTrac Device form opens. The process for editing a device account is the same as for creating the account. For more information, see "Registering MACTrac Devices " on page 557.</p> 
<p>Print</p>	<p>Lets you print a copy of the device account's details. The Account Details form opens and includes print options.</p> 
<p>Remove</p>	<p>Lets you disable or delete a device account. A confirmation dialog opens. You may specify either Disable or Delete, and then click Make Changes. To enable a disabled account, click its Activate link.</p> 

Registering MACTrac Devices

The **Register Device** form is used by MACTrac operators to create their device accounts on their local network. There is no limit to the number of accounts a MACTrac operator can create, and no expiration time is set on device accounts.

To register a MACTrac device, log in to ClearPass Guest as a MACTrac operator and go to **Guest > Create Device**. The **Register Device** form opens.

Figure 407 *The Register Device Form*

Register Device	
* MAC Address:	AA-BB-CC-11-22-33 <small>MAC address of the device.</small>
Device Name:	MyDevice <small>Name of the Device.</small>
Device Type:	Windows
Device Platform:	
Browser Vendor/Version:	Google Chrome
* Enabled By:	mactrac2 <small>Name of the person sponsoring this visitor account.</small>

The default **Register Device** form is described here. ClearPass administrators can customize this form with additional fields.

Table 255: *Register Device Form, MACTrac Devices*

Field	Description
MAC Address	(Required) The MAC address of the MACTrac device is prepopulated for the user. This is enabled in the Mobility Controller. For more information, see "Automatically Supplying the MACTrac Device Address" on page 559.
Device Name	Name for the MACTrac device.
Device Type	The type of device (computer, printer, or other device type). This value is prepopulated if detected.
Device Platform	The device platform (Windows, Mac, Linux, or Android platform, and whether it is a mobile phone). This value is prepopulated if detected.
Browser Vendor/Version	The vendor and version of the browser (Internet Explorer, Google Chrome, Mozilla Firefox, or other browser). This value is prepopulated if detected.
Enabled By	The sponsoring operator's name.
Create MAC	Registers the device and creates the account. The device account is included in the MACTrac Devices list, and can be shared with the operator's other registered devices.

About MAC Addresses

A MAC address is a number that uniquely identifies your device's network interface. A MAC address is sometimes referred to as an Ethernet hardware address (EHA), hardware address, or physical address.

MAC addresses are usually formatted as twelve characters grouped in pairs separated by either colons or hyphens. They may consist of only number pairs, or include number pairs and letter pairs, and in some cases do not include separators—for example:

00:11:22:33:44:55

00-11-22-33-44-55

11:22:33:AA:BB:CC

112233AABBCC

If for some reason the **Mac Address** field on the **Register Device** form is not prepopulated, you might need to find your device's address. Methods for finding the MAC address differ according to the type of device and operating system. Due to the variety of devices, these methods cannot all be described here, but they are easy to find on the Internet. An Internet search for "mac address" will return a number of pages describing how to quickly find MAC addresses for different device types.

Automatically Supplying the MACTrac Device Address

To ensure that the MAC address, device type, and browser vendor/version are prepopulated on the **MACTrac Register Device** form, verify that these options are set in the Mobility Controller.

To set MACTrac prepopulating options:

1. Log in to the Mobility Controller.
2. In the **Configuration** tab, go to **Security > Authentication** in the left menu.
3. Click the **L3 Authentication** tab, and then choose **Captive Portal Authentication Profile > cpg-qa-captiveportal**.
4. On the form, select the check box in the **Add switch IP address in the redirection URL** row.

Figure 408 Setting MACTrac Prepopulation Options in the Mobility Controller

The screenshot shows the Mobility Controller configuration interface. The top navigation bar includes Dashboard, Monitoring, Configuration (selected), Diagnostics, Maintenance, and Plan. A 'Save Configuration' button is visible. The left sidebar contains a tree view with categories: WIZARDS, NETWORK, SECURITY (selected), and WIRELESS. Under SECURITY, 'Authentication' is selected. The main content area is titled 'Security > Authentication > L3 Authentication'. It has tabs for Servers, AAA Profiles, L2 Authentication, L3 Authentication (selected), User Rules, and Advanced. A tree view on the left shows 'Captive Portal Authentication Profile' expanded to 'cpg-qa-captiveportal'. The main configuration area is titled 'Captive Portal Authentication Profile > cpg-qa-captiveportal'. It contains a table of settings:

Setting	Value	Default
Default Role	authenticated	Default
Redirect Pause	10 sec	User Lc
Guest Login	<input type="checkbox"/>	Logout
Use HTTP for authentication	<input type="checkbox"/>	Logon v
Logon wait maximum wait	10 sec	logon w thresho
Max Authentication failures	0	Show F
Use CHAP (non-standard)	<input type="checkbox"/>	Login p
Welcome page	/auth/welcome.html	Show V
Add switch IP address in the redirection URL	<input checked="" type="checkbox"/>	Allow o session
White List	<input type="text"/> <input type="button" value="Delete"/> <input type="button" value="Add"/>	Black L
Show the acceptable use policy page	<input type="checkbox"/>	

API Services



API Services includes all APIs and API-related privileges that are available for ClearPass Guest. To work with API services, go to **Administration > API Services**.

This section includes:

- "API Clients" on page 560
- "Configuring the API Framework Plugin" on page 639
- "Setting API Privileges in Operator Profiles" on page 565
- "About OAuth" on page 566
- "SOAP Web Services and API" on page 570
- "The XML-RPC Interface and API" on page 597

API Clients



You can create and manage multiple API clients. You may configure each API client's operator profile, grant type, refresh token, and other information.

The API Framework plugin provides API services. To configure the plugin, see ["Configuring the API Framework Plugin" on page 639](#).

To work with API clients, go to **Administration > API Services > API Clients**. The API Clients list view opens.

Figure 409 *The API Clients List View*

Filter:			
Client ID	Grant Types	Access Token	Operator Profile
Client1 Example client	password refresh_token	8 hours	Network Administrator
ExampleClient1 Example client	client_credentials	8 hours	API Guest Operator
Edit Disable Delete Generate Access Token			
My API Client Example client	client_credentials	8 hours	Super Administrator

All API clients that have been created are included in the list. You can click an API client's row in the list for additional options:

Table 256: API Clients List Options

Field	Description
Edit	Lets you edit theAPI client's attributes. The Edit API Client form opens. For more information, see "Creating and Editing API Clients" on page 561.
Disable	Disables the API client. You will be asked to confirm the action. Disabling an API client also invalidates any access tokens, refresh tokens, or authorization codes associated with it.
Enable	Enables a disabled API client.
Delete	Deletes the API client. You will be asked to confirm the deletion.
Generate Access Token	Generates a new access token. The form expands to show details, including its HTTP authorization, expiration, and syntax. This option is only available if Client credentials was selected as the grant type for the client.
Create API Client	Opens the Create API Client form. For more information, see "Creating and Editing API Clients" on page 561.
API Explorer	Opens the API Explorer. For more information, see "API Explorer" on page 564.

Figure 410 Generate Access Token Details

OAuth2 Access Token	
HTTP Authorization:	Bearer 404c816ed8009fe2e34b4ba3576faae73a3f4ac8
Expires:	Saturday, 31 January 2015, 1:52 AM
Details:	<p> Hide</p> <pre>array ('access_token' => '404c816ed8009fe2e34b4ba3576faae73a3f4ac8', 'expires_in' => 28800, 'token_type' => 'Bearer', 'scope' => NULL,)</pre>

Creating and Editing API Clients

To create or edit an API client, go to **Administration > API Services > API Clients** and either click the **Edit** link for an API client in the list, or click the **Create API client** link in the upper-right corner. The **Edit API Client** or **Create API Client** form opens. The procedure is the same for both forms.

Figure 411 *The Create API Client Form*

Create API Client

* Client ID:	<input style="width: 90%;" type="text" value="Example API Client 2"/> <small>The unique string identifying this API client. Use this value in the OAuth2 "client_id" parameter.</small>
Description:	<input style="width: 90%; height: 20px;" type="text" value="This is an example API client."/> <small>Use this field to store comments or notes about this API client.</small>
Enabled:	<input checked="" type="checkbox"/> Enable API client
* Operator Profile:	<input style="width: 90%;" type="text" value="Network Administrator"/> ▾ <small>The operator profile applies role-based access control to authorized OAuth2 clients. This determines what API objects and methods are available for use.</small>
* Grant Type:	<input style="width: 90%;" type="text" value="Username and password credentials (grant_type=password)"/> ▾ <small>Only the selected authentication method will be permitted for use with this client ID.</small>
Public Client:	<input type="checkbox"/> This client is a public (trusted) client <small>Public clients have no client secret.</small>
Refresh Token:	<input checked="" type="checkbox"/> Allow the use of refresh tokens for this client <small>An OAuth2 refresh token may be used to obtain an updated access token. Use grant_type=refresh_token for this.</small>
Client Secret:	8I+TPmcRbrCj8PmKPAD38f/DCsilSqJAJT9Mg0SFGFlr <small>Use this value in the OAuth2 "client_secret" parameter. NOTE: This value is encrypted when stored and cannot be displayed again.</small>
Access Token Lifetime:	<input style="width: 50px;" type="text" value="8"/> <input style="width: 50px;" type="text" value="hours"/> ▾ <small>Specify the lifetime of an OAuth2 access token.</small>
Refresh Token Lifetime:	<input style="width: 50px;" type="text" value="14"/> <input style="width: 50px;" type="text" value="days"/> ▾ <small>Specify the lifetime of an OAuth2 refresh token.</small>

Create API Client
 Cancel

Table 257: *Create API Client*

Field	Description
Client ID	(Required) Name for the API client. Enter a unique string. (Use this value in the OAuth2 client_id parameter)
Description	Additional information or comments about the API client.
Enabled	If selected, enables the API client.
Operator Profile	(Required) Specifies the role that can access this API client, and determines which API objects and methods are available. Options include: <ul style="list-style-type: none"> ● API Guest Operator ● BYOD Operator ● Device Registration ● Help Desk ● Network Administrator ● Null Profile ● Operations and Marketing ● Read-only Administrator ● Receptionist ● Super Administrator

Field	Description
Grant Type	(Required) Specifies the OAuth2 grant type authentication method to be used with this API client ID. Only the selected authentication method will be allowed. Options include: <ul style="list-style-type: none"> ● Client credentials (grant_type=client_credentials) ● Username and password credentials (grant_type=password)
Public Client	If selected, the API client will be a public (trusted) client, and will not require a client secret.
Refresh Token	If selected, an OAuth2 refresh token may be used to obtain an updated access token. (Use grant_type=refresh_token)
Client Secret	If a client secret is required, it is displayed in this field. Record this value for reference. When the API client is created, this value is encrypted and cannot be displayed again. When you edit an existing API client, this field includes the option to generate and display a new secret. (Use this value in the OAuth2 client_secret parameter)
Access Token Lifetime	Specifies the lifetime of the OAuth2 access token. Enter a number in the first text field, and use the drop-down list to indicate the unit of time. Options include: <ul style="list-style-type: none"> ● seconds ● minutes ● hours ● days ● weeks
Refresh Token Lifetime	Specifies the lifetime of the OAuth2 refresh token, if one was specified. Enter a number in the first text field, and use the drop-down list to indicate the unit of time. Options include: <ul style="list-style-type: none"> ● seconds ● minutes ● hours ● days ● weeks
Create API Client	Creates the API client. It is included in the API Clients list view.

API Explorer

The **API Explorer** provides access to various APIs used for configurations in Guest and Onboard. To see the APIs, go to **Administration > API Services > API Clients** and click the **API Explorer** link. The **API Explorer** opens.

Figure 412 *The API Explorer's Top-Level Index Page*

API	Services	Versions
ApiFramework	ApiAuthentication, ApiClient	v1
Authentication	AuthMethod	v1
Dictionaries	Attribute, ContextServerAction, Fingerprint	v1
Extension	Instance, InstanceConfig, InstanceLog, InstanceRestart, InstanceStart, InstanceStop, Store	v1
GuestManager	ActiveSession, ActiveSessionDisconnect, ActiveSessionReauthorize, Configuration, Device, Guest, GuestSponsor, WebLogin	v1
Identity	Endpoint, LocalUser, Role, StaticHostList	v1
Insight	Endpoint	v1
Network	NetworkDevice, NetworkDeviceGroup, ProxyTarget	v1
Onboard	Certificate, CertificateChain, CertificateExport, CertificateImport, CertificateNew, CertificateReject, CertificateRequest, CertificateRevoke, CertificateSign, Device, User	v1
OperatorLogins	GetAccount, GetPrivileges, ListAllPrivileges, OperatorProfile	v1
Platform	AccessControl, ClusterDbSync, ClusterWideParameter, ServerConfiguration, ServerFips, ServerSnmp, ServerVersion, Service	v1
SmsServices	SmsSend	v1
UsersAndPrivileges	AdminPrivilege, AdminUser	v1

The Explorer includes the following APIs:

- **ApiFramework**
- **Authentication**
- **Dictionaries**
- **Extension**
- **GuestManager**
- **Identity**
- **Insight**
- **Network**
- **Onboard**
- **OperatorLogins**
- **Platform**
- **SmsServices**
- **UsersAndPrivileges**

Setting API Privileges in Operator Profiles

To use ClearPass Guest's API services, the API privileges must be set up in the user's operator profile. Existing operator profiles that have the Administrator privilege set to Full Access must be updated to specifically include the appropriate privilege in order for XML-RPC clients to work.

To set up API privileges:

1. Go to **Administration > Operator Logins > Profiles**, and either click the **Edit** link for an existing profile in the list or click the **Create a new operator profile** link to create a new profile. The **Operator Profile Editor** form opens.

Figure 413 The Operator Profile Editor Form

The screenshot shows the 'Operator Profile Editor' form. At the top, there is a header 'Operator Profile Editor'. Below it, there are two main sections: 'Name' and 'Description'. The 'Name' field is labeled '* Name:' and contains the text 'API Guest Operator'. Below it is a small instruction: 'Enter a name for this operator profile.'. The 'Description' field is labeled 'Description:' and contains the text 'Operators with this profile can use the API to manage guest accounts.'. Below it is a small instruction: 'Comments or descriptive text about the operator profile.'. Below the description field is the 'Access' section. It is titled 'Access' and has a sub-header 'These options control what operators with this profile are permitted to do.'. Below this is the 'Enabled:' section, which has a checked checkbox for 'Allow operator logins' and a sub-instruction: 'If unchecked, operators with this profile will not be able to log in.'. Below the 'Enabled:' section is the 'Operator Privileges' section. It is titled 'Operator Privileges' and contains a list of privileges with their respective access levels. The privileges listed are: Administrator (No Access), Advertising Services (No Access), AirGroup Services (No Access), API Services (Custom...), Allow API Access (Allow Access), Configure SOAP Web Services (Legacy) (Read Only), List SOAP Web Services (Legacy) (Full), Manage API Clients (No Access), SOAP API (Legacy) (Full), and XMLRPC API (Legacy) (Allow Access). Each privilege has a small icon to its left and a brief description of its function. The 'API Services' privilege is expanded to show a list of sub-privileges with their respective access levels: Allow API Access (Allow Access), Configure SOAP Web Services (Legacy) (Read Only), List SOAP Web Services (Legacy) (Full), Manage API Clients (No Access), SOAP API (Legacy) (Full), and XMLRPC API (Legacy) (Allow Access).

2. In the **Privileges** field, select **Custom** in the **API Services** drop-down list. The field expands to show the API privileges. Privileges included here are:
 - **Allow API Access**
 - **Configure SOAP Web Services**
 - **List SOAP Web Services**
 - **Manage API Clients**
 - **SOAP API**
 - **XMLRPC API**
3. For the **Allow API Access** privilege, select the **Allow Access** radio button.
4. For each of the remaining privileges in the list, select the appropriate access level. Access levels include:
 - **No Access**
 - **Read Only**

- **Full**
 - **Allow Access**
5. If you want to allow the API operator profile to query for Guest Manager configuration settings, set the **Manage Customization** privilege to **Read Only** access.
 6. Complete the rest of the settings appropriately for the operator profile and then click **Save Changes**. For more information, see ["Creating an Operator Profile" on page 673](#).

About OAuth

The OAuth 2 RFC 6749 specification for accessing a new set of modern API's is supported by ClearPass 6.4 and later. All OAuth2 requests MUST use the SSL endpoint available at **https://<ClearPass IP or FQDN>/api/oauth**.

OAuth 2.0 is a simple and secure authorization framework. It allows applications to acquire an access token for ClearPass through a variety of workflows supported within the OAuth2 specification. After an application has an access token, it can access the various APIs serviced by ClearPass either to configure the platform itself or act on behalf of a ClearPass Operator. To use OAuth for authorization:

- Decide on the use case for API Access — Either ClearPass administrative configuration, or managing ClearPass data on behalf of a ClearPass Operator (Guest Management, Onboarded devices, Device Registration etc).
- Create a ClearPass API Client definition that matches the use case above — Either **Service Account** (client credentials) or **Authorized User Account** (resource owner password), respectively.
- Request an Access Token using the Client ID details from the ClearPass API client definition created in the previous step.
- Make authorized API calls to the ClearPass APIs by including the Bearer <access_token> in the HTTP Authorization header.

This section includes:

- ["OAuth Basics" on page 566](#)
- ["OAuth2 Client or App for OAuth" on page 567](#)
- ["Client ID and Secret for OAuth" on page 567](#)
- ["Redirect URI" on page 567](#)
- ["Anti-Forgery State Token for OAuth" on page 567](#)
- ["Authorization Grant Types for OAuth" on page 568](#)
- ["Application Service Accounts for OAuth" on page 569](#)

OAuth Basics

The best way to understand the different use cases for OAuth2 is to start with the various roles that make up a possible OAuth2 transaction.

Resource Owner

The resource owner is the person or application that owns the data that is to be shared. For example, a user on Facebook or Twitter could be a resource owner, in the same way as an Operator on ClearPass. The resource they own is their data. Typically the resource owner is thought of as a person but it could also be an application. The OAuth 2.0 specification supports different workflows for each of these use cases.

Resource Server

The resource server is the server hosting the resources. For example, either a platform such as Facebook or a ClearPass appliance could be considered a resource server. It is essentially the server hosting the protected content that will be accessed via the APIs.

Client Application

The client application is the application requesting access to the protected resources stored on the resource server.

Authorization Server

The authorization server authorizes the client application to access the resources of the resource owner. The authorization server and the resource server can be deployed as part of the same server, but the OAuth 2.0 specification does not dictate whether they should be co-located or separated. For simplicity, the rest of this document assumes the resource server and authorization server are co-located on the same server.

OAuth2 Client or App for OAuth

Before any OAuth transactions can be processed, the first step is to register a new app with the service (API Client definition in ClearPass). When you register a new app with the Authorization Server, you specify basic information such as the application name and the OAuth2 grant type. Depending on the grant type selected, a redirect URI may also be requested in order to whitelist the redirect destination for OAuth2 workflows that are initiated from Web server, browser-based, or mobile apps.

The output of registering an OAuth2 app is a client id and client secret.

Client ID and Secret for OAuth

After you register your app, you will receive a client ID and a client secret. The client ID is considered public information, and is used to build login URLs, or is included in JavaScript source code on a page. The client secret must be kept confidential. If a deployed app such as JavaScript or native apps cannot keep the secret confidential, then the secret is not used.

Redirect URI

During registration of the new OAuth app, often a redirect URI must be included. This redirect URI is used when a resource owner grants authorization to the client application. When a resource owner has successfully authorized the client application via the authorization server, the resource owner is redirected back to the client application, to the redirect URI. It is important to maintain the redirect URI accurately as this forms a key security mechanism of OAuth2 to whitelist the redirect destination and avoid hi-jacking of the authorization workflow, as publicized in articles such as http://tetrapp.com/covert_redirect/oauth2_openid_covert_redirect.html.

Anti-Forgery State Token for OAuth

To protect the security of your users by preventing request forgery attacks, the client app should create an anti-forgery state token. The first step is to create a unique session token that holds state between your app and the user's client. The app later match this unique session token with the authentication response returned by the Authorization server to verify that the user is making the request, and not a malicious attacker. These tokens are often referred to as cross-site request forgery (CSRF) tokens.

Authorization Grant Types for OAuth

OAuth 2 provides several "grant types" for different use cases. ClearPass supports the following defined grant types:

- **Password**— For logging in with a username and password
- **Client credentials**— For application access

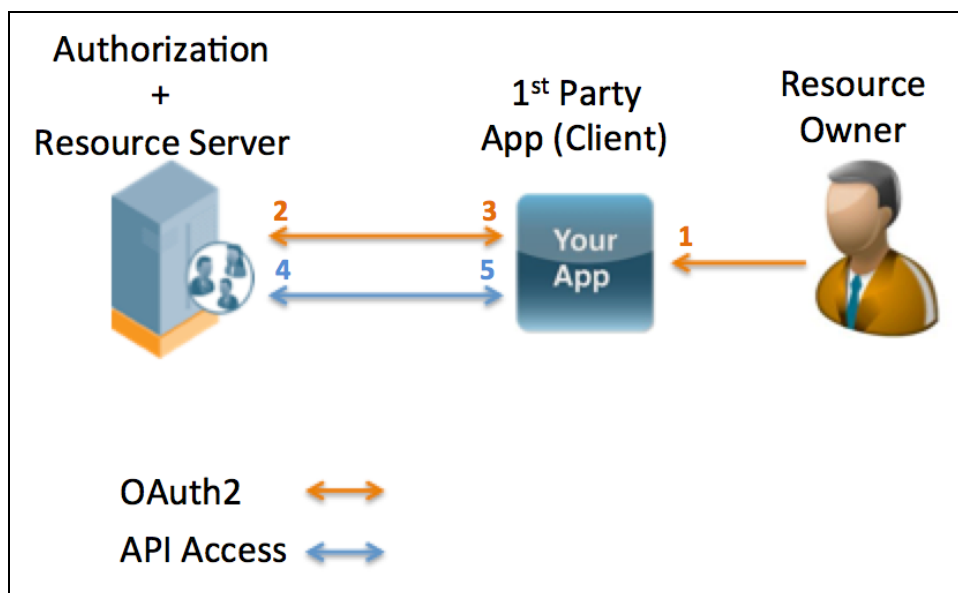
Resource Owner Password Grant Type

OAuth 2 also provides a password grant type, which can be used to exchange a username and password for an access token directly. This is often compared with HTTP basic authentication because the same credentials are being exchanged, but it has the same security benefits as the other OAuth2 grant types in expiring the access token and the ability to refresh the access token without the need to cache or resubmit the user credentials.

Since this requires the application to natively collect the user's credentials, this grant type should only be used for apps with a direct relationship (first party) with the authorization server. A real world example would be the official mobile app for a social networking site versus allowing 3rd party developers to leverage APIs to develop their own mobile experience for the social platform (they should be leveraging the Implicit flow).

The following diagram shows the transaction flow of password grant type.

Figure 414 Password Grant Type Transaction Flow



1. The user enters credentials directly into the app's native user interface. The app should not cache user credentials under any circumstances.
2. The app submits the user credentials to the authorization server. Credentials include `grant_type=password`, `user`, `password`, `client_id`, and `client_secret`. The `client_secret` is not required if the OAuth2 app is defined as a public client.
3. The resource server returns the access token to use in subsequent API calls. This includes `access_token`, `expiry_time`, `token_type=bearer`, and `refresh_token`.
4. The app includes the access token in the HTTP Authorization header. This includes the Bearer `access_token`.
5. The resource server returns the authenticated API payload.

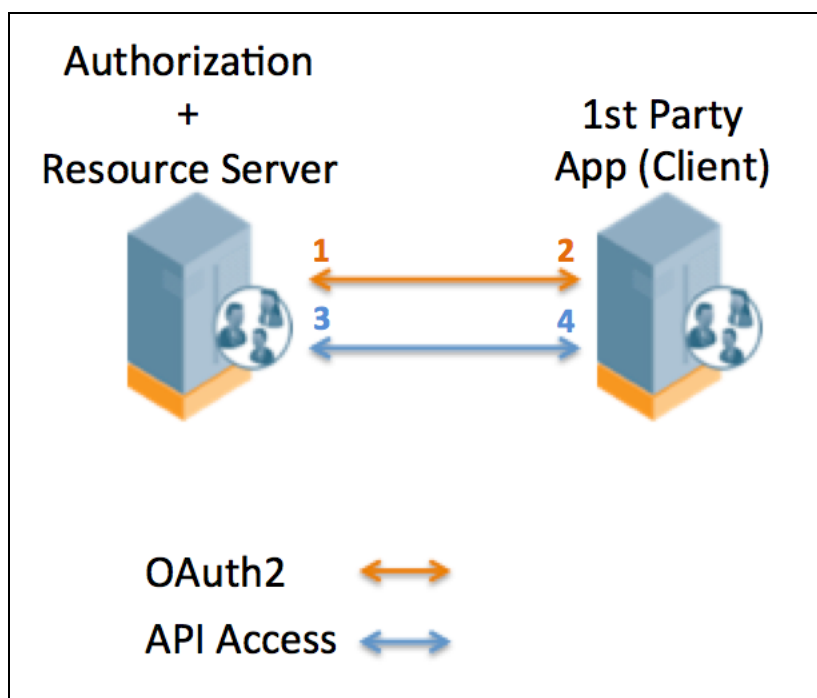
Client Credentials Grant Type

The simplest grant type offered by OAuth2 doesn't include a 3rd party user at all and is essentially intended for server-to-server integrations for updating the application server configuration. In this case, applications need a way to get an access token for their own user and need to do this outside the context of any specific user. OAuth provides the client credentials grant type for this purpose.

Given the simplicity of this grant type, many developers may use its basic workflow to recover an access token so they can quickly get started with the APIs. That being said, client credentials should never be used in production where an untrusted 3rd party developer has access to the client secret.

The following diagram shows the transaction flow of the client credentials grant type.

Figure 415 Credentials Grant Type Transaction Flow



1. The first-party app submits an access token request to the authorization server. This includes `grant_type=client_credentials`, `client_id`, and `client_secret`.
2. The resource server returns the access token to use in subsequent API calls. This includes `access_token`, `expiry time`, and `token_type=bearer`.
3. The app includes the access token in the HTTP Authorization header. This includes `Bearer access_token`.
4. The resource server returns authenticated API payload.

Application Service Accounts for OAuth

Google APIs such as the Prediction API and Google Cloud Storage can act on behalf of your application without accessing user information. In these situations your application needs to prove its own identity to the API, but no user consent is necessary. Similarly, in enterprise scenarios, your application can request delegated access to some resources.

For these types of server-to-server interactions you need a service account, which is an account that belongs to your application instead of to an individual end-user. Your application calls Google APIs on behalf of the service

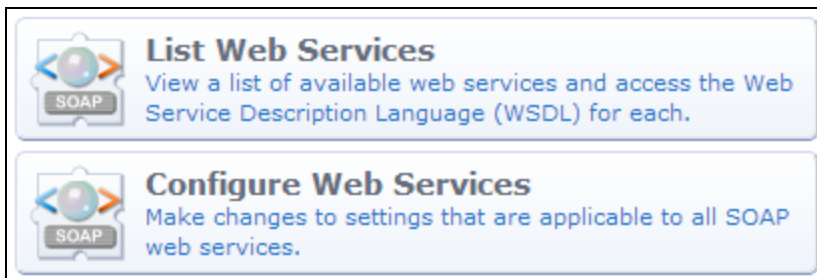
account, and user consent is not required. (In non-service-account scenarios, your application calls Google APIs on behalf of end-users, and user consent is sometimes required.)

SOAP Web Services and API



SOAP Web Services provide a way of transferring data across the Internet to integrate Web-based applications. Web services let businesses share data and processes programmatically, and can be added to a user interface to provide functionality.

To access this feature in ClearPass Guest, you must have the SOAP Web Services plugin installed.



Viewing Available Web Services

To view the Web services available in ClearPass Guest:

1. Go to **Administration > API Services > SOAP Web Services**. The **SOAP Web Services** list opens.

Figure 416 *The SOAP Web Services List*



2. To view details for a service, click its image in the **Web Service** field. The form expands to include the **Service URL** and **Service Info** fields for that Web service.

Figure 417 The SOAP Web Services List with a Service Selected



3. The **Service Info** field briefly describes the processes this Web service provides. In the **Service URL** field, you can click the link to view the Web Service Description Language (WSDL) that defines that service. The WSDL opens in a new tab.

Figure 418 The Web Service Description Language (WSDL) for a Service



4. When you have finished reviewing the available Web services, click **Done**.

SOAP API Introduction

The SOAP interface is available to third-party applications that will integrate with the ClearPass Guest Visitor Management Appliance.

Audience

This API is intended for developers of applications that must interoperate with a ClearPass Guest-based visitor management solution. Solution developers are assumed to be familiar with HTTP-based Web services and the associated concepts and technologies related to these services, including Extensible Markup Language (XML), XML Schemas, Web Service Definition Language (WSDL), and the Simple Object Access Protocol (SOAP).

Many software development tools provide assistance with Web services integration. While this document cannot cover all possible integration methods, examples are given using Microsoft Visual C# 2008.

API Documentation Overview

- ["About the SOAP API" on page 572](#) provides a high-level overview of the API, explaining what it is and how to use it.
- ["Integration Example" on page 577](#) provides an integration example to demonstrate the usage of SOAP Web Services.
- ["API Documentation" on page 582](#) contains a detailed list of the available API calls, including documentation about each method defined by the web services.

Disclaimer

The topics of network design, security architectures, and visitor access are complex subjects, and no single document can hope to cover all of the possible combinations of network equipment, network design, deployment requirements, and device configurations, nor can all the possible security implications for a particular recommendation be covered. Therefore, while you read this document, it is best to consider it as a guide to developing your own understanding of the network design topics covered, and as a basis for further investigation.

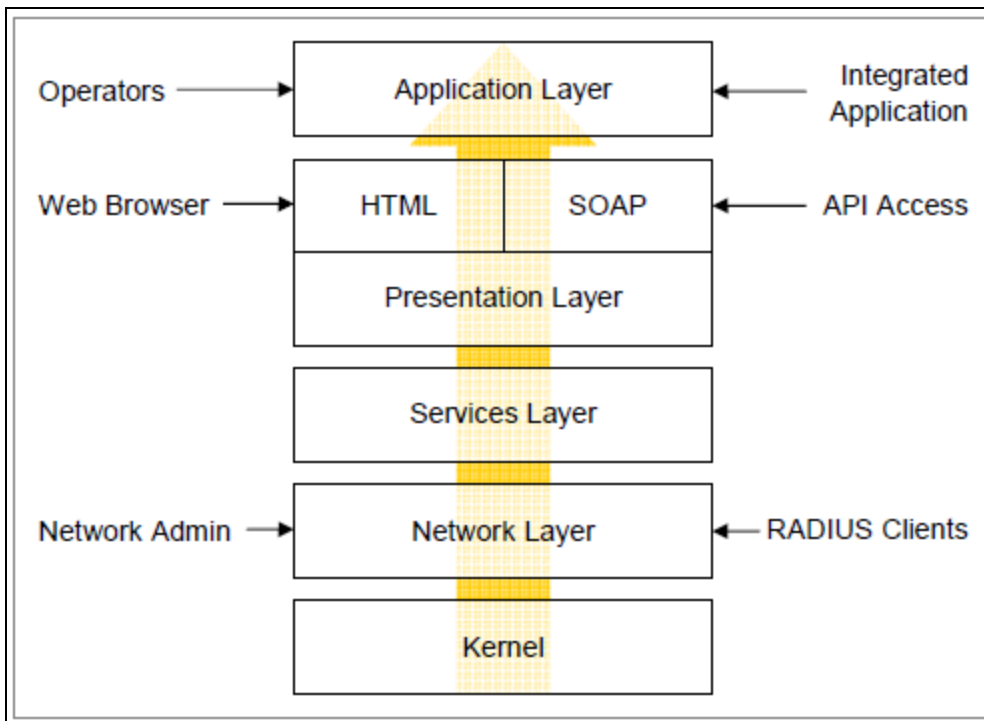
About the SOAP API

The ClearPass Guest SOAP API provides direct access to the underlying functionality of ClearPass Guest. Developers wishing to provide integrated applications can make use of this API to programmatically perform actions that would otherwise require manual operation of the user interface.

Architecture Overview

The ClearPass Guest software is built using multiple layers:

Figure 419 Layers of Software in ClearPass Guest



- At the lowest level, the kernel provides basic functions common to the entire system. This includes the Web interface framework, appliance operating system, and runtime support services.
- The network layer provides critical networking support, including the RADIUS server and the ability for network administrators to manage and control the networking aspects of the appliance.
- The services layer provides one or more implementations of application services that are used by the layers above. Examples of these services include managing a user database used for AAA, handling the authentication of operators, and providing translated text resources.
- The presentation layer supplies the tools and framework necessary for the appliance software to interact with the outside world. The basic presentation layer services include authentication checks, session establishment, input checking, validation and conversion, and command execution. Both SOAP and HTML presentation methods are supplied, which adapt the underlying basic presentation to appropriate conventions suitable for a machine-to-machine or human-to-machine interaction.
- The application layer provides the page templates, business logic, and the concrete features making up visitor management applications such as Guest Manager or Hotspot Manager. These applications are built using the services provided by the lower layers.

Authentication and Access Control

SOAP API requests require that operator authentication information is provided using HTTP Basic authentication.

Page privileges are applied to SOAP authenticated sessions in the same way as the HTML user interface. However, SOAP access also requires the SOAP API privilege to be granted.

Refer to "[Using the SOAP API](#)" on page 575 for details on creating an operator profile with suitable privileges for SOAP API access.

HTTP headers

When making a SOAP API request, the **SOAPAction** HTTP header is required. The value of this header indicates the type of request being made.

The **Content-Type** header must be specified as either **text/xml** or the **application/soap+xml** MIME type.

The **Authorization** header must contain a valid HTTP Basic authentication string, as specified in RFC 2617.

Character Set Encoding

ClearPass Guest supports the Unicode character set, using the UTF-8 encoding. Although other character sets are supported, it is recommended that all SOAP API requests be constructed using the UTF-8 character set, as this eliminates the need for character set conversions while also allowing all Unicode characters to be expressed directly.

The character set encoding of a request may be specified using the Content-Type header, for example:

```
Content-Type: text/xml; charset=utf-8
```

SOAP Faults

SOAP 1.1 defines a generalized fault response which is used to indicate that the server could not process the body of the request. The SOAP <Fault> element contains a description of the error, which is divided into a <faultcode> that briefly summarizes the problem, and a <faultstring> that contains a description of the error.

Additionally, the API-specific details of the error are provided in a <details> element.

The following table lists the fault codes and corresponding descriptions that might be encountered while using the SOAP API:

Table 258: *Fault Codes and Descriptions*

Fault	Reason for Fault
Client.BadRequest	Request exceeds the maximum allowable size. Increase the maximum SOAP request size, or reduce the size of the request.
Client.Authentication	Invalid username or password. Check that the credentials supplied are correct.
Client.MethodNotFound	The SOAP method request was not found.
Client.Error	Another non-specific client error occurred. Check the <faultstring> for more details.
Server.MethodNotImplemented	The SOAP method requested is not implemented.
Server.Error	An error occurred while attempting to convert data, or another non-specific server error occurred. Check the <faultstring> for more details.

Certain conditions might also cause errors that are not reported as a fault. These cases are typically caused by errors in constructing the SOAP request. In these cases, a non-XML result may be returned; check the body of the result, or the application log for details about the cause of the error.

Using the SOAP API

This section describes how to access, configure, and debug Web Services, create a SOAP API operator, and access the WSDL.

Accessing and Configuring SOAP Web Services

To access the SOAP Web Services user interface, go to **Administration > API Services > SOAP Web Services**. Click the **Configure SOAP Web Services** link to make changes to system settings affecting the SOAP API.

Figure 420 *The Configure SOAP Web Services Form*

Configure SOAP Web Services	
WSDL Access:	<input checked="" type="checkbox"/> Allow anonymous access to WSDL Control whether Web Service Description Language (WSDL) requests require an operator to be logged in.
* Maximum Request Size:	200 <input type="text"/> KB The maximum permissible size of a SOAP request, in kilobytes. Requests larger than this size will be rejected.
* SOAP Debugging:	1 - Log SOAP errors only <input type="text"/> Sets the debugging level for SOAP service requests. Higher levels will cause more information to be logged to the application log.
<input type="button" value="Save Configuration"/>	

SOAP Debugging

Select a higher level for the **SOAP Debugging** configuration option to log additional details to the application log.

To access the application log, go to **Administration > Plugin Manager > Application Log**.

At the highest debugging level of **4**, every SOAP request and response will be logged including full HTTP headers and contents, which may be useful when trying to identify the exact cause of a problem.

Creating a SOAP API Operator

The SOAP API requires both authentication and authorization components.

- **Authentication** means that suitable credentials must be provided via the HTTP “basic” access authentication method. A valid ClearPass Guest operator username and password must be provided.
- **Authorization** for the SOAP API requires that the corresponding user account has sufficient privileges to perform the requested operation. In the ClearPass Guest role-based access control system, this requires at a minimum that the SOAP API privilege is granted, as well as any additional privileges required for the operation requested.

While the default administrative account will automatically gain SOAP API privileges, for security reasons it is strongly recommended that a specific operator profile be created for use by SOAP API clients.

To create a suitable operator profile, go to **Administration > Operator Logins > Profiles**, then click the **Create a new operator profile** link.

In the **Privileges** list, select either **Full Access** for the **SOAP Web Services** privilege, or choose **Custom...** and then select either **Read Only** or **Full** for the **SOAP API** privilege.

You should also select suitable permissions for the **Guest Manager** privilege, depending on the type of requests that will be made.

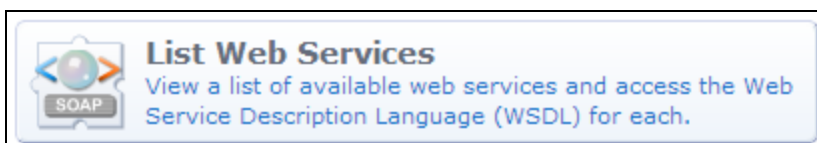
An example profile is shown below.

Figure 421 Example Profile in the Operator Profile Editor

The screenshot displays the "Operator Profile Editor" interface. At the top, the title "Operator Profile Editor" is centered in a dark blue header. Below the header, the "Name" field is set to "SOAP API User" with a subtext "Enter a name for this operator profile." The "Description" field contains "Profile for use by SOAP API clients." and a subtext "Comments or descriptive text about the operator profile." The "Access" section is titled "Access" and includes the instruction "These options control what operators with this profile are permitted to do." Under "Enabled:", the checkbox "Allow operator logins" is checked, with a subtext "If unchecked, operators with this profile will not be able to log in." The "Privileges" section lists various services with their corresponding access levels: Administrator (No Access), AirGroup Services (No Access), Guest Manager (Full Access), Hotspot Manager (No Access), IP Phone Services (No Access), Onboard (No Access), Operator Logins (No Access), Platform (No Access), SMS Services (No Access), SMTP Services (No Access), SOAP Web Services (Full Access), and Support Services (No Access). The "Guest Manager" and "SOAP Web Services" entries are highlighted with red boxes.

After you have created a suitable operator profile, create the operator login. See "Local Operator Authentication" on page 680 and "External Operator Authentication" on page 680.

Accessing the WSDL



Use the **List Web Services** command link to browse the available Web services and obtain additional details about each one.

Figure 422 *The SOAP Web Services List*



In the **Web Service** field, click the icon for **GuestManager Web Services** to view the Service URL and additional information about the service.



If the "Allow anonymous access to WSDL" option is specified in the SOAP Web Services configuration, accessing the WSDL through the specified Service URL does not require logging in to the ClearPass Guest user interface. For more information, see "Configuring the SOAP Web Services Plugin" on page 661.

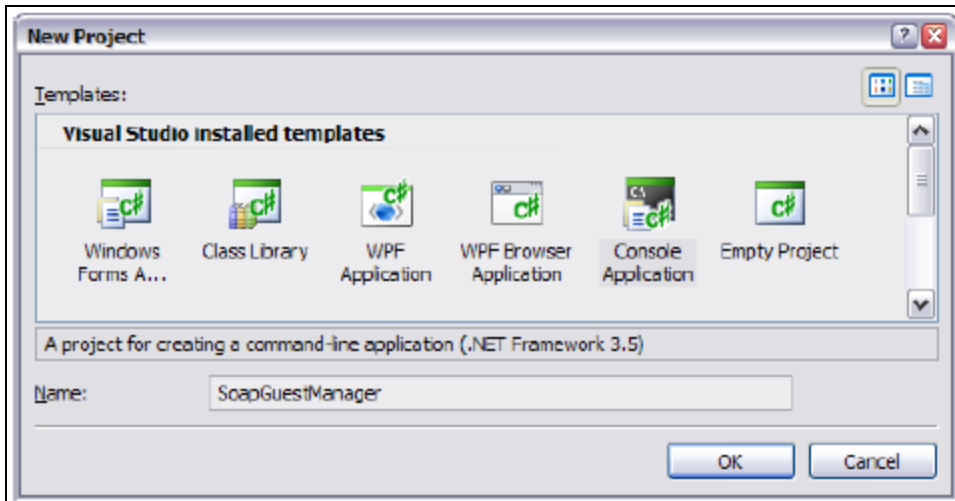
Integration Example

In this section, a simple console application will be developed using Microsoft Visual C# 2008 Express Edition. The "Add Service Reference" feature of this development tool will be used to automatically create a Web service interface which can then be used from the code.

Create a New Project

From the **File** menu, choose **New Project**.

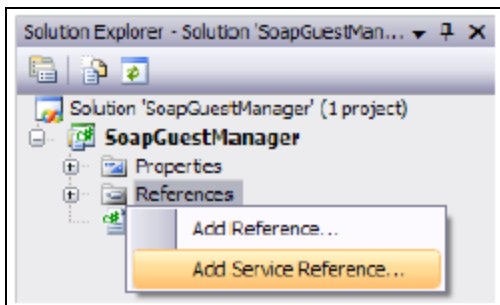
Figure 423 *The New Project Dialog*



Add Service Reference

1. In the **Solution Explorer**, right-click the **References** folder, and then click **Add Service Reference**.

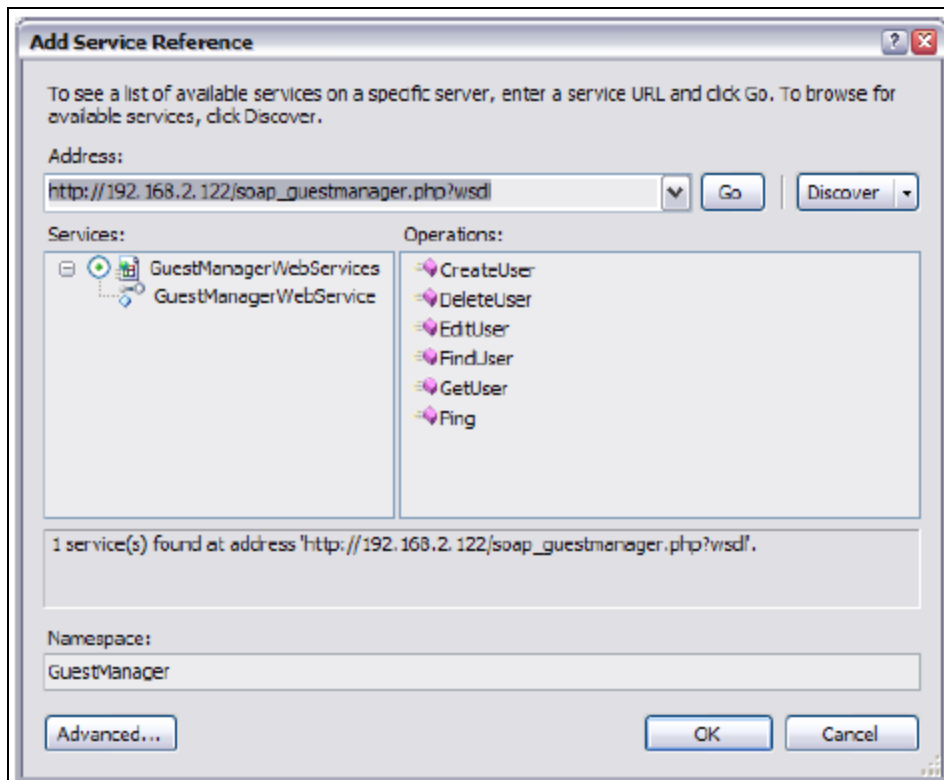
Figure 424 *Solution Explorer, Add Service Reference*



2. The **Add Service Reference** dialog box appears. Enter the **Service URL** for the GuestManager Web Services into the **Address** box, and click the **Go** button.

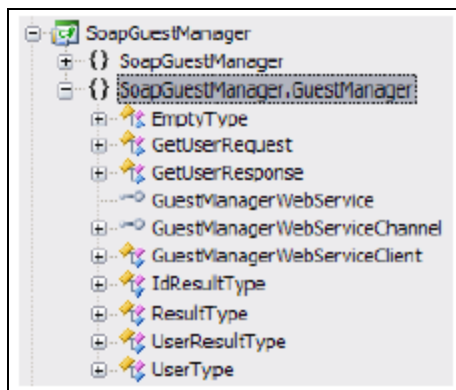
The WSDL is downloaded, and a list of the Web services and operations found is displayed.

Figure 425 *The Add Service Reference Dialog*



3. In the **Namespace** text field, type in a name. This name is used to organize the automatically generated code that interfaces with the Web service.
4. Click the **OK** button to create the Web service reference.
5. To browse the created classes, double-click the **GuestManager** service reference. The **Object Browser** is displayed with the selected namespace highlighted.

Figure 426 *The Object Browser*



Configuring HTTP Basic Authentication

Performing a simple API call, such as the “Ping” operation described in ["Operations" on page 586](#), can be used to verify that the Web service is correctly configured and ready for use.

Because the SOAP API requires HTTP Basic authentication, ensure that you have a suitable operator profile and operator login credentials, as explained in ["Using the SOAP API" on page 575](#).

Configuring the Web service reference to use authentication requires editing the app.config file to make two changes:

- The **mode** attribute of the <security> tag must be changed to "TransportCredentialOnly".
- The **clientCredentialType** attribute of the <transport> tag must be changed to "Basic".

The updated app.config file is shown below, with the appropriate changes highlighted.

Figure 427 *The Updated app.config File*

```
<?xml version="1.0" encoding="utf-8" ?>
<configuration>
  <system.serviceModel>
    <bindings>
      <basicHttpBinding>
        <binding name="GuestManagerSoapBinding" closeTimeout="00:01:00"
          openTimeout="00:01:00" receiveTimeout="00:10:00"
          sendTimeout="00:01:00"
          allowCookies="false" bypassProxyOnLocal="false"
          hostNameComparisonMode="StrongWildcard"
          maxBufferSize="65536" maxBufferPoolSize="524288"
          maxReceivedMessageSize="65536"
          messageEncoding="Text" textEncoding="utf-8"
          transferMode="Buffered"
          useDefaultWebProxy="true">
          <readerQuotas maxDepth="32" maxStringContentLength="8192"
            maxArrayLength="16384"
            maxBytesPerRead="4096" maxNameTableCharCount="16384" />
          <security mode="TransportCredentialOnly">
            <transport clientCredentialType="Basic"
              proxyCredentialType="None"
              realm="" />
            <message clientCredentialType="UserName"
              algorithmSuite="Default" />
          </security>
        </binding>
      </basicHttpBinding>
    </bindings>
    <client>
      <endpoint address="http://192.168.2.122/soap/service.php"
        binding="basicHttpBinding"
        bindingConfiguration="GuestManagerSoapBinding"
        contract="GuestManager.GuestManagerWebService"
        name="GuestManagerWebServicePort" />
    </client>
  </system.serviceModel>
</configuration>
```

Performing an API Call

This section outlines the C# code required to use the Web service.

First, add a using declaration for the namespace containing the Web services:

```
using SoapGuestManager.GuestManager;
```

The following code can now be added to invoke the Ping operation and display the result.

Figure 428 Code to Add for Invoking the Ping Operation

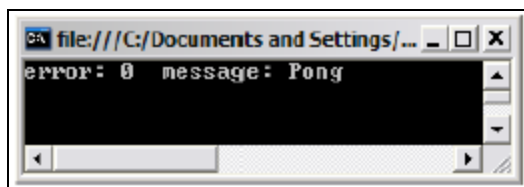
```
// Create the client
GuestManagerWebServiceClient client = new GuestManagerWebServiceClient();
client.ClientCredentials.UserName.UserName = "soapapi";
client.ClientCredentials.UserName.Password = "bubbles";

// Perform a Ping operation
EmptyType pingRequest = new EmptyType();
ResultType pingResponse = client.Ping(pingRequest);

// Display the response
System.Console.Out.WriteLine("error: {0} message: {1}",
    pingResponse.error, pingResponse.message);
```

When invoked, this performs the Ping operation and displays the following output:

Figure 429 Output Displayed after the Ping Operation



Securing Web Services Using HTTPS

Because HTTP Basic authentication is insecure, it is strongly recommended that the HTTPS transport be used for all SOAP API calls.

To use HTTPS as the transport for SOAP API requests, the following changes should be made to the application configuration file:

- The **mode** attribute of the <security> tag must be changed to "Transport".
- The **address** attribute of the <endpoint> tag must be changed to a URL including the "https:" prefix.

The updated app.config file is shown below, with the relevant changes highlighted.

Figure 430 *The Updated app.config File*

```
<?xml version="1.0" encoding="utf-8" ?>
<configuration>
  <system.serviceModel>
    <bindings>
      <basicHttpBinding>
        <binding name="GuestManagerSoapBinding" ...>
          <readerQuotas ... />
          <security mode="Transport">
            <transport clientCredentialType="Basic"
              proxyCredentialType="None"
              realm="" />
            <message clientCredentialType="UserName"
              algorithmSuite="Default" />
          </security>
        </binding>
      </basicHttpBinding>
    </bindings>
    <client>
      <endpoint address="https://192.168.2.122/soap_service.php"
        binding="basicHttpBinding"
        bindingConfiguration="GuestManagerSoapBinding"
        contract="GuestManager.GuestManagerWebService"
        name="GuestManagerWebServicePort" />
    </client>
  </system.serviceModel>
</configuration>
```

Additionally, if a self-signed certificate is being used on the remote server, you will need to provide a suitable `ServerCertificateValidationCallback` implementation to validate the peer's certificate.

The following code is a minimal implementation that accepts all server certificates without verification:

```
// Trust self-signed certificates
System.Net.ServicePointManager.ServerCertificateValidationCallback =
  ((sender, certificate, chain, sslPolicyErrors) => true);
```



In a production environment, it is strongly recommended that you deploy an SSL certificate that is signed by a trusted root CA known to all parties, and use the built-in server certificate validation procedures. This will ensure the security of the transaction cannot be compromised by a man-in-the-middle attack.

API Documentation

This section describes the following:

- "XML Namespaces" on page 582
- "SOAP Addressing" on page 583
- "Types" on page 583
- "Operations" on page 586

XML Namespaces

The XML namespace for the GuestManager Web Services is:

<http://www.amigopod.com/go/GuestManager.wSDL>

The table below indicates additional XML namespaces that are referenced:

Table 259: XML Namespaces

Component	XML Namespace
SOAP Envelope	http://schemas.xmlsoap.org/wsdl/soap/
SOAP Encoding	http://schemas.xmlsoap.org/soap/encoding/
WSDL	http://schemas.xmlsoap.org/wsdl/
XML Schema	http://www.w3.org/2001/XMLSchema

SOAP Addressing

Web Service Endpoint

The endpoint of the SOAP service is located at the relative URL:

soap_guestmanager.php.

This path is relative to the full Guest URL, which can be constructed using http: or https: and the fully-qualified domain name of the ClearPass Guest appliance.

- Example: http://192.168.2.122/guest/soap_guestmanager.php
- Example: https://192.168.2.122/guest/soap_guestmanager.php (secure)

Web Service Definition

The WSDL for the web service may be accessed by appending ?wsdl to the service URL.

- Example: http://192.168.2.122/guest/soap_guestmanager.php?wsdl

Types

This section describes the types defined in the WSDL schema.

EmptyType

This type must be empty, that is, containing zero child elements.

- Example:

```
<ping/>
```

ErrorFlagType

The error flag indicates if the operation completed successfully.

Only the values zero (0) and one (1) are supported.

- A successful operation is indicated with:

```
<error>0</error>
```

- A failed operation is indicated with:

```
<error>1</error>
```

IdResultType

Standard result type), with an optional <id> element.

- Example:

```
<result>
  <error>0</error>
  <id>551</id>
</result>
```

- Example:

```
<result>
  <error>1</error>
  <message>This username is already in use</message>
</result>
```

IdType

Specifies a user ID. The user ID is a positive integer value, starting at 1.

- Example:

```
<id>551</id>
```

ResultType

Operations return a standard result type. The `<error>` flag indicates if the operation completed successfully. If the operation failed, the `<message>` contains a description of the error.

- Example of a successful operation:

```
<result>
  <error>0</error>
  <message/>
</result>
```

- Example of a successful operation with message:

```
<result>
  <error>0</error>
  <message>Pong</message>
</result>
```

- Example of an unsuccessful operation:

```
<result>
  <error>1</error>
  <message>This username is already in use</message>
</result>
```

UserResultType

Standard result type, with an optional `<user>` element.

- Example of a successful operation:

```

<result>
  <error>0</error>
  <message></message>
  <user>
    <creator_name>soapapi</creator_name>
    <do_expire>4</do_expire>
    <do_schedule>>false</do_schedule>
    <enabled>>true</enabled>
    <expire_time>2010-03-18T16:14:25+10:00</expire_time>
    <id>3</id>
    <role_id>2</role_id>
    <role_name>Guest</role_name>
    <schedule_time>1970-01-01T10:00:00+10:00</schedule_time>
    <simultaneous_use>1</simultaneous_use>
    <username>demo@example.com</username>
  </user>
</result>

```

- Example of an unsuccessful operation:

```

<result>
  <error>1</error>
  <message>Cannot find account with ID 3</message>
</result>

```

UserType

The User type defines a visitor account, which consists of a number of fields.

The fields available may be customized in Guest Manager. Go to **Guest Manager > Configuration > Fields** to create new fields or modify existing fields.



Adding or removing fields will update the UserType schema in the WSDL for GuestManager Web Services. Ensure that you update any clients using this WSDL if the fields are modified.

Each field of the visitor account corresponds to an XML element with the same name as the field.

All fields within the UserType schema are marked as optional; however, certain operations may require that particular fields are provided.

- Example of a user definition:

```

<user>
  <creator_name>soapapi</creator_name>
  <do_expire>4</do_expire>
  <do_schedule>>false</do_schedule>
  <enabled>>true</enabled>
  <expire_time>2010-03-18T16:14:25+10:00</expire_time>
  <id>3</id>
  <role_id>2</role_id>
  <role_name>Guest</role_name>
  <schedule_time>1970-01-01T10:00:00+10:00</schedule_time>
  <simultaneous_use>1</simultaneous_use>
  <username>demo@example.com</username>
</user>

```

Operations

CreateUser

Creates a new user account.

Headers	
Name	Value
SOAPAction	amigopod.guest.create
Input Parameters (Request)	
Name	Type
user	UserType ▪ See "Notes" below
Output Parameters (Response)	
Name	Type
result	IdResultType
Access Control	
Privilege	Value
SOAP API	Full Access
Create New Guest Account	Full Access
Notes	

- The standard business logic for visitor account creation applies to visitor accounts created with the SOAP API. For details, refer to the section "Business logic for account creation" in the ClearPass Guest User Guide, or search for this term in the online help.
- The **creator_accept_terms** field must be set to the Boolean value "true" in order to create an account.
- A value for the **role_id** field must be specified to create a visitor account. The SOAP API user must also be permitted to create visitor accounts with this role.

Examples

Example code implementing visitor account creation:

```

static string TestCreate(GuestManagerWebServiceClient client)
{
    System.Console.Out.WriteLine("Sending CreateUser request...");

    // Perform a CreateUser operation
    UserType createRequest = new UserType();
    createRequest.username = "demo@example.com";
    createRequest.creator_accept_terms = true;
    createRequest.creator_accept_termsSpecified = true;
    createRequest.expire_after = "12";
    createRequest.creator_name = client.ClientCredentials.UserName.UserName;
    createRequest.role_id = "2"; // Guest

    IdResultType createResponse = client.CreateUser(createRequest);

    // Display the response
    System.Console.Out.WriteLine("CreateUser response: error: {0} message: {1}",
        createResponse.error, createResponse.message);
    return createResponse.id;
}

```

Example request for CreateUser:

```

<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/">
  <s:Body xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema">
    <CreateUser xmlns="http://www.amigopod.com/go/GuestManager.wsdl">
      <user xmlns="">
        <creator_accept_terms>true</creator_accept_terms>
        <creator_name>soapapi</creator_name>
        <expire_after>12</expire_after>
        <role_id>2</role_id>
        <username>demo@example.com</username>
      </user>
    </CreateUser>
  </s:Body>
</s:Envelope>

```

Successful response:

```

<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:ns1="http://www.amigopod.com/go/GuestManager.wsdl">
  <SOAP-ENV:Body>
    <ns1:CreateUserResponse>
      <result>
        <error>0</error>
        <message>Created guest account for demo@example.com</message>
        <id>1</id>
      </result>
    </ns1:CreateUserResponse>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>

```

Failure response:

```

<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:ns1="http://www.amigopod.com/go/GuestManager.wsdl">
  <SOAP-ENV:Body>
    <ns1:CreateUserResponse>
      <result>
        <error>1</error>
        <message>This username is already in use</message>
      </result>
    </ns1:CreateUserResponse>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>

```

DeleteUser

Deletes a user account by ID or matching fields

Headers	
Name	Value
SOAPAction	amigopod.guest.delete
Input Parameters (Request)	
Name	Type
user	UserType ▪ See "Notes" below
Output Parameters (Response)	
Name	Type
result	ResultType
Access Control	
Privilege	Value
SOAP API	Full Access
Remove Accounts	Full Access
Notes	

- This operation deletes a single visitor account that matches all of the field values specified in the user parameter.
- Exactly one account must match; if more than one match is found, or if no match is found, an error will be returned and no visitor accounts will be deleted.

Examples

Example code implementing visitor account deletion:


```

static void TestDelete(GuestManagerWebServiceClient client, UserType user)
{
    System.Console.Out.WriteLine("Sending DeleteUser request...");

    // Perform a DeleteUser operation
    ResultType deleteResponse = client.DeleteUser(user);

    // Display the response
    System.Console.Out.WriteLine("DeleteUser response: error: {0} message: {1}",
        deleteResponse.error, deleteResponse.message);
}

```

Example request for DeleteUser:

```

<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/">
  <s:Body xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema">
    <DeleteUser xmlns="http://www.amigopod.com/go/GuestManager.wsdl">
      <user xmlns="">
        <id>6</id>
      </user>
    </DeleteUser>
  </s:Body>
</s:Envelope>

```

Successful response:

```

<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:ns1="http://www.amigopod.com/go/GuestManager.wsdl">
  <SOAP-ENV:Body>
    <ns1:DeleteUserResponse>
      <result>
        <error>0</error>
        <message>Deleted guest account demo@example.com. User has no active
connections to disconnect.</message>
      </result>
    </ns1:DeleteUserResponse>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>

```

Failure response:

```

<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:ns1="http://www.amigopod.com/go/GuestManager.wsdl">
  <SOAP-ENV:Body>
    <ns1:DeleteUserResponse>
      <result>
        <error>1</error>
        <message>Cannot find account with ID 3</message>
      </result>
    </ns1:DeleteUserResponse>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>

```

EditUser

Modifies properties of a user account by ID.

Headers	
Name	Value
SOAPAction	amigopod.guest.edit
Input Parameters (Request)	
Name	Type
user	UserType ▪ See "Notes" below
Output Parameters (Response)	
Name	Type
result	ResultType
Access Control	
Privilege	Value
SOAP API	Full Access
Remove Accounts	Full Access
Notes	

- This operation modifies the properties of a visitor account to match the field values specified in the `user` parameter.
- The `id` field must be specified to indicate the ID of the visitor account to modify. This field is assigned by the system when the visitor account is created and cannot be changed.

Examples

Example code implementing visitor account modification:

```
static void TestEdit(GuestManagerWebServiceClient client, UserType user)
{
    System.Console.Out.WriteLine("Sending EditUser request...");

    // Perform an EditUser operation
    ResultType editResponse = client.EditUser(user);

    // Display the response
    System.Console.Out.WriteLine("EditUser response: error: {0} message: {1}",
        editResponse.error, editResponse.message);
}
```

Example request for EditUser:

```

<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/">
  <s:Body xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema">
    <EditUser xmlns="http://www.amigopod.com/go/GuestManager.wsdl">
      <user xmlns="">
        <creator_name>soapapi</creator_name>
        <do_expire>4</do_expire>
        <do_schedule>>false</do_schedule>
        <enabled>>true</enabled>
        <expire_time>2010-03-18T18:29:50+10:00</expire_time>
        <id>5</id>
        <role_id>2</role_id>
        <role_name>Guest</role_name>
        <schedule_time>1970-01-01T10:00:00+10:00</schedule_time>
        <simultaneous_use>1</simultaneous_use>
        <username>demo@example.com</username>
      </user>
    </EditUser>
  </s:Body>
</s:Envelope>

```

Successful response:

```

<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:ns1="http://www.amigopod.com/go/GuestManager.wsdl">
  <SOAP-ENV:Body>
    <ns1:EditUserResponse>
      <result>
        <error>0</error>
        <message>
          Updated user account demo@example.com in the database<br />
        </message>
      </result>
    </ns1:EditUserResponse>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>

```

Failure response:

```

<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:ns1="http://www.amigopod.com/go/GuestManager.wsdl">
  <SOAP-ENV:Body>
    <ns1:EditUserResponse>
      <result>
        <error>1</error>
        <message>Invalid UserType: id must be specified</message>
      </result>
    </ns1:EditUserResponse>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>

```

FindUser

Returns properties of a user account by matching fields.

Headers	
Name	Value
SOAPAction	amigopod.guest.find
Input Parameters (Request)	
Name	Type
user	UserType
Output Parameters (Response)	
Name	Type
result	UserResultType
Access Control	
Privilege	Value
SOAP API	Read Only Access
List Guest Accounts	Read Only Access

Notes

- This operation locates a single visitor account that matches all of the field values specified in the `user` parameter.
- Exactly one account must match; if more than one match is found, or if no match is found, an error will be returned.
- If a visitor account was found, its properties will be returned in the `<user>` element of the result.

Examples

Example code implementing search for a visitor account based on a username.

```

static UserType TestFind(GuestManagerWebServiceClient client, string username)
{
    System.Console.Out.WriteLine("Sending FindUser request for {0}...",
        username);

    // Perform a FindUser operation
    UserType findRequest = new UserType();
    findRequest.username = username;
    UserResultType findResponse = client.FindUser(findRequest);

    // Display the response
    System.Console.Out.WriteLine("FindUser response: error: {0} message: {1}",
        findResponse.error, findResponse.message);
    if (findResponse.user != null)
    {
        System.Console.Out.WriteLine(" id: {0}", findResponse.user.id);
    }
    return findResponse.user;
}

```

Example request for FindUser:

```

<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/">
  <s:Body xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema">
    <FindUser xmlns="http://www.amigopod.com/go/GuestManager.wsdl">
      <user xmlns="">
        <username>demo@example.com</username>
      </user>
    </FindUser>
  </s:Body>
</s:Envelope>

```

Successful response:

```

<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:ns1="http://www.amigopod.com/go/GuestManager.wsdl">
  <SOAP-ENV:Body>
    <ns1:FindUserResponse>
      <result>
        <error>0</error>
        <message></message>
        <user>
          <creator_name>soapapi</creator_name>
          <do_expire>4</do_expire>
          <do_schedule>>false</do_schedule>
          <enabled>>true</enabled>
          <expire_time>2010-03-18T16:30:59+10:00</expire_time>
          <id>4</id>
          <role_id>2</role_id>
          <role_name>Guest</role_name>
          <schedule_time>1970-01-01T10:00:00+10:00</schedule_time>
          <simultaneous_use>1</simultaneous_use>
          <username>demo@example.com</username>
        </user>
      </result>
    </ns1:FindUserResponse>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>

```

Failure response:

```

<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:ns1="http://www.amigopod.com/go/GuestManager.wsdl">
  <SOAP-ENV:Body>
    <ns1:FindUserResponse>
      <result>
        <error>1</error>
        <message>No user account found</message>
        <user/>
      </result>
    </ns1:FindUserResponse>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>

```

GetUser

Returns properties of a user account by ID.

Headers	
Name	Value
SOAPAction	amigopod.guest.get
Input Parameters (Request)	
Name	Type
id	IdType
Output Parameters (Response)	
Name	Type
result	UserResultType
Access Control	
Privilege	Value
SOAP API	Read Only Access
List Guest Accounts	Read Only Access

Notes

- Returns a <user> element corresponding to the visitor account with the specified ID.
- If the specified ID is invalid, no <user> element is returned and the <error> flag is set to 1.

Examples

Example code implementing a guest lookup operation:

```

static UserType TestGet(GuestManagerWebServiceClient client, string id)
{
    System.Console.Out.WriteLine("Sending GetUser request for ID {0}...", id);

    // Perform a GetUser operation
    UserResultType getResponse = client.GetUser(id);

    // Display the response
    System.Console.Out.WriteLine("GetUser response: error: {0} message: {1}",
        getResponse.error, getResponse.message);
    if (getResponse.user != null)
    {
        System.Console.Out.WriteLine(" username: {0}", getResponse.user.username);
    }
    return getResponse.user;
}

```

Example request for GetUser:

```

<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/">
  <s:Body xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema">
    <GetUser xmlns="http://www.amigopod.com/go/GuestManager.wsdl">
      <id xmlns="">3</id>
    </GetUser>
  </s:Body>
</s:Envelope>

```

Successful response:

```

<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:ns1="http://www.amigopod.com/go/GuestManager.wsdl">
  <SOAP-ENV:Body>
    <ns1:GetUserResponse>
      <result>
        <error>0</error>
        <message></message>
        <user>
          <creator_name>soapapi</creator_name>
          <do_expire>4</do_expire>
          <do_schedule>false</do_schedule>
          <enabled>true</enabled>
          <expire_time>2010-03-18T16:14:25+10:00</expire_time>
          <id>3</id>
          <role_id>2</role_id>
          <role_name>Guest</role_name>
          <schedule_time>1970-01-01T10:00:00+10:00</schedule_time>
          <simultaneous use>1</simultaneous use>
          <username>demo@example.com</username>
        </user>
      </result>
    </ns1:GetUserResponse>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>

```

Failure response -- for example, user ID not found:

```

<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:ns1="http://www.amigopod.com/go/GuestManager.wsdl"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <SOAP-ENV:Body>
    <ns1:GetUserResponse>
      <result xsi:type="ns1:ResultType">
        <error>1</error>
        <message>Cannot find account with ID 3</message>
      </result>
    </ns1:GetUserResponse>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>

```

Ping

Checks that the SOAP server is alive.

Headers	
Name	Value
SOAPAction	amigopod.guest.ping
Input Parameters (Request)	
Name	Type
ping	EmptyType
Output Parameters (Response)	
Name	Type
result	ResultType
Access Control	
Privilege	Value
SOAP API	Read Only Access
Notes	

- Returns a standard result type with the **message** set to "pong".

Examples

Example code implementing a Ping test operation.

```

static void TestPing(GuestManagerWebServiceClient client)
{
    System.Console.Out.WriteLine("Sending Ping request...");

    // Perform a Ping operation
    EmptyType pingRequest = new EmptyType();
    ResultType pingResponse = client.Ping(pingRequest);

    // Display the response
    System.Console.Out.WriteLine("Ping response: error: {0} message: {1}",
        pingResponse.error, pingResponse.message);
}

```

Example request for Ping:

```

<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/">
  <s:Body xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema">
    <Ping xmlns="http://www.amigopod.com/go/GuestManager.wsdl">
      <ping xmlns=""/>
    </Ping>
  </s:Body>
</s:Envelope>

```

Successful response:


```
<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope xmlns:SOAP-
ENV="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:ns1="http://www.amigopod.com/go/GuestManager.wsdl">
  <SOAP-ENV:Body>
    <ns1:PingResponse>
      <result>
        <error>0</error>
        <message>Pong</message>
      </result>
    </ns1:PingResponse>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

The XML-RPC Interface and API

This section describes the XML-RPC interface available to third-party applications that will integrate with the ClearPass Guest Visitor Management Appliance.

Audience:

- Developers of integrated applications. Some familiarity with HTTP based web services and XMLRPC is assumed.
- System administrators of the ClearPass Guest application.

System Requirements:

- ClearPass Guest 6.1.0 (minimum)
- XML-RPC client

For more details about XML-RPC, or to read the XML-RPC specification, visit <http://xmlrpc.scripting.com/>.

This section includes the following:

- "About the XML-RPC API" on page 597
- "Accessing the API" on page 600
- "Invoking the API" on page 603
- "Method Summary" on page 604
- "API Documentation" on page 604

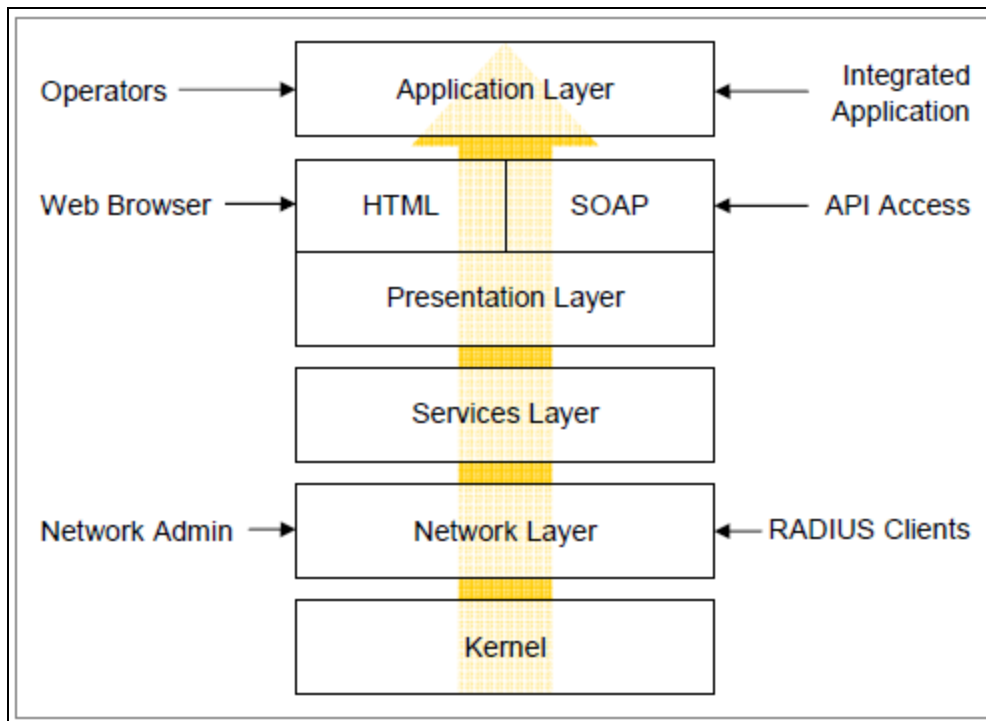
About the XML-RPC API

The ClearPass Guest XML-RPC API provides direct access to the underlying functionality of the ClearPass Guest Visitor Management Appliance. Developers wishing to provide integrated applications can use this API to programmatically perform actions that would otherwise require manual operation of the user interface.

Architecture Overview

The ClearPass Guest VMA software is built using multiple layers of software.

Figure 431 Layers of VMA Software in ClearPass Guest



At the lowest level, the kernel provides basic functions common to the entire system. This includes the Web interface framework, appliance operating system, and runtime support services.

The network layer provides critical networking support, including the RADIUS server and the ability for network administrators to manage and control the networking aspects of the VMA.

The services layer provides one or more implementations of application services that are used by the layers above. Examples of these services include managing a user database used for AAA, handling the authentication of operators, and providing translated text resources.

The presentation layer supplies the tools and framework necessary for the VMA software to interact with the outside world. The basic presentation layer services include authentication checks, session establishment, input checking, validation and conversion, and command execution. Both XML-RPC and HTML presentation methods are supplied, which adapt the underlying basic presentation to appropriate conventions suitable for a machine-to-machine or human-to-machine interaction.

The application layer provides the page templates, business logic, and the concrete features making up visitor management applications, such as Guest Manager or Hotspot Manager. These applications are built using the services provided by the lower layers.

API Symmetry

Because ClearPass Guest VMA applications are built using the framework supplied by the presentation layer, there is a direct symmetry between application features provided to operators using a Web browser (HTML presentation), and application features provided to external applications using the XML-RPC presentation.

In particular, the following items are shared between HTML and XML-RPC presentations:

- Access control
- Parameter names
- Parameter validation rules

- Customized fields and their rules

Access Control

Page privileges are applied to XML-RPC authenticated sessions in the same way as the HTML user interface. However, XML-RPC access also requires the XML-RPC API privilege to be granted.

Parameter Names

The parameter names passed to the XML-RPC interface are the same as the field names in the HTML user interface.

Parameter Validation

Each field of the forms in the HTML user interface is subject to validation according to the rules defined for that field. The same rules also apply to XML-RPC parameters.

If a required field is missing, or an invalid value for a field is supplied, an error is generated by the presentation layer and returned to the XML-RPC client.

Field Customization

Some forms in the HTML user interface are customizable. New fields may be defined (for example, stored with a guest account) and used as part of the form in the presentation layer. Policy-based processing of fields includes form validation, data conversion and input formatting, and user interface metadata (for example, the list of valid options for a multiple-choice “dropdown” control).

These custom fields are automatically inherited as XML-RPC parameters, and the same policy-based processing is applied to them.

Parameter Types

The XML-RPC specification supports a wide range of data types. The following data types are supported by the XML-RPC presentation layer:

Table 260: *Data Types Supported by XML-RPC*

Data Type	Description
Array	Associative array using numeric keys with a 0-based index
Boolean	True or false
Flag	Scalar value of 0 or 1, implicitly Boolean
Integer	Integer, 32-bit range
Number	Numeric value, floating point OK
Scalar	Non-array value
String	String, UTF-8 encoded
Struct	Associative array using string keys May be nested (shown in the syntax as first.second, etc.)

Data Representation

Unless otherwise specified, all strings should be considered to be UTF-8 encoded Unicode.

Dates and times are represented in an ISO-8601 compatible format:

```
YYYY-MM-DD hh:mm:ss
```

XML-RPC Faults

An XML-RPC Fault is a specific kind of return value indicating that an error has occurred in the presentation layer. The return value is a struct containing three named values:

Table 261: XML-RPC Faults

Name	Type	Description
error	Flag	Set to 1 for an XML-RPC Fault
faultCode	Integer	Status code indicating the cause of the fault
faultString	String	Description of the fault

This type of return might appear as:

```
'error' => 1,  
'faultCode' => 401,  
'faultString' => 'Invalid username or password',
```

These are the predefined XML-RPC Fault codes:

Table 262: XML-RPC Faults

Code	Description
401	Authentication problem -- invalid username or password
404	File implementation of XML-RPC method not found
501	XML-RPC implementation not found
502	XML-RPC method registration failed
503	XML-RPC server creation failed
504	Access denied
505	No XML-RPC implementation for this page

Accessing the API

Accessing the API requires an operator account with a profile that has the XML-RPC API privilege, plus any privileges required for the API calls. You will first create the operator profile, then create the role, a local user, and a translation rule to map the role name to the profile. Some steps are performed in ClearPass Guest and some steps are performed in ClearPass Policy Manager.

Creating the Profile

To create a sample XML-RPC API profile:

1. In **ClearPass Guest**, go to **Administration > Operator Logins > Profiles** and click the **Create a new operator profile** link. The **Operator Profile Editor** form opens.
2. Enter a name and description that clearly identify the profile.

3. In the **Access** area, select the **Allow operator logins** check box.
4. In the **Administrator** drop-down list, select **Custom**. The row expands to include additional options.
5. For the **XMLRPC API** option, select the **Allow Access** radio button.
6. In the **Guest Manager** drop-down list, select **Full Access**.

Figure 432 The Operator Profile Editor Form

Operator Profile Editor

* Name:
Enter a name for this operator profile.

Description:
Comments or descriptive text about the operator profile.

Access
These options control what operators with this profile are permitted to do.

Enabled: Allow operator logins
If unchecked, operators with this profile will not be able to log in.

Privileges:

Operator Privileges

Administrator Custom...
Select operator permissions for system administration and management tasks.

- Application Log No Access Read Only
Operators with the Application Log privilege can view logged messages and events.
- Export Configuration No Access Read Only Full
Operators with the Export Configuration privilege can make configuration backups.
- Object Permissions No Access Read Only Full
Operators with the Object Permissions privilege can manage the permissions of objects.
- Plugin Configuration No Access Read Only Full
Operators with the Plugin Configuration privilege can edit the plugin configuration.
- Plugin Manager No Access Read Only Full
Operators with the Plugin Manager privilege can manage web application components.
- XMLRPC API** No Access Allow Access
Operators with the XMLRPC API privilege can access system functions through the XMLRPC API.

AirGroup Services No Access
Select operator permissions for access to AirGroup services.

Guest Manager Full Access
Select operator permissions for managing guest users for a network.

Hotspot Manager No Access
Select operator permissions for managing self-provisioned guest access.

IP Phone Services No Access
Select operator permissions for IP phone administration and management tasks.

Onboard No Access
Select operator permissions for managing Onboard device provisioning.

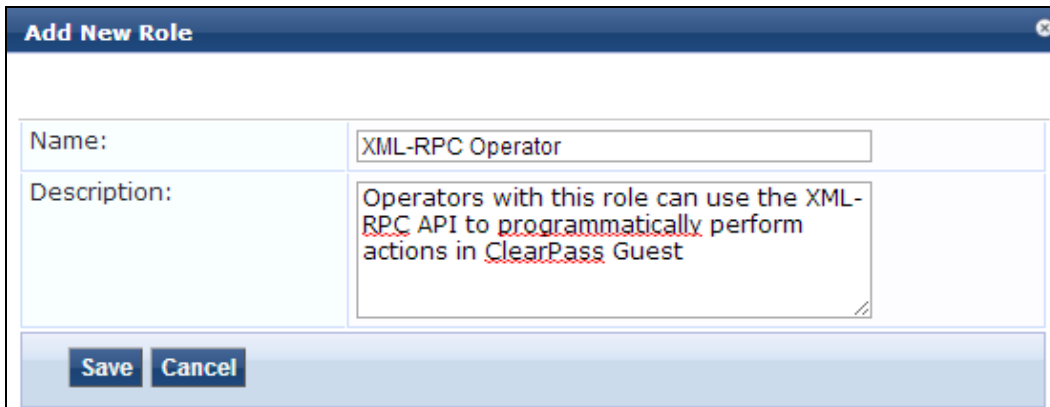
7. Click **Save Changes**. The profile is added to the **Operator Profiles** list.

Creating the Role

After you create the profile, the next step is to create the role:

1. In **ClearPass Policy Manager**, go to **Configuration > Identity > Roles** and click the **Add User** link. The **Add New Role** form opens.
2. Enter a name and description that clearly identify the role.

Figure 433 *The Add New Role Form*



Add New Role	
Name:	XML-RPC Operator
Description:	Operators with this role can use the XML-RPC API to programmatically perform actions in ClearPass Guest
Save Cancel	

3. Click **Save**. The role is added to the **Roles** list.

Creating the Local User

After you create the role, you create the local user:

1. In **Clear Pass Policy Manager**, go to **Configuration > Identity > Local Users** and click **Add User**. The **Add Local User** form opens.
2. In the **Role** drop-down list, select the **XML-RPC Operator** role you created.
3. Complete the rest of the fields appropriately, then click **Add**. The new XML-RPC operator is added to the **Local Users** list.

Creating the Translation Rule

After you have created the profile, role, and local user (operator), create a translation rule to map the role name to the operator profile.

1. In **ClearPass Guest**, go to **Administration > Operator Logins > Translation Rules** and click the **Create new translation rule** link. The **Edit Translation Rule** form opens.

Figure 434 The Edit Translation Rule Form

Edit Translation Rule	
* Name:	<input type="text" value="MatchXML-RPC"/> <small>Enter a name for this translation rule.</small>
Enabled:	<input checked="" type="checkbox"/> Use this rule when processing reply attributes
Attribute Name:	<input type="text" value="admin_privileges"/> <small>Enter the name of the attribute (e.g. memberof). Use * for all attributes.</small>
Matching Rule:	<input type="text" value="equals"/> <small>Select the matching rule to apply to the value of the attribute.</small>
Value:	<input type="text" value="XML-RPC Operator"/> <small>Enter the value to match the attribute against.</small>
On Match:	<input type="text" value="Assign fixed operator profile"/> <small>Select what happens when this translation rule matches an attribute.</small>
Operator Profile:	<input type="text" value="XML-RPC"/> <small>Select the operator profile to assign.</small>
Fallthrough:	<input checked="" type="checkbox"/> Continue translation if rule matches <small>Check this box if you want to apply multiple translation rules.</small>

2. In the **Name** field, enter a descriptive name for the translation rule. In the example shown above, the translation rule is to check that the operator is an XML-RPC user, hence the name MatchXML-RPC.
3. Select the **Enabled** check box to enable this rule after you create it. If you do not select this check box, the rule you create will appear in the rules list, but will not be active until you enable it.
4. In the **Matching Rule** drop-down list, select **equals**.
5. In the **Value** field, enter the name of the XML-RPC Operator role you defined.
6. In the **On Match** drop-down list, select **Assign fixed operator profile**. The form expands to include the **Operator Profile** row.
7. In the **Operator Profile** drop-down list, select the XML-RPC profile.
8. If you want to use multiple translation rules, select the **Fallthrough** check box.
9. Click **Save Changes**.

The user you created can now use the XML-RPC API functions.

Invoking the API

An XMLRPC method call consists of:

- An XML document specifying the method name and parameters,
- sent as a HTTP POST with `Content-Type: text/xml`,
- using HTTP Basic user authorization,
- at `https://amigopod/xmlrpc.php`

SSL Security

Different levels of certificate validation checks may be necessary, depending on the SSL certificate that has been installed. This corresponds to the user interface provided by Web browsers for certificate trust and verification.

The examples presented in this document assume a self-signed certificate has been installed, and reduce the level of SSL verification accordingly. In a secure environment, make use of the peer verification that SSL provides by either installing an SSL certificate signed by a well-known Certificate Authority, or issue your own certificates from a network's Certificate Authority.

Method Summary

These methods are currently available:

Table 263: XML-RPC Method Summary

Method Name	Synopsis
amigopod.guest.change.expiration	Change the expiration time of a guest account
amigopod.guest.create	Create a new guest account
amigopod.guest.delete	Disable or remove a guest account
amigopod.guest.edit	Change one of more properties of a guest account
amigopod.guest.enable	Enable a guest account
amigopod.guest.get	List one or more guest accounts
amigopod.guest.list	List guest accounts
amigopod.guest.reset.password	Reset a guest account's password
amigopod.mac.create	Create a new MAC device account
amigopod.mac.edit	Change one or more properties of a device account
amigopod.mac.list	List MAC device accounts

For more details on these methods, refer to ["API Documentation" on page 604](#).

API Documentation

This section describes the following methods:

- ["Method amigopod.guest.change.expiration" on page 605](#)
- ["Method amigopod.guest.create" on page 606](#)
- ["Method amigopod.guest.delete" on page 607](#)
- ["Method amigopod.guest.edit" on page 609](#)
- ["Method amigopod.guest.enable" on page 611](#)
- ["Method amigopod.guest.get" on page 612](#)
- ["Method amigopod.guest.list" on page 614](#)
- ["Method amigopod.guest.reset.password" on page 615](#)

- ["Method amigopod.mac.create" on page 616](#)
- ["Method amigopod.mac.edit" on page 618](#)
- ["Method amigopod.mac.list" on page 621](#)

Method amigopod.guest.change.expiration

Change the expiration time of a guest account.

Parameters

Table 264: *Parameters, amigopod.guest.change.expiration*

Name	Type	Description
uid	Scalar	ID of the guest account to update
guestaccountexpiry	Scalar	Amount of time in hours before the guest account will expire

Return Values

Table 265: *Return Values, amigopod.guest.change.expiration*

Name	Type	Description
error	Flag	0 if successful, 1 if an error occurred
message	String	Status message describing the operation
item	Struct	Updated user information record
*_error	String	Field-specific error message
*_error_flag	Flag	Field-specific error flag, set to 1 if present

Access Control

Requires the **change_expiration** privilege (**Guest Manager > Change Expiration** in the Operator Profile Editor).

Example Usage

Sample parameters for the call:

```
'uid' => 162,
'guestaccountexpiry' => 24,
```

Result returned by a successful operation:

```
'error' => 0,
'message' => 'Changed expiration time of guest account
Account will expire at 2014-11-28 23:27:00',
'item' => array (
  'id' => 162,
  'do_expire' => 4,
  'expire_time' => 1196256420,
  'username' => '',
)
```

Result returned by a failed operation:

```
'uid' => 162,
'username' => '',
'expiration_time' => '',
```

```
'user_enabled' => '',
'guestaccountexpiry_error' => 'Please choose from one of these options.',
'guestaccountexpiry_error_flag' => 1,
'error' => 1,
```

Method amigopod.guest.create

Create a new guest account.

Parameters

Table 266: *Parameters, amigopod.guest.create*

Name	Type	Description
sponsor_name	String	Name of the person sponsoring the guest account.
visitor_name	String	Name of the visitor.
visitor_company	String	Company name of the visitor.
email	String	The visitor's email address. This will become their username to log in to the network.
expire_after	Numeric	Amount of time before the account will expire. Specified in hours.
expire_time	String	Optional date and time at which the guest account will expire.
role_id	Integer	RADIUS role ID to assign to the guest account.
creator_accept_terms	Flag	Set to 1 to indicate acceptance of the service's terms of use.
*	*	Other fields as specified by create_user form customization.

Return Values

Table 267: *Return Values, amigopod.guest.create*

Name	Type	Description
error	Flag	Set to 1 if the guest account was not created
id	Integer	Set to the ID of the guest account if the account was created
password	String	Set to a randomly-generated value (default behavior only)
*_error	String	Field-specific error message
*_error_flag	Flag	Field-specific error flag, set to 1 if present

Access Control

Requires the **create_user** privilege (**Guest > Create Guest Account** in the Operator Profile Editor).

Example Usage

Sample parameters for the call:

```
'sponsor_name' => 'Sponsor Name',
'visitor_name' => 'Visitor Name',
'visitor_company' => 'Visitor Company',
'email' => 'demo@example.com',
'expire_after' => 4,
'expire_time' => '',
'role_id' => 2,
'visitor_phone' => '0',
'creator_accept_terms' => 1,
```

Result returned by a successful operation:

```
'username' => 'demo@example.com',
'password' => '73067792',
'role_id' => 2,
'role_name' => 'Guest',
'simultaneous_use' => '1',
'do_schedule' => 0,
'enabled' => true,
'expire_time' => 1196769257,
'do_expire' => 4,
'expire_postlogin' => 0,
'sponsor_name' => 'Sponsor Name',
'visitor_name' => 'Visitor Name',
'visitor_company' => 'Visitor Company',
'email' => 'demo@example.com',
'creator_accept_terms' => true,
'id' => 1,
```

Result returned by a failed operation:

```
'password' => 78342029',
'expire_time' => '',
'submit' => '',
'sponsor_name_error' => 'You cannot leave this field blank.',
'sponsor_name_error_flag' => 1,
'visitor_name_error' => 'You cannot leave this field blank.',
'visitor_name_error_flag' => 1,
'visitor_company_error' => 'You cannot leave this field blank.',
'visitor_company_error_flag' => 1,
'email_error' => 'Please enter a valid email address.',
'email_error_flag' => 1,
'expire_after_error' => 'Please choose from one of the available options.',
'expire_after_error_flag' => 1,
'expire_time_error' => 'Please enter a valid date and time.',
'expire_time_error_flag' => 1,
'role_id_error' => 'Parameter must be provided.',
'role_id_error_flag' => 1,
'creator_accept_terms_error' => 'You must accept the terms of use to continue.',
'creator_accept_terms_error_flag' => 1,
'error' => 1,
```

Method `amigopod.guest.delete`

Disable or remove a guest account.

Parameters

Table 268: *Parameters, amigopod.guest.delete*

Name	Type	Description
uid	Integer	ID of the guest account to delete
delete_account	Flag	Set to 0 to disable the guest account, 1 to delete the guest account

Return Values



This function might return a Boolean false value if some input parameters are invalid.

Table 269: *Return Values, amigopod.guest.delete*

Name	Type	Description
error	Flag	Set to 1 if the guest account was not deleted
message	String	Message describing the success or failure of the operation
item	Struct	User structure containing updated field values
uid	Integer	ID of the guest account
*_error	String	Field-specific error message
*_error_flag	Flag	Field-specific error flag, set to 1 if present

Access Control

Requires the **remove_account** privilege (**Guest Manager > Remove Accounts** in the Operator Profile Editor).

Example Usage

Sample parameters for the call:

```
'uid' => '162',
'delete_account' => '0',
```

Result returned by a successful operation:

```
'error' => 0,
'message' => 'Disabled guest account ',
'item' =>
array (
  'id' => 162,
  'enabled' => 0,
  'username' => '',
),
```

Result returned by a failed operation:

```
'uid' => 162,
'username' => '',
'expiration_time' => '',
'user_enabled' => '',
'delete_account_error' => 'Please choose from one of these options.',
```

```
'delete_account_error_flag' => 1,
'error' => 1,
```

Method `amigopod.guest.edit`

Change one of more properties of a guest account.

Parameters

Table 270: *Parameters, `amigopod.guest.edit`*

Name	Type	Description
uid	Integer	ID of the guest account to edit
username	String	Name of the guest account
password	String	May be: random_password to indicate the guest account's password should be set to a random password password_value to indicate the guest account's password should be set to the value in the <code>password_value</code> field The empty string to leave the password unmodified
password_value	String	Optional password to set the guest account's password (if the password field is password_value)
role_id	Integer	RADIUS role ID to assign to the guest account
enabled	Flag	Boolean value indicating whether the guest account is enabled
simultaneous_use	Integer	Number of simultaneous sessions allowed by the guest account
do_schedule	Flag	Flag indicating if the guest account should be enabled at <code>schedule_time</code>
schedule_time	String	Date and time at which the guest account will be enabled
do_expire	Integer	Action to take when the <code>expire_time</code> is reached
expire_time	String	Time at which the guest account will expire
expire_postlogin	Integer	Time period for which the guest account will be valid after the first login, or 0 for indefinitely

Return Values

Table 271: Return Values, *amigopod.guest.edit*

Name	Type	Description
error	Flag	Set to 1 if the guest account was not modified
message	String	Message describing the success or failure of the operation
item	Struct	User structure containing updated field values
uid	Integer	ID of the guest account
*_error	String	Field-specific error message
*_error_flag	Flag	Field-specific error flag, set to 1 if present

Access Control

Requires the **full_user_control** privilege (**Guest Manager > Full User Control** in the Operator Profile Editor).

Example Usage

Sample parameters for the call:

```
'uid' => 162,
'username' => 'demo@example.com',
'password' => 'password_value',
'password_value' => 'password',
'role_id' => 2,
'enabled' => 1,
'simultaneous_use' => 1,
'do_schedule' => 0,
'schedule_time' => '',
'do_expire' => 4,
'expire_time' => '2014-12-01 00:00:00',
'expire_postlogin' => 0,
```

Sample successful call:

```
'error' => 0,
'message' => 'Edited properties of guest account demo@example.com',
'item' =>
array (
  'id' => 162,
  'username' => 'demo@example.com',
  'role_id' => 2,
  'enabled' => true,
  'simultaneous_use' => 1,
  'do_schedule' => 0,
  'do_expire' => 4,
  'expire_postlogin' => 0,
  'role_name' => 'Guest',
  'expire_time' => 1196431200,
),
```

Sample failed call:

```
'uid' => 162,
'random_password' => '59447116',
'password_value' => '',
'schedule_time' => '',
'expire_time' => '',
'user_enabled' => '',
'username_error' => 'You cannot leave this field blank.',
'username_error_flag' => 1,
'password_error' => 'Please choose from one of the available options',
'password_error_flag' => 1,
'role_id_error' => 'Please choose from one of the available options',
'role_id_error_flag' => 1,
'enabled_error' => 'Parameter must be provided',
'enabled_error_flag' => 1,
'simultaneous_use_error' => 'Please enter a non-negative integer value.',
'simultaneous_use_error_flag' => 1,
'do_schedule_error' => 'Please choose from one of the available options',
'do_schedule_error_flag' => 1,
'schedule_time_error' => 'Parameter must be a string',
'schedule_time_error_flag' => 1,
'do_expire_error' => 'Please choose from one of the available options',
'do_expire_error_flag' => 1,
'expire_time_error' => 'Parameter must be a string',
'expire_time_error_flag' => 1,
'expire_postlogin_error' => 'Please choose from one of the available options',
'expire_postlogin_error_flag' => 1,
'error' => 1,
```

Method `amigopod.guest.enable`

Enable a guest account.

Parameters

Table 272: *Parameters, `amigopod.guest.enable`*

Name	Type	Description
uid	Integer	ID of the guest account to enable

Return Values

This function might return a Boolean **false** value if some input parameters are invalid.



Table 273: *Return Values, `amigopod.guest.enable`*

Name	Type	Description
error	Flag	Set to 1 if the guest account was not enabled
message	String	Message describing the success or failure of the operation
item	Struct	User structure containing updated field values

Table 273: Return Values, *amigopod.guest.enable*(Continued)

Name	Type	Description
uid	Integer	ID of the guest account
*_error	String	Field-specific error message
*_error_flag	Flag	Field-specific error flag, set to 1 if present

Access Control

Requires the **remove_account** privilege (**Guest Manager > Remove Accounts** in the Operator Profile Editor).

Example Usage

Sample parameters for the call:

```
'uid' => '162',
```

Sample successful call:

```
'error' => 0,  
'message' => 'Guest account has been re-enabled',  
'item' =>  
array (  
  'id' => 162,  
  'enabled' => 1,  
  'username' => '',  
) ,
```

Sample failed call:

```
'error' => 1,  
'message' => 'Account not found: ID 162',
```

Method *amigopod.guest.get*

List one or more guest accounts.

Parameters

Table 274: Parameters, *amigopod.guest.get*

Name	Type	Description
id	Integer Array	Retrieve a single guest account by ID (integer parameter), or multiple guest accounts by ID (array parameter)

Return Values

Table 275: *Return Values, amigopod.guest.get*

Name	Type	Description
id	Mixed	ID or IDs of the guest accounts being returned
users	Array	<ul style="list-style-type: none">• If a single ID was requested, users contains the guest account requested (or an error field if an error occurred)• If multiple IDs were requested, users contains an array of results

Access Control

Requires the **guest_users** privilege (**Guest Manager > List Guest Accounts** in the Operator Profile Editor).

Example Usage

Sample parameters:

```
'id' => array(150, 162)
```

Sample successful call:

```
'id' =>
array (
    0 => 150,
    1 => 162,
),
'users' =>
array (
    0 =>
        array (
            'id' => '150',
            'username' => '44454318',
            'enabled' => '1',
            'role_id' => '2',
            'email' => '',
            'notes' => 'GuestManager account 22 of 30 created by root from 192.168.2.3',
            'do_expire' => '0',
            'expire_time' => '',
            'simultaneous_use' => '1',
            'expire_postlogin' => '0',
            'do_schedule' => '0',
            'schedule_time' => '',
            'ip_address' => '',
            'netmask' => '',
        ),
    1 =>
        array (
            'id' => '162',
            'username' => 'demo@example.com',
            'enabled' => '1',
            'role_id' => '2',
            'email' => 'demo@example.com',
            'notes' => '',
            'do_expire' => '4',
            'expire_time' => '1196253480',
            'simultaneous_use' => '1',
            'expire_postlogin' => '0',
```

```

        'do_schedule' => '0',
        'schedule_time' => '',
        'ip_address' => '',
        'netmask' => '',
        'auto_send_sms' => '',
        'creator_accept_terms' => '1',
        'role_name' => 'Guest',
        'sponsor_name' => 'Sponsor Name',
        'visitor_company' => 'Visitor Company',
        'visitor_name' => 'Visitor Name',
        'visitor_phone' => '0',
    ),
),

```

Sample failed call:

```

'id' => 162,
'users' =>
array (
    'error' => 1,
    'message' => 'Account not found: ID 162',
),

```

Method `amigopod.guest.list`

List guest accounts. (To retrieve devices, see ["Method amigopod.mac.list" on page 621](#))

Parameters

Table 276: *Parameters, amigopod.guest.list*

Name	Type	Description
details	Flag	Optional parameter; if set to 1 then full details of all guest accounts are returned, otherwise only the IDs are returned
sort	string	Optional parameter. If set to 1, then sorts first by the specified column, and then by username. For the field_name and +field_name formats, sort order will be ascending (A to Z); for the -field_name format the sort order will be descending (Z to A).
filter	string	Allows searching for multiple values when using the equality (=) or inequality (!=) operators. For more information, see the Filter description in "Managing Single Guest Accounts" on page 64 .

Return Values

Table 277: *Return Values, amigopod.guest.list*

Name	Type	Description
ids	Array	Array of guest account IDs (if details was 0)
users	Array	Array of guest account structures (if details was 1)

Access Control

Requires the **guest_users** privilege (**Guest Manager > List Guest Accounts** in the Operator Profile Editor).

Example Usage

Sample parameters:

```
'details' => 0,
```

Sample successful call:

```
'ids' =>  
array (  
  0 => '37',  
  1 => '141',  
  2 => '40',  
  ...  
) ,
```

Method amigopod.guest.reset.password

Reset a guest account's password to a random value.

Parameters

Table 278: *Parameters, amigopod.guest.reset.password*

Name	Type	Description
uid	Integer	ID of the guest account to reset the password for

Return Values

Table 279: *Return Values, amigopod.guest.reset.password*

Name	Type	Description
error	Flag	Set to 1 if the password was not reset
message	String	Message describing the success or failure of the operation
item	Struct	User structure containing updated field values
*_error	String	Field-specific error message
*_error_flag	Flag	Field-specific error flag, set to 1 if present

Access Control

Requires the **reset_password** privilege (**Guest Manager > Reset Password** in the Operator Profile Editor).

Example Usage

Sample parameters for the call:

```
'uid' => 162,
```

Sample successful call:

```
'error' => 0,  
'message' => 'Guest account password reset for  
Password changed to 37172833',  
'item' =>  
array (  
  'id' => 162,  
  'password' => '37172833',  
  'username' => '',  
) ,
```

Sample failed call:

```
'error' => 1,  
'message' => 'Account not found: ID 162',
```

Method **amigopod.mac.create**

Create a new MAC device account.

Parameters

Table 280: *Parameters, amigopod.mac.create*

Name	Type	Description
sponsor_name	String	Name of the person sponsoring the device account.
visitor_name	String	Name of the visitor.
visitor_company	String	Company name of the visitor.
email	String	The visitor's email address. This will become their username to log in to the network.
expire_after	Numeric	Amount of time before the device account will expire. Specified in hours.
expire_time	String	Optional date and time at which the device account will expire.
role_id	Integer	RADIUS role ID to assign to the device account.
creator_accept_terms	Flag	Set to 1 to indicate acceptance of the service's terms of use.
*	*	Other fields as specified by create_user form customization.

Return Values

Table 281: *Return Values, amigopod.mac.create*

Name	Type	Description
error	Flag	Set to 1 if the device account was not created
id	Integer	Set to the ID of the device account if the account was created
password	String	Set to a randomly-generated value (default behavior only)
*_error	String	Field-specific error message
*_error_flag	Flag	Field-specific error flag, set to 1 if present

Access Control

Requires the **mac_create** privilege (**Guest Manager > Create New MAC Authentication** in the Operator Profile Editor).

Example Usage

Sample parameters for the call:

```
'sponsor_name' => 'Sponsor Name',
'visitor_name' => 'Visitor Name',
'visitor_company' => 'Visitor Company',
'email' => 'demo@example.com',
'expire_after' => 4,
'expire_time' => '',
'role_id' => 2,
'visitor_phone' => '0',
'creator_accept_terms' => 1,
```

Result returned by a successful operation:

```
'username' => 'demo@example.com',
'password' => '73067792',
'role_id' => 2,
'role_name' => 'Guest',
'simultaneous_use' => '1',
'do_schedule' => 0,
'enabled' => true,
'expire_time' => 1196769257,
'do_expire' => 4,
'expire_postlogin' => 0,
'sponsor_name' => 'Sponsor Name',
'visitor_name' => 'Visitor Name',
'visitor_company' => 'Visitor Company',
'email' => 'demo@example.com',
'creator_accept_terms' => true,
'id' => 1,
```

Result returned by a failed operation:

```
'password' => '78342029',
'expire_time' => '',
'submit' => '',
'sponsor_name_error' => 'You cannot leave this field blank.',
'sponsor_name_error_flag' => 1,
```

```
'visitor_name_error' => 'You cannot leave this field blank.',
'visitor_name_error_flag' => 1,
'visitor_company_error' => 'You cannot leave this field blank.',
'visitor_company_error_flag' => 1,
'email_error' => 'Please enter a valid email address.',
'email_error_flag' => 1,
'expire_after_error' => 'Please choose from one of the available options.',
'expire_after_error_flag' => 1,
'expire_time_error' => 'Please enter a valid date and time.',
'expire_time_error_flag' => 1,
'role_id_error' => 'Parameter must be provided.',
'role_id_error_flag' => 1,
'creator_accept_terms_error' => 'You must accept the terms of use to continue.',
'creator_accept_terms_error_flag' => 1,
'error' => 1,
```

Method amigopod.mac.edit

Change one of more properties of a device account.

Parameters

Table 282: *Parameters, amigopod.mac.edit*

Name	Type	Description
uid	Integer	ID of the device account to edit
username	String	Name of the device account
password	String	May be: random_password to indicate the device account's password should be set to a random password password_value to indicate the device account's password should be set to the value in the password_value field The empty string to leave the password unmodified
password_value	String	Optional password to set the device account's password (if the password field is password_value)
role_id	Integer	RADIUS role ID to assign to the device account
enabled	Flag	Boolean value indicating whether the device account is enabled
simultaneous_use	Integer	Number of simultaneous sessions allowed by the device account
do_schedule	Flag	Flag indicating if the device account should be enabled at schedule_time
schedule_time	String	Date and time at which the device account will be enabled
do_expire	Integer	Action to take when the expire_time

Table 282: Parameters, amigopod.mac.edit(Continued)

Name	Type	Description
		is reached
expire_time	String	Time at which the device account will expire
expire_postlogin	Integer	Time period for which the device account will be valid after the first login, or 0 for indefinitely

Return Values

Table 283: Return Values, amigopod.mac.edit

Name	Type	Description
error	Flag	Set to 1 if the device account was not modified
message	String	Message describing the success or failure of the operation
item	Struct	User structure containing updated field values
uid	Integer	ID of the device account
*_error	String	Field-specific error message
*_error_flag	Flag	Field-specific error flag, set to 1 if present

Access Control

Requires the **full_user_control** privilege (**Guest Manager > Full User Control** in the Operator Profile Editor).

Example Usage

Sample parameters for the call:

```
'uid' => 162,
'username' => 'demo@example.com',
'password' => 'password_value',
'password_value' => 'password',
'role_id' => 2,
'enabled' => 1,
'simultaneous_use' => 1,
'do_schedule' => 0,
'schedule_time' => '',
'do_expire' => 4,
'expire_time' => '2014-12-01 00:00:00',
'expire_postlogin' => 0,
```

Sample successful call:

```
'error' => 0,
'message' => 'Edited properties of guest account demo@example.com',
'item' =>
array (
```

```
'id' => 162,  
'username' => 'demo@example.com',  
'role_id' => 2,  
'enabled' => true,  
'simultaneous_use' => 1,  
'do_schedule' => 0,  
'do_expire' => 4,  
'expire_postlogin' => 0,  
'role_name' => 'Guest',  
'expire_time' => 1196431200,  
)
```

Sample failed call:

```
'uid' => 162,  
'random_password' => '59447116',  
'password_value' => '',  
'schedule_time' => '',  
'expire_time' => '',  
'user_enabled' => '',  
'username_error' => 'You cannot leave this field blank.',  
'username_error_flag' => 1,  
'password_error' => 'Please choose from one of the available options',  
'password_error_flag' => 1,  
'role_id_error' => 'Please choose from one of the available options',  
'role_id_error_flag' => 1,  
'enabled_error' => 'Parameter must be provided',  
'enabled_error_flag' => 1,  
'simultaneous_use_error' => 'Please enter a non-negative integer value.',  
'simultaneous_use_error_flag' => 1,  
'do_schedule_error' => 'Please choose from one of the available options',  
'do_schedule_error_flag' => 1,  
'schedule_time_error' => 'Parameter must be a string',  
'schedule_time_error_flag' => 1,  
'do_expire_error' => 'Please choose from one of the available options',  
'do_expire_error_flag' => 1,  
'expire_time_error' => 'Parameter must be a string',  
'expire_time_error_flag' => 1,  
'expire_postlogin_error' => 'Please choose from one of the available options',  
'expire_postlogin_error_flag' => 1,  
'error' => 1,
```


Method `amigopod.mac.list`

List MAC device accounts. (To retrieve guest accounts, see "[Method `amigopod.guest.list`](#)" on page 614)

Parameters

Table 284: *Parameters, `amigopod.mac.list`*

Name	Type	Description
details	Flag	Optional parameter; if set to 1 then full details of all device accounts are returned, otherwise only the IDs are returned.
sort	string	Optional parameter. If set to 1, then sorts first by the specified column, and then by username. For the field_name and +field_name formats, sort order will be ascending (A to Z); for the -field_name format the sort order will be descending (Z to A).
filter	string	Allows searching for multiple values when using the equality (=) or inequality (!=) operators. For more information, see the Filter description in " Managing Single Guest Accounts " on page 64.

Return Values

Table 285: *Return Values, `amigopod.mac.list`*

Name	Type	Description
ids	Array	Array of device account IDs (if details was 0).
users	Array	Array of device account structures (if details was 1).

Access Control

Requires the **mac_list** privilege (**Guest Manager > List MAC Authentication Accounts** in the Operator Profile Editor).

Example Usage

Sample parameters:

```
'details' => 0,
```

Sample successful call:


```
'ids' =>  
array (  
  0 => '37',  
  1 => '141',  
  2 => '40',  
  ...  
)
```

Data Retention



The Data Retention Policy form (**Administration > Data Retention**) lets you manage historical data by deleting it.

Figure 435 *The Manage Data Retention Form*

Manage Data Retention	
* Enable:	<input checked="" type="checkbox"/> Enable data retention policy If enabled, records will be deleted at the time set below.
Time of Day:	3 : 0 Select the time of day at which data retention will run.
Onboard Device Certificates	
Certificate Retention:	➔ Configure Onboard data retention on a per-CA basis
 Set Data Retention Policy	

1. To enable the data retention policy option, select the **Enable** check box, and then enter the time of day at which records will be deleted.
2. To configure Onboard certificate retention, click the link in the **Certificate Retention** row. The **Certificate Authorities** list in the Onboard module opens.

If you wish to configure the times after which expired accounts are deleted, refer to the ClearPass Policy Manager documentation for cluster-wide parameters. Data retention of guest accounts and logs is configured in Policy Manager under **Administration > Server Configuration > Cluster-Wide Parameters**.

3.9 Configuration Import






To help ClearPass Guest 3.9 customers transition to ClearPass Guest 6.x, the **Import Configuration** forms let you:

- Create a full or custom backup of your Guest implementation. See ["Creating a Customized Configuration Backup"](#) on page 623.
- Upload a 3.9 configuration backup file to your ClearPass Guest 6.x file system, making the items in it available for import. See ["Uploading the 3.9 Backup File"](#) on page 623.
- Select items from it to import, restoring those configurations in your ClearPass Guest 6.x system. See ["Restoring Configuration Items"](#) on page 625
- Review details for configuration items after import, including anything that might be different between 3.9 and 6.2 and any actions you might need to take. See ["Viewing Imported Item Details"](#) on page 627 and ["Import Information for Specific Import Items"](#) on page 629.

Creating a Customized Configuration Backup

You can use the **Configuration Backup** form to create and export a full or customized configuration backup file.

To create a configuration backup:

1. Go to **Administration > Import Configuration > Import Configuration**, and then click the **Create a customized backup** link in the upper-right corner. The **Export Configuration** form opens.
2. In the **Backup Mode** drop-down list, select either **Complete backup** or **Custom backup**, as appropriate.
3. In the **Backup Name** field, enter the name of the backup file.
4. If you selected **Custom backup**, the form expands to include the **Backup Set** field, which displays a list of items to choose from. When this list first opens, all items are included by default. Categories are displayed—for example, Guest Manager, SMS Services, and so on—and subordinate items in the categories are hidden. To configure a custom backup, use the controls in the **Backup Set** list to specify just the items you want to include:
 -  The green arrow and **bold** font indicate an item and all its subordinate items will be included.
 -  The blue arrow is a visual aid marking an item as a category that has subordinate items listed below it. To view the subordinate items, click the blue arrow. If the arrow is gray, there are no subordinate items.
 -  To exclude an item from the import, click the **X** in the item's row. The X turns red to indicate it will be excluded. You can click the **X** for a category to exclude all items in that category. To include an excluded item, click the arrow in its row.
5. When you have completed and verified your selections, click **Download Backup**. The configuration backup is saved to your Downloads folder as a .dat file. You can then click either the **Restore a backup configuration** link, or **Import Configuration > Import Configuration** in the left navigation to upload and restore the file.

Uploading the 3.9 Backup File

To upload a Guest 3.9 configuration to ClearPass Guest 6.x:

1. Upgrade your 3.9 system to the latest 3.9.x monthly patch.
2. Deploy your 6.x system, and upgrade it to the latest 6.x monthly patch.
3. In your 3.9 system, make a complete configuration backup. For details on how to back up your system, refer to the "Backup and Restore" section in the "Administrator Tasks" chapter of your "ClearPass Guest 3.9 Deployment Guide."



Be sure to use the **Complete backup** option in your 3.9 system's Backup Mode drop-down list to ensure that references between items are properly migrated. Partial imports might not work as expected.

4. In your 6.x system, go to **Administration > Import Configuration > Import Configuration**. The **Import Configuration: Step 1** page opens with the **Upload File** form displayed.
5. If your file does not exceed the 15.0 MB size limit, you can use this **Upload File** form to browse to the location where you stored your 3.9 backup file. To use the Upload File form, click the **Browse** button in the **Backup File** row to navigate to and select the backup file you want to restore.

Figure 436 *The Upload File Form*

Upload File	
Size Limit:	Maximum file upload size: 15.0 MB.
* Backup File:	<input type="button" value="Choose File"/> 3.9-complete-backup.dat Select the backup file to start the restore process.
<input type="button" value="Continue"/>	

If your file is larger than the maximum file upload size of 15.0 MB, you must specify a URL instead. Click the **Restore a backup from a URL** link above the **Upload File** form. The **Specify Backup File** form is displayed. Enter the URL for the backup file.

Figure 437 *The Specify Backup File Form*

Specify Backup File	
* URL:	<input type="text" value="http://192.0.2.12/amg/backups/3.9-complete-backup.dat"/> Specify the URL of the backup file.
<input type="button" value="Continue"/>	

6. Click **Continue**. The backup file is uploaded to your 6.x system, making the items available for import, and the **Import Configuration: Step 2** page opens.

Figure 438 *The Configuration Backup List View*

Configuration Backup		
Backup:	3.9-complete-backup (complete)	
Configuration Item	Restore	
AirGroup Services	<input type="checkbox"/>	<input checked="" type="checkbox"/>
AirGroup Services Configuration	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Cisco IP Phones	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Service Instances	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Guest Manager	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Guest Manager Configuration	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Guest Manager Custom Fields	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Guest Manager Custom Forms	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Guest Manager Custom Views	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Guest Manager Print Templates	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Guest Manager Self Registration	<input type="checkbox"/>	<input checked="" type="checkbox"/>
LDAP Sponsor Lookups	<input type="checkbox"/>	<input checked="" type="checkbox"/>
MAC Authentication Configuration	<input type="checkbox"/>	<input checked="" type="checkbox"/>
High Availability	<input type="checkbox"/>	<input checked="" type="checkbox"/>
High Availability Local Configuration	<input type="checkbox"/>	<input checked="" type="checkbox"/>
High Availability Shared Configuration	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Hotspot Manager	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Hotspot Configuration	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Transaction Processors	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Onboard	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Onboard Configuration	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Operator Logins	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Operator Login Configuration	<input type="checkbox"/>	<input checked="" type="checkbox"/>

This form shows every configuration item in your backup file, and provides options for restoring items or excluding them from the restoration. For more information, see the next section, "Restoring Configuration Items" on page 625.

Restoring Configuration Items

This section describes how to use the **Import Configuration: Step 2** form to import 3.9 configuration items to your 6.2 system after you upload them.

To select and restore your configuration items:

1. Go to **Administration > Import Configuration > Import Configuration** and complete the steps described in "Uploading the 3.9 Backup File" on page 623.
2. When the **Import Configuration: Step 2** form is displayed, review the list of items. You can use the options in the **Restore** column to select the items to import.



Partial imports might not work as expected. To ensure that references between items are properly migrated, use the default Restore settings.

Figure 439 The Configuration Backup List View

Backup: **3.9-complete-backup** (complete)

Configuration Item	Restore
AirGroup Services	X ↓ ✓
AirGroup Services Configuration	X ✓
Cisco IP Phones	X ↓ ✓
Service Instances	X ✓
Guest Manager	X ↓ ✓
Guest Manager Configuration	X ✓
Guest Manager Custom Fields	X ✓
Guest Manager Custom Forms	X ✓
Guest Manager Custom Views	X ✓
Guest Manager Print Templates	X ✓

X Unselect All 10 rows per page

Select the items from this configuration backup to restore.

* Restore settings from backup
 Confirm: Select this option to confirm the restore operation. Caution! This may overwrite your current settings.

Restore Configuration

- To exclude an item from the import, click the **X** in the item's row. The **X** turns red to indicate it will be excluded. You can click the **X** for a category to exclude all items in that category.
 - To make it easier to select just a few items, you can scroll to the bottom of the list and click the **Unselect All** link. All items are then marked with a red X and will be excluded from the import. You can then select the green check marks for just the items you want.
 - The blue arrow is a visual aid marking an item as a category that has subordinate items listed below it.
 - To include an item in the import, click the check mark in the item's row. The check mark turns green and the item's name is highlighted in **bold** font to indicate it will be included. You can click the check mark for a category to include all items in the category.
3. Select the items in the list that you want to restore, then mark the **Restore settings from backup** check box to confirm.



Restoring the backup will overwrite your current settings.

- Click **Restore Configuration**. System progress is displayed while items are being imported. When the import is complete, the **Finished Import** page displays the **Import Notices** list for the restored items. For more information, see "[Viewing Imported Item Details](#)" on page 627.

Viewing Imported Item Details

After you click **Restore Configuration** to import your 3.9 configuration to your 6.2 system, the **Finished Import** page displays the **Import Notices** list for the restored items. You can click an item's row in the list for additional options. For some items, a link is provided to the relevant page in the application.

To view information for imported configuration items:

- Go to **Administration > Import Configuration > Last Import**. The **Import Notices** list opens.

Figure 440 *The Import Notices List View*









Status	Operation / Notice	Count
✓ Imported	Import AirGroup Services Configuration	1
➔ Migrated	Import Guest Manager Configuration	1
✓ Imported	Import Guest Manager Custom Field	77
Show Details Go to Fields		
➔ Migrated	Import Guest Manager Custom Field	26
ⓘ Obsolete	Import Guest Manager Custom Field	2
➔ Migrated	Import Guest Manager Custom Form	17
✓ Imported	Import Guest Manager Custom Form	3
➔ Migrated	Import Guest Manager Custom View	6
✓ Imported	Import Guest Manager Custom View	1
⚠ Action Required	Import Guest Manager Print Template	11
✓ Imported	Import LDAP Sponsor Lookups	1
➔ Migrated	Import MAC Authentication Configuration	1
➔ Migrated	Import Service Handler	5
➔ Migrated	Import Operator Login Configuration	1
ⓘ Obsolete	Import Operator Login	4
✗ Error	Import Service Handler	1
✗ Error	Import Operator Servers	1
✓ Imported	Import LDAP Translation Rules	8
⚠ Action Required	Import LDAP Translation Rules	1
✓ Processed	Import Palo Alto Network Services Configuration	1
✓ Processed	Import RADIUS Authentication Servers	2
⊘ Unsupported	Import RADIUS Certificates	1
ⓘ Obsolete	Import RADIUS Database Connections	1

The **Import Notices** list provides information about items that were handled during the last import. This list includes the following columns:

- Status** -- The import status of the item in the same row. Possible statuses include Imported, Migrated, Obsolete, Action Required, Error, Processed, Unsupported, and Warning. These statuses are described more fully in the table below.

- **Operation/Notice** -- This column shows the operation performed on the item, and the name of the item. If the item was imported, the value in this column will be "Import <item name>". If the item could not be imported, you can click the row to view the item details for more information.
 - **Count** -- The number of items imported for each configuration item. For example, the number shown in the **Count** column for **Guest Manager Custom Fields** indicates the number of customized fields that were imported.
2. You can click a configuration item's row in the list for additional options.
- For some items, you can click a link to go to the relevant page in the application.
 - To view details for a configuration item, click its **Show Details** link. The form expands to show details of the import results for the item. The details explain the import status, and advise you of any further action that might be required.

Table 286: Configuration Import Statuses

Status		Description
	Imported	The item was successfully imported with no changes.
	Migrated	The item was successfully imported but some aspects were modified for 6.2, as described in Show Details for the item. For example, if a field imported in a 3.9 configuration has a different name in 6.2 but was successfully matched and updated, the change is indicated by an arrow: Migrated field: schedule_time --> start_time
	Processed	The item was processed for the import but was not applicable and was ignored, as described in Show Details for the item. For example, a disabled network configuration, or a service that is now handled in Policy Manager instead of Guest, or a plugin version that was already up to date.
	Action Required	Items with this status might or might not have been imported, and require further verification or manual configuration, as described in Show Details for the item. For example, print templates that should be reviewed, reports that should be recreated using Insight instead of Reporting Manager, custom database settings that are not supported, items that should now be configured in Policy Manager instead of Guest, or server addresses that should be verified to ensure they are current.
	Unsupported	The item was not imported because it is not supported in 6.2. For example, RADIUS certificates, RADIUS Dictionary, custom items for which no handler could be found, or items such as the system log or RADIUS database that are now managed in Policy Manager.
	Obsolete	The item was not imported because it is obsolete in 6.2. For example, fields that no longer exist, obsolete operator login settings, RADIUS database settings or server configurations, or deleted user accounts.
	Error	The item was not imported because it was missing or unavailable. For example, missing service handler implementations or unavailable skin plugins.
	Warning	The item was imported but the details include information the operator should be aware of. For example, plugins might have been exported from your 3.9 system by out-of-date plugin versions.

For import details specific to each import item, see ["Import Information for Specific Import Items "](#) on page 629.

Import Information for Specific Import Items

For each configuration category on the Import Notices list, this section describes items that might be changed, unsupported, or obsolete, and any actions you might need to take.

This section includes the following:

- ["Import Information: AirGroup Services" on page 629](#)
- ["Import Information: Cisco IP Phones" on page 629](#)
- ["Import Information: Guest Manager" on page 629](#)
- ["Import Information: High Availability \(HA\)" on page 630](#)
- ["Import Information: Hotspot Manager" on page 631](#)
- ["Import Information: Onboard" on page 631](#)
- ["Import Information: Operator Logins" on page 631](#)
- ["Import Information: Palo Alto Network Services" on page 631](#)
- ["Import Information: RADIUS Services" on page 631](#)
- ["Import Information: Reporting Manager Definitions" on page 633](#)
- ["Import Information: Server Configuration" on page 633](#)
- ["Import Information: SMS Services" on page 634](#)
- ["Import Information: SMTP Services" on page 634](#)

Import Information: AirGroup Services

- The following AirGroup 3.9 fields are renamed:

Table 287: *Renamed AirGroup Fields*

3.9 Name		6.1 Name
shared_location	=	airgroup_shared_location
shared_role	=	airgroup_shared_role
shared_user	=	airgroup_shared_user

- The definitions of some fields are also updated.
- AirGroup controller names default to the hostname.

Import Information: Cisco IP Phones

- The user database is the default ClearPass Policy Manager user database.
- The SMS service handler ID might be updated.

Import Information: Guest Manager

Guest Manager Configuration

- The new default for the Expire Action setting is 1. Any non-default setting is updated to this new default.

- Any Account Retention setting is removed.
- Any non-default Session Warning setting is updated to the new default.

Custom Fields:


-  The following 3.9 custom fields are obsolete and are not imported:
 - do_schedule
 - delete_time
- The following 3.9 custom fields are renamed:


Table 288: *Renamed Guest Manager Fields*

3.9 Name		6.2 Name
schedule_time	=	start_time
modify_schedule_time	=	modify_start_time
schedule_after	=	start_after

Custom Forms and Views:

- Forms and views that referenced renamed fields are updated to reference the new field name.
- Forms and views that referenced obsolete fields have those fields removed from the definition.


Print Templates:

-  Print templates are flagged as Action Required. Print templates might require changes where defaults have changed or fields have been renamed. Review the templates and correct as necessary to fix fields that have been changed.

Self Registration:

- The user database is the default ClearPass Policy Manager user database.



LDAP Sponsor Lookups:

- All LDAP operator servers and translation rules are imported. All 6.2 LDAP translation rules are also kept, because the new default LDAP rules are required for correct operation.
-  Imported LDAP translation rules should be reviewed for correct order.

MAC Authentication Configuration:

- Non-default MAC Separator settings are updated to the new default (-).
- Non-default MAC Case settings are updated to the new default (lower).
- AirGroup Debug settings are obsolete and are removed.

Import Information: High Availability (HA)

- If HA was not configured, the shared configuration is processed but ignored.
-  If HA was configured, it is unsupported.
-  If HA nodes were configured, do the following for each shared configuration :
 - Configure a Virtual IP address in ClearPass.

- Configure Publisher Redundancy in ClearPass.

Import Information: Hotspot Manager

- Non-default User Database settings are updated to the default ClearPass Policy Manager user database.
- Non-default Transaction Processing settings reference the correct transaction processor.
- A cookie check (nwa_cookiecheck) is added to the default hotspot plan template.

Import Information: Onboard



To restore your Onboard device provisioning pages, you must import RADIUS Web logins.

- The server certificate in ClearPass might need to be configured before provisioned devices can connect to the network.
- The QuickConnect client provisioning address might need to be verified as the correct one for the new server.

Import Information: Operator Logins

Operator Login Configuration

- A client-side cookie check (nwa_cookiecheck) is added to the Login Message setting.

Operator Logins

- Operator logins are obsolete.

Operator Profiles

- If the IT Administrators profile is imported, it is updated to keep existing privileges and is migrated.
- Any non-default Password Change Policy is removed and the profile is migrated.
- Any non-default user skins are reset to the default skin and the profile is migrated.

Operator Servers

- Operator servers are imported as service handlers.

Operator Translation Rules

- If there are any new translation rules, the translation rules should be reviewed for correct order.

Import Information: Palo Alto Network Services


- If Palo Alto Network Services Configuration was disabled, it is processed and ignored.
- If it was enabled, it must be configured in ClearPass.

Import Information: RADIUS Services

RADIUS services are now handled in ClearPass Policy Manager instead of ClearPass Guest.

RADIUS Authentication Servers


- Default authentication servers are processed but ignored (Local User Database, Local Certificate Authority)

-  For all other authentication servers, an authentication source must be created in ClearPass.



RADIUS Certificates

-  RADIUS certificates are unsupported.


RADIUS Database Accounting Records

-  RADIUS database accounting records are unsupported.


RADIUS Database Connections

-  The RADIUS database connection for the local RADIUS server is obsolete.
-  For any custom user databases, an authentication source must be created in ClearPass.

RADIUS Database User Accounts

- User accounts are migrated and keep the status (disabled, pending, active, expired) they had in 3.9. Any field names that differ in 6.2 are updated.
-  User accounts with the Deleted status are obsolete.











RADIUS Dictionary

-  The RADIUS dictionary is unsupported.



RADIUS NAS List

- Each RADIUS network access server (NAS) is imported as a ClearPass network access device (NAD) client.

RADIUS Server Configuration

-  Non-default RADIUS Server Number settings are obsolete.
-  Non-default RADIUS Server Port settings are obsolete.
- Default RADIUS Server Options are not applicable; they are processed and ignored.
-  For any non-default RADIUS Server Options, an authentication source must be created in ClearPass.
-  Non-default Case Insensitive Username settings are obsolete.
-  Non-default Include Active Sessions settings are obsolete.
-  Non-default EAP Server settings are obsolete.
-  Non-default AAA Debug settings are obsolete.
-  Non-default Extra RADIUS Attributes settings are obsolete.
-  Non-default Interim Accounting settings are obsolete.
-  RADIUS Server Configuration is imported (and flagged as imported or action required)

RADIUS User Roles

-  For any role that does not have the default attributes (Reply-Message := <?= \$role['name'], the role must be manually configured in ClearPass.
-  For any role that had MAC caching enabled, the role must be manually configured in ClearPass.

RADIUS Web Logins

- RADIUS Web logins are imported.

Import Information: Reporting Manager Definitions

-  Reports must be re-created in ClearPass Insight.


Import Information: Server Configuration

-  ClearPass settings are obsolete.


Data Retention

- Data Retention settings for Onboard are imported.

Database Configuration

- Default (empty) database configuration settings are processed and ignored.
-  Non-default database configuration settings should be reviewed for potential issues.



Installed Plugin List

-  For imported plugins that were not up-to-date (e.g. pre-3.9), you must review the version numbers provided in Show Details, upgrade those plugins in your 3.9 system, and import the plugins again.

Network Hostname

-  The network hostname must be set in ClearPass.


Network Hosts

-  Default hosts files (references to localhost only) are obsolete.
-  For a non-default hosts file, the DNS must be properly configured.

Network Interface Configuration

-  Network interfaces are unsupported.

Security Audit Settings

-  Security audit settings are obsolete.


Server Time Setup

-  Server time settings must be configured in ClearPass.




SNMP Configuration

-  If SNMP was enabled, settings must be configured in ClearPass.


SSL Certificate Setup

- The backup certificate is processed and ignored.
-  For other certificates, the certificate and the private key should be downloaded and the certificate imported into ClearPass.

Subscription IDs

- If the following settings do not have default values, they are updated to the new default values and migrated:
 - Session ID
 - Update URL
 - Facility
-  For non-default Application URLs, changes should be reviewed.
-  Subscription IDs must be added to ClearPass.
-  For non-default HTTP Proxy settings, the HTTP proxy must be configured in ClearPass.



System HTTP Proxy

-  For non-default HTTP Proxy settings, the HTTP proxy must be configured in ClearPass.


System Kernel Configuration

-  System kernel configuration is obsolete.

System Log Setup

-  System log setup is obsolete.
-  If a local collector was enabled, it is unsupported.

Web Application Configuration

- Default Application Configuration settings are processed and ignored.
-  For non-default Application Configuration settings, PHP settings must be configured in ClearPass.


Web Server Configuration

-  Web server configuration is obsolete.

Import Information: SMS Services

- SMS gateways are imported as service handlers.

Import Information: SMTP Services

-  The following settings are updated to the new defaults and the configuration is migrated:
 - Additional Headers
 - Copies To
 - Email Receipt
 - Enable warnings

- From Address
- Logout Warnings
- Mail Transfer Settings
- Override From
- Password
- Reply-To
- Send Copies
- Skin
- SMTP Port
- SMTP Server
- Subject Line
- Username
- Use Sendmail
- Use SSL encryption

Plugin Manager



Plugins are the software components that fit together to make your Web application. The **Available Plugins** list shows all the plugins currently included in your application. It lets you view information about each plugin and configure some aspects of most plugins. You can click a plugin's name to go directly to that area of the application—for example, clicking the name of the **SMTP Services** plugin opens the **Customize Email Receipt** page in the **Configuration** module.















Viewing Available Plugins



To access the list of available plugins list, go to **Administration > Plugin Manager**. The **Available Plugins** list view opens. Plugins are listed by category and include:

- **Standard Plugins**—Provide corresponding functionality in the application for interactive use by operators
- **Kernel Plugins**—Provide the basic framework for the application
- **Operator Login Plugins**—Control access to the Web application
- **Skin Plugins**—Provide the style for the application's visual appearance
- **Transaction Processor Plugins**—Provide transaction service handlers for interfacing with various payment solution providers
- **Translation Plugins**—Provides configurable language settings for the application

Figure 441 *The Available Plugins List View*

Icon	Name	Version	Status
Standard Plugins			
	Advertising Services Control the delivery of advertising content.	6.5.0	Enabled
	 Configuration  About		
	AirGroup Services Provides services to send device ownership and sharing information to AirGroup-enabled controllers.	6.5.0	Enabled
	 Configuration  About		
	API Framework Provides application programming interface (API) services.	6.5.0	Enabled
	 Configuration  About		
	Cisco IP Phone Services Provides guest account creation services to Cisco IP phones.	6.5.0	Enabled
	 Configuration  About		
	ClearPass Guest Services Provides guest management and platform integration services for the Policy Manager.	6.5.0	Enabled
	 Configuration  About		



The  **About** link displays information about the plugin, including the installation date and update date. The **About** page for the Kernel plugin also includes links to verify the integrity of all plugin files or perform an application check.

Figure 442 *The Plugin Information View for the ClearPass Guest Services Plugin*




Plugin Information	
	ClearPass Guest Services
Version:	6.0.0 build 22366
Type:	Standard Plugin
Installed:	26 September 2012
Last Updated:	Not Available
Configurable:	Yes
Copyright:	Copyright © 2012 Aruba Networks, Inc.

Click a plugin's  **Configuration** link to view or modify its settings. See "Configuring Plugins" on page 636 for details about the configuration settings.

Configuring Plugins

You can configure most standard, kernel, skin, and translation plugins. Skin plugins can also be enabled or disabled, letting you choose which skin to use. To work with plugins, go to **Administration > Plugin Manager**. The **Available Plugins** list view opens.

Figure 443 *Options for a Plugin in the List*

	ClearPass Guest Services Provides guest management and platform integration services for the Policy Manager.	6.0.0	Enabled
	 Configuration  About		



To view or change the configuration settings for a plugin, click the plugin's  **Configuration** link. The **Configure Plugin** form shows the current configuration settings for a plugin, and allows you to make changes to these settings.

Figure 444 *The Configuration Form for the MAC Authentication Plugin*



Configure MAC Authentication 6.0.1-22683	
* MAC Detect:	<input type="checkbox"/> Allow users to be detected via their MAC address Provides access to user configuration for headers, footers, etc on login and registration pages. Please note that a passed MAC can be easily changed by the user, so personal details should not be displayed. Requires a vendor that passed the mac as part of the redirection.
Device Filter:	<input checked="" type="checkbox"/> List Accounts <input type="checkbox"/> Edit Accounts Select which views should not display devices (user accounts with the `mac_auth` field set).
 Save Configuration	

To undo any changes to the plugin's configuration, click the plugin's  **Restore default configuration** link. The plugin's configuration is restored to the factory default settings.

In most cases, plugin configuration settings do not need to be modified directly. Use the customization options available elsewhere in the application to make configuration changes.

For more information about plugin configuration:

- **AirGroup Services**—See "Configuring AirGroup Services" on page 638
- **API Services**—See "Configuring the API Framework Plugin" on page 639
- **Aruba ClearPass Skin**—See "Configuring the Aruba ClearPass Skin Plugin" on page 641
- **Guest Manager**—See "Default Settings for Account Creation" on page 277
- **IP Phone Services**—See "Configuring the IP Phone Services Plugin" on page 650
- **Kernel**—See "Configuring the Kernel Plugin" on page 651
- **MAC Authentication**—See "Configuring the MAC Authentication Plugin" on page 653
- **Platform Services**—See "Configuring the Platform Services Plugin" on page 654
- **SMS Services**—See "Configuring the SMS Services Plugin" on page 654
- **SMTP Services**—See "Email Receipt Options" on page 438
- **Translation Services**—See "Configuring the Translations Plugin" on page 659
- **Web Analytics** —See "Configuring the Web Analytics Plugin" on page 660
- **SOAP Web Services**—See "Configuring the SOAP Web Services Plugin" on page 661

Configuring AirGroup Services

To enable support for dynamic notification of AirGroup events when new devices are added, each AirGroup-enabled controller must also be defined in ClearPass Guest. Configuration options include specifying roles to exclude from the user interface, and setting an automatic polling schedule, message parameters, and logging levels.

To configure AirGroup Services, go to **Administration > AirGroup Services > Configuration**. The **Configure AirGroup Services** form opens.

Figure 445 *The Configure AirGroup Services Form*

Configure AirGroup Services

AirGroup Controller Options
Options for collecting and using the configuration of AirGroup controllers.

Exclusions:
List any role names, AP group names, or AP names that should be excluded from the AirGroup user interface, one per line. Items are matched case-insensitively. Comments may be entered on a line starting with '#'.

Polling: Automatically read configuration from AirGroup controllers on a schedule

Schedule:
Select how frequently to run the task.

* Run At:
Select when the task should run.

Sharing Options
Options for different AirGroup sharing types.

Group Names:
List the user groups that are available in the 'Shared Groups' field. This list is automatically updated as new user group names are entered. Note that removing a group name from this list does not remove it from any shared group lists.

General Options
Network and logging options for AirGroup services.

* Network Interface:
AirGroup will use this network interface to send outbound notification messages. To enable using a virtual IP address, select the appropriate network interface. 'Automatic' uses the RFC-3576 Bind Address from Configuration » Authentication.

* Timeout: seconds
Timeout for sending an AirGroup message.

* Attempts:
Maximum number of attempts to use when sending an AirGroup message.

* AirGroup Logging:
Select an option for logging events related to AirGroup Services.

Table 289: *Configure AirGroup Services*

Field	Description
Exclusions	Role names, AP group names, or AP names that should not be displayed in the AirGroup user interface. Enter each item on a separate line. Entries are not case-sensitive. To add a comment, enter it on a separate line that begins with the "#" character.
Polling	If selected, schedules automatic polling of AirGroup controller configuration. The form expands to include scheduling options.
Schedule	Choose one of the following options from the drop-down list and complete the scheduling details: <ul style="list-style-type: none"> None -- Run task at once: In the Run At field, use the calendar picker to specify the month, day, and time to poll for configuration. Hourly: In the Minute field, enter the number of minutes past the hour to poll for configuration, or 00 to poll on the hour. If you do not need to poll every hour, you can use

Field	Description
	<p>the check boxes in the Hours field to specify which hours of the day the poll should run.</p> <ul style="list-style-type: none"> ● Daily: Use the text boxes in the Time of Day field to enter the hour and minute of the day the poll should run. ● Weekly: Use the check boxes in the Weekdays field to specify the day or days of the week the poll should run, then use the text boxes in the Time of Day field to enter the hour and minute of the day the poll should run. ● Monthly: Use the check boxes in the Months field to specify which month or months the poll should run, then use the text boxes in the Days field to specify the day or days of the month. Use the text boxes in the Time of Day field to enter the hour and minute of the day the poll should run. ● Yearly: In the Run On field, use the drop-down list to select a month, then enter the day and time in the text boxes. <p>When a poll is run, you may click Show Details in the Controllers list to view the updated configuration. For more information, see "AirGroup Controllers" on page 538. Automatic polling is run only on the publisher node.</p>
Group Names	<p>Enter names of shared groups that should be available in the Shared Groups field for users to choose from when they share a device. If additional user groups are also entered by users when they share a device, the list in the configuration is automatically updated to capture these fields. Removing a group name from this list does not remove it from other shared group lists.</p> <p>When you type a name for the group in the Group Names field, press the Enter key, and click Save, the group is created in the system and appears as a "tag". For more information, see "About AirGroup Time-Based Sharing" on page 89.</p> <p>Each group name may not exceed 64 characters. A maximum of 32 group names may be entered. The maximum character limit for the list is 320 characters (including comma separators).</p>
Network Interface	<p>Specifies the interface AirGroup will use to send outbound notification messages. To enable using a virtual IP address, select the appropriate interface. Options include:</p> <ul style="list-style-type: none"> ● Automatic — Automatically chooses the appropriate source IP address; either the management port or the data port, depending on the controller's IP address. ● Management port [MGMT] — Always uses the management port as the source address. ● Data/External port [DATA] — Always uses the data port as the source address.
Timeout	Number of seconds after which an attempt to send an AirGroup message will time out.
Attempts	Maximum number of times the system should attempt to send an AirGroup message.
AirGroup Logging	<p>Specifies the logging level. Options include:</p> <ul style="list-style-type: none"> ● Disabled—Do not log AirGroup related events ● Standard (Recommended)—Log basic information ● Extended—Log additional information ● Debug—Log debug information ● Trace—Log all debug information

Configuring the API Framework Plugin

The API Framework plugin supports OAuth2 authentication and authorization, and provides all application programming interface (API) services for ClearPass Guest. Settings you can configure for this plugin include the access token lifetime, refresh token lifetime, API logging level, and security settings for Cross-Origin Resource Sharing (CORS).

To view or configure the API Framework plugin:

1. Go to **Administration > Plugin Manager**. The **Available Plugins** list opens.

2. Scroll to the **Standard Plugins > API Framework** row and click its **Configuration** link. The **Configure API Framework** form opens.

Figure 446 *The API Framework Plugin Configuration Form*

Configure API Framework 6.6.0-32073	
Access Token Lifetime:	<input type="text" value="8"/> <input type="text" value="hours"/> <input type="button" value="v"/> Specify the default lifetime for an OAuth2 access token. This parameter may be configured separately for each API client.
Refresh Token Lifetime:	<input type="text" value="14"/> <input type="text" value="days"/> <input type="button" value="v"/> Specify the lifetime of an OAuth2 refresh token. This parameter may be configured separately for each API client.
* API Logging:	<input type="text" value="Standard (Recommended) — log basic information"/> <input type="button" value="v"/> Select an option for logging API-related events. <ul style="list-style-type: none">• 'Extended' will log most API calls.• 'Trace' will log full details of all API calls, including authorization failures.
Allowed Origins:	<input type="text"/> Security settings for Cross-Origin Resource Sharing (CORS). List the allowed origins for browser-initiated API requests, one per line. Specify * to allow all origins. This may also be used as a wildcard, e.g. *.example.com. Leave blank to never allow cross-domain API requests.
Arbitrary Sort:	<input type="checkbox"/> Allow API calls to specify arbitrary sort fields Enable this option if you receive a "Cannot sort by field" error. Note: This has performance implications when large query results are involved.
<input type="button" value="Save Configuration"/>	

Table 290: API Framework Plugin Configuration

Field	Description
Access Token Lifetime	<p>(Optional) Specifies the default lifetime of an OAuth2 access token. Unless it is changed, the default value is 8 hours. To change the value, enter a number in the first text field, and use the drop-down list to indicate the unit of time. Options include:</p> <ul style="list-style-type: none"> • seconds • minutes • hours • days • weeks <p>The value for this parameter may also be configured separately for each API client (see "Creating and Editing API Clients" on page 561).</p>
Refresh Token Lifetime	<p>Specifies the default lifetime of an OAuth2 refresh token. Unless it is changed, the default value is 14 days. To change the value, enter a number in the first text field, and use the drop-down list to indicate the unit of time. Options include:</p> <ul style="list-style-type: none"> • seconds • minutes • hours • days • weeks <p>The value for this parameter may also be configured separately for each API client (see "Creating and Editing API Clients" on page 561).</p>
API Logging	<p>(Required) Specifies the logging level for API-related events. Options include:</p> <ul style="list-style-type: none"> • Disabled - do not log API-related events • Standard (Recommended) - log basic information • Extended - log additional information — (this option logs all API calls) • Debug - log debug information • Trace - log all debug information — The 'Trace' logging level exposes the following security risks: <ul style="list-style-type: none"> ■ Information disclosure: Full request/response traces are logged, including potentially sensitive information such as access tokens, passwords, and/or shared secrets. ■ Denial-of-service: Every API request generates a log message, including authentication and authorization failures.
Security Warning	<p>Displays security risks warnings if you selected Trace - log all debug information in the API Logging field.</p>
Allowed Origins	<p>Specifies a list of hostnames that may be used for Cross-Origin Resource Sharing (CORS). Enter each hostname on a separate line. The asterisk character may be used by itself to allow all origins, or it can be used as a wildcard (*.example.com). To never allow cross-domain API requests, leave this field blank.</p>
Arbitrary Sort	<p>If selected, overrides default sort-field settings and allows any field to be specified as the sort column through the API. Users should be aware that large query results might cause a performance impact.</p>
Save Configuration	<p>Commits your changes.</p>

Configuring the Aruba ClearPass Skin Plugin

A Web application's skin determines its visual style—the colors, menus, and graphics. You can use either the standard Aruba ClearPass skin plugin, the ClearPass Guest skin, a Galleria skin, a blank plugin if you are

providing your own complete HTML page, or custom skin plugins that let you configure the colors, navigation, logo, and icons.

To view or configure the standard Aruba ClearPass skin plugin:

1. Go to **Administration > Plugin Manager**. The **Available Plugins** list opens.
2. Scroll to the **Skin Plugins > Aruba ClearPass Skin** row and click its **Configuration** link. The **Configure Aruba ClearPass Skin** form opens.

Figure 447 *The Aruba ClearPass Skin Plugin Configuration Form*

Configure Aruba ClearPass Skin 6.0.0-22334	
* Navigation Layout:	(Use Default) <small>Override the navigation layout.</small>
Page Heading:	<input type="text"/> <small>Customize the text displayed in the page heading.</small>
Print Template Options <small>The following colors and styles are used in the stock HTML-based print templates.</small>	
Font Family:	Verdana, "Bitstream Vera Sans", Arial, sans-serif <small>Enter a list of fonts as the font family.</small>
* Welcome Background Color:	EF851F <small>Select the background color to be used in the welcome block.</small>
* Welcome Foreground Color:	FFFFFF <small>Select the foreground color to be used in the welcome block.</small>
* Welcome Highlight:	7B3D00 <small>Select the color to highlight the name.</small>
* Network Color:	292929 <small>Select the color for the network section.</small>
* Network Highlight:	5A5A5A <small>Select the color to highlight the network.</small>
* Instructions Color:	838383 <small>Select the color for the instructions.</small>
* Instructions Highlight:	292929 <small>Select the highlight color for the instructions.</small>
<input type="button" value="Save Configuration"/>	

Table 291: *Configure Aruba ClearPass Skin Form*

Field	Description
Navigation Layout	Specifies the navigation's expansion level. The default navigation layout is "expanded." Options include: <ul style="list-style-type: none"> • Use Default • simple — Only the current L1 item has L2 items, L3 only when L2 active • expando — Show items in expanding/collapsing lists • expanded — All L1 items have L2 items, L3 only when L2 active • all-expanded — All items shown to L3 • I1 expanded — All L1 items have L2 items, L3 only when L1 active • all-I1 — All current L1 items shown to L3 • No navigation
Page Heading	Additional custom heading text to display at the very top of the page.
Font Family	List of fonts to use as the font family.
(Color fields)	Specify the colors and highlight colors for various areas. To change a color in any of the color fields, click the color sample box to open the color picker. Set a color, then click Select in the color picker for that item. Repeat for each color you want to change. <ul style="list-style-type: none"> • Welcome Background Color — Background color for the welcome block • Welcome Foreground Color — Foreground color for the welcome block • Welcome Highlight — Highlight color for the name • Network Color — Color for the network area • Network Highlight — Highlight color for the network • Instructions Color — Color for the instructions • Instructions Highlight — Highlight color for the instructions
Save Configuration	Saves your changes.

The default skin used by the ClearPass Guest application is the one that is enabled in the Plugin Manager. To change the default skin globally, go to the plugin list and click the **Enable** link for the skin you would like to use as the default. When you install a new custom skin, it is automatically enabled and becomes the default skin. If your application's appearance does not automatically change, find the custom plugin in the list, click **Configure**, and click its **Enable** link. If you prefer to use the standard Aruba ClearPass skin, navigate to it in the **Available Plugins** list and click its **Enable** link.

The default skin is displayed on all visitor pages, and on the login page if no other skin is specified for it. However, you can override this for a particular operator profile, an individual operator, or give the login page a different appearance than the rest of the application. You can also specify a skin for guest self-registration pages.

- To use a different skin for a particular operator profile, see ["Creating an Operator Profile" on page 673](#).
- To use a different skin for an individual operator login, see ["Local Operator Authentication" on page 680](#).
- To have the login page use a different skin than the rest of the application, see ["Operator Logins Configuration" on page 668](#).
- To specify a skin for a customized guest self-registration page, see ["Configuring Basic Properties for Self-Registration" on page 350](#).

Configuring the Guest Manager Plugin

The **Configure Guest Manager** plugin configuration form lets you control the default settings for account creation.

To modify settings for the Guest Manager plugin configuration, go to **Configuration > Guest Manager**. The **Configure Guest Manager** form opens.

You can also access this form from the **Administration > Plugin Manager > Guest Manager > Configuration** link.

Figure 448 *The Configure Guest Manager Form, Username Options Area*

Configure Guest Manager	
Username Options	
* Username Type:	<input type="text" value="Random digits"/> <small>The method used to generate random account usernames.</small>
* Username Length:	<input type="text" value="8"/> <small>The length, in characters, of generated account usernames.</small>
Username Example:	29087953 Generate
Initial Sequence:	<input type="text"/> <small>Create multi next available sequence number. These values will be used when multi_initial_sequence is set to -1.</small>

Table 292: *Configure Guest Manager Form, Username Options Area*

Field	Description
Username Type	(Required) Specifies the default method used to generate random account usernames (when creating groups of accounts). This may be overridden by using the random_username_method field.
Username Length	(Required) Default length of random account usernames (when creating groups of accounts). This may be overridden by using the random_username_length field. This field is displayed if the Username Type is set to "Random digits", "Random letters", "Random letters and digits" or "Sequential numbering".
Username Example	Displays a sample username generated according to the rules specified by the selections in the Username Type and Username Length fields. You can click the Generate link to view different examples.
Username Format	Specifies the format of the username to be created. This field is displayed if the Username Type is set to "Format picture". See " Format Picture String Symbols " on page 736 for a list of the special characters that may be used in the format string. This may be overridden by using the random_username_picture field.
Initial Sequence	This field contains the next available sequence number for each username prefix that has been used. Automatic sequence numbering is used when the value of the multi_initial_sequence field is set to -1. The username prefix is taken from the multi_prefix field when usernames are automatically generated using the "nwa_sequence" method. You can edit the values stored here to change the next sequence numbers that will be used. This is an automatically managed field; in most situations there is no need to edit it.

Figure 449 *The Configure Guest Manager Form, Password Options Area*

Password Options	
* Random Password Type:	<input type="text" value="Random digits"/> The method used to generate a random account password.
* Random Password Length:	<input type="text" value="8"/> Number of characters to include in randomly-generated account passwords.
* Password Complexity:	<input type="text" value="No password complexity requirement"/> Password complexity to enforce for manually-entered guest passwords. Requires the random password type 'A password matching the password complexity requirements' and the field validator 'NwaisValidPasswordComplexity' for manual password entry.
* Minimum Password Length:	<input type="text" value="8"/> The minimum number of characters that a guest password must contain.
* Disallowed Password Characters:	<input type="text"/> Characters which cannot appear in a user-generated password.
Disallowed Password Words:	<input type="text"/> Comma separated list of words disallowed in the random words password generator. Note there is an internal exclusion list built into the server.
Password Example:	33248842 Generate
Password Logging:	<input checked="" type="checkbox"/> Log guest account passwords Whether to record passwords for guest accounts in the application log.
Password Display:	<input type="checkbox"/> View guest account passwords If selected, guest account passwords may be displayed in the list of guest accounts. This is only possible if operators have the View Passwords privilege.

Table 293: *Configure Guest Manager Form, Password Options Area*

Field	Description
Random Password Type	(Required) Default method used to generate random account passwords (when creating groups of accounts). This may be overridden by using the random_password_method field.
Random Password Length	(Required) Default length of random account passwords (when creating groups of accounts). This may be overridden by using the random_password_length field.
Password Format	(Required) Specifies the format of the password to be created. This may be overridden by using the random_password_picture field. This field is displayed if the Password Type field is set to "Format picture". See " Format Picture String Symbols " on page 736 for a list of the special characters that may be used in the format string.
Password Complexity	(Required) Policy to enforce when guests change their account passwords using the guest self-service user interface. Different levels of password complexity can require guests to select passwords that contain different combinations of uppercase letters, lowercase letters, digits and symbols (!#\$%&()*+,-./:;<=>?@[\\]^_{ }~),. Options include: <ul style="list-style-type: none"> • No password complexity requirement • At least one uppercase and one lowercase letter • At least one digit • At least one letter and one digit • At least one of each: uppercase letter, lowercase letter, digit • At least one symbol • At least one of each: uppercase letter, lowercase letter, digit, and symbol
Minimum Password Length	(Required) Minimum acceptable password length for guests changing their account passwords. The original default password length is six characters.
Disallowed	(Required) Special characters that should not be allowed in a guest password. Spaces are not

Table 293: *Configure Guest Manager Form, Password Options Area(Continued)*

Field	Description
Password Characters	allowed by default. You can specify special characters, numbers, and letters to exclude from passwords—for example, letters and numbers that can look similar, such as i, l, 1, 0, O, o, 5, S, 8, B.
Disallowed Password Words	Comma- separated list of words that are disallowed and will not be created by the random words password generator.
Password Example	Displays a sample password generated according to the rules specified by the selections in the Password Type and Password Length fields. You can click the Generate link to view different examples.
Password Logging	If selected, passwords for created guest accounts are logged in the application log and may be recovered from there. For increased security, you may prevent this password from being logged by deselecting this check box.
Password Display	If selected, enables the display of visitor account passwords in the user list. To reveal passwords, the password field must be added to the “guest_users” or “guest_edit” view, and the operator profile in use must also have the View Passwords privilege.

Figure 450 *The Configure Guest Manager Form, Expiration Options Area*

Expiration Options

* **Expire Action:** Disable at specified time
Default action to take when the expire_time is reached.
 Note that a logout can only occur if the NAS is RFC-3576 compliant.

* **Expiration Options:** 1 | 1 hour
2 | 2 hours
3 | 3 hours
4 | 4 hours
6 | 6 hours
8 | 8 hours
12 | 12 hours
16 | 16 hours
20 | 20 hours
The available options to select from when choosing the expiration time of a guest account (expire_after).
 Expiration times are specified in hours.

* **Modify Expiration Options:** none | Account will not expire
now | Now
plus 1h | Lengthen expiration time
by 1 hour
plus 1d | Lengthen expiration time
by 1 day
plus 1w | Lengthen expiration time
by 1 week
minus 1h | Shorten expiration time
The available options to select from when modifying an account's expiration (modify_expire_time).
 Note some items may be dynamically removed based on the state of the account.

* **Lifetime Options:** 0 | N/A
60 | 1 hour
120 | 2 hours
180 | 3 hours
240 | 4 hours
360 | 6 hours
480 | 8 hours
720 | 12 hours
1440 | 1 day
The available options to select from when choosing the lifetime of a guest account (expire_postlogin).
 Lifetime values are specified in minutes.

Table 294: *Configure Guest Manager Form, Expiration Options Area*

Field	Description
Expire Action	(Required) Default action when the expiration time is reached. Available options available are: <ul style="list-style-type: none"> ● Disable at specified time ● Delete and logout at specified time ● Delete at specified time ● Disable and logout at specified time
Expiration Options	(Required) The options that should be available to select from when choosing the expiration time of a guest account (expire_after). These options are displayed as the values of the “Expires After” field when creating a user account. Values are in hours for relative account expiration times.
Modify Expiration Options	(Required) The options that should be available to select from when modifying an account's expiration (modify_expire_time). Some items may be dynamically removed based on the state of the account.
Lifetime Options	(Required) The options that should be available to select from when choosing the lifetime for a guest account (expire_postlogin). These options are displayed as the values of the “Account Lifetime” field when creating a user account. Values are in minutes for relative account lifetimes.

Figure 451 *The Configure Guest Manager Form, Expiration Warning Options Area*

Expiration Warning Options

Account Expiry Warning: Notify users before their user credentials expire
If checked users will receive an email notification when their device's network credentials are due to expire.

* If Email is Unknown:
Specify where to send emails to if the users account doesnt have an email address recorded

* Subject Line:
Enter a subject for the notification email.

* Email Message:
The plain text or HTML print template to use when generating an email message

* Email Skin:
The format in which to send email receipts

* Send Copies:
Specify when to send to the recipients in the Copies To list.

Table 295: *Configure Guest Manager Form, Expiration Warning Options Area*

Field	Description
Account Expiry Warning	If selected, users will receive an email notification before their device's network credentials are about to expire. Expiration warning configuration options are added to the form.
Account Expiry Notification	(Required) Number of days before account expiration that the notification email will be sent. You may specify a number from 1 through 30.
If Email is Unknown	(Required) Specifies where to send emails if the user's account does not have an email address recorded. Options include: <ul style="list-style-type: none"> ● Do not send any message ● Send a message to a fixed email address ● Send a message to username@domain
Subject Line	(Required) Enter the subject line for the notification email.
Email	(Required) Specifies the print template to use when generating the email message. Options

Table 295: *Configure Guest Manager Form, Expiration Warning Options Area(Continued)*

Field	Description
Message	include: <ul style="list-style-type: none"> ● Account List ● Certificate Expiry ● Download Receipt ● Guest Account Expiry ● GuestManager Receipt ● One account per page ● SMS Receipt ● SMS Sponsor Confirmation Alert ● Sponsorship Confirmation ● Two-column scratch cards
Email Skin	(Required) Specifies the format for the email receipts. Options include: <ul style="list-style-type: none"> ● No skin - Plain text only ● No skin - HTML only ● No skin - Native receipt format ● Use the default skin ● Aruba ClearPass Skin ● Blank Skin ● ClearPass Guest Skin ● Custom Skin 1 ● Custom Skin 2 ● Galleria Skin ● Galleria Skin 2
Send Copies	(Required) Specifies when to send to recipients in the Copies To list. Options include: <ul style="list-style-type: none"> ● Do not send copies ● Always send using "cc:" ● Always send using "Bcc:"

Figure 452 *The Configure Guest Manager Form, Receipt Options Area*

Receipt Options	
Site SSID:	<input type="text" value="Aruba"/> <p><small>The SSID of the wireless LAN, if applicable. This will appear on guest account print receipts.</small></p>
Site WPA Key:	<input type="text"/> <p><small>The WPA key for the wireless LAN, if applicable. This will appear on guest account print receipts.</small></p>
Receipt Printing:	<input type="checkbox"/> Require click to print <small>Guest receipts can print simply by selecting the template in the dropdown, or by clicking a link.</small>

Table 296: *Configure Guest Manager Form, Receipt Options Area*



Field	Description
Site SSID	Public name of the wireless local area network (WLAN). The default setting for this field is Aruba , and can be changed. The site SSID is displayed in the guest receipt as the WiFi Network , shown below this table.
Site WPA Key	Encryption key used to secure the wireless network. If a value is entered in this field, it will appear on guest print receipts.
Receipt Printing	<p>If selected, the receipt page provides a drop-down list of print templates and a Print link that must be clicked to display the account receipt:</p> <div style="border: 1px solid #ccc; padding: 5px; margin: 5px 0;"> Select a print template... ▼  Print </div> <p>If this option is <u>not</u> selected, the default behavior is to provide a drop-down list of print templates and to open a new window when one is selected:</p> <div style="border: 1px solid #ccc; padding: 5px; margin: 5px 0;">  Open print window using template... ▼ </div>

Figure 453 *Example Guest Receipt, Showing Site SSID Displayed as the WiFi Network*



Figure 454 The Configure Guest Manager Form, General Options Area

Table 297: Configure Guest Manager Form, General Options Area

Field	Description
Terms of Use URL	<p>URL of a terms and conditions page provided to sponsors. The default, terms.php, displays the preconfigured Web page provided at Configuration > Pages > Web Pages > Terms and Conditions. You can edit that page, or you can use Content Manager to upload an HTML file describing the terms and conditions of use (See "Managing Content: Private Files and Public Files" on page 274).</p> <ul style="list-style-type: none"> • If your site is hosted externally, be sure the proper access control lists (ACLs) are in place. • If terms are required, it is best practice to edit the terms field on you forms to a UI type "hidden" and an initial value of 1.
Active Sessions	<p>Default maximum number of active sessions that should be allowed for a guest account. This may be overridden by using the simultaneous_use field when creating or editing a guest account.</p>
About Guest Network Access	<p>Specifies the template code to display on the Guest Manager start page under the "About Guest Network Access" heading.</p> <ul style="list-style-type: none"> • To use the default text, leave this field blank. • To specify custom text, select an item in the drop-down list. • To remove the default text and the heading, enter a single hyphen (-) in this field.

Configuring the IP Phone Services Plugin

The Cisco IP Phone Services plugin configuration allows you to configure debugging levels for Cisco IP Phone service requests. The higher the debugging level, the more information will be included in the application log.

To view or configure the Cisco IP Phone Services plugin:

1. Go to **Administration > Plugin Manager**. The **Available Plugins** list opens.
2. Scroll to the **Standard Plugins > Cisco IP Phone Services** row and click its **Configuration** link. The **Configure Cisco IP Phone Services** form opens.

Figure 455 The IP Phone Services Plugin Configuration Form

Table 298: *Configure Cisco IP Phone Services Plugin Form*

Field	Description
Debugging	(Required) Specifies the debugging level for Cisco IP Phone service requests. Higher levels provide more information in the application log. Options include: <ul style="list-style-type: none"> • 0 — No debugging output • 1 — Log requests • 2 — Log requests with full details
Save Configuration	Saves your changes.

Configuring the Kernel Plugin

The Kernel Plugin provides the basic framework for the application. Settings you can configure for this plugin include the application title, the debugging level, the base URL, and the application URL, and autocomplete.

To view or configure the Kernel plugin:

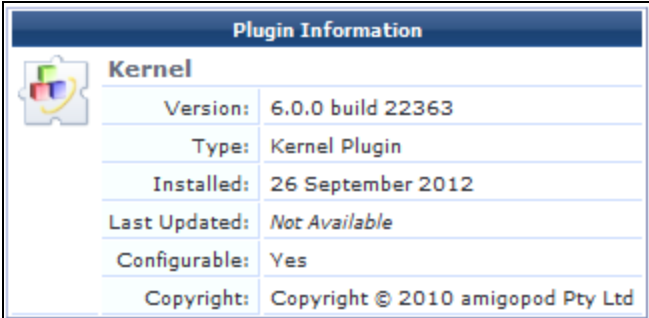
1. Go to **Administration > Plugin Manager**. The **Available Plugins** list opens.
2. Scroll to the **Kernel Plugins > Kernel** row and click its **Configuration** link. The **Configure Kernel** form opens.

Figure 456 *The Kernel Plugin Configuration Form*

Configure Kernel 6.1.0-24093

* Application Title:	<input style="width: 90%;" type="text" value="Unified Visitor Management"/> <small>The title of the web application. This is displayed as the title of the main page.</small>
* Debug Level:	<input style="width: 50%;" type="text" value="1"/> <small>Debugging level for the application. Zero is off, 1 logs PHP messages, and 2 logs PHP messages with full debugging details.</small>
Application URL:	<input style="width: 90%;" type="text"/> <small>Base URL for the application.</small>
* Form Auto Complete:	<input type="checkbox"/> Request browsers to not save password information <small>Select this option if your policy is to never remember form fields and credentials.</small>
* Security:	<input checked="" type="checkbox"/> Enable protection against 'Clickjacking' attacks (recommended) <small>Select this option to prevent the web application from being used from within another frame.</small>
* SSL Verification:	<input type="checkbox"/> Allow insecure outbound HTTPS connections <small>Select this option to allow access to secure web sites providing an invalid certificate. Outbound access includes SMS, APIs, etc.</small>

Table 299: *Configure Kernel Plugin Form*

Field	Description
Application Title	Name to display as the title of your Web application (for example, your company name).
Debug Level	The Debug Level and Application URL options should not be modified unless you are instructed to do so by Aruba support.
Application URL	
Form Auto Complete	If selected, turns turn off autocomplete on forms. Selecting this option will disable credentials caching.
Security	If selected, enables protection against clickjacking attacks and prevents the Web application from being used from within another frame.
Template Scripting	Specifies allowing {php} tags in template processing. Options include: <ul style="list-style-type: none"> • Secure • Insecure — Enable templating engine • Warn — Allow but log usage of restricted calls
SSL Verification	If selected, allows access to secure Web sites providing an invalid certificate.
Default Language	Specifies the default language for the application. Options include: <ul style="list-style-type: none"> • Arabic Translations • Chinese Translations • Danish Translations • Dutch Translations • English Translations • French Translations • German Translations • Japanese Translations • Korean Translations • Spanish Translations
Save Configuration	Saves your changes.
Restore default configuration	<p>Restores the plugin's configuration to the original settings. A message alerts you that the change cannot be undone, and a comparison of the current and default settings highlights the changes that will be made.</p>  <p>Review the differences between the current settings and the default configuration. To commit the change to the default settings, click the Restore Default Configuration link.</p>

Configuring the MAC Authentication Plugin

Different vendors format the client MAC address in different ways—for example:

- 112233AABBCC
- 11:22:33:aa:bb:cc
- 11-22-33-AA-BB-CC

ClearPass Guest supports adjusting the expected format of a MAC address. To configure formatting of separators and case in the address, as well as user detection and device filtering for views, go to **Administration > Plugin Manager** and click the **Configuration** link for the **MAC Authentication** plugin. The **MAC Authentication Configuration** page opens.

Figure 457 MAC Authentication Plugin Configuration

Table 300: The Configure MAC Authentication Form

Field	Description
MAC Detect	(Required) If selected, users can be detected by their MAC address, providing access to user configuration for headers, footers, etc. on login and registration pages. Requires a vendor that passed the MAC address as part of the redirect. Because a passed MAC address can easily be changed by the user, personal details should not be displayed.
Device Filter	Specifies which views should not display devices (user accounts with the “mac_auth” field set). Views that can be specified include: <ul style="list-style-type: none"> • Manage Accounts • Manage Multiple Accounts
Save Configuration	Saves your changes.

On the controller, the fields look as follows:

Figure 458 MAC Authentication Profile

Configuring the Platform Services Plugin

The **Platform Services** plugin may be used to set default options for ClearPass platform services.

To view or configure platform services options:

1. Go to **Administration > Plugin Manager**. The **Available Plugins** list opens.
2. Scroll to the **Standard Plugins > Platform Services** row and click its **Configuration** link. The **Configure Platform Services** form opens.

Figure 459 *The Configure Platform Services Form*

The screenshot shows a web form titled "Configure Platform Services 6.6.0-31971". It contains two main sections, each with a label, a text input field, and a description. The first section is "Captive Portal Whitelist" with the value "/AppleTV/" and a description: "Regular expression used to match the User-Agent header of captive portal clients. Clients that match this expression will be shown the captive portal without any redirects." The second section is "Captive Portal Blacklist" with the value "/Skype WISPr/" and a description: "Regular expression used to match the User-Agent header of captive portal clients. Clients that match this expression will be denied access to the captive portal." At the bottom of the form is a "Save Configuration" button.

Table 301: *Configure Platform Services Form*

Field	Description
Captive Portal Whitelist	Regular expression used to match the User-Agent header of captive portal clients. Clients that match this expression will be shown the captive portal without any redirects. You can enter a list of regular expressions used to match the User-Agent headers of captive portal clients, separated by the forward-slash character (/).
Captive Portal Blacklist	Regular expression used to match the User-Agent header of captive portal clients. Clients that match this expression will be denied access to the captive portal. You can enter a list of regular expressions used to match the User-Agent headers of captive portal clients, separated by the forward-slash character (/).
Save Configuration	Saves your changes to this form.

Configuring the SMS Services Plugin

The SMS Services plugin configuration allows you to configure options related to SMS receipts. You may also configure SMS receipt options in the Customization module (see "[Customizing SMS Receipt](#)" on page 442).

To view or configure SMS services and receipt options:

1. Go to **Administration > Plugin Manager**. The **Available Plugins** list opens.
2. Scroll to the **Standard Plugins > SMS Services** row and click its **Configuration** link. The **Configure SMS Services** form opens.

Figure 460 *The SMS Services Plugin Configuration Form*

Configure SMS Services 6.0.1-22673

Service Provider: Test ▼
The default SMS gateway to use when sending SMS messages.

Receipt Options
Select options for the SMS receipt.

SMS Receipt: SMS Receipt ▼
The plain-text format print template to use when generating an SMS receipt.

Fields
Select the visitor account fields related to the SMS receipt.

Phone Number Field: visitor_phone ▼
The field containing the visitor's phone number.

Auto-Send Field: visitor_phone ▼
The field which, if it contains a non-empty string or non-zero value, will cause an account receipt SMS to be automatically sent upon creation of a visitor account.

* Credit Warning: 50
When the number of available credits reaches this threshold, a warning message is sent to the system administrator.

* Advanced Gateways: Allow advanced SMS handlers
Select this option to create more types of SMS gateways and define custom SMS gateways.

* SMS via SMTP: Enable management of SMTP Carrier List
Select this option to enable support for sending SMS messages via SMTP (e-mail).

Phone Number Normalization
Options for the NwaNormalizePhoneNumber conversion function.

Default Number Format: Use the visitor's value ▼
Optionally force the addition or removal of a country code.

Save Configuration

Table 302: *Configure SMS Services Plugin Form*

Field	Description
Service Provider	Specifies the default SMS gateway to use when sending messages. Options include ClearPass Guest SMS and any other gateways that have been configured.
SMS Receipt	Specifies the plain-text format print template to use when an SMS receipt is generated. Options include: <ul style="list-style-type: none"> • ClearPass demo SMS Receipt • Download Receipt • SMS Receipt • SMS Sponsor Confirmation Alert
Phone Number Field	Specifies the guest account field that contains the guest's mobile telephone number. This field is used to determine the SMS recipient address.
Auto-Send Field	Specifies the guest account field which, if set to a non-empty string or non-zero value, will trigger an automatic SMS when the guest account is created or updated. The auto-send field can be

Table 302: Configure SMS Services Plugin Form(Continued)

Field	Description
	used to create an “opt-in” facility for guests. Use a check box for the auto_send_sms field and add it to the create_user form, or a guest self-registration instance, and SMS messages will be sent to the specified phone number only if the check box has been selected.
Credit Warning	(Required) The number of available credits at which a warning is sent. When the remaining number of SMS credits reaches this threshold, the system will send a warning to the system administrator.
Sponsor Phone Number Field	Specifies the field containing the sponsor’s phone number.
Sponsor SMS Receipt	Specifies the plain-text format print template to use when an SMS receipt is generated.
Advanced Gateways	If selected, lets you configure SMS gateways from multiple SMS providers and define custom gateways. For more information, see "Creating or Editing an SMS Gateway" on page 454 .
SMS via SMTP	If selected, enables support for sending SMS messages by SMTP. Visitor account receipt messages will be sent in an email using the defined SMTP server.
Default Number Format	Specifies forcing the addition or removal of a country code. Otherwise, the phone number normalization process translates phone strings that are entered in various formats into a single standard format. Options include: <ul style="list-style-type: none"> • Use the visitors value — When you select this option, the SMS gateway will always send the SMS message using the phone number and country code entered by the visitor. • Always include the country code — When you select this option, the SMS gateway will always send the SMS message using the global country code and default phone number length specified in the Default Country Code and Default Phone Length fields. For example, consider an Australian mobile phone number with a default number length of 9 plus a leading zero, and a country code of 61. If you selected the Always include the country code option, the Australian mobile number <i>0412345678</i> would normalize to <i>+61412345678</i> in the internationalized format. • Never include the country code — When you select this option, any country code specified by the visitor is removed before the SMS message is sent.
Default Country Code	The global country code used for phone number normalization.
Default Phone Length	The number of digits required to normalize the phone number. To ignore the length, enter a value of 0 .
Save Configuration	Saves your changes.



ClearPass Guest 3.9 and earlier used www.amigopod.com for a number of actions, including updates, SMS, and network diagnostics. The address used now is clearpass.arubanetworks.com. If you have host-specific openings in your firewall for the ClearPass appliance, please update them to the new address.

Configuring the SMTP Services Plugin

The **SMTP Services** plugin may be used to set default options for SMTP Services and email receipts.

To view or configure SMTP services options:

1. Go to **Administration > Plugin Manager**. The **Available Plugins** list opens.
2. Scroll to the **Standard Plugins > SMTP Services** row and click its **Configuration** link. The **Configure SMTP Services** form opens.

Figure 461 *The Configure SMTP Services Form*

Configure SMTP Services 6.6.0-31918	
Receipt Options Select options for the email receipt.	
Subject Line:	<input type="text" value="Visitor account receipt for {\$email}"/> Template specifying the subject line for visitor account receipts sent by email.
* Email Receipt:	<input type="text" value="GuestManager Receipt"/> The plain text or HTML print template to use when generating an email receipt.
* Skin:	<input type="text" value="Use the default skin"/> The format in which to send email receipts.
Copies To:	<input type="text"/> An optional list of email addresses to which copies of visitor account receipts will be sent. Enter '_admin' to have the email sent to the sponsor's email address.
* Send Copies:	<input type="text" value="Use 'Bcc:' if sending to a visitor"/> Specify when to send visitor account receipts to the recipients in the Copies To list.
Reply-To:	<input type="checkbox"/> Allow the reply-to address to be overridden per operator If checked, the reply-to address will be overridden by the sponsor_email field of a user, or the admin's email. Leave unchecked to use the global from address.
Fields Select the visitor account fields related to the email receipt.	
* Email Field:	<input type="text" value="email"/> The field containing the visitor account's email address.
* Auto-Send Field:	<input type="text" value="auto_send_smtp"/> The field which, if it contains a non-empty string or non-zero value, will cause an account receipt email to be automatically sent upon creation of a visitor account.
Sponsorship Confirmation Global settings for sponsored access.	
Request Subject Line:	<input type="text" value="Wireless access request from: {\$email}"/> Template specifying the subject line for sponsorship requests.
* Sponsorship Receipt:	<input type="text" value="Sponsorship Confirmation"/> The plain text or HTML print template to use when sending a sponsorship request.
Request Subject Line:	<input type="text" value="Device provisioning request from: {if \$email}{\$email}{else}{\$usemame}{/if}"/> Template specifying the subject line for sponsored Onboard requests.
* Sponsorship Receipt:	<input type="text" value="Sponsor Device Provisioning"/> The plain text or HTML print template to use when sending a sponsored Onboard request.
<input type="button" value="Save Configuration"/>	

Table 303: Configure SMTP Services Form

Field	Description
Subject Line	Template specifying the subject line for visitor account receipts sent by email. May contain template code, including references to guest account fields. The default value, Visitor account receipt for { \$email } , uses the value of the email field. See " Smarty Template Syntax " on page 700 for more information on template syntax.
Email Receipt	(Required) Specifies the plain text or HTML template to use for the email receipt.
Skin	<p>(Required) Specifies the email format or skin to use to provide the basic appearance of the email. Options include:</p> <ul style="list-style-type: none"> ● No skin – Plain text only – A skin is not used, and the email will be sent in plain text format. Use this option to remove all formatting from the email. ● No skin – HTML only – A skin is not used, but the email will be sent in HTML format. Use this option to provide a basic level of formatting in the email. ● No skin – Native receipt format – A skin is not used. The email will be sent in either plain text or HTML format, depending on the type of print template that was selected. ● Use the default skin – The skin currently marked as the default skin is used. ● Aruba ClearPass Skin ● Blank Skin ● ClearPass Guest Skin ● Custom Skin 1 ● Custom Skin 2 ● Galleria Skin ● Galleria Skin 2 <p>When sending an email message using HTML formatting, the images and other resources required to display the page will be included in the message.</p>
Copies To	Creates an optional list of additional email addresses that are designated to receive copies of the generated email receipts. To have the email receipt sent to the sponsor's email address, enter the keyword _admin in this field. In this case the email receipt will be sent to the current operator.
Send Copies	<p>(Required) Specifies how copies of the email receipts will be sent to the additional email addresses listed in the Copies To field:</p> <ul style="list-style-type: none"> ● Do not send copies – The Copies To list is ignored and email is not copied. ● Always send using 'cc:' – The Copies To list is always sent a copy of any guest account receipt (even if no guest account email address is available). ● Always send using 'bcc:' – The Copies To list is always sent a blind copy of any guest account receipt (even if no guest account email address is available). ● Use 'cc:' if sending to a visitor – If a guest account email address is available, the email addresses in the Copies To list will be copied. ● Use 'bcc:' if sending to a visitor – If a guest account email address is available, the email addresses in the Copies To list will be blind copied.
Reply-To	If selected, the Reply-To address will be overridden by the sponsor_email field

Field	Description
	of the user, or by the admin's email. When you select this check box, the Override From field is added to the form. To use the global From Address, do <i>not</i> select the check box in this field.
Override From	If selected, overrides the From Address instead of using the Reply-To value.
Email Field	(Required) Specifies the field that will contain the visitor's email address.
Auto-Send Field	(Required) Specifies the field that will cause an account receipt email to be automatically sent when a visitor account is created. The email receipt will only be sent if the field selected here contains a non-empty string of non-zero value.
Request Subject Line	Template specifying the subject line for sponsorship requests.
Sponsorship Receipt	Specifies the plain text or HTML print template to use when sending a sponsorship request. Options include: <ul style="list-style-type: none"> ● Account List ● Certificate Expiry ● Download Receipt ● Guest Account Expiry ● GuestManager Receipt ● One account per page ● SMS Receipt ● SMS Sponsor Confirmation Alert ● Sponsor Device Provisioning ● Sponsorship Confirmation ● Two-column scratch cards
Request Subject Line	Template specifying the subject line for sponsored Onboard requests.
Sponsorship Receipt	Specifies the plain text or HTML print template to use when sending a sponsored Onboard request. Options include: <ul style="list-style-type: none"> Account List Certificate Expiry Download Receipt Guest Account Expiry GuestManager Receipt One account per page SMS Receipt SMS Sponsor Confirmation Alert Sponsor Device Provisioning Sponsorship Confirmation Two-column scratch cards
Save Configuration	Saves your changes to this form.

Configuring the Translations Plugin


The Translation Assistant plugin shows the current version, type, original installation date, date of last update, whether it can be configured, and the copyright date. The Translation Assistant plugin cannot be configured.

To view the Translation Assistant plugin:

1. Go to **Administration > Plugin Manager**. The **Available Plugins** list opens.

2. Scroll to the **Standard Plugins > Translation Assistant** row and click its **About** link. The **Plugin Information** form opens.

Figure 462 *The Translation Assistant Plugin Information View*

Plugin Information	
	Translation Assistant
Version:	6.4.0 build 30420
Type:	Standard Plugin
Installed:	30 July 2014
Last Updated:	<i>Not Available</i>
Configurable:	No
Copyright:	Copyright © 2008 amigopod Pty Ltd

By default, the display language for the ClearPass Guest user interface is automatically detected based on the user's browser settings. To enable or disable language packs, set a default language for ClearPass Guest, or customize label and message text, see "[About Translations](#)" on page 465.

Configuring the Web Analytics Plugin

The Web Analytics plugin configuration allows you to configure a tracking code and specify which pages should include it.

To view or configure the Web Analytics plugin:

1. Go to **Administration > Plugin Manager**. The **Available Plugins** list opens.
2. Scroll to the **Standard Plugins > Web Analytics** row and click its **Configuration** link. The **Configure Web Analytics** form opens.

Figure 463 *The Web Analytics Plugin Configuration Form*

Configure Web Analytics 6.6.0-31823

Tracking Code:	<div style="border: 1px solid #ccc; height: 80px; width: 100%;"></div> <p style="font-size: small; color: #003366;">Page tracking code that will be added immediately before the </body> tag. Note: If you use this feature to add page tracking code for guests using a restricted pre-authentication role, be sure to whitelist any required URLs or domains for that role.</p>
* Insert Into:	<div style="border: 1px solid #ccc; padding: 2px;">All pages ▼</div> <p style="font-size: small; color: #003366;">Choose the pages within the application that will receive the tracking code. Operator pages are those for which an operator login is required.</p>


 Save Configuration

Table 304: *Configure Web Analytics Plugin Form*

Field	Description
Tracking Code	The page tracking code to add before the </body> tag. If you use this field to add page tracking code for guests using a restricted pre-authentication role, be sure to whitelist any required URLs or domains for that role.
Insert Into	Specifies the pages in the application that will receive the tracking code. Options include: <ul style="list-style-type: none">• All pages• Operator pages only• Guest access pages only The tracking code will be added immediately before the </body> tag on the specified pages. The tracking code does not collect any user information.
Save Configuration	Saves your changes.

Configuring the SOAP Web Services Plugin

SOAP Web Services provide a way of transferring data across the Internet to integrate Web-based applications. Web services let businesses share data and processes programmatically, and can be added to a user interface to provide functionality.

To configure the SOAP Web Services plugin, do one of the following:

- Go to **Administration > Web Services > Configure Web Services**. The **Configure SOAP Web Services** form opens.

Or:

1. Go to **Administration > Plugin Manager**. The **Available Plugins** list opens.
2. Scroll to the **Standard Plugins > SOAP Web Services** row and click its **Configuration** link. The **Configure SOAP Web Services** form opens.

Figure 464 *The SOAP Web Services Plugin Configuration Form*

Configure SOAP Web Services	
WSDL Access:	<input checked="" type="checkbox"/> Allow anonymous access to WSDL Control whether Web Service Description Language (WSDL) requests require an operator to be logged in.
* Maximum Request Size:	200 <input type="text"/> KB The maximum permissible size of a SOAP request, in kilobytes. Requests larger than this size will be rejected.
* SOAP Debugging:	1 - Log SOAP errors only <input type="text"/> Sets the debugging level for SOAP service requests. Higher levels will cause more information to be logged to the application log.
<input type="button" value="Save Configuration"/>	


Table 305: *Configure SOAP Web Services Plugin Form*


Field	Description
WSDL Access	If selected, allows operators to make (WSDL) requests without being logged in.
Maximum Request Size	Maximum size in kilobytes that will be allowed for a SOAP request. Requests larger than this value will be rejected.
SOAP Debugging	Specifies the debugging level for SOAP service requests. Options include: <ul style="list-style-type: none">• 0 — No debugging output• 1 — Log SOAP errors only• 2 — Log SOAP errors with full request body• 3 — Log all SOAP requests• 4 — Log all SOAP requests with full details
Save Configuration	Saves your changes. The configuration is applied to all SOAP Web Services in the application.


Support



The **Administration > Support** page provides links to ClearPass Guest documentation, the application log, and Aruba Customer Support contact information.

 **Documentation**
View the user's manual, or one of the available network integration guides.

 **Contact Support**
Information about obtaining customer support.

 **View Application Log**
View the application log file. You can choose different log files, search for log records and export the log to different formats here.

Viewing the Application Log



To view events and messages generated by the application, go to **Administration > Support > Application Log**. The **Application Log** view opens.

Figure 465 *The Application Log List View*

Time	IP	User	Severity	Message
2012-12-06 09:28:02	192.0.2.16	admin	info	Updated user account android in the database
2012-12-06 09:26:51	192.0.2.16	admin	warning	PHP Message: strlen() expects parameter 1 to be string, array given
2012-12-06 09:26:51	192.0.2.16	admin	warning	PHP Message: strlen() expects parameter 1 to be string, array given
2012-12-06 03:00:01	192.0.2.16		info	Finished processing data retention policy (0.0 seconds).
2012-12-06 03:00:01	192.0.2.16		info	Processing data retention policy.
2012-12-05 09:52:00	192.0.2.16	admin	info	Modified operator profile: IT Administrators
2012-12-05 09:51:41	192.0.2.16	admin	info	Operator login: admin
2012-12-05 09:51:41	192.0.2.16		debug	Performed eTIPS web-auth request
2012-12-05 09:51:03	192.0.2.16	admin	info	Operator login: admin
2012-12-05 09:51:03	192.0.2.16		debug	Performed eTIPS web-auth request

To view in-depth information about an event, click the event's row. The form expands to show details. Click the event's row again to close it.

Figure 466 *Information Displayed for an Event in the Application Log*

Time	IP	User	Severity	Message
2012-09-26 21:43:26	192.0.2.16	admin	info	Operator login: admin

```

Operator login: admin

Client: 10.240.104.88:63701
App User: admin
Script: /guest/auth_login.php
Function: NwaAuthLoginForm
Details: (
  'user_agent' => 'Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)',
  'auth_source' => 'ClearPass operator logins',
  'profile' => 'IT Administrators',
)
    
```

To view the logs for a different server when in a cluster, use the **Server** drop-down list above the table.

To search for a particular log record, use the **Keywords** field above the table to enter search terms. You can use the hyphen character (-) in front of a keyword to exclude items, and you can use quotes (" ") to group words as a key phrase.

The **Application Log** lists the events, messages, and configuration changes for the past seven days. To view events and messages for a different period, or to limit the search items, click the **Filter** tab. The **Filter Settings** form opens.

Figure 467 *The Filter Settings Form*

Table 306: *Application Log Filter*

Field	Description
Times	Specifies a time period to search.
Severity	Specifies the minimum severity of messages to search for: <ul style="list-style-type: none"> ● Error— Returns Error items ● Warning— Returns Error and Warning items ● Info— Returns Error, Warning, and Info items ● Debug— Returns Error, Warning, Info, and Debug items
Options	If selected, all fields of the log record will be searched. The default setting is to search only the Client IP and Message fields.
Apply Filter	Applies your filter settings and runs a new search. Results are displayed in the Application Log list.
Reset	Cancels your entries in the filter and restores the default filter settings.

Events are stored in the Application Log for seven days by default. To review a record of significant runtime events prior to the last seven days, you can use the Audit Viewer in ClearPass Policy Manager’s Monitoring module.

Exporting the Application Log

To save the log in other formats, click the **Export** tab on the **Administration > Support > Application Log** view. The Application Log expands to include the **Export Application Logs** form.

Figure 468 *The Export Application Logs Form*

Table 307: *Export Application Logs Form*

Field	Description
Format	Specifies the format in which to save the file and export the logs. Options include: <ul style="list-style-type: none"> • Comma-Separated Values (*.csv) — This is the default format • HTML document (*.html) • Tab-Separated Values (*.tsv) • Text file (*.txt) • XML document (*.xml)
Range	Specifies the range of pages to save. Options include: <ul style="list-style-type: none"> • Single page — export the current page only • Multiple from current — start the export from the current page • Multiple from first — start the download from the first page that matched
Download Limit	If you entered a range of pages in the Range drop-down list, the form expands to include the row. Maximum number of log messages to download if you entered a range of pages in the Range field. To download all messages, leave this field empty. Users should be aware that downloading all messages could take a long time.
Export	Exports the log file and downloads it to your system.

Contacting Support

To view contact information for Aruba Support, go to **Administration > Support > Contact Support**. The **Contact Support** page opens. This page provides the following information:

- Toll-free telephone numbers for North American support
- A link to contact Aruba Support by email
- A link to Aruba's online Contact Support page, which includes telephone numbers and other contact information for over 30 countries

Viewing Documentation



To view ClearPass Guest documentation, go to **Administration > Support > Documentation**. The **Documentation** page opens.

- To view this User Guide in your browser as online help, click **Browse Documentation**. The document opens in a separate browser tab.
- To view the User Guide as a PDF, click **Deployment Guide**. The PDF file opens in a separate tab.

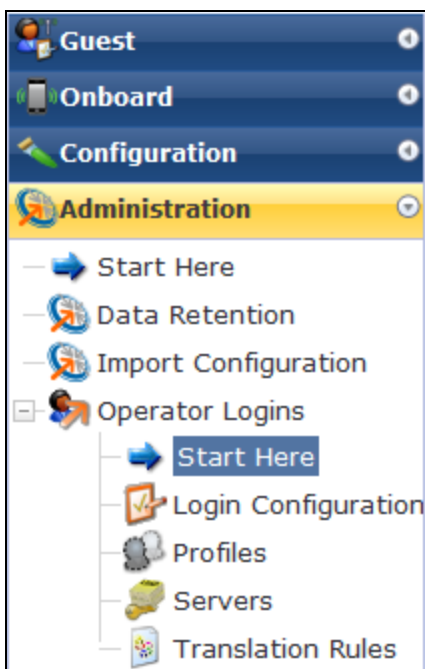


An operator is a company's staff member who is able to log in to ClearPass Guest. Different operators may have different roles that can be specified with an operator profile. These profiles might be to administer the ClearPass Guest network, manage guests, or run reports.

Operators may be defined locally in ClearPass Guest, or externally in an LDAP directory server.

Accessing Operator Logins

To access ClearPass Guest's operator login features, click the **Administration** link in the left navigation, then click **Operator Logins**.



About Operator Logins

ClearPass Guest supports role-based access control through the use of operator profiles. Each operator using the application is assigned a profile which determines the actions that the operator may perform, as well as global settings such as the look and feel of the user interface.

Your profile may only allow you to create guest accounts, or your profile might allow you to create guest accounts as well as print reports. What your profile permits is determined by the network administrator.

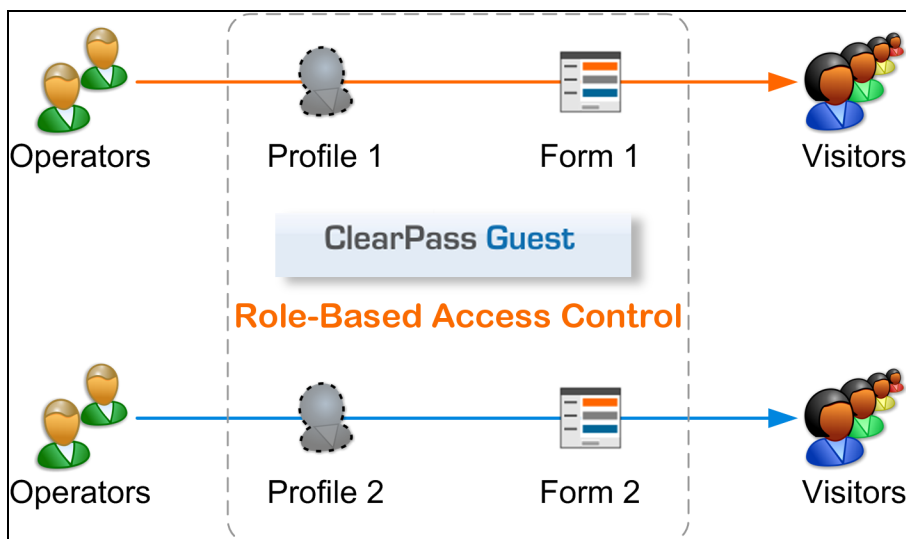
Two types of operator logins are supported: local operators and operators who are defined externally in your company's directory server. Both types of operators use the same login screen.

Role-Based Access Control for Multiple Operator Profiles

Using the operator profile editor, the forms and views used in the application may be customized for a specific operator profile, which enables advanced behaviors to be implemented as part of the role-based access control model.

This process is shown in the following diagram.

Figure 469 Operator Profiles and Visitor Access Control



See ["About Operator Logins"](#) on page 667 for details on configuring different forms and views for operator profiles.

Operator Logins Configuration



You are able to configure a message on the login screen that will be displayed to all operators. This must be written in HTML. You may also use template code to further customize the appearance and behavior of the login screen.

To modify these configuration parameters, go to **Administration > Operator Logins > Login Configuration**. The **Operator Logins Configuration** form opens.

Operator Login UI Area

If you are deploying ClearPass Guest in a multi-lingual environment, options in the **Operator Login UI** area of the form let you specify different login messages depending on the currently selected language.

Figure 470 The Operator Logins Configuration Form, Operator Login UI Area

Table 308: Operator Logins Configuration Form, Operator Login UI Area

Field	Description
Login Message	(Required) HTML for the message that will be displayed in the header of the operator login screen. You can also use the drop-down list to add images or other content items or links (content items must first have been uploaded in Content Manager).
Login Footer	HTML for the message that will be displayed in the footer of the operator login screen. You can also use the drop-down list to add images or other content items or links (content items must first have been uploaded in Content Manager).
Login Skin	Specifies the skin for the operator login screen. Options include: <ul style="list-style-type: none"> • (Default) • Aruba ClearPass Skin • Blank Skin • ClearPass Guest Skin • Custom Skin 1 • Custom Skin 2 • Galleria Skin • Galleria Skin 2

The following example of a custom login message from the demonstration site uses Danish (da), Spanish (es), and the default language English, as highlighted in bold:

```

{if $current_language == 'da'}

<p>
  Indtast brugernavn og password for at <br>
  få adgang til ClearPass Guest
</p>
<p>
  Kontakt <a href="http://www.airwire.dk/">Airwire</a> (Norden) for at få demoadgang
</p>
{elseif $current_language == 'es'}
<p>

```

```

Para entrar en el web demo de ClearPass Guest, <br>
necesitas un nombre y contraseña.
</p>
<p>
Si no tienes un login, puedes obtener uno<br>
<a href="http://www.arubanetworks.com/">contactando con Aruba Networks</a>.
</p>
{else}
<p>
The ClearPass Guest demo site <br>
requires a username and password.
</p>
<p>
If you don't have a login, <br>
<a href="http://www.arubanetworks.com/">contact Aruba Networks</a> to obtain one.
</p>
{/if}
<br clear="all">

```

Advanced Options Area

The **Advanced Options** area lets you configure such things as logging levels, service handler ranking, and session parameters.

Figure 471 The Operator Logins Configuration Form, Advanced Options Area

Advanced Options
 These options do not normally need to be modified.

* Logging:	Log only web logins Select the level of logging to use when the application is accessed.
* Local Priority:	10 The priority rank of the service handler for authentication of local operators. Lower numbers represent higher priorities.
* Logout After:	4 hours The idle timeout for operator login sessions, in hours.
* Session Checking:	Full checking The amount of validity checking to perform on operator login sessions at each page load. Higher settings reduce performance.
* Check Interval:	15 seconds Minimum interval in seconds between checks of a session's validity.

Save Changes

Table 309: Operator Logins Configuration Form, Advanced Options Area

Field	Description
Logging	Specifies the level of logging to use when the application is accessed. Log messages for operator logins, whether successful or unsuccessful, are shown in the application log. Options include: <ul style="list-style-type: none"> • No logging • Log only failed operator login attempts • Log only Web logins • Log only XMLRPC access • Log all access
ClearPass Operator Priority	The priority rank of the service handler for authentication of ClearPass operators. Lower numbers represent higher priorities.
Logout After	Amount of idle time, in hours, after which an operator's session will be ended. You can use

Table 309: *Operator Logins Configuration Form, Advanced Options Area(Continued)*

Field	Description
Session Checking	Specifies the amount of validity checking to perform on operator login sessions at each page load. Higher settings reduce performance. Options include: <ul style="list-style-type: none">• No checking• Check operator is enabled• Full checking
Check Interval	Minimum interval in seconds between checks of a session's validity.
Save Changes	Saves your changes to the login configuration.

Operator Profiles






















An operator profile determines what actions an operator is permitted to take when using ClearPass Guest.

Some of the settings in an operator profile may be overridden in a specific operator's account settings. These customized settings will take precedence over the default values defined in the operator profile.

To define new operator profiles and to make changes to existing operator profiles, go to **Administration > Operator Logins > Profiles**. The **Operator Profiles** list view opens.

Figure 472 The Operator Profiles List View

Name	Description
 AirGroup Administrator	Operators with this profile can manage multiple devices that are shared with all users based on location.
 AirGroup Operator	Operators with this profile can self-provision up to 5 devices within their personal WLAN.
 Show Details  Edit  Delete  Duplicate  Show Usage	
 BYOD Operator	Operators with this profile can view and manage their own provisioned devices
 Device Registration	Operators with this profile can self-provision their devices, for use with MAC authentication and AirGroup sharing.
 Help Desk	A help desk operator logs in to troubleshoot problems reported by end user.
 IT Administrators	Default administrative profile.
 Kiosk-operator	Operators with this profile can create multiple accounts
 MACTrac Operator	Operators with this profile can create devices which could get authenticated by their MAC.
 Network Administrator	A network administrator is allowed to configure all the policies in the system
 Null Profile	Default profile with no permissions.
 Operations and Marketing	Complete profile including print templates and application customization options.
 Read-only Administrator	A Read-only administrator is allowed to view all the policies in the system
 Reception and Front Desk	Limited to creating new accounts and sending receipts only. Defaults to create user form on login.
13 operator profiles  Reload Show all rows ▼	

All operator profiles that have been created are included in the list. You can click a profile's row in the list for additional options:

Table 310: Operator Profiles Options


Field	Description
View Details	Displays or hides configuration details for the selected operator profile, including the profile name, description, operator login access, and the settings for the defined skin, start page, language and time zone.
Hide Details	
Edit	Lets you edit the properties of the specified operator profile.
Delete	Removes the operator profile from the Operator Profiles list. You will be asked to confirm the deletion.
Duplicate	Creates a copy of the operator profile to use as a basis for a new profile.
Show	The form expands to show a list of operator login names associated with that operator profile.

Table 310: *Operator Profiles Options(Continued)*

Field	Description
Operators	
Show Usage	The form expands to show whether the profile is in use, and lists any LDAP authentication servers, LDAP translation rules, and operator logins associated with that profile. Each entry in this window appears as a link to the form that lets you edit that LDAP or operator login setting.
Create a new operator profile	Lets you create a new operator login associated with the selected operator profile. The Create Operator Login form opens.

Creating an Operator Profile



To create a new operator profile, on the **Administration > Operator Logins > Profiles** page, click the  **Create a new operator profile** link.

The **Operator Profile Editor** form opens. This form has several sections, which are described in more detail below.

Figure 473 *The Operator Profile Editor Form, Basic Properties Area*

Operator Profile Editor












* Name:	<input style="width: 90%;" type="text" value="Reception and Front Desk"/> <small>Enter a name for this operator profile.</small>
Description:	<div style="border: 1px solid #ccc; padding: 5px; min-height: 40px;"> Limited to creating new accounts and sending receipts only. Defaults to create user form on login. </div> <small>Comments or descriptive text about the operator profile.</small>
Access	
<small>These options control what operators with this profile are permitted to do.</small>	
Enabled:	<input checked="" type="checkbox"/> Allow operator logins <small>If unchecked, operators with this profile will not be able to log in.</small>

Table 311: *Operator Profile Editor Form, Basic Properties*

Field	Description
Name	(Required) Name for this operator profile. Operator profile names must be unique.
Description	Brief description of or additional information about this operator profile.
Enabled	If selected, allows operators with this profile to log in. To disable the profile, unmark the Allow Operator Logins check box. If a profile is disabled, any operators with that profile will be unable to log in to the system. This can be useful when performing system maintenance tasks.

Figure 474 *The Operator Profile Editor Form, Privileges List*

Operator Privileges

- 
Administrator No Access ▼
Select operator permissions for system administration and management tasks.
- 
Advertising Services No Access ▼
Select operator permissions for managing advertising content and services.
- 
AirGroup Services No Access ▼
Select operator permissions for access to AirGroup services.
- 
API Services No Access ▼
Select operator permissions for API access and management.
- 
Guest Manager No Access ▼
Select operator permissions for managing guest users for a network.
- 
Hotspot Manager No Access ▼
Select operator permissions for managing self-provisioned guest access.
- 
IP Phone Services No Access ▼
Select operator permissions for IP phone administration and management tasks.
- 
Onboard No Access ▼
Select operator permissions for managing Onboard device provisioning.
- 
Operator Logins No Access ▼
Select permissions for managing local operator logins.
- 
Pass Services No Access ▼
Select operator permissions for managing digital passes.
- 
Platform No Access ▼
Select operator permissions for platform administration tasks.
- 
SMS Services No Access ▼
Select operator permissions for access to SMS services.
- 
SMTP Services No Access ▼
Select operator permissions for SMTP services.
- 
Support Services No Access ▼
Select operator permissions for access to support services.
- 
Translation Assistant No Access ▼
Select operator permissions for tasks related to translation.

Show descriptions

Table 312: *Operator Profile Editor Form, Privileges List*

Field	Description
Privileges	<p>For each ClearPass Guest functionality area, specifies the appropriate permissions for this operator profile. The default in all cases is No Access. This means that you must select the appropriate privileges in order for the profile to work. Options include:</p> <ul style="list-style-type: none"> ● No Access — Default ● Read Only Access ● Full Access ● Custom — The form expands to include additional privileges specific to that item. Select the appropriate permission level for each additional option. <p>For details about the available access levels for each privilege, see "Operator Profile Privileges" on page 679.</p>

Figure 475 The Operator Profile Editor Form, Access Area

User Roles:	<table border="1"> <thead> <tr> <th colspan="2">Name</th> </tr> </thead> <tbody> <tr> <td><input checked="" type="checkbox"/></td> <td> ClearPass Policy Manager</td> </tr> <tr> <td><input type="checkbox"/></td> <td>[Contractor]</td> </tr> <tr> <td><input type="checkbox"/></td> <td>[Guest]</td> </tr> <tr> <td><input type="checkbox"/></td> <td>[Employee]</td> </tr> </tbody> </table> <p style="text-align: right;">10 rows per page ▼</p> <p>Select the visitor account roles that these operators are permitted to use.</p>	Name		<input checked="" type="checkbox"/>	ClearPass Policy Manager	<input type="checkbox"/>	[Contractor]	<input type="checkbox"/>	[Guest]	<input type="checkbox"/>	[Employee]
Name											
<input checked="" type="checkbox"/>	ClearPass Policy Manager										
<input type="checkbox"/>	[Contractor]										
<input type="checkbox"/>	[Guest]										
<input type="checkbox"/>	[Employee]										
* Operator Filter:	<p>No operator filter ▼</p> <p>Select the default operator filtering to apply to guest accounts.</p>										
User Account Filter:	<p><input type="text"/></p> <p>Enter a comma-delimited list of field=value pairs to create an account filter.</p>										
Session Filter:	<p><input type="text"/></p> <p>Enter a comma-delimited list of field=value pairs to create a session filter.</p>										
Account Limit:	<p><input type="text"/></p> <p>Maximum number of accounts the operator can create. Leave blank for no limit.</p>										

Table 313: Operator Profile Editor Form, Access Area

Field	Description
User Roles	<p>If selected, each check box specifies a user databases and visitor account role that operators with this operator profile can access. Options include:</p> <ul style="list-style-type: none"> • [Contractor] • [Guest] • [Employee] • [PersonalDevice] <p>If one or more roles are selected, then only those roles will be available for the operator to select from when creating a new guest account. The guest account list is also filtered to show only guest accounts with these roles.</p> <p>If a database is selected in the User Roles list but no roles within that database are selected, then all roles defined in the database will be available. This is the default option.</p>
Operator Filter	<p>Specifies the default operator filtering to apply to guest accounts. This can be used to limit the types of accounts that can be viewed by operators. Options include:</p> <ul style="list-style-type: none"> • No operator filter • Only show accounts created by the operator • Only show accounts created by operators with this profile
User Account Filter	<p>Lets you create a persistent filter to apply to the user account list. For example, this can be useful in large deployments where an operator only wants to have a filtered view of some accounts. To create an account filter, enter a comma-delimited list of field-value pairs. Supported operators are described below in "Operators Supported in Filters" on page 676.</p>

Table 313: Operator Profile Editor Form, Access Area(Continued)

Field	Description
Session Filter	Lets you create a filter that only lasts for a single session. To create a session filter, enter a comma-delimited list of field-value pairs. Supported operators are described below in "Operators Supported in Filters" on page 676.
Account Limit	Maximum number of accounts an operator with this operator profile can create. Disabled accounts are included in the account limit. To set no limit, leave this field empty. When you create or edit an AirGroup operator, the value you enter in this field specifies the maximum number of devices an AirGroup operator with this profile can create.

Operators Supported in Filters

When you create a session filter or a persistent user account filter, the user can enter a simple substring to match a portion of the username or any other fields that are configured for search, and may include the following operators:

Table 314: Operators Supported in Filters

Operator	Meaning	Additional Information
=	is equal to	<p>You can search for multiple values when using the equality (=) or inequality (!=) operators. To specify multiple values, list them separated by the pipe character ().</p> <p>For example, specifying the filter "role_id=2 3, custom_field=Value" restricts the user accounts displayed to those with role IDs 2 and 3 (Guest and Employee), and with the field named "custom_field" set to "Value".</p>
!=	is not equal to	
>	is greater than	
>=	is greater than or equal to	
<	is less than	
<=	is less than or equal to	
~	matches the regular expression	
!~	does not match the regular expression	

Configuring the User Interface

The fields in the **User Interface** area of the form determine elements of the application's visual appearance and behavior that operators with this profile will see. The **Skin**, **Start Page**, **Language**, and **Time Zone** options specify the defaults to use for operators with this profile. Individual operator logins may have different settings, which will be used instead of the values specified in the operator profile. For information on specifying options at the individual operator level, see "Local Operator Authentication" on page 680.

Figure 476 The Operator Profile Editor Form, User Interface Area

User Interface	
These options control the visual appearance and behavior of the application.	
Skin:	(Default) <input type="button" value="v"/> Choose the skin to use for operators with this profile.
Start Page:	Create New Guest Account <input type="button" value="v"/> The initial page to show this operator after logging in.
Language:	Auto-detect <input type="button" value="v"/> Select the default language to use for operators with this profile.
Time Zone:	(Default) <input type="button" value="v"/> Select the default time zone for operators with this profile.
Customization:	<input type="checkbox"/> Override the application's forms and views If checked, you can specify different default forms and views to use.

Table 315: Operator Profile Editor Form, User Interface Area

Field	Description
Skin	Specifies the skin to use for operators with this profile. For more information on skins, see " Plugin Manager " on page 635. Options include: <ul style="list-style-type: none"> • (Default) — Indicates that the skin plugin currently marked as enabled in the Plugin Manager will be used. • Aruba ClearPass Skin • Blank Skin • ClearPass Guest Skin • Custom Skin 1 • Custom Skin 2 • Galleria Skin • Galleria Skin 2
Start Page	Specifies the initial ClearPass application page to show to this operator after they log in. The Default setting option indicates that the application's standard Home page will be the first page displayed after login. To have a different start page displayed to users with this operator profile, choose a page from the drop-down list. For example, if a profile is designed for users who do only certain tasks, you might want the application to open at the module where those tasks are performed.
Language	Specifies the default language to use for operators with this profile. Options include: <ul style="list-style-type: none"> • Auto-detect — Default. This lets the application determine the operator's language preference from their local system settings. • Danish • German • English • Spanish • French • Dutch • Arabic • Japanese • Chinese

Table 315: Operator Profile Editor Form, User Interface Area(Continued)

Field	Description
	<ul style="list-style-type: none"> • Korean
Time Zone	Specifies the default time zone for operators with this profile. The Default setting indicates that the operator's time zone will default to the system's currently configured time zone.
Customization	If selected, lets you override the application's default forms and views and specify different ones to use for the operator profile. The form expands to show the forms and views that can be modified. If alternative forms or views have been created, you may use the drop-down lists to specify which ones to use. See Figure 477 .
Save Changes	Saves your changes and creates the operator profile.

Figure 477 The Operator Profile Editor Form, User Interface Area, Customization Options

Custom Forms and Views	
Active Sessions:	(Use default: guest_sessions "Active Sessions") <input type="button" value="v"/> Override the Active Sessions view.
Change Expiration:	(Use default: change_expiration "Change Expiration") <input type="button" value="v"/> Override the Change Expiration form.
Create Guest Accounts:	(Use default: create_multi "Create Guest Accounts") <input type="button" value="v"/> Override the Create Guest Accounts form.
Edit Account:	(Use default: guest_edit "Edit Account") <input type="button" value="v"/> Override the Edit Account form.
Edit Accounts:	(Use default: guest_multi "Edit Accounts") <input type="button" value="v"/> Override the Edit Accounts view.
Edit Guest Accounts:	(Use default: guest_multi_form "Edit Guest Accounts") <input type="button" value="v"/> Override the Edit Guest Accounts form.
Edit MAC:	(Use default: mac_edit "Edit MAC") <input type="button" value="v"/> Override the Edit MAC form.
Export Guest Manager Accounts:	(Use default: guest_export "Export Guest Manager Accounts") <input type="button" value="v"/> Override the Export Guest Manager Accounts view.
Guest Manager Accounts:	(Use default: guest_users "Guest Manager Accounts") <input type="button" value="v"/> Override the Guest Manager Accounts view.
MAC Authentication Accounts:	(Use default: mac_list "MAC Authentication Accounts") <input type="button" value="v"/> Override the MAC Authentication Accounts view.
New MAC Authentication:	(Use default: mac_create "New MAC Authentication") <input type="button" value="v"/> Override the New MAC Authentication form.
New Visitor Account:	(Use default: create_user "New Visitor Account") <input type="button" value="v"/> Override the New Visitor Account form.
<input type="button" value="Save Changes"/>	

Operator Profile Privileges

The privilege selections available for an operator profile (see ["Creating an Operator Profile" on page 673](#)) provide you with control over the functionality that is available to operators. Refer to the description of each individual operator privilege to determine what the effects of granting that permission will be.

Table 316: *Operator Profile Privilege Levels*

Privilege Level	Description
No Access	The operator will have no access to the particular area of functionality. Options for that functionality will not appear for that operator in the menus.
Read Only Access	The operator can see the options available but is unable to make any changes to them.
Full Access	All the options are available to be used by the operator.
Custom	Allows you to specify individual permissions within each group. For example, Guest Manager allows you to control access to the following areas: <ul style="list-style-type: none">• Active sessions management• Viewing historical data for active sessions• Changing expiration time of guest accounts• Creating multiple guest accounts• Creating new guest accounts• Editing multiple guest accounts• Exporting guest account data• Full user control of guest accounts• Importing guest accounts• Listing guest accounts• Managing customization of guest accounts• Managing print templates• Removing or disabling guest accounts• Resetting guest passwords

Configuring AirGroup Operator Device Limit

By default, an AirGroup operator can create up to five personal devices. To change this default:

1. Go to **Administration > Operator Logins > Profiles**, then select the **AirGroup Operator** profile in the list.
2. Click the **Edit** link. The **Edit Operator Profile** form opens.
3. In the **Account Limit** field, specify an appropriate value. This is the maximum number of personal devices that an operator with this profile can create.
4. Click **Save Changes**.

You can create a set of operator profiles and configure each profile with a different account limit. This makes it easy to assign operator profiles appropriately for small groups, larger groups, or events. To create each profile in the set, duplicate the built-in AirGroup Operator profile, and update the **Account Limit** field in the new profile.

Local Operator Authentication



ClearPass Policy Manager profiles and ClearPass Guest profiles are different. To create a ClearPass Guest operator login, local users are first defined in ClearPass Policy Manager with a role that matches an operator profile in Guest, then rules are used to map the role to the Guest operator profile.

Creating a New Operator



To create a new operator or administrator for ClearPass Guest or AirGroup, some steps are performed in ClearPass Policy Manager, and some steps are performed in ClearPass Guest, as described below:

1. Create an operator profile in ClearPass Guest, or use an existing one. See ["Operator Profiles" on page 671](#).
 - To create an AirGroup user, choose either the **AirGroup Administrator** or **AirGroup Operator** profile, as appropriate. These profiles are automatically included in ClearPass Guest when the AirGroup Services plugin is installed.
 - MACTrac users are created entirely in Policy Manager.
2. Create a ClearPass role for the operator: In Policy Manager, go to **Configuration > Identity > Roles** and create a role that matches the operator profile. Refer to the ClearPass Policy Manager documentation for information on creating the role.
 - When creating AirGroup users or MACTrac users, the appropriate roles are already created in ClearPass.
3. Create a local user for the operator: In Policy Manager, go to **Configuration > Identity > Local Users** and click **Add User**. In the **Add Local User** form, complete the fields and choose the appropriate role from the **Role** drop-down list.
 - To create an AirGroup user, choose either the **AirGroup Administrator** or **AirGroup Operator** role, as appropriate.
 - To create a MACTrac user, choose the **MACTrac Operator** role. This form completes MACTrac user creation; the following steps are not required.
4. Create a translation rule to map the ClearPass role name to the ClearPass Guest operator profile: In ClearPass Guest, go to **Administration > Operator Logins > Translation Rules**.
5. In the **Translation Rules** list, find the profile in the list, look at the **Action** column to verify the operator profile assignment, and then click its **Edit** link. The row expands to include the **Edit Translation Rule** form.
6. Edit the fields appropriately to match the ClearPass role name to the ClearPass Guest operator profile. See ["LDAP Translation Rules" on page 689](#).
7. Click **Save Changes**.

External Operator Authentication

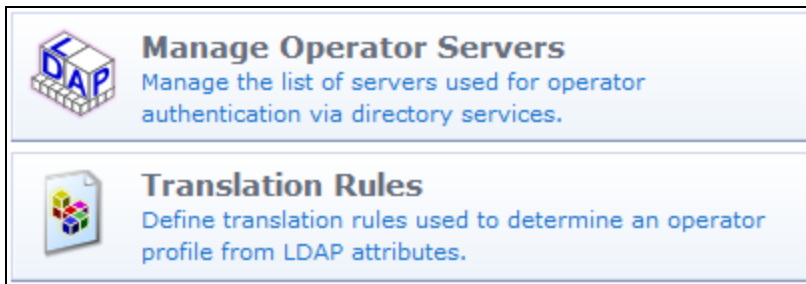


Operators defined externally in your company's directory server form the second type of operator.

Authentication of the operator is performed using LDAP directory server operations. The attributes stored for

an authenticated operator are used to determine what operator profile should be used for that user.

At **Administration > Operator Logins > Start Here**, the **Manage Operator Servers** and the **Translation Rules** commands allow you to set up operator logins integrated with a Microsoft Active Directory domain or another LDAP server.



The operator management features, such as creating and editing operator logins, apply only to local operator logins defined in ClearPass Guest. You cannot create or edit operator logins using LDAP. Only authentication is supported.

Managing LDAP Operator Authentication Servers



ClearPass Guest supports a flexible authentication mechanism that can be readily adapted to any LDAP server's method of authenticating users by name. There are built-in defaults for Microsoft Active Directory servers and POSIX-compliant directory servers.

When an operator attempts to log in, each LDAP server that is enabled for authentication is checked, in order of priority from lowest to highest.

When a server is found that can authenticate the operator's identity (typically with a username and password), the LDAP server is queried for the attributes associated with the user account.

These LDAP attributes are then translated to operator attributes using the rules defined in the LDAP translation rules. In particular, an operator profile will be assigned to the authenticated user with this process, which controls what that user is permitted to do.

Viewing the LDAP Server List

If you have defined one or more LDAP servers, those servers will appear in the LDAP server list at **Administration > Operator Logins > Servers**.

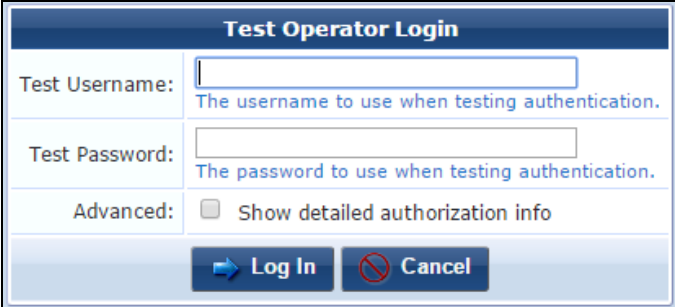
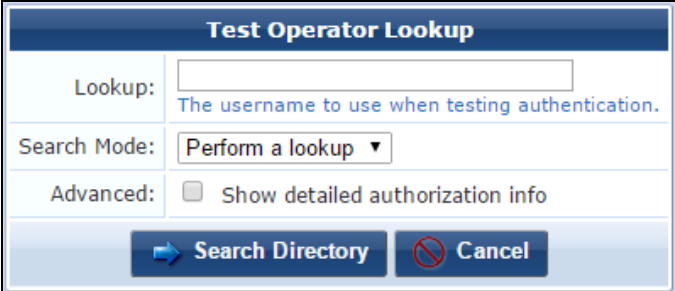
Figure 478 *The Operator Servers List View*

The screenshot shows a web-based interface for managing LDAP servers. It features a table with columns for Name, Priority, Lookups, Logins, Server Type, and Default Profile. Below the table are action buttons for Edit, Delete, Duplicate, Ping, and Test Auth. At the bottom, there is a '2 items' indicator, a 'Reload' button, and a 'Show all rows' dropdown menu.

Name	Priority	Lookups	Logins	Server Type	Default Profile
Example Server	50	No	No	Active Directory	Null Profile
My LDAP Server	50	No	No	Active Directory	Null Profile

Select any of the LDAP servers in the list to display options to perform the following actions on the selected server:

Table 317: *Operator Servers List View*

Field	Description
Edit	Lets you make changes to the properties of the LDAP server. The Server Configuration form opens.
Delete	Removes the server from the LDAP server list. You will be asked to confirm the deletion.
Duplicate	Creates a copy of an LDAP server to use as a basis for a new server.
Disable	Temporarily disables the server while retaining its entry in the server list.
Enable	Re-enables a disabled LDAP server.
Ping	Sends a ping message (echo request) to the LDAP server to verify connectivity between the LDAP server and the ClearPass Guest server. The form expands to show the ping test progress and results.
Test Auth	<p>Adds a Test Operator Login area in the LDAP servers list that allows you to test authentication of operator login values.</p> 
Test Lookup	<p>Adds a Test Operator Lookup form in the LDAP servers list that allows you to look up sponsor names. This option is only available if sponsor lookup has been enabled for the server on the Edit Authentication Server page.</p> 

Creating an LDAP Server




To create an LDAP server, go to **Administration > Operator Logins > Servers**, and click the  **Create new LDAP server** link in the upper-right corner. The authentication **Server Configuration** form opens.

Figure 479 *The Server Configuration Form, General Properties and User Search Areas*



Server Configuration	
* Name:	<input type="text"/> Enter a name for this authentication server.
* Priority:	<input type="text" value="50"/> The priority rank of the service handler for authentication of local operators. Lower numbers represent higher priorities.
* Server Type:	<input type="text" value="Microsoft Active Directory"/> Select the type of server you are connecting to.
* Server URL:	<input type="text"/> URL of the LDAP server, e.g. ldap://hostname/ or ldap://192.168.88.1/ou=IT-Services,ou=Departments,dc=amigopod,dc=com
Bind DN:	<input type="text"/> The Distinguished Name to use when binding to the LDAP server, or empty to perform anonymous bind.
Bind Username:	<input type="text"/> The username and domain to use when binding to the directory (username@domain, or domain\username format), or empty for an anonymous bind.
Bind Password:	<input type="password"/> The password to use when binding to the LDAP server, or empty for an anonymous bind.
User Search Enable searching for users in the directory.	
Enabled:	<input checked="" type="checkbox"/> Use this server to search for matching users
* Filter:	<input type="text" value="Use the default LDAP filter"/> The default filter looks for people based on their full name or their user ID.
* Display Attributes:	<input type="text" value="#sAMAccountName = id
displayName = text
title = desc
userPrincipalName = desc"/> List the LDAP attributes to retrieve from the directory, and their type. Use the syntax 'attributeName = type', where type may be: 'id', 'text' or 'desc'.
Sort By:	<input type="text" value="displayName"/> Name of the LDAP attribute on which the results should be sorted.
* Maximum Results:	<input type="text" value="30"/> Limit the number of results returned for each query.
AirGroup	
Tip:	 To enable user search in AirGroup, change the user interface of the 'airgroup_shared_user' field to 'Multiple selection list', and then check the Select2 Options for additional properties.  Edit airtgroup_shared_user field

Table 318: *Server Configuration Form, General Properties and User Search Areas*

Field	Description
Name	(Required) Name for this authentication server.
Priority	(Required) Priority rank of the service handler for authentication of local operators. Lower numbers represent higher priorities.
Server Type	(Required) Specifies the type of server your system will connect to. Options include: <ul style="list-style-type: none"> Microsoft Active Directory — For more information on the Microsoft Active Directory server type, see "Advanced LDAP URL Syntax" on page 686.

Table 318: Server Configuration Form, General Properties and User Search Areas(Continued)



Field	Description
	<ul style="list-style-type: none"> • POSIX Compliant • Custom
Server URL	<p>(Required) The URL of the LDAP server.</p> <p>Examples:</p> <p>ldap://hostname/ or ldap://192.168.88.1/ou=IT-Services,ou=Departments,dc=amigopod,dc=com</p> <p>To specify a basic LDAP server connection (hostname and optional port number), use a server URL of the form ldap://hostname/ or ldap://hostname:port/. See "Advanced LDAP URL Syntax" on page 686 for more details about the types of LDAP URL you may specify.</p>
Bind DN	The password to use when binding to the LDAP server. For an anonymous bind, leave this field empty.
Bind Username	<p>The username and domain to use when binding to the directory. Use either of the following formats:</p> <ul style="list-style-type: none"> • username@domain • domain\username <p>To perform an anonymous bind, leave this field empty.</p>
Bind Password	<p>The password to use when binding to the LDAP server. Leave this field blank to use an anonymous bind.</p> <p>If you selected Microsoft Active Directory in the Server Type field, and if your LDAP server does not use anonymous bind, you must supply the required credentials to bind to the directory.</p>
Base DN	The Distinguished Name to use for the LDAP search.
Unique ID	The name of an LDAP attribute used to match the username.
Filter	Additional LDAP filters to use to search for the server.
Attributes	List of LDAP attributes to retrieve. To retrieve all attributes, leave this field empty (the default).
User Search Area	
Enabled	If selected, The form expands to include AirGroup and Sponsor Lookup options.
Filter	<p>(Required) Specifies the LDAP filter to use. Options include:</p> <ul style="list-style-type: none"> • Use the default LDAP filter — The default filter looks for people based on their full name or their user ID. • Specify a custom LDAP filter
Filter Expression	(Required) The LDAP filter expression to use when searching. The keyword @SEARCH@ will be replaced with the search query.
Display Attributes	<p>(Required) The LDAP attributes to retrieve from the directory, and their type.</p> <p>Use the syntax "attributeName = type", where type may be: "id", "text" or "desc".</p>
Sort By	Name of the LDAP attribute on which the results should be sorted.

Table 318: *Server Configuration Form, General Properties and User Search Areas(Continued)*

Field	Description
Maximum Results	(Required) The maximum number of results to return for each query.
AirGroup Area	
Tip	Displays information about how to enable user search in AirGroup, and provides a link to the related configuration form.

Figure 480 *The Server Configuration Form, Operator Logins and Authentication Parameters Areas*

Sponsor Lookups

Tip:  To enable sponsor lookups in a self-registration, add the 'sponsor_lookup' field to the registration and change the user interface to 'Multiple selection list', and then check the Select2 Options for additional properties.
 [Edit sponsor_lookup field](#)

*** Attribute Mapping:**

```
sponsor_name | sAMAccountName
#sponsor_name | cn
sponsor_email | userPrincipalName
#sponsor_email | mail
```

Enter the attribute mappings to apply to the guest configuration.
Enter a list of "FORM_FIELD | LDAP_ATTRIBUTE" pairs one per line.

Operator Logins

Enabled: Use this server to authenticate operator logins

LDAP server configuration for operator logins has been deprecated. Please configure with Policy Manager.

* Default Profile:

Select the default operator profile to assign to operators authorized by this server.

Authentication Parameters

Test: Perform authentication test
 Perform lookup test

Test Username:

The username to use when testing authentication.

Test Password:

The password to use when testing authentication.

Advanced: Show detailed authorization info

Table 319: *Server Configuration Form, Operator Logins and Authentication Parameters Areas*

Field	Description
Sponsor Lookups Area	
Tip	Displays information about how to enable sponsor lookups in a self-registration, and provides a link to the related configuration form. If you want to enable the validation of sponsor emails during self-registration, follow the instructions provided. The server will then look up sponsors during self-registration and double-check the attribute used for emails on the LDAP server. This option requires that the sponsor_email and do_ldap_lookup fields are enabled in the registration form, and that you have the LDAP Sponsor Lookup plugin installed. Use the Plugin Manager to verify that this plugin is available.
Attribute Mapping	(Required) The attribute mappings to apply to the configuration. Enter a list of "FORM_FIELD LDAP_ATTRIBUTE" pairs, one per line.

Table 319: Server Configuration Form, Operator Logins and Authentication Parameters Areas(Continued)

Field	Description
Operator Logins Area	
Enabled	If selected, this server will be used to authenticate operator logins. LDAP servers for operator logins are configured in Policy Manager.
Default Profile	(Required) Specifies the default operator profile to assign to operators authorized by this server.
Authentication Parameters Area	
Test	The type of test to run, either authentication or lookup.
Test Username	The username to use when performing an authentication or lookup test.
Test Password	The password to use when performing an authentication test. The minimum password length is six characters.
Advanced	If selected, detailed test results are displayed.
Search Mode	The type of search mode to use, either lookup or search.
Test Settings	Lets you test your settings when your entries on this form are complete and you have provided a test username and test password. If the authentication or search is successful, the operator profile assigned to the username is displayed. If the authentication fails, an error message is displayed. See "LDAP Operator Server Troubleshooting" on page 687 for information about common error messages and troubleshooting steps to diagnose the problem.
Search Directory	
Save Changes	Saves your changes and creates this LDAP Server. If the server is marked as enabled, subsequent operator login attempts will use this server for authentication immediately.

Advanced LDAP URL Syntax

If you select Microsoft Active Directory as the **Server Type** on the **Administration > Operator Logins > Servers > Server Configuration** form, the LDAP server connection will use a default distinguished name of the form **dc=domain,dc=com**, where the domain name components are taken from the bind username.

To specify a different organizational unit within the directory, include a distinguished name in the LDAP server URL, using a format such as:

```
ldap://192.0.2.1/ou=IT%20Services,ou=Departments,dc=server,dc=com
```

To specify a secure connection over SSL/TLS, use the prefix **ldaps://**.

To specify the use of LDAP v3, use the prefix **ldap3://**, or **ldaps3://** if you are using LDAP v3 over SSL/TLS.

When Microsoft Active Directory is selected as the **Server Type**, LDAP v3 is automatically used.

An LDAP v3 URL has the format **ldap://host:port/dn?attributes?scope?filter?extensions**.

- **dn** is the base X.500 distinguished name to use for the search.
- **attributes** is often left empty.
- **scope** may be 'base', 'one' or 'sub'.
- **filter** is an LDAP filter string, for example, (objectclass=*)


- **extensions** is an optional list of name=value pairs.

Refer to [RFC 2255](#) for further details.

LDAP Operator Server Troubleshooting

At **Administration > Operator Logins > Servers**, you can use the LDAP **Operator Servers** list to troubleshoot network connectivity and operator authentication, and to look up operator usernames.

Testing Connectivity

To test network connectivity between an LDAP server and the ClearPass Guest server, click the  **Ping** link in the server's row. The results of the test appear below the server entry in the LDAP server table.

Testing Operator Login Authentication


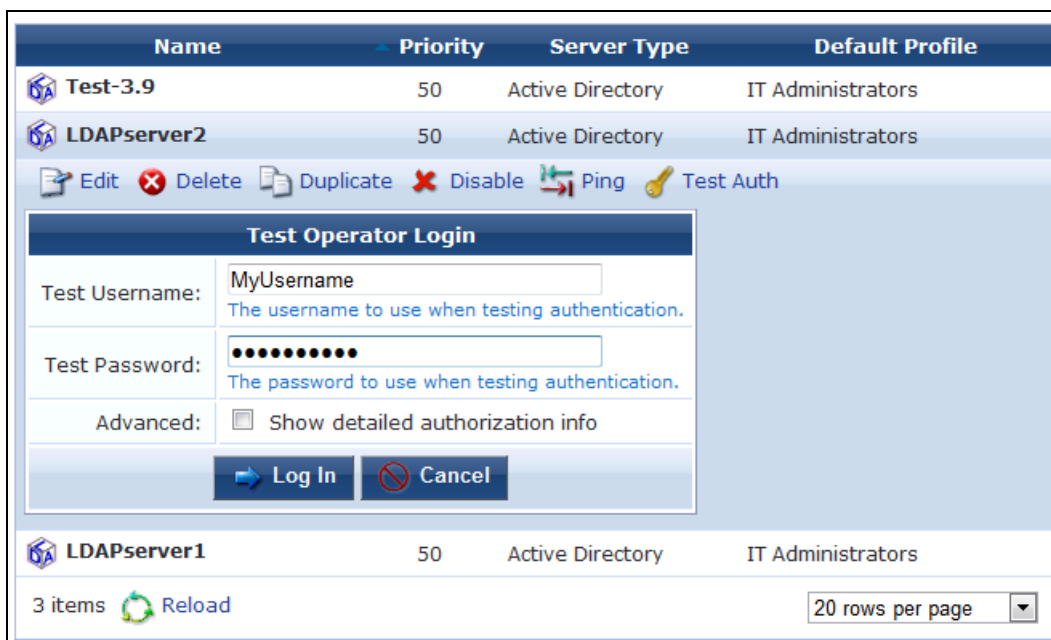










1. To test authentication of operator login values, select a server name in the LDAP Server table, then click the  **Test Auth** link. The form expands to include the **Test Operator Login** form.

Figure 481 *The Test Operator Login Form in the Operator Servers List View*



Name	Priority	Server Type	Default Profile
 Test-3.9	50	Active Directory	IT Administrators
 LDAPserver2	50	Active Directory	IT Administrators
 Edit  Delete  Duplicate  Disable  Ping  Test Auth			
<div style="border: 1px solid #ccc; padding: 5px;"> <h4 style="text-align: center; margin: 0;">Test Operator Login</h4> <p>Test Username: <input type="text" value="MyUsername"/> <small>The username to use when testing authentication.</small></p> <p>Test Password: <input type="password" value="••••••••"/> <small>The password to use when testing authentication.</small></p> <p>Advanced: <input type="checkbox"/> Show detailed authorization info</p> <p style="text-align: center;"> <input type="button" value="Log In"/> <input type="button" value="Cancel"/> </p> </div>			
 LDAPserver1	50	Active Directory	IT Administrators

3 items  Reload 20 rows per page



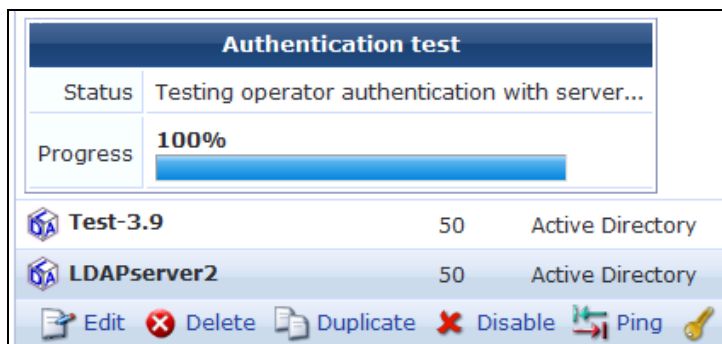

2. Enter an operator username and password for the LDAP Server. The minimum password length is six characters.
3. (Optional) To display detailed authorization information for the specified operator, select the **Advanced** check box.
4. Click  **Log In** to attempt to authenticate the LDAP server, or click  **Cancel** to cancel the test. The **Authentication Test** area is added above the server names to indicate the test's progress.




Figure 482 *The Authentication Test Progress Area*



You can also verify operator authentication when you create a new LDAP server configuration using the  **Test Settings** button on the **LDAP Configuration** form (See "Creating an LDAP Server" on page 683 for a description).

Looking Up Sponsor Names

This option is only available if sponsor lookup has been enabled for the server on the **Edit Authentication Server** page.

1. To look up a sponsor, select a server name in the LDAP Server table, then click the  **Test Lookup** link. The **Test Operator Lookup** area is added to the LDAP servers list.
2. In the **Lookup** field, enter a lookup value. This can be an exact username, or you can include wildcards. If you use wildcards, the search might return multiple values.
3. In the **Search Mode** field, use the drop-down list to specify whether to search for an exact match or use wildcard values.
4. (Optional) To display detailed authorization information for the specified sponsor, select the **Advanced** check box.
5. Click  **Search Directory** to attempt to find sponsor names that match the lookup values, or click  **Cancel** to cancel the test. The **Authentication Test** area is added above the server names to indicate the search's progress.

Troubleshooting Error Messages

The error messages in the following table can be used to diagnose error messages. For example, in the following error message:

"LDAP Bind failed: Invalid credentials (80090308: LdapErr: DSID-0C090334, comment: AcceptSecurityContext error, data **525**, vece), bind DN was: ...",

...the number **525** is identified in the following table as "User not found".

Table 320: *LDAP Error Messages*

Error Data	Reason
525	User not found
52e	Invalid credentials (password is incorrect)
530	Not permitted to log on at this time

Error Data	Reason
531	Not permitted to log on at this workstation
532	Password has expired
533	Account is disabled
701	Account has expired
773	User must reset password
775	User account is locked

Other items to consider when troubleshooting LDAP connection problems:

- **Verify that you are using the correct LDAP version** – use ldap:// for version 2 and ldap3:// to specify LDAP version 3.
- **Verify that you are using an SSL/TLS connection** – use ldaps:// or ldap3s:// as the prefix of the Server URL.
- **Verify that the Bind DN is correct** – the correct DN will depend on the structure of your directory, and is only required if the directory does not permit anonymous bind.
- **Verify that the Base DN is correct** – the Base DN for user searches is fixed and must be specified as part of the Server URL. If you need to search in different Base DN's to match different kinds of operators, then you should define multiple LDAP Servers and use the priority of each to control the order in which the directory searches are done.

LDAP Translation Rules



To create and work with LDAP operator translation rules, go to **Administration > Operator Logins > Translation Rules**. The **Operator Translation Rules** list view opens.

Figure 483 *The Operator Translation Rules List View*

#	Name	Expression	Action	Stop
0	Map Operator Mail	mail	Assign value to operator field email	↓
1	Override Display Name	displayname	Assign value to operator field username	↓
2	RemoveAttrs	instancetype, usncreated, usnchanged, objectsid, o...	Remove attribute	↓
3	MatchDomain	memberof contains CN=Domain Admins	Assign operator profile IT Administrators	✓
Edit Delete Duplicate Disable Edit Profile Move Up Move Down				
4	MatchAdmin	memberof contains CN=Administrators	Assign operator profile IT Administrators	✓
5	MatchGroup	memberof contains CN=Group Name	Assign operator profile Null Profile	✓
6	MatchName	cn matches /^test/	Assign operator profile Null Profile	✓
7	ClearPass Super Administrator	admin_privileges = [TACACS Super Admin]	Assign operator profile IT Administrators	✓
8	ClearPass Super Administrator	admin_privileges = Super Administrator	Assign operator profile IT Administrators	✓
9	ClearPass Network Administrator	admin_privileges = [TACACS Network Admin]	Assign operator profile Network Administrator	✓
10	ClearPass Network Administrator	admin_privileges = Network Administrator	Assign operator profile Network Administrator	✓
11	ClearPass Read-only Administrator	admin_privileges = [TACACS Read-only Admin]	Assign operator profile Read-only Administrator	✓

All translation rules that have been created are included in the list. You can click a translation rule's row in the list for additional options:

Table 321: *Operator Translation Rules List View*

Field	Description
Edit	Lets you edit the configuration of the translation rule. The form expands to include the Edit Translation Rule form. See "Configuring LDAP Translation Rules" on page 690 .
Delete	Deletes the translation rule. You are asked to confirm the deletion.
Duplicate	Creates a copy of an the translation rule to use as a basis for a new rule.
Disable	Temporarily disables the translation rule without deleting it from the rule list.
Enable	Re-enables a disabled translation rule.
Edit Profile	Lets you edit the operator profile assigned to the translation rule. The Edit Operator Profile form opens.
Move Up	Moves the rule up to a higher priority or down to a lower priority in the rule list. Translation rules are processed in order until a matching rule is found that does not have the Fallthrough field set.
Move Down	
Create new translation rule	Lets you create a new translation rule. The Edit Translation Rule form opens in a new page. See "Configuring LDAP Translation Rules" on page 690 .
Operator Servers	Lets you work with an LDAP server. The Operator Servers list view opens. See "Managing LDAP Operator Authentication Servers " on page 681 .

Configuring LDAP Translation Rules

LDAP translation rules specify how to determine operator profiles based on LDAP attributes for an authenticated operator.

To create a new LDAP translation rule, go to **Administration > Operator Logins > Translation Rules**, and then click the **Create new translation rule** link. The **Edit Translation Rule** form opens.

Figure 484 *The Edit Translation Rule Form*

Table 322: *Edit Translation Rule Form*

Field	Description
Name	(Required) Name for this translation rule that describes what the rule does. In the example shown in Figure 484 , the translation rule is to check that the user is an administrator, hence the name MatchAdmin .
Enabled	If selected, this rule will be used when processing reply attributes. If this check box is not selected, the rule will appear in the rules list, but will not be active until you enable it.
Attribute Name	Name of the attribute; for example, "memberof". For all attributes, use an asterisk (*).
Matching Rule	Specifies the matching rule to apply to the value of the attribute. Options include: <ul style="list-style-type: none"> • always match • contains — Case-insensitive substring match anywhere in string. • matches — Regular expression match, where the value is a Perl-compatible regular expression including delimiters. For example, to match the regular expression "admin" case-insensitively, use the value /admin/i. See "Regular Expressions" on page 749 for more details about regular expressions. • equals — Case-insensitive string comparison, matches on equality. • does not equal — Case-insensitive string comparison, matches on inequality. • less than — Numerical value is less than the match value. • greater than — Numerical value is greater than the match value. • starts with — Case-insensitive substring match at start of string. • ends with — Case-insensitive substring match at end of string.

Table 322: Edit Translation Rule Form(Continued)

Field	Description
Value	The value against which to match the attribute. In the example shown in Figure 484 , the value CN=Administrators is used to look for a specific group of which the user is a member.
On Match	<p>Specifies the action the system should take when the translation rule matches an attribute. Options include:</p> <ul style="list-style-type: none"> • Do nothing — Makes no changes. • Assign fixed operator profile — Assigns the selected Operator Profile to the operator. • Assign attribute's value to operator field — Uses the value of the attribute as the value for an operator field. This option can be used to store operator configuration details in the directory. (For operator profiles from enforcement profiles, matching can be performed on either their IDs or their name values, even if the Fallthrough option is not selected) • Assign custom value to operator field — Uses a template to assign a value to a specific operator field. If you choose this option, the form expands to include the Custom text box for you to enter your custom template code. See "Custom LDAP Translation Processing" on page 693. (For operator profiles from enforcement profiles, matching can be performed on either their IDs or their name values, even if the Fallthrough option is not selected) • Apply custom processing — Evaluates a template that may perform custom processing on the LDAP operator. If you choose this option, the form expands to include the Custom text box for you to enter your custom template code. See "Custom LDAP Translation Processing" on page 693. • Remove attribute from operator — Removes the selected LDAP attribute from the operator.
Operator Profile	Specifies which operator profile to assign if there is a rule match. In the example shown in Figure 484 , if the Administrator group is matched, the IT Administrators profile will be assigned.
Operator Field	<p>Specifies which operator field the profile will be assigned to. Options include:</p> <ul style="list-style-type: none"> • username • email • comment • profile • enabled • start_page • userskin • lang • timezone_id • password_action • password_action_time
Custom	Custom template code to apply when the rule matches. You can use the drop-down list to add images, links, or other content items. To be included in this list, content items must first be uploaded to Content Manager .
Fallthrough	If selected, multiple translation rules can be applied. When you create multiple rules, you can build a complete logical structure to perform any type of processing on the LDAP attributes available in your directory.
Save Changes	Saves the your changes. If you are creating a new rule, it is added to the Operator Translation Rules list.

Custom LDAP Translation Processing



When matching an LDAP translation rule, custom processing may be performed using a template.

The template variables available are listed in [Table 323](#).

Table 323: *Template Variables*

Variable	Description
<code>\$attr</code>	The name of the LDAP attribute that was matched.
<code>\$user</code>	Contains settings for the operator, including all LDAP attributes returned from the server.

For a Smarty template syntax description, See "[Smarty Template Syntax](#)" on page 700. These may be used to make programmatic decisions based on the LDAP attribute values available at login time.

For example, to permit non-administrator users to access the system only between the hours of 8:00 am and 6:00 pm, you could define the following LDAP translation rule:

Figure 485 *The Edit Translation Rule Form Showing an Example Custom Rule*

Edit Translation Rule	
* Name:	<input type="text" value="CustomEnabledHours"/> <small>Enter a name for this translation rule.</small>
Enabled:	<input checked="" type="checkbox"/> Use this rule when processing reply attributes
Attribute Name:	<input type="text" value="memberof"/> <small>Enter the name of the attribute (e.g. memberof). Use * for all attributes.</small>
Matching Rule:	<input type="text" value="contains"/> <small>Select the matching rule to apply to the value of the attribute.</small>
Value:	<input type="text"/> <small>Enter the value to match the attribute against.</small>
On Match:	<input type="text" value="Assign custom value to operator field"/> <small>Select what happens when this translation rule matches an attribute.</small>
Operator Field:	<input type="text" value="enabled"/> <small>Select the operator field to assign the value to.</small>
Custom:	<pre>{strip} {of stripof(\$user.memberof, "CN-Administrators") ! ==false} 1 {elseif date('H') >= 8 && date('H') < 18} 1 {else} 0 {/if} {/strip}</pre> <input type="button" value="Insert content item..."/> <small>Enter custom template code applied when the translation rule matches.</small>
Fallthrough:	<input checked="" type="checkbox"/> Continue translation if rule matches <small>Check this box if you want to apply multiple translation rules.</small>

The Custom rule is:

```
{strip}
{if stripof($user.memberof, "CN=Administrators")!==false}
1
{elseif date('H') >= 8 && date('H') < 18}
1
{else}
0
{/if}
{/strip}
```

Explanation: The rule will always match on the “memberof” attribute that contains the user’s list of groups. The operator field “enabled” will determine if the user is permitted to log in or not. The custom template uses the {strip} block function to remove any whitespace, which makes the contents of the template easier to understand. The {if} statement first checks for membership of the Administrators group using the PHP [stripof](#)

[\(\)](#) function for case-insensitive substring matching; if matched, the operator will be enabled. Otherwise, the server's current time is checked to see if it is after 8am and before 6pm; if so, the operator will be enabled. If neither condition has matched, the "enabled" field will be set to 0 and login will not be permitted.

This chapter includes the following sections:

- "Basic HTML Syntax" on page 697
- "Standard HTML Styles" on page 698
- "Smarty Template Syntax" on page 700
- "Date/Time Format Syntax" on page 716
- "Programmer's Reference" on page 719
- "Field, Form, and View Reference" on page 724
- "LDAP Standard Attributes for User Class" on page 748
- "Regular Expressions" on page 749

Basic HTML Syntax

ClearPass Guest allows different parts of the user interface to be customized using the Hypertext Markup Language (HTML).

Most customization tasks only require basic HTML knowledge, which is covered in this section.

HTML is a markup language that consists primarily of *tags* that are enclosed inside angle brackets, for example, **<p>**. Most tags are paired to indicate the start and end of the text being marked up; an end tag is formed by including the tag inside the angle brackets with a forward slash, for example, **</p>**.

Use the following standard HTML tags in customization:

Table 324: *Standard HTML Tags*

Item	HTML Syntax
Basic Content	
	<code><h1>Main Heading</h1></code>
	<code><h2>Subheading</h2></code>
	<code><h3>Section heading</h3></code>
	<code><p>Paragraph text</p></code>
	<code>
</code> <code>
</code> - equivalent syntax (XHTML)
	<code></code> <code>List item text</code> <code></code>

Item	HTML Syntax
	<pre> List item text </pre>
Text Formatting	
	<pre>words to be made bold equivalent syntax</pre>
	<pre><i>words to be made italic</i> equivalent syntax</pre>
	<pre><u>words to underline</u></pre>
	<pre><tt>Shown in fixed-width font</tt></pre>
	<pre>Uses CSS formatting Uses predefined style</pre>
	<pre><div style="...">Uses CSS formatting</div> <div class="...">Uses predefined style</div></pre>
Hypertext	
	<pre>Link text to click on</pre>
	<pre> - XHTML equivalent</pre>
	<pre></pre>

For more details about HTML syntax and detailed examples of its use, consult a HTML tutorial or reference guide.

Standard HTML Styles

ClearPass Guest defines standard CSS classes you can use to provide consistent formatting within the user interface.

Examples of these styles are given below.

Figure 486 Example Formatting of Some Standard CSS Classes

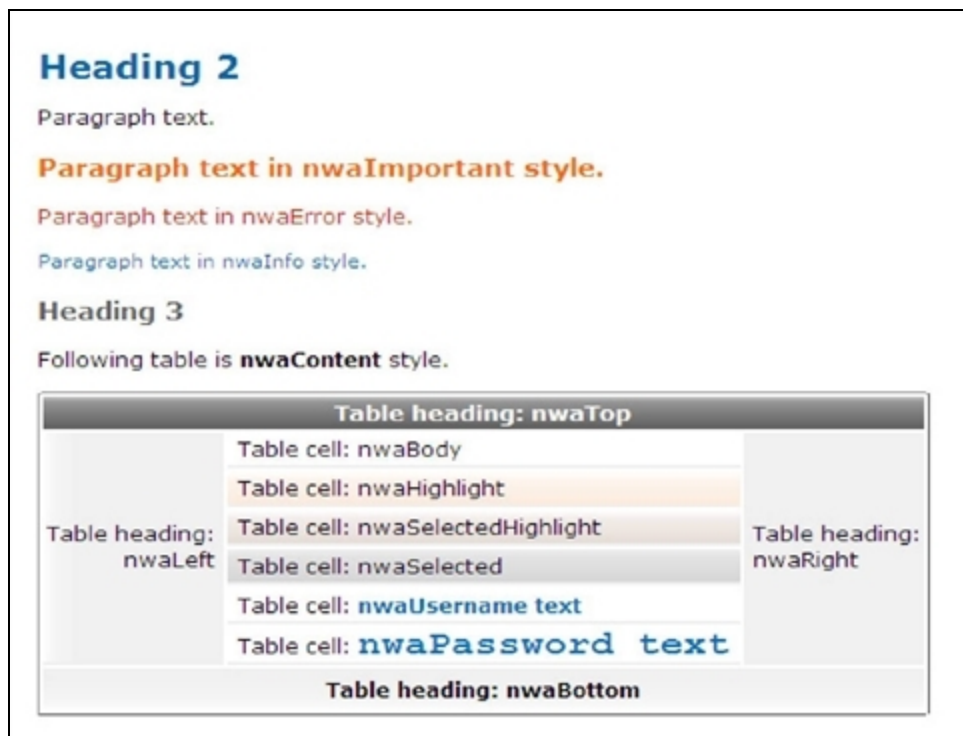


Table 325: Formatting Classes

Class Name	Applies To	Description
nwaIndent	Tables	Indent style used in tables
nwaLayout	Tables	Used when you want to lay out material in a table without the material looking as if it is in a table; in other words, without borders
nwaContent	Tables	Class used for a standard table with borders
nwaTop	Table Header	Table heading at top
nwaLeft	Table Header	Left column of table
nwaRight	Table Header	Right column of table
nwaBottom	Table Header	Table heading at bottom
nwaBody	Table Cell	Style to apply to table cell containing data
nwaHighlight	Table Cell	Highlighted text (used for mouseover)
nwaSelected	Table Cell	Selected text (table row after mouse click)
nwaSelectedHighlight	Table Cell	Selected text with mouseover highlight
nwaInfo	All	Informational text message
nwaError	All	Error text message

Class Name	Applies To	Description
nwaImportant	All	Text that should be prominently displayed Table subheadings
nwaUsername	All	Text used to display a username
nwaPassword	All	Text used to display a password

Smarty Template Syntax

ClearPass Guest's user interface is built using the Smarty template engine. This template system separates the program logic and visual elements, enabling powerful yet flexible applications to be built.

When customizing template code that is used within the user interface, you have the option of using Smarty template syntax within the template. Using the programming features built into Smarty, you can add your own logic to the template. You can also use predefined template functions and block functions to ensure a consistent user interface.

Basic Template Syntax

Following is a brief introduction to the usage of the Smarty template engine. For more information, please refer to the Smarty documentation at <http://www.smarty.net/docs.php>, or the Smarty Crash Course at <http://www.smarty.net/crashcourse.php>.

Text Substitution

Simple text substitution in the templates may be done with the syntax **{*variable*}**, as shown below:

```
The current page's title is: {title}
```

Template File Inclusion

To include the contents of another file, this can be done with the following syntax:

```
{include file="public/included_file.html"}
```

Smarty template syntax found in these files is also processed, as if the file existed in place of the **{include}** tag itself.

Comments

To remove text entirely from the template, comment it out with the Smarty syntax **{* *commented text* *}**. Be aware that this is different from an HTML comment, in that the Smarty template comment will never be included in the page sent to the Web browser.

Variable Assignment

To assign a value to a page variable, use the following syntax:

```
{assign var=name value=value}
```

The "value" can be a text value (string), number, or Smarty expression to be evaluated, as shown in the examples below:

```
{assign var=question value="forty plus two"}  
The question is: {question}
```



```

{assign var=answer value=42}
The answer is: {$answer}
{assign var=question_uppercase value=$question|strtoupper}
THE QUESTION IS: {$question_uppercase}

```

Conditional Text Blocks

To include a block of text only if a particular condition is true, use the following syntax:

```

{if $username != ""}
  <tr>
    <td class="nwaBody">Username:</td>
    <td class="nwaBody">{$username}</td>
  </tr>
{else}
  <!-- No user name, no table row -->
{/if}

```

The condition tested in the **{if} ... {/if}** block should be a valid PHP expression. The **{else}** tag does not require a closing tag.

Script Blocks

The brace characters **{** and **}** are specially handled by the Smarty template engine. Using text that contains these characters, such as CSS and JavaScript blocks, requires a Smarty block **{literal} ... {/literal}**:

```

<script type="text/javascript" language="JavaScript">
{literal}
<!--
function my_function() {
    // some Javascript code here
}
// -->
{/literal}
</script>

```

Failing to include the **{literal}** tag will result in a Smarty syntax error when using your template. Single instances of a **{** or **}** character can be replaced with the Smarty syntax **{ldelim}** and **{rdelim}** respectively.

Repeated Text Blocks

To repeat a block of text for each item in a collection, use the **{section} ... {/section}** tag:

```

{section loop=$collection name=i}
<tr>
  <td class="nwaBody">
    {$collection[i].name}
  </td>
</tr>
{sectionelse}
  <!-- included if $collection is empty -->
{/section}

```

The content after a **{sectionelse}** tag is included only if the **{section}** block would otherwise be empty.

Foreach Text Blocks

An easier to use alternative to the **{section} ... {/section}** tag is to use the **{foreach} ... {/foreach}** block:

```

{foreach key=key_var item=item_var from=$collection}
  {$key_var} = {$item_var}
{foreachelse}
  <!--included if $collection is empty -->
{/foreach}

```

The advantage of this syntax is that each item in the collection is immediately available as the named item variable, in this example **{item_var}**. This construct is also useful when iterating through associative arrays indexed by key, as the key is immediately available with each item.

A `name=` attribute may be supplied with the opening **{foreach}** tag. When a name is supplied, the following additional Smarty variables are available for use inside the **{foreach} ... {/foreach}** block:

- **{\$smarty.foreach.name.first}** – true if the item being processed is the first item in the collection
- **{\$smarty.foreach.name.last}** – true if the item being processed is the last item in the collection
- **{\$smarty.foreach.name.index}** – counter for the current item, starting at 0 for the first item
- **{\$smarty.foreach.name.iteration}** – counter for the current item, starting at 1 for the first item
- **{\$smarty.foreach.name.total}** – value indicating the total number of items in the collection

The content after a **{foreachelse}** tag is included only if the **{foreach}** block would otherwise be empty.

Modifiers

Smarty provides *modifiers* that can be used to gain greater control over the formatting of data. Modifiers can be included by following a variable with a vertical bar | and the name of the modifier. Any arguments to the modifier can be specified using a colon : followed by the arguments.

The following example prints a date using the YYYY-MM-DD syntax:

```
{$expire_time|nwdateformat:"%Y-%m-%d"}
```

See ["Date/Time Format Syntax" on page 716](#) for detailed information on the date/time format modifiers, and see [Table 326](#).

Table 326: *Smarty Modifiers*

Modifier	Description
htmlspecialchars	Escapes characters used in HTML syntax with the equivalent HTML entities (& for &, < for < and > for >)
nl2br	Replaces newline characters in the value with HTML line breaks ()
number_format	Formats a numerical value for display; an optional modifier argument may be used to specify the number of decimal places to display (default is 0)
nwdateformat	Date/time formatting; see "nwdateformat Modifier" on page 716 for details about this modifier function
nwatimeformat	Date/time formatting; see "Date/Time Format String Reference" on page 718 for details about this modifier function
nwamoneyformat	Formats a monetary amount for display purposes; an optional modifier argument may be used to specify the format string. This modifier is equivalent to the <code>NwaMoneyFormat()</code> function; see "NwaMoneyFormat" on page 721 for details.
strtolower	Converts the value to lowercase
strtoupper	Converts the value to uppercase
ucfirst	Converts the first character of the value to uppercase
ucwords	Converts the first character of each word in the value to uppercase

Predefined Template Functions

Template functions are used to perform different kinds of processing when the template is used. The result of a template function takes the place of the function in the output of the template.

Functions are of two kinds: *block functions*, which have a beginning and ending tag enclosing the text operated on by the function, and *template functions*, which have just a single tag and do not enclose text.

To use a function, enclose the function name in curly braces `{ }` and provide any attributes that may be required for the function. Block functions also require a closing tag.

dump

```
{dump var=$value}
```

Smarty registered template function. Displays the value of a variable.

Use the following Smarty syntax to print a variable's contents:

```
{dump var=$var_to_dump export=html}
```

The contents of the variable are printed in a **<pre>** block. Use the attribute "export=1" to use PHP's `var_export()` format, or omit this attribute to get the default behavior – PHP's `var_dump()` format.

Use the attribute "html=1" to escape any HTML special characters in the content. This can also be done with attribute "export=html", and is recommended for use in most situations (so that any embedded HTML is not interpreted by the browser).

nwa_commandlink

```
{nwa_commandlink} ... {/nwa_commandlink}
```

Smarty registered block function. Generates a "command link" consisting of an icon, main text and explanatory text.

Command links are block elements and are roughly the equivalent of a form button. A command link is typically used to represent a choice the user should make to proceed. The command link contains an icon, command text (that sums up the action taken by the command link), and any explanatory text needed for the command.

Usage example:

```
{nwa_commandlink icon="images" command="Command Link" linkwidth="400"
commandclass="nwaImportant" text="This is a sentence explaining the command."
textclass="nwaInfo"}link_here.php{/nwa_commandlink}
```

- The "icon" parameter is the SRC to the image of the icon. This should normally be a relative path.
- The "command" parameter is the main text of the command link.
- The "text" parameter is the explanatory text describing the action that lies behind the command link. (This is optional.)
- The "linkwidth" parameter, if specified, indicates the width of the command link in pixels. This should be at least 250; the recommended value is 400.
- The "width" and "height" parameters, if specified, provide the dimensions of the icon to display. If not specified, this is automatically determined from the image.
- The "onclick" parameter, if specified, provides the contents for the onclick attribute of the link.
- The "commandclass" parameter, if specified, sets the class attribute of the DIV element enclosing the command text. The default class is "nwaImportant".

- The “textclass” parameter, if specified, sets the class attribute of the P element enclosing the command link’s descriptive text. The default class is “nwaInfo”.
- The “alt” parameter, if specified, sets the ALT attribute of the command link’s icon. If not specified, the default alt text used is the command text.
- The “target” parameter, if specified, sets the TARGET attribute of the hyperlink. If not specified, no TARGET attribute is provided.

The body of the element is the HREF of the command link. The “icon” and “command” parameters are required. All other parameters are optional.

nwa_iconlink

```
{nwa_iconlink} ... {/nwa_iconlink}
```

Smarty registered block function. Generates a combined icon and text link to a specified URL.

Usage example:

```
{nwa_iconlink icon="images/icon-info22.png" text="More Information"}more_information.php{/nwa_iconlink}
```

- The “icon” parameter is the SRC to the image of the icon. This should normally be a relative path.
- The “text” parameter is the text to display next to the icon. This will also be used as the alternate text (that is, a tooltip) for the icon image.
- The “width” and “height” parameters, if specified, provide the dimensions of the icon to display. If not specified, this is automatically determined from the image.
- The “onclick” parameter, if specified, provides the contents for the onclick attribute of the link.
- The “target” parameter, if specified, provides the contents for the target attribute of the link.
- The “alt” parameter, if specified, sets the ALT attribute of the icon. If not specified, the default alt text used is the icon text.
- The “style” parameter, if specified, provides CSS for the SPAN element used to implement the icon link.

The body of the element is the HREF of the link. This HREF will be added to both the icon and the text. If the content of the link is empty, no link will be inserted. This can be used to insert an icon and text as an inline group. No HTML entity escaping is performed when inserting content using this function.

nwaicontext

```
{nwaicontext} ... {/nwaicontext}
```

Smarty registered block function. Generates a block of text with a marker icon displayed in the top left.

Usage examples:

```
{nwaicontext icon="images/icon-info22.png"}Text to display{/nwaicontext}
{nwaicontext type="info"}Information block{/nwaicontext}
```

- The “icon” parameter, if specified, is the SRC to the image of the icon. This should normally be a relative path.
- The “width” and “height” parameters, if specified, provide the dimensions of the icon to display. If not specified, this is automatically determined from the image.
- The “alt” parameter, if specified, provides the alternate text for the icon.
- The “class” parameter, if specified, is the style name to apply to a containing DIV element wrapped around the content. If this is empty, and a default is not provided through the “type” parameter, no wrapper DIV is added.

- The “style” parameter, if specified, is the CSS inline style to apply to a containing DIV element, as for the “class” parameter.
- The “type” parameter, if specified, indicates a predefined style to apply; this may be one of the following:
 - **error** – red cross symbol
 - **fatal** – skull symbol
 - **info** – information symbol
 - **note** (or **arrow**) – right-pointing arrow
 - **ClearPass Guest** – ClearPass Guest logo
 - **ok** (or **tick**) – green tick mark
 - **warn** (or **warning**) – warning symbol
 - **wait** – animated spinner

If “noindent=1” is specified, the block is not indented using the ‘nwalndent’ style. If “novspace=1” is specified, the block uses a ‘DIV’ element, rather than a ‘P’ element. If neither “icon” nor “type” is supplied, the default behavior is to insert an “info” type image. Specifying a “type” is equivalent to specifying an “icon”, “width”, “height” and “alt” parameter, and may also include a “class” depending on the type selected.

Usage example:

```
{nwa_icontext struct=$error}{/nwa_icontext}
```

The “struct” parameter, if specified, uses a standard result type. If the “error” key is set and non-zero, the “type” parameter is set to the value error, and the “message” key is converted to a HTML formatted error message for display.

nwa_quotejs

```
{nwa_quotejs} ... {/nwa_quotejs}
```

Smarty registered block function. Quotes its content in a string format suitable for use in JavaScript. This function also translates UTF-8 sequences into the corresponding JavaScript Unicode escape sequence (\uXXXX)

Usage example:

```
{nwa_quotejs}String with ' and "{/nwaquote_js}
```

The output of this will be:

```
'String with \' and \'"'
```

The “body” parameter, if set, indicates that the string quotes are already supplied; in this case the beginning and ending quotes are not included in the output.

nwa_radius_query

```
{nwa_radius_query _method=MethodName _assign=var ...}
```

Smarty registered template function. Performs accounting-based queries on the RADIUS server and returns the result for use in a template.

Usage example:

```
{nwa_radius_query _method=GetCallingStationTraffic
  callingstationid=$dhcp_lease.mac_address
  from_time=86400 in_out=out _assign=total_traffic}
```

This example uses the `GetCallingStationTraffic` query function and passes the “callingstationid”, “from_time” and “in_out” parameters. The result is assigned to a template variable called `total_traffic`, and will not generate any output.

This template function accepts the following parameters to select a RADIUS database and other connection options:

- **_db** – ID of the RADIUS database service handler (this parameter is optional, the default service handler will be used if it not set)
- **_debug** – Set to a nonzero value to enable debugging
- **_quiet** – Set to a nonzero value to inhibit warning/error messages

The following parameters control the query to be executed:

- **_method** (required) – Name of the query function to execute. A brief listing of the available methods is provided below.
- **_arg0, _arg1, ..., _argN** (optional) – Positional arguments for the query function.
- Named arguments may also be supplied; the arguments must be named identically to the function arguments listed in the documentation for the query function.

The following parameters control how the result should be processed:

- **_assign** – Name of a page variable to store the output; if not set, output is sent to the browser as the result of evaluating the template function.
- **_output** – Index of item to return from the RPC result; if not set, the complete result is returned. This may be of use when an array containing multiple values is returned and only one of these values is required.
- **_default** – Default value to display or return if an error occurs or the `_output` field is not available in the result.

For ease of use, “assign” is also supported as a synonym for “_assign”.

This template function does not generate any output if the **_assign** parameter is set.

The methods that are available for use with this function are listed below. The `$criteria` array consists of one or more criteria on which to perform a database search. The array is used for advanced cases where pre-defined helper functions do not provide required flexibility.

ChangeToRole()

```
ChangeToRole($username, $role_name)
```

Changes the RADIUS role assigned to the user. If the user currently has active sessions, this function will trigger an RFC 3576 Change-of-Authorization (CoA) Request to the network access server.

The `$username` parameter specifies the user account to modify; use the expression `GetAttr('User-Name')` to use the value from the RADIUS User-Name attribute.

The `$role_name` parameter specifies the name of the RADIUS User Role to apply to the user.

Example:

Use the following as a conditional expression for an attribute. If the user's traffic in the past 24 hours exceeds 50 MB, the user is changed to the "Over-Quota" role.

```
return GetUserTraffic(86400) > 50e6 && ChangeToRole("Over-Quota");
```

GetCallingStationCurrentSession()

```
GetCallingStationCurrentSession($callingstationid, $mac_format = null)
```

Looks up the current (most recent) active session for the specified calling station ID.

Because different NAS equipment can send differently-formatted MAC addresses in the Calling-Station-Id attribute, the `$mac_format` argument may be specified. This should be a sprintf-style format string that accepts 6 arguments (the octets of the MAC address). The default if not specified is the IEEE 802 standard format, `%02X-%02X-%02X-%02X-%02X-%02X` – that is, uppercase hexadecimal with each octet separated with a hyphen.

See ["GetCurrentSession\(\)" on page 708](#) for details of the return value.

GetCallingStationSessions()

```
GetCallingStationSessions($callingstationid, $from_time, $to_time = null, $mac_format = null)
```

Calculate the number of sessions for accounting records matching a specific calling-station-id. The calling station id address is looked up automatically from the RADIUS Access-Request (Calling-Station-ID attribute).

Because different NAS equipment can send differently-formatted MAC addresses in the Calling-Station-Id attribute, the `$mac_format` argument may be specified. This should be a sprintf-style format string that accepts 6 arguments (the octets of the MAC address). The default if not specified is the IEEE 802 standard format, `%02X-%02X-%02X-%02X-%02X-%02X` – that is, uppercase hexadecimal with each octet separated with a hyphen.

See ["GetTraffic\(\)" on page 710](#) for details on how to specify the time interval.

GetCallingStationTime()

```
GetCallingStationTime($callingstationid, $from_time, $to_time = null, $mac_format = null)
```

Calculate sum of session times in a specified time interval.

Because different NAS equipment can send differently-formatted MAC addresses in the Calling-Station-Id attribute, the `$mac_format` argument may be specified. This should be a sprintf-style format string that accepts 6 arguments (the octets of the MAC address). The default if not specified is the IEEE 802 standard format, `%02X-%02X-%02X-%02X-%02X-%02X` – that is, uppercase hexadecimal with each octet separated with a hyphen.

The calling station ID is looked up automatically from the RADIUS Access-Request (Calling-Station-ID attribute).

See ["GetTraffic\(\)" on page 710](#) for details on how to specify the time interval.

GetCallingStationTraffic()

```
GetCallingStationTraffic($callingstationid, $from_time, $to_time = null, $in_out = null, $mac_format = null)
```

Calculate sum of traffic counters in a time interval. Sessions are summed if they have the same Calling-Station-Id attribute as that specified in the RADIUS Access-Request.

If no Calling-Station-Id attribute was included in the request, returns zero.

Because different NAS equipment can send differently-formatted MAC addresses in the Calling-Station-Id attribute, the `$mac_format` argument may be specified. This should be a sprintf-style format string that accepts 6 arguments (the octets of the MAC address). The default if not specified is the IEEE 802 standard format, `%02X-%02X-%02X-%02X-%02X-%02X` – that is, uppercase hexadecimal with each octet separated with a hyphen. This string matches what ClearPass Guest sees from the NAS.

The time interval specified by `$from_time` and optionally `$to_time` is also used to narrow the search.

If `$to_time` is not specified, `$from_time` is a “look back” time, that is, the time interval in seconds before the current time.

If `$to_time` is specified, the interval considered is between `$from_time` and `$to_time`.

`$in_out` may be “in” to count only input octets, “out” to count only output octets, or any other value to count both input and output octets towards the traffic total.

Examples:

- Use the following as the condition expression for a RADIUS role attribute. Authorizes a user only if their total traffic (in + out) in the past day does not exceed 10 MB. Be aware that the attribute with this condition expression will never be included in the response!
- `return GetUserTraffic(86400) > 10485760 && AccessReject()`
- Like the above, but only considers output (that is, user downloads):
- `return GetUserTraffic(86400,'out') > 10485760 && AccessReject()`
- Another way to limit the past 30 days downloads to 100 MB:
- `return GetUserTraffic($now - 86400*30, $now, 'out') > 100*1024*1024 && AccessReject()`
- Limit by MAC address, 50 MB download in past 24 hours:
`return GetCallingStationTraffic(86400, 'out') > 50000000 && AccessReject()`

GetCurrentSession()

```
GetCurrentSession($criteria)
```

Looks up the details for an active session, based on the specified criteria.



This is a multi-purpose function that has a very flexible query interface. For ease of use, consider using one of the related functions ["GetCallingStationCurrentSession\(\)" on page 706](#), ["GetIpAddressCurrentSession\(\)" on page 709](#), or ["GetUserCurrentSession\(\)" on page 711](#).

Returns null if there is no matching session, otherwise returns a single session array – a typical result follows:

```
array (
  'id' => '2073',
  'acctsessionid' => '4a762dbf00000002',
  'acctuniqueid' => 'c199b5a94ebf5184',
  'username' => 'demo@example.com',
  'realm' => '',
  'role_name' => 'Guest',
  'nasipaddress' => '192.168.2.20',
  'nasportid' => '',
  'nasporttype' => '',
  'calledstationid' => '',
  'callingstationid' => '',
  'acctstarttime' => '1249258943',
  'connectinfo_start' => '',
  'acctstoptime' => NULL,
  'connectinfo_stop' => NULL,
  'acctsessiontime' => 0,
  'acctinputoctets' => 0,
  'acctoutputoctets' => 0,
  'acctterminatecause' => NULL,
  'servicetype' => '',
  'framedipaddress' => '192.168.2.3',
  'framedprotocol' => '',
  'acctauthentic' => '',
  'nastype' => 'cisco_3576',
```



```

    'nas_name' => 'centos',
    'total_traffic' => 0,
    'state' => 'stale',
    'traffic_input' => 0,
    'traffic_output' => 0,
    'traffic_usage' => 0,
    'session_time' => 29641260,
)

```

GetIpAddressCurrentSession()

```
GetIpAddressCurrentSession($ip_addr = null)
```

Looks up the current (most recent) active session for the specified client IP address. If `ip_addr` is not specified, it defaults to the current value of `$smarty.server.REMOTE_ADDR`, which may not be the same value as the IP address of the session if there is a NAT.

See "[GetCurrentSession\(\)](#)" on page 708 for details of the return value.

GetIpAddressSessions()

```
GetIpAddressSessions($ip_addr, $from_time = null, $to_time = null)
```

Calculate the number of sessions for accounting records matching a specific IP address. The IP address attribute is looked up automatically from the RADIUS Access-Request (Framed-IP-Address attribute).

See "[GetTraffic\(\)](#)" on page 710 for details on how to specify the time interval.

See "[GetIpAddressTraffic\(\)](#)" on page 709 for additional details on the `$ip_addr` argument.

GetIpAddressTime()

```
GetIpAddressTime($ip_addr, $from_time = null, $to_time = null)
```

Calculate sum of session times in a specified time interval. The IP address is looked up automatically from the RADIUS Access-Request (Framed-IP-Address attribute).

See "[GetTraffic\(\)](#)" on page 710 for details on how to specify the time interval.

See "[GetIpAddressTraffic\(\)](#)" on page 709 for additional details on the `$ip_addr` argument.

GetIpAddressTraffic()

```
GetIpAddressTraffic($ip_addr, $from_time = null, $to_time = null, $in_out = null)
```

Calculate sum of traffic counters in a time interval. The IP address used is determined based on the context. If processing a RADIUS Access-Request, the IP address is determined using the Framed-IP-Address attribute. If processing a HTTP request, the current client IP address is assumed (from `$_SERVER['REMOTE_ADDR']`).

Specifying an empty value for the IP address (such as `null`, `false`, or empty string) also causes the current client IP address to be used.

See "[GetTraffic\(\)](#)" on page 710 for details on how to specify the time interval.

GetSessions()

```
GetSessions($criteria, $from_time, $to_time = null)
```

Calculate the number of sessions from accounting records in the database.



This is a multi-purpose function that has a very flexible query interface. For ease of use, consider using one of the related functions "[GetCallingStationSessions\(\)](#)" on page 707, "[GetIpAddressSessions\(\)](#)" on page 709, "[GetUserActiveSessions\(\)](#)" on page 711, or "[GetUserSessions\(\)](#)" on page 711.

`$criteria` is the criteria on which to search for matching accounting records.

As well as the criteria specified, the time interval specified by `$from_time` and optionally `$to_time` is also used to narrow the search.

If `$to_time` is not specified, `$from_time` is a “look back” time, that is, the time interval in seconds before the current time.

If `$to_time` is specified, the interval considered is between `$from_time` and `$to_time`.

Returns the total number of sessions for matching accounting records in the time interval specified.

GetSessionTimeRemaining()

```
GetSessionTimeRemaining($username, $format = "relative")
```

Calculates the session time remaining for a given user account, if the user account was to be authenticated at the moment of the call.

The `$username` parameter is required. This is the username for the authentication.

The `$format` parameter is optional, and defaults to “relative” if not otherwise specified. This parameter may be one of the following values:

- “relative” or “session_time”: Calculates the session timeout as for the Session-Timeout RADIUS attribute, that is, the number of seconds before the session should end. If the session does not have a session timeout, the value returned is 0.
- “time”: Calculates the session end time, as the UNIX time at which the session should end. If the session does not have an expiration time, the value returned is 0.
- Other values: These are interpreted as a date format (see “NwaDateFormat”) and the session end time is returned in this format. (Examples: “iso8601”, “longdate”, “recent”, “%Y-%m-%d %H:%M”, etc.). If the session does not have an expiration time, the value returned is a blank string.

GetTime()

```
GetTime($criteria, $from_time, $to_time = null)
```

Calculate the sum of session times for accounting records in the database.



This is a multi-purpose function that has a very flexible query interface. For ease of use, consider using one of the related functions. See ["GetCallingStationTime\(\)" on page 707](#), ["GetIpAddressTime\(\)" on page 709](#), or ["GetUserTime\(\)" on page 712](#).

`$criteria` is the criteria on which to search for matching accounting records.

As well as the criteria specified, the time interval specified by `$from_time` and optionally `$to_time` is also used to narrow the search.

If `$to_time` is not specified, `$from_time` is a “look back” time, that is, the time interval in seconds before the current time.

If `$to_time` is specified, the interval considered is between `$from_time` and `$to_time`.

Returns the total session time for all matching accounting records in the time interval specified.

GetTraffic()

```
GetTraffic($criteria, $from_time, $to_time = null, $in_out = null)
```

Calculate the sum of traffic counters for accounting records in the database.



Revoking access for a device is only possible This is a multi-purpose function that has a very flexible query interface. For ease of use, consider using one of the related functions ["GetCallingStationTraffic\(\)" on page 707](#), ["GetIpAddressTraffic\(\)" on page 709](#), or ["GetUserTraffic\(\)" on page 712](#).

`$criteria` is the criteria on which to search for matching accounting records. The time interval specified by `$from_time` and optionally `$to_time` is used with the criteria to narrow the search.

If `$to_time` is not specified, `$from_time` is a "look back" time, that is, the time interval in seconds before the current time. If `$to_time` is specified, the interval considered is between `$from_time` and `$to_time`.

`$in_out` may be "in" to count only input octets, "out" to count only output octets, or any other value to count both input and output octets towards the traffic total. This argument returns the computed total of traffic for all matching accounting records.

GetUserActiveSessions()

```
GetUserActiveSessions($username, $callingstationid = null)
```

Looks up the list of all sessions for the specified username.

The username attribute is looked up automatically from the RADIUS Access-Request (User-Name attribute). If a `$callingstationid` argument is supplied, sessions that match that Calling-Station-Id are excluded from the count of active sessions.

GetUserActiveSessionCount()

```
GetUserActiveSessionCount($username)
```

Counts the number of currently active sessions for the current username.

The username attribute is looked up automatically from the RADIUS Access-Request (User-Name attribute).

GetUserCumulativeUsage()

```
GetUserCumulativeUsage($username)
```

Looks up the total cumulative time for the username.

The username attribute is looked up automatically from the RADIUS Access-Request (User-Name attribute).

GetUserCurrentSession()

```
GetUserCurrentSession($username)
```

Looks up the current (most recent) active session for the specified username.

See ["GetCurrentSession\(\)" on page 708](#) for details of the return value.

GetUserFirstLoginTime()

```
GetUserFirstLoginTime($username)
```

Looks up the first login time for the specified username.

The username attribute is looked up automatically from the RADIUS Access-Request (User-Name attribute).

GetUserSessions()

```
GetUserSessions($username, $from_time, $to_time = null)
```

Calculate the number of sessions for accounting records matching a specific user-name. The username attribute is looked up automatically from the RADIUS Access-Request (User-Name attribute).

See ["GetTraffic\(\)" on page 710](#) for details on how to specify the time interval.

GetUserTime()

```
GetUserTime($username, $from_time, $to_time = null)
```

Calculate sum of session times in a specified time interval.

See "[GetTraffic\(\)](#)" on page 710 for details on how to specify the time interval.

GetUserTraffic()

```
GetUserTraffic($username, $from_time, $to_time = null, $in_out = null)
```

Calculate sum of traffic counters in a time interval. Sessions are summed if they have the same User-Name attribute as that specified in the RADIUS Access-Request.

See "[GetCallingStationTraffic\(\)](#)" on page 707 for details on how to specify the time interval.

Advanced Developer Reference

The reference documentation in this section is intended for advanced usage by developers.

nwa_assign

```
{nwa_assign ...}
```

Smarty registered template function. Assigns a page variable based on the output of a generator function.

Simple usage example:

```
{nwa_assign var=my_variable value=my_value}
```

- The “var” parameter specifies the page variable that will receive the output.
- The “value” parameter specifies the value to assign to “var”.

The various request variables may also be accessed using the following supported method:

- `{nwa_assign var=smarty.get.get_variable value=...}`

Alternative usage example:

```
{nwa_assign var=userskin_plugin generator=NwaGetPluginDetails arg=$u.userskin}
```

- The “generator” parameter specifies the generator function to be called.
- A single “arg” parameter, if specified, provides a 1-argument form of calling the function; alternatively, “arg1”, “arg2”, ... may be specified to form an array of arguments to pass to the generator.

nwa_bling

```
{nwa_bling ...}
```

Smarty registered template function. Adds various kinds of visual effects to the page.

Usage example:

```
{nwa_bling id=$some_id type=fade}
```

The “id” parameter is the ID of the HTML element to which you will add ‘bling’ effects The “type” parameter is the kind of bling desired:

- “fade”: element smoothly fades in and out
- “blink”: element blinks slowly

nwa_makeid

```
{nwa_makeid ...}
```

Smarty registered template function. Creates a unique identifier and assigns it to a named page variable. Identifiers are unique for a given page instantiation.

Usage example:

```
{nwa_makeid var=some_id}
```

The “var” parameter specifies the page variable that will be assigned.

Alternative usage:

```
{nwa_makeid var=some_id file=filename}
```

The “file” parameter specifies a file which contains a unique ID. This allows issued IDs to be unique across different page loads. To return the value rather than assign it to a variable, use the syntax:

```
{nwa_makeid [file=filename] output=1}
```

Otherwise, this template function does not generate any output.

nwa_nav

```
{nwa_nav} ... {/nwa_nav}
```

Smarty registered block function. Defines a block area for navigation, a control, or generates navigation control HTML of a particular type.

Blocks are individual components of the navigation area, which basically consist of HTML. Blocks for actual navigation items have substitution tags in the form **@tagname@**.

The recognized tags are described in the table below.

Table 327: *Navigation Tags*

Tag	Description
@a@	navigation name
@name@	navigation item name (HTML safe)
@jsname@	navigation item name (JavaScript quoted)
@href@	navigation item hyperlink
@jshref@	navigation item hyperlink (JavaScript quoted)
@icon@	navigation item icon, if specified

When used with the “block” parameter, the {nwa_nav} control does not generate any HTML. When used with the “type” parameter, the {nwa_nav} control uses the previously defined blocks to generate the HTML navigation area. The following types are recognized:

- **simple** – Only the current L1 item has L2 items, L3 only when L2 active
- **all-l1** – All current L1 items are shown to L3, otherwise L1 only
- **expanded** – All L1 items have L2 items, L3 only when L2 active
- **all-expanded** – All items shown to L3

The “reset” parameter may be specified to clear any existing navigation settings.

Usage example:

```
{nwa_nav block=level1_active}<li class="active">@a</li>{/nwa_nav}{nwa_nav block=level1_inactive}<li>@a</li>{/nwa_nav}...{nwa_nav type=simple}{/nwa_nav} { * this generates the HTML * }
```

Block types can be one of the following types:

- enter_level1_item

- enter_level2_item
- enter_level3_item
- exit_level1_item
- exit_level2_item
- exit_level3_item
- between_level1_items
- between_level2_items
- between_level3_items
- level1_active
- level1_inactive
- level2_active
- level2_inactive
- level2_parent_active
- level2_parent_inactive
- level3_active
- level3_inactive
- enter_level1
- enter_level2
- enter_level3
- exit_level1
- exit_level2
- exit_level3

nwa_plugin

```
{nwa_plugin ...}
```

Smarty registered template function. Generates plugin information based on the parameters specified. Specifying which plugin:

- The 'id' parameter specifies a plugin ID.
- The 'name' parameter specifies a plugin name, or plugin filename.
- The 'page' parameter specifies a page name provided by the plugin.
- The 'privilege' parameter specifies a privilege defined by the plugin.

If none of the above is specified, the default is the same as specifying the 'page' parameter with the current script name as argument (that is, the current page).

Specifying the output:

- The 'notfound' parameter specifies the return value, if the plugin was not found (default is the empty string).
- The 'output' parameter specifies the metadata field to return

If 'output' is not specified, the default is 'output=id'; that is, the plugin ID is returned.

nwa_privilege

```
{nwa_privilege} ... {/nwa_privilege}
```

Smarty registered block function. Includes output only if a certain kind of privilege has been granted.

Usage examples:

```
{nwa_privilege access=create_user} .. content .. {/nwa_privilege}
```

The “access” parameter specifies the name of a privilege to check for any access.

```
{nwa_privilege readonly=create_user} .. content .. {/nwa_privilege}
```

The “readonly” (synonym “ro”) parameter specifies the name of a privilege to check for read-only access. Be aware that an operator with read-write access also has read-only access. To include content if the user **ONLY** has read access, that is, not if the user has full access, prefix the privilege name with a **#** character and use the parameter name “readonly” (or “ro”).

```
{nwa_privilege full=create_user} .. content .. {/nwa_privilege}
```

The “full” (synonym “rw”) parameter specifies the name of a privilege to check for full read-write access. The “name” parameter is the name of the privilege to check. If “name” is prefixed with a “!”, the output is included only if that privilege is **NOT** granted (inverts the sense of the test). An optional “level” parameter may be specified, which is the level of access to the privilege required (default is 0, or any access).

nwa_replace

```
{nwa_replace 1=... 2=...} ... {/nwa_replace}
```

Smarty registered block function. Replace %1, %2, etc with the passed parameters 1=, 2=, etc.

Usage example:

```
{nwa_replace 1=$param1 2=$param2 ...}
This is the text resource to be replaced, where %1 and %2
are the arguments, etc.
{/nwa_replace}
```

The numbered parameters are expanded in the translated string with the positional arguments **%1**, **%2** and so forth.

nwa_text

```
{nwa_text} ... {/nwa_text}
```

Smarty registered block function. Translates the block’s content, if a language pack is available.

Usage example:

```
{nwa_text id=TEXT_ID 1=$param1 2=$param2 ...}
This is the text resource to be translated, where %1 and %2 are the arguments, etc.
{/nwa_text}
```

- The “id” parameter is the text ID of the resource.
- The numbered parameters are expanded in the translated string with the positional arguments **%1**, **%2** and so forth.

nwa_userpref

```
{nwa_userpref ...}
```

Smarty template function. Returns the current setting of a user preference (stored with the Web application user account)

Usage examples:

```
{nwa_userpref name=prefName}
{nwa_userpref name=prefName default=10}
{nwa_userpref has=prefName}
```

- “name”: return the named user preference
- “default”: supply a value to be returned if the preference is not set
- “has”: return 1 if the named preference exists for the current user, 0 if the preference does not exist

nwa_youtube

```
{nwa_youtube video=ID width=cx height=cy ...} ... {/nwa_youtube}
```

Smarty registered block function. Provides simple support for embedding a YouTube video in the body of a page. The content of this block is the initial “alternate content” that will be presented until the YouTube player can be embedded (if it can be embedded).



Not all devices are capable of playing back YouTube video content.

Usage example:

```
{nwa_youtube video=Y7dpJ0oseIA width=320 height=240}
YouTube is the world’s most popular online video community.
{/nwa_youtube}
```

The supported parameters for this block function are:

- **video** (required) – the YouTube video ID to embed.
- **width** (required) – the width in pixels of the video.
- **height** (required) – the height in pixels of the video.
- **autoplay** (optional) – if true, auto-play the video.
- **chrome** (optional) – if true, use the chromed player; that is, provide a user experience with playback controls.
- **version** (optional) – the minimum version required to play the video.
- **onended** (optional) – the name of a global function (that is, a member of the JavaScript “window” object) that is to be called at the end of video playback.

Date/Time Format Syntax

This section describes the two basic modifiers available for you to use in ClearPass Guest:

- ["nwadateformat Modifier" on page 716](#)
- ["nwatimeformat Modifier" on page 717](#)

nwadateformat Modifier

The date format takes one or two arguments – the format description and an optional default value (used if there is no time/date to display). UTF-8 is the character encoding used throughout the application, as this covers languages such as Spanish that use non-ASCII characters.

The full list of special formats is:

Table 328: *Date and Time Formats*

Preset Name	Date/Time Format	Example
hhmmss	%H%M%S	141345
hh:mm:ss	%H:%M:%S	14:13:45
iso8601	%Y%m%d	20080407
iso8601t	%Y%m%d%H%M%S	20080407141345
iso-8601	%Y-%m-%d	2008-04-07
iso-8601t	%Y-%m-%d %H:%M:%S	2008-04-07 14:13:45
longdate	%A, %d %B %Y, %l:%M %p	Monday, 07 April 2008, 2:13 PM
rfc822	%a, %d %b %Y %H:%M:%S %Z	Mon, 07 Apr 2008 14:13:45 EST
displaytime	%l:%M %p	2:13 PM
recent	-	2 minutes ago

The % items on the right hand side are the same as those supported by the php function [strftime\(\)](#).

The string “?:”, if present will return the string following the “?:” if the time value is 0. Otherwise, the format string up to the “?:” is used.

See "Date/Time Format String Reference" on page 718 in this chapter for a full list of the supported date/time format string arguments.

Examples of date formatting using the nwadateformat Smarty modifier are as follows:

{`$u.expire_time` |nwadateformat:"longdate"}

Monday, 07 April 2008, 2:13 PM

{`$u.expire_time` |nwadateformat:"iso8601"}

20080407

{`$u.expire_time` |nwadateformat:"iso-8601t"}

2008-04-07 14:13:45

{`$u.expire_time` |nwadateformat:"iso8601?:N/A"}

20080407 (or N/A if no time specified)

{`$u.expire_time` |nwadateformat:"%m/%d/%Y"}

04/07/2008

nwatimeformat Modifier

The nwatimeformat modifier takes one argument – the format description. The “minutes_to_natural” argument converts an argument specified in minutes to a text string describing an equivalent but more natural

measurement for the time interval (hours, days or minutes depending on the value). An example of this usage is for the `expire_postlogin` field which has a value measured in minutes:

```
{ $u.expire_postlogin|nwatimeformat:"minutes_to_natural" }
```

The other formats accepted for this modifier are the same as those described for the `nwdateformat` modifier. See "[nwdateformat Modifier](#)" on page 716.

Date/Time Format String Reference

Table 329: *Date and Time Format Strings*

Format	Result
%a	Abbreviated weekday name for the current locale
%A	Full weekday name for the current locale
%b	Abbreviated month name for the current locale
%B	Full month name for the current locale
%c	Preferred date and time representation for the current locale
%C	Century number (2-digit number, 00 to 99)
%d	Day of the month as a decimal number (01 to 31)
%D	Same as %m/%d/%y
%e	Day of the month as a decimal number; a single digit is preceded by a space (' 1' to '31')
%h	Same as %b
%H	Hour as a decimal number (00 to 23)
%I	Hour as a decimal number (01 to 12)
%m	Month as a decimal number (01 to 12)
%M	Minute as a decimal number (00 to 59)
%p	"AM" or "PM"
%r	Local time using 12-hour clock (%I:%M %p)
%R	Local time using 24-hour clock (%H:%M)
%S	Second as a decimal number (00 to 60)
%T	Current time (%H:%M:%S)
%u	Weekday as a decimal number (1=Monday...7=Sunday)
%w	Weekday as a decimal number (0=Sunday...6=Saturday)

Format	Result
%x	Preferred date representation for the current locale, without the time
%X	Preferred time representation for the current locale, without the date
%y	Year as a decimal number without the century (00 to 99)
%Y	Year as a decimal number
%%	A literal % character

Programmer's Reference

This section describes the following:

- ["NwaAlnumPassword"](#) on page 719
- ["NwaBoolFormat"](#) on page 719
- ["NwaByteFormat"](#) on page 720
- ["NwaByteFormatBase10"](#) on page 720
- ["NwaComplexPassword"](#) on page 720
- ["NwaCsvCache"](#) on page 720
- ["NwaDigitsPassword\(\\$len\)"](#) on page 720
- ["NwaDynamicLoad"](#) on page 720
- ["NwaGeneratePictureString"](#) on page 721
- ["NwaGenerateRandomPasswordMix"](#) on page 721
- ["NwaLettersDigitsPassword"](#) on page 721
- ["NwaLettersPassword"](#) on page 721
- ["NwaMoneyFormat"](#) on page 721
- ["NwaParseCsv"](#) on page 722
- ["NwaParseXml"](#) on page 722
- ["NwaPasswordByComplexity"](#) on page 723
- ["NwaSmsIsValidPhoneNumber"](#) on page 723
- ["NwaStrongPassword"](#) on page 723
- ["NwaVLookup"](#) on page 723
- ["NwaWordsPassword"](#) on page 724

NwaAlnumPassword

```
NwaAlnumPassword($len)
```

Generates an alpha-numeric password (mixed case) of length \$len characters.

NwaBoolFormat

```
NwaBoolFormat($value, $options = null)
```

Formats a Boolean value as a string. If 3 function arguments are supplied, the 2nd and 3rd arguments are the values to return for false and true, respectively. Otherwise, the `$options` parameter specifies how to do the conversion:

- If an integer 0 or 1, the string values “0” and “1” are returned.
- If a string containing a “|” character, the string is split at this separator and used as the values for false and true respectively.
- If an array, the 0 and 1 index values are used for false and true values.
- Otherwise, the string values “true” and “false” are returned.

NwaByteFormat

```
NwaByteFormat($bytes, $unknown = null)
```

Formats a non-negative size in bytes as a human readable number (bytes, KB, MB, GB, etc.) Assumes that 1 KB = 1024 bytes, 1 MB = 1024 KB, etc. If a negative value is supplied, returns the `$unknown` string. If a non-numeric value is supplied, that value is returned directly.

NwaByteFormatBase10

```
NwaByteFormatBase10($bytes, $unknown = null)
```

Formats a non-negative size in bytes as a human readable number (bytes, KB, MB, GB, etc.) Assumes “base 10” rules in measurement; that is, 1 KB = 1000 bytes, 1 MB = 1000 KB, etc. If a negative value is supplied, returns the `$unknown` string. If a non-numeric value is supplied, that value is returned directly.

NwaComplexPassword

```
NwaComplexPassword($len = 8)
```

Generates complex passwords of at least `$len` characters in length, where `$len` must be at least 4. A complex password includes at least 1 each of a lower case character, upper case character, digit, and punctuation (symbol).

NwaCsvCache

```
NwaCsvCache($csv_file, $use_cache = true, $options = null)
```

Loads and parses the contents of a CSV file, using a built-in cache. The cache may be cleaned for a specific file by setting `$use_cache` to false. The cache may be cleaned for ALL files by setting `$csv_file` to the empty string and `$use_cache` to false.

CSV parsing options (see ["NwaParseCsv" on page 722](#)) may be specified in `$options`. Additionally, a 2-argument form of this function may be used by passing an array of `$options` as the second argument; in this case, `$use_cache` is assumed to be true. This function returns false if the file does not exist; otherwise, returns an array of arrays containing each of the parsed records from the file.

NwaDigitsPassword(\$len)

```
NwaDigitsPassword($len)
```

Generates digit-only passwords of at least `$len` characters in length.

NwaDynamicLoad

```
NwaDynamicLoad($func)
```

Loads the PHP function `$func` for use in the current expression or code block. Returns true if the function exists (that is, the function is already present or was loaded successfully), or false if the function does not exist.



Attempting to use an undefined function will result in a PHP Fatal Error. Use this function before using any of the standard `Nwa...()` functions.

NwaGeneratePictureString

```
NwaGeneratePictureString($string)
```

Creates a password based on a format string. For details on the special characters recognized in `$string`, see ["Format Picture String Symbols" on page 736](#).

NwaGenerateRandomPasswordMix

```
NwaGenerateRandomPasswordMix($password_len, $lower = 1, $upper = 1, $digit = 1, $symbol = -1)
```

Generates a random password that meets a certain minimum complexity requirement.

- `$password_len` specifies the total length in characters of the generated password. The password returned will be at least `$upper + $lower + $digit + $symbol` characters in length. Any length beyond the required minimum will be made up of any allowed characters.
- `$lower` specifies the minimum number of lowercase characters to include, or -1 to not use any lowercase characters.
- `$upper` specifies the minimum number of uppercase characters to include, or -1 to not use any uppercase characters.
- `$digit` specifies the minimum number of digits to include, or -1 to not use any digits.
- `$symbol` specifies the minimum number of symbol characters to include, or -1 to not use any symbol or punctuation characters.

NwaLettersDigitsPassword

```
NwaLettersDigitsPassword($len)
```

Generates an alpha-numeric password of `$len` characters in length consisting of lowercase letters and digits.

NwaLettersPassword

```
NwaLettersPassword($len)
```

Generates a password of `$len` characters in length consisting of lowercase letters.

NwaMoneyFormat

```
NwaMoneyFormat($amount, $format = null)
```

Formats a monetary amount for display purposes. The current page language is used to adjust formatting to the country specified. Returns a result that is guaranteed to be in UTF-8.

The `$format` argument may be null, to specify the default behavior (U.S. English format), or it may be a pattern string containing the following:

- currency symbol (prefix)
- thousands separator
- decimal point

- number of decimal places

The format “**€1.000,00**” uses the Euro sign as the currency symbol, “.” as the thousands separator, “,” as the decimal point, and 2 decimal places.

If not specified explicitly, the default format is “**\$1,000.00**”.

NwaParseCsv

```
NwaParseCsv($text, $options = null)
```

Parses text containing comma-separated values and returns the result as a list of records, where each record contains a list of fields. Supports CSV escaping using double quotes.

\$options may be specified to control additional parsing options described in the table below.

Table 330: Parsing Options

Function	Description
fs	The field separator character (default is comma “,”)
rs	The record separator character (default is newline “\n”)
quo	The quote character (default is double quote “”)
excel_compatible	If true, recognize “...” syntax as well as “...” (default true)
dos_compatible	If true, convert \r\n line endings to \n (default true)
encoding	If set, specifies the input character set to convert from (default not set)
out_charset	If set, specifies the desired character set to convert to using the iconv() function . (default is "UTF-8//TRANSLIT")
max_records	maximum number of records to return
max_fields	maximum number of fields per record
skip_records	number of records to skip at start of input
skip_fields	number of fields to skip at start of each record
sort	post-processing option; order string for NwaCreateUsortFunc to sort the records by the specified column(s)
slice_offset	post-processing option: starting offset of slice to return; see array_slice() function
slice_length	post-processing option: length of slice to return; see array_slice() function

See “NwaParseCsv” on page 722 and “NwaVLookup” on page 723.

NwaParseXml

```
NwaParseXml($xml_text)
```

Parses a string as an XML document and returns the corresponding document structure as an associative array. Returns an array containing the following elements:

- **error** – set if there was a problem parsing the XML

- **message** – describes the parse error

Otherwise, the return is an array with these elements:

- **name** – name of the document element
- **attributes** – attributes of the document element
- **children** – array containing any child elements
- **content** – element content text

NwaPasswordByComplexity

```
NwaPasswordByComplexity($len, $mode = false)
```

Generates a random password of at least `$len` characters in length, based on one of the standard complexity requirements specified in `$mode`. If `$mode` is false or the empty string, the default password complexity is taken from the Guest Manager plugin configuration.

Otherwise, `$mode` should be one of the following values:

- **none** – No password complexity requirement
- **case** – At least one uppercase and one lowercase letter
- **number** – At least one digit
- **punctuation** – At least one symbol
- **complex** – At least one of each: uppercase letter, lowercase letter, digit, and symbol

NwaSmsIsValidPhoneNumber

```
NwaSmsIsValidPhoneNumber($phone_number)
```

Validates a phone number supplied in E.164 international dialing format, including country code.

- Any spaces and non-alphanumeric characters are removed.
- If the first character is a plus sign (+), the phone number is assumed to be in E.164 format already and the plus sign is removed; otherwise, if the SMS service handler national prefix is set and the phone number starts with that prefix, then the prefix is replaced with the country code.
- The phone number must contain no fewer than 5 and no more than 15 digits.
- The phone number is validated for a valid country code prefix.
- If all the foregoing conditions are met, the validator returns TRUE; otherwise, the validator returns FALSE.

NwaStrongPassword

```
NwaStrongPassword($len)
```

Generate strong passwords of `$len` characters in length.

A strong password may contain uppercase letters, lowercase letters, digits and certain symbols. The strong password does not contain commonly-confused characters such as “O” and “0” (capital O and zero), “l” and “1” (capital I and lowercase L), “2” and “Z” (two and capital Z), or “8” and “B” (eight and capital B).

NwaVLookup

```
NwaVLookup($value, $table, $column_index, $range_lookup = true, $value_column = 0, $cmp_fn = null)
```

Table lookup function, similar to the Excel function VLOOKUP(). This function searches for a value in the first column of a table and returns a value in the same row from another column in the table. This function supports the values described in the table below.

Table 331: *NwaVLookup Options*

Option	Description
\$value	The value to be searched for
\$table	A 2D array of data to search; for example, a data table returned by NwaCsvCache() or NwaParseCsv()
\$column_index	The desired index of the data
\$range_lookup	Specifies whether to find an exact or approximate match. If true (default), assumes the table is sorted and returns either an exact match, or the match from the row with the next largest value that is less than \$value. If false, only an exact match is returned; NULL is returned on no match
value_column	Specifies the column index in the table that contains the values; the default is 0; in other words, the first column.
\$cmp_fn	Specifies a comparison function to use for values; if null, the default is used (simple equality operator ==, or the == and > operators if using binary search). The comparison function should take 2 arguments and return a value < 0, == 0, > 0 depending on the sort ordering of the arguments.

Be aware of the following differences from Excel VLOOKUP:

- Column indexes are 0-based.
- Column indexes can also be strings.

See "[NwaParseCsv](#)" on page 722 and "[NwaCsvCache](#)" on page 720.

NwaWordsPassword

`NwaWordsPassword($len)`

Generates a password consisting of two randomly-chosen words, separated by a small number (1 or 2 digits); that is, in the format **word1XXword2**. The random words selected will have a maximum length of \$len characters, and a minimum length of 3 characters. \$len must be at least 3.

Field, Form, and View Reference

This section describes the following:

- "[GuestManager Standard Fields](#)" on page 725
- "[Hotspot Standard Fields](#)" on page 733
- "[SMS Services Standard Fields](#)" on page 734
- "[SMTP Services Standard Fields](#)" on page 734
- "[Format Picture String Symbols](#)" on page 736
- "[Form Field Validation Functions](#)" on page 737
- "[Form Field Conversion Functions](#)" on page 744

- ["Form Field Display Formatting Functions" on page 745](#)
- ["View Display Expression Technical Reference" on page 747](#)

GuestManager Standard Fields

The table below describes standard fields available for the GuestManager form.

Table 332: *GuestManager Standard Fields*

Field	Description
account_activation	String. The current account activation time in long form. This field is available on the change_expiration and guest_enable forms. The value is generated from the start_time field, and may be one of the following: <ul style="list-style-type: none"> • Account will be enabled at <i>date andtime</i> • Account is currently active • No account activation
auto_update_account	Boolean flag indicating that an already existing account should be updated, rather than failing to create the account. This field should normally be enabled for guest self-registration forms, to ensure that a visitor that registers again with the same email address has their existing account automatically updated. Set this field to a non-zero value or a non-empty string to enable automatic update of an existing account. This field controls account creation behavior; it is not stored with created visitor accounts.
auto_update_account	Boolean flag indicating that an already existing account should be updated, rather than failing to create the account. This field should normally be enabled for guest self-registration forms, to ensure that a visitor that registers again with the same email address has their existing account automatically updated. Set this field to a non-zero value or a non-empty string to enable automatic update of an existing account. This field controls account creation behavior; it is not stored with created visitor accounts.
captcha	Special field used to enable the use of a CAPTCHA security code on a form. This field should be used with the user interface type "CAPTCHA security code" and the standard validator NwaCaptchalsValid in order to provide the standard security code functionality.
change_of_authorization	Boolean flag indicating that any existing sessions for a visitor account should be disconnected or modified using RFC 3576. If this field is not specified on a form that modifies the visitor account, the default value is taken from the configuration for the RADIUS Services plugin. Set this field to a non-zero value or a non-empty string to enable RFC 3576 updates for active sessions. Set this field to a zero value or the empty string to disable RFC 3576 updates for active sessions.
create_time	Integer. Time at which the account was created. The creation time is specified as a UNIX timestamp. This field is automatically configured with the current time when the Initial Value is set to: <code>array('generator' => 'time')</code>
creator_accept_terms	Boolean flag indicating that the creator has accepted the terms and conditions of use. When creating an account, this field must be present, and must be set to the value 1 . If this field is unset, or has any other value, account creation will fail with an error message. To set the correct value for this field, use a check box (to require confirmation from the creator) or a hidden field (if use of the form is considered acceptance of the terms and conditions). This field controls account creation behavior; it is not stored with created visitor accounts.

Field	Description
creator_name	String. Name of the creator of the account. This field does not have a default value. See "sponsor_name" on page 732 .
do_expire	Integer that specifies the action to take when the expire time of the account is reached. See "expire_time" on page 727 . <ul style="list-style-type: none"> 0—Account will not expire 1—Disable 2—Disable and logout 3—Delete 4—Delete and logout <p>“Disable” indicates that the enabled field will be set to 0, which will prevent further authorizations using this account.</p> <p>“Logout” indicates that a RADIUS Disconnect-Request will be used for all active sessions that have a username matching the account username. This option requires the NAS to support RFC 3576 Dynamic Authorization. See "RFC 3576 Dynamic Authorization" on page 37 for more information.</p>
dynamic_expire_time	Integer. Time at which the account will expire, calculated according to the account’s expiration timers. The value of this field is a UNIX timestamp. This field is available when modifying an account using the <code>change_expiration</code> or <code>guest_edit</code> forms.
dynamic_is_authorized	Boolean flag indicating if the user account is authorized to log in. This field is available when modifying an account using the <code>change_expiration</code> or <code>guest_edit</code> forms.
dynamic_is_expired	Boolean flag indicating if the user account has already expired. This field is available when modifying an account using the <code>change_expiration</code> or <code>guest_edit</code> forms.
dynamic_session_time	Integer. The maximum session time that would be allowed for the account, if an authorization request was to be performed immediately. Measured in seconds. Set to 0 if the account is either unlimited (<code>dynamic_is_expired</code> is false), or if the account has expired (<code>dynamic_is_expired</code> is true). This field is available when modifying an account using the <code>change_expiration</code> or <code>guest_edit</code> forms.
email	String. Email address for the account. This field may be up to 100 characters in length. When creating an account, if the username field is not set then the email field is used as the username of the account.
enabled	Boolean flag indicating if the account is enabled. Set this field to 0 to disable the account. If an account is disabled, authorization requests for the account will always fail. Set this field to 1 to enable the account.
expiration_time	String. Description of the account’s expiration time. This field is set when modifying an account. This field is available on the <code>change_expiration</code> and <code>guest_enable</code> forms. The value is generated from the do_expire , expire_time , expire_postlogin and expire_usage fields, and may be one of the following: <ul style="list-style-type: none"> Account will expire at <i>date andtime</i>, or <i>interval</i> after first login, or after <i>interval</i> total usage Account will expire at <i>date andtime</i> or <i>interval</i> after first login Account will expire at <i>date andtime</i> or after <i>interval</i> total usage Account will expire at <i>date andtime</i> Expires <i>interval</i> after first login or after <i>interval</i> total usage Expires <i>interval</i> after first login

Field	Description
	<ul style="list-style-type: none"> Expires after <i>interval</i> total usage No expiration time set
expire_time	<p>Integer. Time at which the account will expire. The expiration time should be specified as a UNIX timestamp.</p> <p>Setting an expire_time value also requires a non-zero value to be set for the do_expire field; otherwise, the account expiration time will not be used. Set this field to 0 to disable this account expiration timer.</p> <p>If the expire_timezone field is used in conjunction with expire_time and a time zone and date are selected, the date calculation is adjusted relative to the time zone.</p>
expire_timezone	<p>String. Provides a drop-down list of time zones to use in conjunction with expire_time and start_time. When expire_timezone is selected and a date is chosen, the date is adjusted to be relative to the time zone. Receipts and edits made after an account is created are displayed in the account's local time zone.</p> <p>By default, expire_timezone uses the NwaGenerateTimeZoneList options generator. To use a smaller subset of time zones, change the Options Generator to (Use options) and provide your "value name" pairs. Please reference the default list for valid time zone values.</p>
expire_usage	<p>Integer. The total time period in seconds for which the account may be used. Usage is calculated across all accounting sessions with the same username. Set this field to 0 to disable this account expiration timer.</p>
http_user_agent	<p>String. Identifies the Web browser that you are using. This tracks user's browsers when they are registering. This is stored with the user's account.</p>
id	<p>String. Internal user ID used to identify the guest account to the system.</p>
ip_address	<p>String. The IP address to assign to stations authenticating with this account. This field may be up to 20 characters in length. The value of this field is not currently used by the system. However, a RADIUS user role may be configured to assign IP addresses using this field by adding the Framed-IP-Address attribute, and setting the value for the attribute to: <code><?=\$user["ip_address"]</code></p>
modify_expire_postlogin	<p>String Value indicating how to modify the expire_postlogin field.</p> <p>This field is only of use when editing a visitor account. It may be set to one of the following values:</p> <ul style="list-style-type: none"> "expire_postlogin" to set the post-login expiration time to the value in the expire_postlogin field; "plus X" or "minus X", where X is a time measurement, to extend or reduce the post-login expiration timer by X (minutes, but may have a "ywdhms" suffix to indicate years, weeks, days, hours, minutes, seconds respectively); A number, to set the post-login expiration time to the value specified; Any other value to leave expire_postlogin unmodified. <p>This field controls account modifications; it is not stored with the visitor account.</p>
modify_expire_time	<p>String. Value indicating how to modify the expire_time field.</p> <p>This field may be provided when creating or editing a visitor account. It may be set to one of the following values:</p> <ul style="list-style-type: none"> "none" to disable the account expiration timer (do_expire and expire_time will both be set to 0); "now" to disable the account immediately; "expire_time" to use the expiration time specified in the expire_time field;

Field	Description
	<ul style="list-style-type: none"> • “expire_after” to set the expiration time to the current time, plus the number of hours in the expire_after field; • “plus <i>X</i>” or “minus <i>X</i>”, where <i>X</i> is a time measurement, to extend or reduce the expiration time by <i>X</i> (hours, but may have a “ywdhms” suffix to indicate years, weeks, days, hours, minutes, seconds respectively); • A time measurement “<i>X</i>”, to set the expiration time to the current time plus <i>X</i>; • Any other value to leave expire_time unmodified. <p>This field controls account creation and modification behavior; it is not stored with created or modified visitor accounts.</p>
modify_expire_usage	<p>String. Value indicating how to modify the expire_usage field. This field is only of use when editing a visitor account. It may be set to one of the following values:</p> <ul style="list-style-type: none"> • “expire_usage” to set the cumulative usage expiration timer to the value in the expire_usage field; • “plus <i>X</i>” or “minus <i>X</i>”, where <i>X</i> is a time measurement, to extend or reduce the cumulative usage expiration timer by <i>X</i> (seconds, but may have a “ywdhms” suffix to indicate years, weeks, days, hours, minutes, seconds respectively); • A number, to set the cumulative usage expiration time to the value specified; • Any other value to leave expire_usage unmodified. <p>This field controls account modifications; it is not stored with the visitor account.</p>
modify_password	<p>String. Value indicating how to modify the account password.</p> <ul style="list-style-type: none"> • It may be one of the following values: • “random_password” to use the password specified in the random_password field; • “reset” to create a new password, using the method specified in the random_password_method field (or the global defaults, if no value is available in this field); • “password” to use the value from the password field; • Any other value leaves the password unmodified. <p>This field controls account creation and modification behavior; it is not stored with created or modified visitor accounts.</p>
modify_start_time	<p>String. Value indicating how to modify the start_time field.</p> <p>It may be one of the following values:</p> <ul style="list-style-type: none"> • “none” to disable the account activation time; • “now” to activate the account immediately; • “start_time” to use the activation time specified in the start_time form field (normally a UNIX time, but may be 0 to disable activation time); • “start_after” to set the activation time to the current time plus the number of hours in the start_after field; • “plus <i>X</i>”, where <i>X</i> is a time measurement, to extend the activation time by <i>X</i>. The time measurement is normally hours, but may have a “ywdhms” suffix to indicate years, weeks, days, hours, minutes, or seconds, respectively. Alternatively, this operation may be written equivalently as ‘+<i>X</i>’, ‘p<i>X</i>’, ‘plus<i>X</i>’, ‘add <i>X</i>’, ‘add<i>X</i>’, or ‘a<i>X</i>’. Example: to delay activation time by 2 days, use the value +2d. • “minus <i>X</i>”, where <i>X</i> is a time measurement, to reduce the activation time by <i>X</i>. See above for details about specifying a time measurement. Alternatively, this operation may be written equivalently as ‘-<i>X</i>’, ‘m<i>X</i>’, ‘minus<i>X</i>’, ‘sub <i>X</i>’, ‘sub<i>X</i>’, or ‘s<i>X</i>’. Example: to bring forward activation time by 12 hours, use the

Field	Description
	<p>value -12h.</p> <ul style="list-style-type: none"> • A time measurement "X", to set the activation time to the current time plus X. • A time and date specification, to set the activation time to that time and date. Many different formats are specified; for clarity it is recommended that a standard format such as ISO-8601 is used ("YYYY-MM-DD hh:mm:ss" format). • Any other value to leave start_time unmodified. <p>This field controls account creation and modification behavior; it is not stored with created or modified visitor accounts.</p>
multi_initial_sequence	Integer. Initial sequence number. This field is used when creating guest accounts and the random_username_method field is set to "nwa_sequence". If this field is not set, the next available sequence number for the given multi_prefix is used. Sequence numbering will start with 0 if no initial sequence number has been set.
multi_prefix	String. The prefix of each username generated when creating guest accounts and the random_username_method field is set to "nwa_sequence".
netmask	String. Network address mask to use for stations using the account. This field may be up to 20 characters in length. The value of this field is not currently used by the system. However, a RADIUS user role may be configured to assign network masks using this field by adding the Framed-IP-Netmask attribute, and setting the value for the attribute to: <code><?= \$user["netmask"]</code>
no_password	Boolean. If set, prevents a user from changing their own password using the guest self-service portal. Set this field to a non-zero value or a non-empty string to disable guest-initiated password changes. The default is to allow guest-initiated password changes, unless this field is set.
no_portal	Boolean. If set, prevents a user from logging into the guest service portal. Set this field to a non-zero value or a non-empty string to disable guest access to the self-service portal. The default is to allow guest access to the self-service portal, unless this field is set.
no_warn_before	Boolean. User does not receive a logout expiration warning. The admin or user can opt out of this option by setting the field to 1.
notes	String. Comments or notes stored with the account. This field may be up to 255 characters in length.
num_accounts	Integer. The number of accounts to create when using the create_multi form. This field controls account creation behavior; it is not stored with created visitor accounts.
password	String. Password for the account. This field may be up to 64 characters in length.
password2	String. Password for the account. If this field is set, its value must match the value of the password field for the account to be created or updated. This can be used to verify that a password has been typed correctly. This field controls account creation and modification behavior; it is not stored with created or modified visitor accounts.
password_action	String. Controls the password changing behavior for a guest account. This field may be set to one of the following values: <ul style="list-style-type: none"> • <i>empty string</i> – Default behavior; that is, guests are not required to change

Field	Description
	<p>their password</p> <ul style="list-style-type: none"> • deny – Prevents the guest from changing their password • first – Requires the guest to change their password on their first login • next – Requires the guest to change their password on their next login • recur – Require the guest to change their password on a regular schedule (as specified by the <code>password_action_recur</code> field) • recur_next – Require the guest to change their password on their next (or first) login, and then on a regular schedule (as specified by the <code>password_action_recur</code> field) <p>If the guest is required to change their password, this will take place during a network login, before the guest is redirected to the NAS for login. Guest password changes are only supported for Web login pages and guest self-registration pages that have the “Perform a local authentication check” option enabled.</p> <p>The default behavior is to leave guest passwords under the control of the guest. With the default behavior, guests are not prevented from changing their password, but are also not required to change it on any particular schedule.</p>
password_action_recur	String. Specifies a date or relative time, after which a guest will be required to change their password. Using this field also requires the password_action field to be set to the value ‘recur’. The value of this field should be a relative time measurement, indicated with a plus sign; for example “+15 days” or “+2 months”.
password_last_change	Integer. The time that the guest’s password was last changed. The password change time is specified as a UNIX timestamp. This field is automatically updated with the current time when the guest changes their password using the self-service portal.
random_password	String. This field contains a randomly-generated password. This field is set when modifying an account (guest_edit form).
random_password_length	String. The length, in characters, of randomly generated account passwords. <ul style="list-style-type: none"> • For nwa_words_password, the random_password_length is the maximum length of the random words to use. Two random words will be used to create the password, joined together with a small number (up to 2 digits). • For nwa_picture_password, the random_password_length is ignored.
random_password_method	String. Identifier specifying how passwords are to be created. It may be one of the following identifiers: <ul style="list-style-type: none"> • nwa_digits_password to create a password using random digits. The length of the password is specified by the <code>random_password_length</code> field. • nwa_letters_password to create a password using random lowercase letters (a through z). The length of the password is specified by the <code>random_password_length</code> field. • nwa_lettersdigits_password to create a password using random lowercase letters and digits (a through z and 0 through 9). The length of the password is specified by the <code>random_password_length</code> field. • nwa_alnum_password to create a password using a combination of random digits, uppercase letters and lowercase letters (a-z, A-Z and 0-9). The length of the password is specified by the <code>random_password_length</code> field. • nwa_strong_password to create a password using a combination of digits, uppercase letters, lowercase letters, and some punctuation. Certain characters are omitted from the password. The length of the password is

Field	Description
	<p>specified by the <code>random_password_length</code> field.</p> <ul style="list-style-type: none"> • nwa_complex_password to create a complex password string which contains uppercase letters, lowercase letters, digits and symbol characters. • nwa_complexity_password is dynamic and matches your complexity setting for password generation. For example, if you require your passwords to have both letters and digits, then this validator will confirm that the password has at least one of each. • nwa_words_password to create a random password using a combination of two randomly-selected words and a number between 1 and 99. The maximum length of each of the randomly-selected words is specified by the random_password_length field. • nwa_picture_password to create a password using the format string specified by the <code>random_password_picture</code> field.
<code>random_password_picture</code>	<p>String. The format string to use when creating a random password, if random_password_method is set to "nwa_picture_password".</p>
<code>random_username_length</code>	<p>The length, in characters, of randomly generated account usernames.</p> <ul style="list-style-type: none"> • For <code>nwa_words_password</code>, the random_username_length is the maximum length of the random words to use. Two random words will be used to create the username, joined together with a small number (up to 2 digits). • For <code>nwa_picture_password</code>, the random_username_length is ignored. • For <code>nwa_sequence</code>, the random_username_length is the length of the sequence number in the username; the sequence number will be zero-padded. For example, specifying a length of 4 will result in sequence numbers 0001, 0002, etc.
<code>random_username_method</code>	<p>String. Identifier specifying how usernames are to be created. It may be one of the following identifiers:</p> <ul style="list-style-type: none"> • nwa_sequence to assign sequential usernames. In this case, the multi_prefix field is used as the prefix for the username, followed by a sequential number; the number of digits is specified by the random_username_length field. • nwa_picture_password to create a random username using the format string specified by the random_username_picture field. • nwa_digits_password to create a username using random digits. The length of the username is specified by the random_username_length field. • nwa_letters_password to create a username using random lowercase letters. The length of the username is specified by the random_username_length field. • nwa_lettersdigits_password to create a username using random lowercase letters and digits. The length of the username is specified by the random_username_length field. • nwa_alnum_password to create a username using a combination of random digits, uppercase letters and lowercase letters. The length of the username is specified by the random_username_length field. • nwa_strong_password to create a username using a combination of digits, uppercase letters, lowercase letters, and some punctuation. Certain characters are omitted from the generated username to ensure its readability (for example, "o", "O" and "0"). The length of the username is specified by the random_username_length field. • nwa_words_password to create a username using a combination of two randomly-selected words and a number between 1 and 99. The maximum length of each of the randomly-selected words is specified by the random_username_length field.

Field	Description
random_username_picture	String. The format string to use when creating a username, if the random_username_method field is set to nwa_picture_password . See "Format Picture String Symbols" on page 736 for a list of the special characters that may be used in the format string.
remote_addr	String. The IP address of the guest at the time the guest account was registered. This field may be up to 20 characters in length. The value of this field is not currently used by the system.
role_id	Integer. Role to assign to the account. The value of this field must be the integer ID of a valid RADIUS user role.
role_name	String. Name of the role assigned to the account.
start_after	Integer. Time period, in hours, after which the account will be enabled. This field is used when the modify_start_time field is set to start_after . The value is specified in hours and is relative to the current time. This field controls account creation behavior; it is not stored with created visitor accounts.
start_time	Integer. Time at which the account will be enabled. The time should be specified as a UNIX timestamp.
secret_answer	String. The guest's answer to the secret question that is stored in the secret_question field. To use this field, first add both the secret_question and secret_answer fields to a guest self-registration form. Then, in the self-service portal for a guest self-registration page, select the "Secret Question" as the Required Field. This configuration requires that guests provide the correct answer in order to reset their account password. Answers must match with regards to case in order to be considered as correct.
secret_question	String. The guest's secret question used to confirm the identity of a guest during a reset password operation.
simultaneous_use	Integer. Maximum number of simultaneous sessions allowed for the account.
sponsor_email	Email address of the sponsor of the account. If the sponsor_email field can be inserted into an email receipt and used future emails, the "Reply-To" email address will always be the email address of the original sponsor, not the current operator.
sponsor_name	String. Name of the sponsor of the account. The default value of this field is the username of the current operator.
submit	No Type. Field attached to submit buttons. This field controls account creation behavior; it is not stored with created visitor accounts.
user_activity	Integer. Login activity of the guest account. This field is available in views and may be used to determine the most recent start and stop time of visitor account sessions.
username	String. Username of the account. This field may be up to 64 characters in length.

Field	Description
visitor_company	String. The visitor's company name.
visitor_name	String. The visitor's full name.
visitor_phone	String. The visitor's contact telephone number.

Hotspot Standard Fields

The table below describes standard fields available for the Hotspot form.

Table 333: *Hotspot Standard Fields*

Field	Description
address	String. The visitor's street address.
card_code	String. The 3 or 4 digit cardholder verification code printed on the credit card. This field is only used during transaction processing.
card_expiry	String. Credit card expiry date. This field is only used during transaction processing.
card_name	String. Name shown on the credit card. This field is only used during transaction processing.
card_number	String. Credit card number. This field is only used during transaction processing.
city	String. The visitor's city or town name.
country	String. The visitor's country name.
first_name	String. The visitor's first name.
hotspot_plan_id	No Type. The ID of the plan (visitor access settings) selected by the visitor.
hotspot_plan_name	No Type. The name of the plan (visitor access settings) selected by the visitor.
last_name	String. The visitor's last name.
password2	String. Password for the account (used to confirm a manually typed password).
personal_details	No Type. Field attached to a form label.
purchase_amount	No Type. Total amount of the transaction. This field is only used during transaction processing.
purchase_details	No Type. Field attached to a form label.
state	String. The visitor's state or locality name.
submit_free	No Type. Field attached to a form submit button.
visitor_accept_terms	Boolean. Flag indicating that the visitor has accepted the terms and conditions of use.
visitor_fax	String. The visitor's fax telephone number.
zip	String. The visitor's zip or postal code.

SMS Services Standard Fields

The table below describes standard fields available for the SMS Services form.

Table 334: *SMS Services Standard Fields*

Field	Description
auto_send_sms	Boolean. Flag indicating that a SMS receipt should be automatically sent upon creation of the account.
sms_auto_send_field	String. This field specifies the name of the field that contains the auto-send flag. If blank or unset, the default value from the SMS plugin configuration is used. Additionally, the special values “_Disabled” and “_Enabled” may be used to never send an SMS or always send an SMS, respectively.
sms_enabled	Boolean. This field may be set to a non-zero value to enable sending an SMS receipt. If unset, the default value is true.
sms_handler_id	String. This field specifies the handler ID for the SMS service provider. If blank or unset, the default value from the SMS plugin configuration is used.
sms_phone_field	String. This field specifies the name of the field that contains the visitor’s phone number. If blank or unset, the default value from the SMS plugin configuration is used.
sms_template_id	String. This field specifies the print template ID for the SMS receipt. If blank or unset, the default value from the SMS plugin configuration is used.
sms_warn_before_message	String. This field overrides the logout warning message. If blank or unset, the default value from the Customize SMS Receipt page is used
visitor_carrier	String. The visitor’s mobile phone carrier.

SMTP Services Standard Fields

The table below describes standard fields available for the SMTP Services.

Table 335: *SMTP Services Standard Fields*

Field	Description
auto_send_smtp	Boolean. Flag indicating that an email receipt should be automatically sent upon creation of the guest account. Set this field to a non-zero value or a non-empty string to enable an automatic email receipt to be sent. This field can be used to create an <i>opt-in</i> facility for guests. Use a check box for the auto_send_smtp field and add it to the create_user form, or a guest self-registration instance, and email receipts will be sent to the visitor only if the check box has been selected. Alternatively, to always send an SMTP receipt, this field can be set to a value of 1 using a hidden field.
smtp_auto_send_field	String. This field specifies the name of the field that contains the auto-send flag. If blank or unset, the default value from the email receipt configuration is used. Additionally, the special values _Disabled and _Enabled may be used to never send email or always send email, respectively.
smtp_cc_action	String. This field specifies how to send copies of email receipts. It may be one of never , always_cc , always_bcc , conditional_cc , or conditional_

Field	Description
	bcc. If blank or unset, the default value from the email receipt configuration is used.
smtp_cc_list	String. This field specifies a list of additional email addresses that will receive a copy of the visitor account receipt. If the value is default , the default carbon-copy list from the email receipt configuration is used.
smtp_email_field	String. This field specifies the name of the field that contains the visitor's email address. If blank or unset, the default value from the email receipt configuration is used. Additionally, the special value _None indicates that the visitor should not be sent any email.
smtp_enabled	String. This field may be set to a non-zero value to enable sending an email receipt. If unset, the default value from the email receipt configuration is used. The special values _Auto (Always auto-send guest receipts by email), _AutoField (Auto-send guest receipts by email with a special field set), _Click (Display a link enabling a guest receipt via email), and _Cc (Send an email to a list of fixed addresses) may also be used.
smtp_receipt_format	String. This field specifies the email format to use for the receipt. It may be one of plaintext (No skin – plain text only), html_embedded (No skin – HTML only), receipt (No skin – Native receipt format), default (Use the default skin), or the plugin ID of a skin plugin to specify that skin. If blank or unset, the default value from the email receipt configuration is used.
smtp_subject	String. This field specifies the subject line for the email message. Template variables appearing in the value will be expanded. If the value is default , the default subject line from the email receipt configuration is used.
smtp_template_id	String. This field specifies the print template ID to use for the email receipt. If blank or unset, the default value from the email receipt configuration is used.
smtp_warn_before_subject	String. This field overrides what is specified in the subject line under Logout Warnings on the email receipt. If the value is "default", the default subject line under the Logout Warnings section on the email receipt configuration is used.
smtp_warn_before_template_id	String. This field overrides the print template ID specified under Logout Warnings on the email receipt. If the value is "default", the default template ID under the Logout Warnings section on the email receipt configuration is used.
smtp_warn_before_receipt_format	String. This field overrides the format in the Email Receipt field under Logout Warnings. It may be one of "plaintext" (No skin – plain text only), "html_embedded" (No skin – HTML only), "receipt" (No skin – Native receipt format), "default" (Use the default skin), or the plugin ID of a skin plugin to specify that skin. If blank or unset, the default value in the Email Receipt Field under the Logout Warnings on the email receipt configuration is used.
smtp_warn_before_cc_list	String. This overrides the list of additional email addresses that receive a copy of the visitor account under Logout Warnings on the email receipt. If the value is "default", the default carbon-copy list under Logout Warnings from the email receipt configuration is used.

Field	Description
smtp_warn_before_cc_action	String. This field overrides how copies are sent as indicated under Logout Warnings on the email receipt. to send copies of email receipts. It may be one of "never", "always_cc", "always_bcc", "conditional_cc", or "conditional_bcc". If blank or unset, the default value from the email receipt configuration is used.
warn_before_from_sponsor	String. This field overrides the Reply To field (that is, the sponsor_email field of a user, or the admin's email) under the Logout Warnings on the email receipt. If the value is "default", the Reply To field under Logout Warnings from the email receipt configuration is used.
warn_before_from	String. This field overrides the Override From field under the Logout Warnings on the email receipt. If the value is "default", the Override From field under Logout Warnings from the email receipt configuration is used.

Format Picture String Symbols

When generating a username or password using the `nwa_picture_password` method, a "picture string" should be provided to specify the format of generated username or password in the **random_username_picture** or **random_password_picture** field.

The picture string is used as the username or password, with the following symbols replaced with a random character:

Table 336: *Picture String Symbols*

Symbol	Replacement
#	Random digit (0-9)
\$ or ?	Random letter (A-Z, a-z)
_	Random lowercase letter (a-z)
^	Random uppercase letter (A-Z)
*	Random letter or digit (A-Z, a-z, 0-9)
!	Random punctuation symbol, excluding apostrophe and quotation marks
&	Random character (letter, digit or punctuation excluding apostrophe and quotation marks)
@	Random letter or digit, excluding vowels

Any other alphanumeric characters in the picture string will be used in the resulting username or password. Some examples of the picture string are shown below:

Table 337: *Picture String Example Passwords*

Picture String	Sample Password
####	3728
user####	user3728
v^#_	vQU3nj
#####	Bh7Pm

Form Field Validation Functions

See ["Form Validation Properties" on page 326](#), and ["Examples of Form field Validation" on page 328](#) for details about using validation functions for form fields.

The built-in validator functions are:

- **isArrayKey** – Checks that the value is one of the keys in the array supplied as the argument to the validator.
- **isArrayValue** – Checks that the value is one of the values in the array supplied as the argument to the validator.
- **isEqual** – Checks that the value is equal to the value supplied as the argument to the validator, allowing for standard type conversion rules.
- **isGreaterThan** – Checks that the value is strictly greater than a specified minimum value supplied as the argument to the validator.
- **isIdentical** – Checks that the value is equal to the value supplied as the argument to the validator, and has the same type.
- **isInRange** – Checks that the value is in a specified range between a minimum and maximum value. The minimum and maximum values are specified as a 2-element array as the argument to the validator.
- **isInOptionsList**—Checks against a list of options in the policy definition.
- **isNonEmpty** – Checks that the value is a non-empty string (length non-zero and not all whitespace), or a non-empty array.
- **isNonNegative** – Checks that the value is numeric and non-negative.
- **isRegexMatch** – Checks that the value matches a regular expression supplied as the argument the validator. The regular expression should be a Perl-compatible regular expression with delimiters. For example, the validator argument `/^a/i` will match any value that starts with an "a", case-insensitively. ["Regular Expressions" on page 749](#) for more information about regular expression syntax.
- **isValidAirGroupSharedGroups** – Checks that the value is a valid shared group list. Otherwise, returns a description of the error(s).

If `$arg` is an array it may specify the following options:

- `syntax_only`: Default `true`. If `false`, requires that the values provided correspond to those from the AirGroup plugin configuration.
- `protocol_version`: Default 2. If 1, changes the default validation properties (see below).

- `max_groups`: Maximum number of groups to allow, default 32.
- `max_group_length`: Maximum length in characters of any single group name, default 64.
- `max_group_list_length`: Maximum total length of the group list, including comma separator characters, default 320.

Shared groups are only available in AirGroup protocol version 2. If validation is performed with AirGroup protocol version 1 (i.e., `$arg` is set to `array ('protocol_version' => 1)`), then a non-empty group list is considered an error.

Setting a `max_*` parameter to 0 disables validation of that property.

- **IsValidAirGroupSharedLocations** – Checks that the value is a valid shared location list. Otherwise, returns a description of the error(s).
 1. Checks if a value consists of valid tag = value pairs. Tag should be AP-Name, AP-Group, or FQLN, else error is thrown.
 2. FQLN format is dot-separated and the format is APname.Floor.Building.Campus. Floor bit has to be "floor" + an integer.
 3. The number of tag=value pairs should not be more than 5.
 4. AP-Name value should not contain a '.'

If `$arg` is an array it may specify the following options:

- `syntax_only`: Default `true`. If `false`, requires that the values provided correspond to those from the AirGroup controller configuration.
- `protocol_version`: Default 2. If 1, changes the default validation properties (see below).
- `max_locations`: Maximum number of location tags to allow, default 100.
- `max_location_length`: Maximum length in characters of any single location tag, default 64.
- `max_location_list_length`: Maximum total length of the shared location list, including comma separator characters, default 1000.
- `include_ap_group`: Default `true`. Allows AP-Group=... tags.
- `include_ap_name`: Default `true`. Allows AP-Name=... tags.
- `include_fqln`: Default `true`. Allows FQLN=... tags.

For the same validation as performed in AirGroup protocol version 1, set `$arg` to `array ('protocol_version' => 1)`.

Setting a `max_*` parameter to 0 disables validation of that property.

- **IsValidAirGroupSharedRoles** – Checks that value is a valid shared role list. Otherwise, returns a description of the error(s).

If `$arg` is an array it may specify the following options:

- `syntax_only`: Default `true`. If `false`, requires that the values provided correspond to those from the AirGroup controller configuration.
- `protocol_version`: Default 2. If 1, changes the default validation properties (see below).
- `max_roles`: Maximum number of roles to allow, default 100.
- `max_role_length`: Maximum length in characters of any single role name, default 64.
- `max_role_list_length`: Maximum total length of the role list, including comma separator characters, default 1000.

For the same validation as performed in AirGroup protocol version 1, set `$arg` to `array('protocol_version' => 1)`.

Setting a `max_*` parameter to 0 disables validation of that property.

- **IsValidAirGroupSharedTime** – Checks that the value is a valid time-based sharing policy. Otherwise, returns a description of the error(s). Validation is first performed on the basic time sharing rules. For information about the type of validation performed, see ["AirGroup Time-Based Sharing Syntax Examples" on page 85](#).

If `$arg` is an array, it may specify any of the options accepted by the sub-validators for shared users, shared roles, shared locations, and shared groups.

General validation options:

- `syntax_only`: Default `true`. If `false`, requires that the values provided correspond to those from the AirGroup controller configuration.
- `protocol_version`: Default 2. If 1, changes the default validation properties (see below).

Validating shared locations:

- `max_locations`: Maximum number of location tags to allow, default 100.
- `max_location_length`: Maximum length in characters of any single location tag, default 64.
- `max_location_list_length`: Maximum total length of the shared location list, including comma separator characters, default 1000.
- `include_ap_group`: Default `true`. Allows AP-Group=... tags.
- `include_ap_name`: Default `true`. Allows AP-Name=... tags.
- `include_fqln`: Default `true`. Allows FQLN=... tags.

Validating shared roles:

- `max_roles`: Maximum number of roles to allow, default 100.
- `max_role_length`: Maximum length in characters of any single role name, default 64.
- `max_role_list_length`: Maximum total length of the role list, including comma separator characters, default 1000.

Validating shared users:

- `max_users`: Maximum number of usernames to allow, default 100.
- `max_user_length`: Maximum length in characters of any single username, default 64.
- `max_user_list_length`: Maximum total length of the username list, including comma separator characters, default 1000.

For the same validation as performed in AirGroup protocol version 1, set `$arg` to `array('protocol_version' => 1)`.

Setting a `max_*` parameter to 0 disables validation of that property.

- **IsValidAirGroupSharedUser** – Checks that the value is a comma-separated user list, where user names should not contain "," or space.

If `$arg` is an array it may specify the following options:

- `protocol_version`: Default 2. If 1, changes the default validation properties (see below).
- `max_users`: Maximum number of usernames to allow, default 100.
- `max_user_length`: Maximum length in characters of any single username, default 64.

- `max_user_list_length`: Maximum total length of the username list, including comma separator characters, default 1000.

For the same validation as performed in AirGroup protocol version 1, set `$arg` to `array('protocol_version' => 1)`.

Setting a `max_*` parameter to 0 disables validation of that property.

- **IsValidBool** – Checks that the value is a standard Boolean truth value. Valid Boolean values are the integers **0** and **1** and the PHP values **false** and **true**.
- **IsValidDateTime** – Checks that the value appears to be a valid time specification string according to the rules of the PHP function [strtotime\(\)](#). Valid date/time syntax includes ISO 8601 standard times (**YYYY-MM-DD hh:mm:ss**) with and without time zone specifications, as well as many other formats. The `$value` is expected to be an integer specifying a UNIX time value (seconds since 1970-01-01 00:00:00 UTC).

`$arg` may be:

- `null`, to not perform any min/max check
- a scalar value, to use as the maximum allowable value
- an array containing "min" or "max" entries

Use the syntax:

```
array(
    'min' => '1 day',
    'max' => '90 days',
)
```

- **IsValidEmail** – Checks that the value appears to be a valid [RFC 822](#)-compliant email address. When using the `IsValidEmail` validator, the validator argument may be specified with a whitelist/blacklist of domain names. Use the syntax:

```
array(
    'allow' => array(
        'corp-domain.com',
        'other-domain.com',
    ),
    'deny' => array(
        'blocked-domain.com',
        'other-blocked-domain.com',
    ),
)
```

- The keys 'whitelist' and 'blacklist' may also be used for 'allow' and 'deny', respectively.
- An 'allow' or 'deny' value that is a string is converted to a single element array.
- Wildcard matching may be used on domain names: the prefix '*' means match any domain that ends with the given suffix. A '*' component can also be used inside the hostname, and will match zero or more domain name components.
- If the 'allow' list is empty or unset, the default behavior is to accept ALL domains other than those listed in the 'deny' list.
- If the 'deny' list is empty or unset, the default behavior is to deny ALL domains other than those listed in the 'allow' list.
- If both 'allow' and 'deny' lists are provided, the default behavior is to accept a domain name that does not match any of the patterns provided. The 'allow' list is checked first, followed by 'deny'. To obtain the opposite behavior, specify the wildcard '*' as the last entry in the 'deny' list.
- **IsValidFileUpload** – Checks that the value is a file upload.

- **IsValidFutureDateTime** – Checks that the value is a valid time specification string according to the rules of the PHP function [strtotime\(\)](#), and that the time specification refers to a point in the future. The `$value` is expected to be an integer specifying a UNIX time value (seconds since 1970-01-01 00:00:00 UTC).

`$arg` may be:

- `null`, to not perform any min/max check
- a scalar value, to use as the maximum allowable value
- an array containing "min" or "max" entries

Use the syntax:

```
array(
    'min' => '1 day',
    'max' => '90 days',
)
```

- **IsValidFutureTimestamp** – Checks that the value is a valid UNIX time referring to a point in the future. The `$value` is expected to be an integer specifying a UNIX time value (seconds since 1970-01-01 00:00:00 UTC).

`$arg` may be:

- `null`, to not perform any min/max check
- a scalar value, to use as the maximum allowable value
- an array containing "min" or "max" entries

Use the syntax:

```
array(
    'min' => '1 day',
    'max' => '90 days',
)
```

- **IsValidHostname** – Checks that the value is a valid IP address or a hostname that resolves to an IP address.
- **IsValidHostnameCidr** – Checks that the value is a valid IP address or hostname, which may also have an optional /N suffix indicating the network prefix length in bits (CIDR notation).
- **IsValidHostnamePort** – Checks that the value is a valid IP address or hostname, which may optionally include a port number specified with the syntax **hostname:port**.
- **IsValidIpAddr** – Checks that the value is a valid IP address.
- **IsValidLdapAttribute** – Checks that the value is a valid LDAP attribute name; that is, a string that starts with a letter, and which contains only letters, numbers, underscore (`_`) and hyphen (`-`).
- **IsValidMacAddress** – Checks that the input looks anything like a valid MAC address. This function accepts MAC addresses in all of the following formats:
 - 3456789abcde
 - 34:56:78:9a:bc:de
 - 3456.789a.bcde
 - 34-56-78-9A-BC-DE
- **IsValidNetmask** – Checks that the value is a valid network mask in dotted-quad notation; that is, an IP address such as 255.255.255.128 that contains a single string of *N* 1 bits followed by (32 – *N*) 0 bits.

- **IsValidNumber** – Checks that the value is numeric; that is, an integer or a decimal value. The validator argument may be an array containing one or more of the following additional options:
 - **no_negative** – if set to true, negative numbers are not accepted as a valid value.
 - **no_zero** – if set to true, zero is not accepted as a valid value.
 - **only_integer** – if set to true, decimal numbers are not accepted and only integer values are valid.
- **IsValidPassword** – Checks that password entries satisfy requirements for guest users. This function is essentially equivalent to IsValidPassword2 but with the settings configured based on Guest Manager's configuration settings. Most deployments with a need to validate passwords should use the IsValidPassword2 validator.
- **IsValidPassword2** – Checks that the value is a valid password that satisfies certain requirements. The validator argument must be an array describing which of the following requirements to check. To perform any password checking, the "minimum_length" and "complexity_mode" fields must be specified.
 - **password2** – specifies the name of the field containing the duplicate password entry (optional, for password validation). Defaults to "password2" if not specified.
 - **password2_required** – if nonzero, indicates that the "password2" entry must be supplied.
 - **username** – specifies the name of the field containing the username. If empty or unset, the password is not checked against this field for a match.
 - **minimum_length** – specifies the minimum length of the password in characters.
 - **disallowed_chars** – if set, specifies characters that are not allowed in the password.
 - **complexity_mode** – specifies the set of rules to use when checking the password.
 - **complexity** – if set, specifies rules for checking the composition of the password. If unset, defaults to a preset value for password complexity with modes "none", "basic", "number", "punctuation" and "complex". These rules check that passwords obey certain requirements according to the following table:

Table 338: *Complexity Requirements*

Rule Set	Min. Length	Description
none	–	No special requirements
basic	8	Non-space characters
number	8	At least 1 digit
punctuation	8	At least 1 punctuation character (non-alphanumeric)
complex	8	At least 1 digit, 1 non-alphanumeric, 1 uppercase and 1 lowercase letter

- **IsValidPatternMatch** – Validator that returns true if \$value matches a certain pattern, specified as a series of 'allow' and 'deny' patterns. The \$arg may be specified with a whitelist/blacklist of patterns.

Use the syntax:

```
array(
  'allow' => array(),
  'deny' => array(
    'gmail.com',
    'yahoo.com',
    '*.cn',
  )
)
```

Allow/deny list syntax:

- The keys 'whitelist' and 'blacklist' may also be used for 'allow' and 'deny', respectively.
- An 'allow' or 'deny' value that is a string is converted to a single element array.
- Wildcard matching may be used in patterns: the '*' character matches zero or more characters, '?' matches a single character.
- If the 'allow' list is empty or unset, the default behavior is to accept ALL values other than those listed in the 'deny' list.
- If the 'deny' list is empty or unset, the default behavior is to deny ALL values other than those listed in the 'allow' list.
- If both 'allow' and 'deny' lists are provided, the default behavior is to check the 'deny' list, followed by the 'allow' list. If the value does not match any pattern, then the default is to accept the value. To obtain the opposite behavior (i.e. deny by default), specify the wildcard '*' as the last entry in the 'deny' list.
- This behavior may be altered using the 'order' and 'default' options described below.

Additional options:

- 'trim' => false may be specified in \$arg to not strip leading and trailing whitespace from the value being checked (and the patterns). The default is 'trim' => true, i.e., leading/trailing whitespace is ignored.
 - 'case_sensitive' => true may be specified in \$arg to perform case-sensitive pattern matching. The default is 'case_sensitive' => false, i.e., case-insensitive matching.
 - 'order' => 'allow,deny' or 'order' => 'deny,allow' may be used to change the order in which the pattern lists are checked. The default is 'allow,deny', i.e., the allow list is checked first, followed by the deny list.
 - 'default' => 'allow' or 'default' => 'deny' may be used to change the result returned when no pattern matches. The default is 'allow'.
 - 'regexp' => '/.../' specifies a complete PCRE pattern (including delimiters and option characters, if required) against which the pattern will be matched on entry. This matching step is performed before any whitelist or blacklist processing is done. A failed match will result in the validator failing.
 - 'use_regexp' => true may be specified if all of the allow/deny patterns are actually complete PCRE patterns (including delimiters and option characters). The default is 'use_regexp' => false, i.e., the pattern rules specified above are used.
- **IsValidSentence** – Checks that the value is considered to be a “sentence”; that is, a string which starts with an upper-case letter and ends in a full stop.
 - **IsValidSpanishDNI** – Checks that a string is a valid Spanish DNI/NIE.
 - **DNI** = Documento Nacional de Identidad
 - **NIE** = Número de Identificación de Extranjeros
- These identifiers are nine letters/digits long, in the format:
- ```
00000000A (DNI)
X0000000A (NIE)
```
- where '0' indicates a number, 'X' indicates a letter, and 'A' indicates a checksum letter.
- **IsValidTimestamp** – Checks that the value is a numeric UNIX timestamp (which measures the time in seconds since January 1, 1970 at midnight UTC).
  - **IsValidTimeZone** – Checks that the value is a valid string describing a recognized time zone.

- **IsValidUrl** – Checks that the value appears to be a valid URL that includes a scheme, hostname and path. For example, in the URL <http://www.example.com/>, the scheme is **http**, the hostname is **www.example.com** and the path is **/**. The validator argument may optionally be an array containing a 'scheme' key that specifies an array of acceptable URL protocols.
- **IsValidUsername** – Checks that the value is a valid username. Usernames cannot be blank or contain spaces.
- **NwaCaptchalsValid** – Checks that the value matches the security code generated in the CAPTCHA image. This validator should only be used with the standard **captcha** field.
- **NwaGuestManagerIsValidRoleId** – Checks that the value is a valid role ID for the current operator and user database.
- **NwaHotspotsIsValidCardCode** – Checks a cardholder verification code.
- **NwaHotspotsIsValidCardExpiry** – Checks a card expiry date. Expects a number in one of the following formats:
  - MMY
  - MM/YY
  - MM-YY
  - MM.YY
  - MMYYY
  - MM/YYYY
  - MM-YYYY
  - MM.YYYY

The year is expected to be between the current year and 2036, inclusive.
- **NwaHotspotsIsValidCardNumber** – Checks the entry of a credit card number.
- **NwaSmsIsValidPhoneNumber** – Validates an E.164 international phone number. E.164 numbers must start with a recognized country code. Additional punctuation such as space, -, and () are removed. A leading + (international prefix) is removed if present.
- **NwalsValidExpireAfter** – Checks that the value is one of the account expiration time options specified in the Guest Manager configuration.
- **NwalsValidLifetime** – Checks that the value is one of the account lifetime options specified in the Guest Manager configuration.

## Form Field Conversion Functions

The Conversion and Value Format functions that are available are listed below:

- **NwaConvertOptionalDateTime** – Converts a string representation of a time to the UNIX time representation (integer value). The conversion leaves blank values unmodified.
- **NwaConvertOptionalInt** – Converts a string representation of an integer to the equivalent integer value. The conversion leaves blank values unmodified.
- **NwaConvertStringToOptions** – Converts a multi-line string representation of the form

```
key1 | value1
key2 | value2
```

to the array representation

```
array (
 'key1' => 'value1',
 'key2' => 'value2',
)
```

- **NwaImplodeComma** – Converts an array to a string by joining all of the array values with a comma.
- **NwaTrim** – Removes leading and trailing whitespace from a string value.
- **NwaTrimAll** – Removes all whitespace from a string (including embedded spaces, newlines, carriage returns, tabs, etc).
- **NwaStrToUpper** – Formats the text string to all uppercase letters.
- **NwaStrToLower** – Formats the text string to all lowercase letters.
- **NwaNormalizePhoneNumber** – Removes all spaces, dashes, parenthesis and non-numerical characters from the phone number.

## Form Field Display Formatting Functions

The Display Functions that are available are listed below:

**Table 339:** *Form Field Display Functions*

| Function          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| NwaBoolFormat     | <p>Formats a Boolean value as a string.</p> <ul style="list-style-type: none"> <li>• If the argument is 0 or 1, a 0 or 1 is returned for false and true, respectively.</li> <li>• If the argument is a string containing a “ ” character, the string is split at the   separator and used for false and true values.</li> <li>• If the argument is an array, the 0 and 1 index values are used for false and true values.</li> </ul> <p>Otherwise, the string values “false” and “true” are returned.</p>                                                                                                                                                             |
| NwaByteFormat     | <p>Formats a non-negative size in bytes as a human readable number (bytes, KB, MB, GB, etc). 1 KB is defined as 1,024 bytes, 1 MB as 1,024 KB (1,048,576 bytes), and 1 GB as 1,024 MB (1,073,741,824 bytes).</p> <ul style="list-style-type: none"> <li>• If a negative value is supplied, returns the argument (or null if no argument was supplied).</li> <li>• If a non-numeric value is supplied, that value is returned directly.</li> </ul>                                                                                                                                                                                                                     |
| NwaCurrencyFormat | <p>Formats a numeric value that indicates a monetary amount as a string.</p> <p>If the argument is null or not supplied, the current locale’s settings are used to format the monetary value.</p> <ul style="list-style-type: none"> <li>• The argument may be an array, which will override the current locale’s settings (see NwaNumberFormat for the list of settings that are used).</li> <li>• The argument may be a numeric value, which is used as the number of fractional digits to use when formatting the monetary amount (other locale settings will remain unchanged in this case).</li> </ul>                                                           |
| NwaDateFormat     | <p>Format a date like the PHP function strftime(), using the argument as the date format string. Returns a result guaranteed to be in UTF-8 and correct for the current page language. See "<a href="#">Date/Time Format Syntax</a>" on <a href="#">page 716</a> for a list of available date/time formats, or use one of the following special format strings:</p> <ul style="list-style-type: none"> <li>• <b>hhmmss, hh:mm:ss</b> – time of day</li> <li>• <b>iso8601, iso8601t, iso-8601, iso-8601t</b> – various ISO 8601 date formats with and without hyphen separators and the time of day</li> <li>• <b>longdate</b> – date and time in long form</li> </ul> |

| Function          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                   | <ul style="list-style-type: none"> <li>● <b>displaytime</b> – time of day</li> <li>● <b>?:</b> – returns the string following the ?: if the time value is 0, or uses the format string before the ?: otherwise</li> <li>● <b>recent</b> – for example, “2 minutes ago”, “3 months ago”</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| NwaDurationFormat | <p>Converts a time measurement into a description of the corresponding duration.</p> <ul style="list-style-type: none"> <li>● Format parameters: seconds, minutes, hours, days, weeks.</li> <li>● Any format can be converted to another.</li> <li>● By default, this function converts an elapsed time value specified in seconds to a value that is displayed in weeks, days, hours, minutes and seconds.</li> </ul> <p>Up to four additional arguments may be supplied to control the conversion:</p> <ul style="list-style-type: none"> <li>● <b>in_format</b> – The current units of the value being converted (seconds, minutes, hours, days, weeks)</li> <li>● <b>max_format</b> – Controls the max increment you want displayed.</li> <li>● <b>min_format</b> – Controls the min increment you want displayed. Only whole numbers are printed.</li> <li>● <b>default</b> – If set, this value will be returned when the resulting duration (after min_format is taken into account) is 0.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| NwaExplodeComma   | <p>Converts a string to an array by splitting the string at each comma and forming an array of all the substrings created in this way.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| NwaNumberFormat   | <p>Formats a numeric value as a string. If the argument is null or not supplied, the current locale’s settings are used to format the numeric value. The argument may be an array or a numeric value. If the argument is an array, it will override the current locale’s settings (see below for the list of settings that are used). If the argument is a numeric value, it is used as the number of fractional digits to use when formatting the string (other locale settings will remain unchanged in this case).</p> <p>The specific locale settings used are from <b>localeconv()</b>, and are listed below.</p> <p><i>For general numeric formatting :</i></p> <ul style="list-style-type: none"> <li>● <b>frac_digits</b> – number of decimal places to display</li> <li>● <b>decimal_point</b> – character to use for decimal point</li> <li>● <b>thousands_sep</b> – character to use for thousands separator</li> </ul> <p><i>For signs for positive/negative values:</i></p> <ul style="list-style-type: none"> <li>● <b>positive_sign</b> – sign for positive values</li> <li>● <b>p_sign_posn</b> – position of sign for positive values (0..4)</li> <li>● <b>negative_sign</b> – sign for negative values</li> <li>● <b>n_sign_posn</b> – position of sign for negative values (0..4)</li> </ul> <p><i>For formatting for monetary amounts:</i></p> <ul style="list-style-type: none"> <li>● <b>mon_decimal_point</b> – decimal point character for monetary values</li> <li>● <b>mon_thousands_sep</b> – thousands separator for monetary values</li> <li>● <b>p_sep_by_space</b> – true if a space separates currency symbol from a positive value</li> <li>● <b>p_cs_precedes</b> – true if currency symbol precedes positive value</li> <li>● <b>n_sep_by_space</b> – true if a space separates currency symbol from a negative value</li> <li>● <b>n_cs_precedes</b> – true if currency symbol precedes negative value</li> </ul> <p>Additionally, the special value <b>monetary</b>, if true, indicates that a currency value should be formatted, rather than a regular numeric value.</p> |

## View Display Expression Technical Reference

A page that contains a view is displayed in an operator's Web browser. The view contains data that is loaded from the server dynamically. Because of this, both data formatting and display operations for the view are implemented with JavaScript in the Web browser.

For each item displayed in the view, a JavaScript object is constructed. Each field of the item is defined as a property of this object. When evaluating the JavaScript Display Expression, the **data** variable is used to refer to this object. Thus, the expression **data.my\_field** would return the value of the field named "my\_field".

**Figure 487** Fields on a List View

| Username        | Role  | Status  | Account Expiration |
|-----------------|-------|---------|--------------------|
| <b>h9147032</b> | Guest | Enabled | 2008-06-13 00:26   |
| <b>h1448161</b> | Guest | Enabled | 2008-06-13 01:07   |
| <b>67284801</b> | Guest | Enabled | N/A                |

In the above view (the **guest\_users** view), the four columns displayed correspond to the **username**, **role\_name**, **enabled**, and **expire\_time** fields.

**Table 340:** Display Expressions for Data Formatting

| Value                                                                                        | Description                                                                                                                                                                                                                                                                                                 |
|----------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Display Expressions                                                                          |                                                                                                                                                                                                                                                                                                             |
| data.username.bold()                                                                         | Displays the username string as bold text.                                                                                                                                                                                                                                                                  |
| data.role_name                                                                               | Displays the name of the role.                                                                                                                                                                                                                                                                              |
| Nwa_BooleanText(data.enabled, "Enabled", "Disabled")                                         | Displays either "Enabled" or "Disabled" depending on the value of the <b>enabled</b> field.                                                                                                                                                                                                                 |
| (parseInt(data.do_expire) != 0) ? Nwa_DateFormat(data.expire_time, "%Y-%m-%d %H:%M") : "N/A" | Displays "N/A" if the account has no expiration time, or a date and time string if an expiration time has been set.                                                                                                                                                                                         |
| JavaScript functions                                                                         |                                                                                                                                                                                                                                                                                                             |
| <b>Nwa_BooleanText</b> (value, if_true, if_false[, if_undefined])                            | Returns the value of <i>if_true</i> or <i>if_false</i> depending on whether the <i>value</i> evaluates to a Boolean true or false, respectively. If the value has an undefined type (in other words, has not been set), and the <i>if_undefined</i> parameter was provided, returns <i>if_undefined</i> .   |
| <b>Nwa_DateFormat</b> (value, format)                                                        | Converts a numerical <i>value</i> (UNIX time) to a string using the date and time format string <i>format</i> . The format string uses similar syntax to the NwaDateFormat() function. See <a href="#">"Date/Time Format String Reference" on page 718</a> for a full list of the supported format strings. |
| <b>Nwa_FloatFormat</b> (value, decimals)                                                     | Converts a numerical <i>value</i> to a string, with the number                                                                                                                                                                                                                                              |

| Value                                                                                                                                                                                                                                                          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                                                                                                                                                                                | of decimal places specified in <i>decimals</i> .                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Nwa_MinutesToNatural</b> ( <i>value</i> )                                                                                                                                                                                                                   | Converts a numeric <i>value</i> measuring a time in minutes to a natural time representation (such as "2 minutes", "3 hours", "11 days").                                                                                                                                                                                                                                                                                                                                |
| <b>Nwa_NumberFormat</b> ( <i>value</i> [, <i>if_undefined</i> ])<br><b>Nwa_NumberFormat</b> ( <i>value</i> , <i>decimals</i> )<br><b>Nwa_NumberFormat</b> ( <i>value</i> , <i>decimals</i> , <i>dec_point</i> , <i>thousands_sep</i> [, <i>if_undefined</i> ]) | Converts a numerical value to a string. If the value has an undefined type (in other words, has not been set), and the <i>if_undefined</i> parameter was provided, returns <i>if_undefined</i> . Otherwise, the number is converted to a string using the number of decimal places specified in <i>decimals</i> (default 0), the decimal point character in <i>dec_point</i> (default "."), and the thousands separator character in <i>thousands_sep</i> (default ","). |
| <b>Nwa_TrimText</b> ( <i>value</i> , <i>length</i> )                                                                                                                                                                                                           | Trims excessively long strings to a maximum of <i>length</i> characters, appending an ellipsis ("...") if the string was trimmed.                                                                                                                                                                                                                                                                                                                                        |
| <b>Nwa_ValueText</b> ( <i>value</i> [, <i>if_undefined</i> ])                                                                                                                                                                                                  | If the <i>value</i> has an undefined type (in other words, has not been set), and the <i>if_undefined</i> parameter was provided, returns <i>if_undefined</i> , or a HTML non-breaking space ("&nbsp;") otherwise. Otherwise, the <i>value</i> is converted to a string for display.                                                                                                                                                                                     |

## LDAP Standard Attributes for User Class

The following list provides some of the attributes for the LDAP User class. For a complete list you should consult [http://msdn2.microsoft.com/en-us/library/ms683980\(VS.85\).aspx#windows\\_2000\\_server\\_attributes](http://msdn2.microsoft.com/en-us/library/ms683980(VS.85).aspx#windows_2000_server_attributes).

- **userPrincipalName:** The userPrincipalName is a single-valued and indexed property that is a string that specifies the user principal name (UPN) of the user. The UPN is an Internet-style login name for the user based on the Internet standard RFC 822. The sAMAccountName property is a single-valued property that is the logon name. The objectSid property is a single-valued property that specifies the security identifier (SID) of the user.
- **accountExpires:** The accountExpires property specifies when the account will expire.
- **badPasswordTime:** The badPasswordTime property specifies when the last time the user tried to log onto the account using an incorrect password.
- **badPwdCount:** The badPwdCount property specifies the number of times the user tried to log on to the account using an incorrect password.
- **codePage:** The codePage property specifies the code page for the user's language of choice. This value is not used by Windows 2000.
- **countryCode:** The countryCode property specifies the country code for the user's language of choice. This value is not used by Windows 2000.
- **lastLogoff:** The lastLogoff property specifies when the last logoff occurred.
- **lastLogon:** The lastLogon property specifies when the last logon occurred.
- **logonCount:** The logonCount property counts the number of successful times the user tried to log on to this account.
- **mail:** The mail property is a single-valued property that contains the SMTP address for the user (such as demo@example.com).



- **memberOf:** The memberOf property is a multi-valued property that contains groups of which the user is a direct member.
- **primaryGroupID:** The primaryGroupID property is a single-valued property containing the relative identifier (RID) for the primary group of the user.
- **sAMAccountType:** The sAMAccountType property specifies an integer that represents the account type.
- **unicodePwd:** The unicodePwd property is the password for the user.

## Regular Expressions

The characters shown in [Table 341](#) can be used to perform pattern matching tasks using regular expressions.

**Table 341:** *Regular Expressions for Pattern Matching*

| Regex       | Matches                                           |
|-------------|---------------------------------------------------|
| a           | Any string containing the letter "a"              |
| ^a          | Any string starting with "a"                      |
| ^a\$        | Only the string "a"                               |
| a\$         | Any string ending with "a"                        |
| .           | Any single character                              |
| \.          | A literal "."                                     |
| [abc]       | Any of the characters a, b, or c                  |
| [a-z0-9A-Z] | Any alphanumeric character                        |
| [^a-z]      | Any character not in the set a through z          |
| a?          | Matches zero or one "a"                           |
| a+          | Matches one or more: a, aa, aaa, ...              |
| a*          | Matches zero or more: empty string, a, aa, aaa... |
| a b         | Alternate matches: Matches an "a" or "b"          |
| (a.*z)      | Grouping: matches sequentially within parentheses |
| a*?         | "Non-greedy" zero or more matches                 |
| \ooo        | The character with octal code ooo                 |
| \040        | A space                                           |
| \d          | Any decimal digit                                 |
| \D          | Any character that is not a decimal digit         |

The regular expression syntax used is Perl-compatible. For further details on writing regular expressions, consult a tutorial or programming manual.





This appendix describes Chromebook functionality in ClearPass Onboard. It provides an introduction to Chromebook in Onboard, and discusses considerations as well as Onboard and Google Admin configuration for Chromebook.

This section includes:

- "About Chromebook in Onboard" on page 751
- "Caveats and Recommendations" on page 752
- "Onboard Configuration for Chromebook" on page 754
- "Google Admin Configuration for Chromebook" on page 755

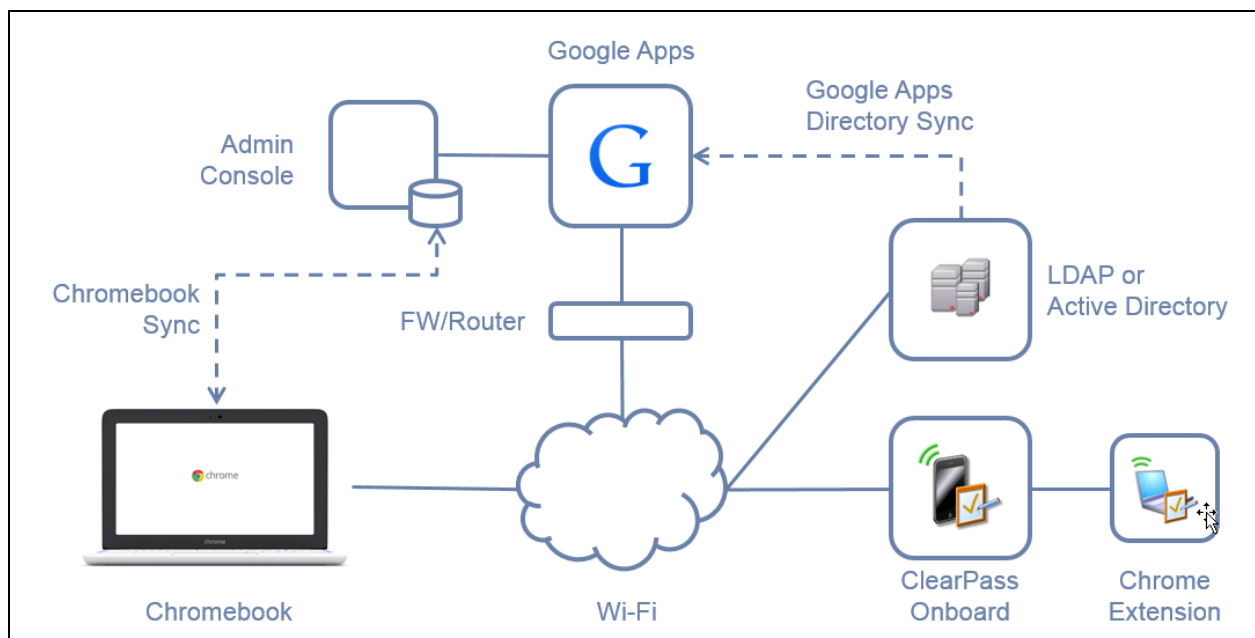
### About Chromebook in Onboard

Chromebook is a managed device. When you use Google Apps for Business or Google Apps for Education, you use the Google Admin console for provisioning, management, and control of Chromebook devices.

However, Chromebook still requires a Wi-Fi connection to work.

Administrators can take advantage of ClearPass Onboard's Chromebook support for certificate enrolling. Users can be provided with EAP-TLS client certificates to securely establish their network identity. All of the existing capabilities of Onboard can then be leveraged to ensure reliable and policy-controlled access to the network.

**Figure 488** Network Architecture



In the network architecture diagram shown in "[Network Architecture](#)" on page 751:

- Chromebook users access the network through the local Wi-Fi.
- The Google Apps domain provides user login services and other apps, such as the Chrome Web Store, Google Docs, Google Sheets, and more.
- The Admin Console is used by administrators to provision new Chromebooks and manage existing Chromebooks.
- Chromebook Sync is used to ensure that settings from the Admin Console are applied to all Chromebooks in the domain.
- Users, groups, and other details can be provisioned in Google Apps from an existing directory using the Google Apps Directory Sync tool.
- ClearPass Onboard provides device provisioning and certificate enrollment services.
- The Chrome Extension provides support for Onboard device provisioning for Chromebook devices.

## Caveats and Recommendations

This section describes requirements related to licenses, extensions, deployment, versions, certificates, provisioning, and authentication sources.

### Google Admin Chromebook License is Required

Chromebook management is only available in the Google Admin console (<https://admin.google.com>) if a suitable license has been added for the domain under management.

### Managed Chromebook Deployment is Required

Chromebook is a managed device, not a "BYOD" device. The support for Onboard is limited to device provisioning and enrollment in an administrator-managed network. Non-managed Chromebook devices cannot be enrolled using ClearPass Onboard.

### Chrome Extension is Required

Chromebook does not natively support device enrollment with products such as ClearPass Onboard. For this, a Chrome extension is required.

Additionally, because of the software security model used by Chromebook, "normal" Chrome extensions (for example, those installed from the Chrome Web Store) do not have permissions to alter the certificate store on the device. To do this requires an administratively configured extension, which is why Chromebook must be managed for Onboard enrollment to work.

For details of how to configure the Google Admin console to automatically install this extension when a user logs into Chromebook, refer to the **Configure Chrome Extension** section in "[Google Admin Configuration for Chromebook](#)" on page 755 .

### Chromebook Release 37 or Later is Required

The Onboard extension requires Chrome version 37 or later. As of the time of this writing (July 2014) this version of Chrome is only available in the development channel.

To provision Chromebook devices with the development channel, create an organizational unit within your organization. For that organizational unit, configure **Device Settings** and set the **Release Channel** to **Move**

**to Development Channel.** Then move one or more devices into this organizational unit to enable the development channel.

When the stable release catches up with the development channel, no special configuration will be required to enable Onboard for Chromebook.

For more information on the Chromebook stable, beta and development channels, refer to this article: <https://support.google.com/chromebook/answer/1086915>

## Chromebook Supports Only “Created by Device” Certificates

Chromebook includes a trusted platform module (TPM) for protection of cryptographic private keys, including the private key for the TLS client certificate issued to the device by Onboard.

Because of this, Chromebook will always create its own private key. The **Key Type** option in the device **Provisioning Settings** will be ignored by Chromebook devices, and will always default to **created by device**.

The key size is 1024 bits or 2048 bits, as specified in the device **Provisioning Settings**.



---

If an unsupported selection is made in the Provisioning Settings form, the default used will be a 2048-bit private key.

---

## A Separate Provisioning SSID is Required

Chromebook cannot be provisioned unless it is already online, in order to sync with the appropriate settings from the Google Admin console.

To handle the initial configuration task, we recommend you follow these steps:

- Configure an Onboard provisioning SSID.
  - Ensure that this SSID has an access-control list that allows the Chromebook to log in and sync with Google Apps. For details on the contents of the ACL, refer to this article: <https://support.google.com/chrome/a/answer/3504942#sslinspection>
  - Use a captive portal on this SSID that redirects users to the Onboard device provisioning page.
  - Note that this SSID can also be used to Onboard other devices that are supported by ClearPass Onboard.
- Ensure that the Chromebook is enrolled.
  - To manually enroll a brand-new Chromebook, press **Ctrl+Alt+E** before attempting to log in with any domain credentials.
  - Be aware that once a user has signed in to a device, you cannot enroll the device. The device must be wiped in order to restart the enrollment process.
  - For more details on enrolling a Chrome device, including details on automatic enrollment, refer to this article: <https://support.google.com/chrome/a/answer/1360534>
- Sign in to the device using the credentials of an account in the Google Apps domain.
  - Connect to the provisioning SSID using the Chrome setup wizard.



---

Do not save the credentials you used to connect to the provisioning SSID.

---

- The device will sync with the Admin console settings.

- This will also install the Onboard Chrome extension, if it is configured correctly in the Google Admin console.
- Open the Chrome browser on the device.
  - The captive portal will redirect you to the device provisioning page.
  - Sign in with appropriate credentials.
  - The Chrome device will be provisioned with a new certificate.
  - The provisioned network should be automatically activated when it is available. If not, manually connect to the network to verify that EAP-TLS is working correctly.

## Directory-Based Authentication Source is Recommended

When a Chromebook user with an EAP-TLS certificate connects to the network, an authorization check is performed to ensure that the certificate is still valid, and that the user account associated with the certificate is still permitted to use the network.

ClearPass Policy Manager provides this capability for multiple authentication sources. However, at this time, no built-in Google Apps authentication source is available.

Many Chromebook deployments will take advantage of Google Apps Directory Sync to use an existing LDAP or Active Directory authentication source. In this environment, a ClearPass authentication source can be used to verify the status of a user account when a device connects to the network.

If your deployment does not have an LDAP or Active Directory source, you can still use Onboard to provision Chromebook devices. However, in this environment you must manually revoke the certificates of users who are no longer authorized to access the network.

## Onboard Configuration for Chromebook

The **Provisioning Settings** form provides Chromebook configuration settings.

### Enable Chromebook Provisioning

You must first enable Chromebook in a provisioning setting. This adds the configuration fields for it:

1. Go to **Onboard > Deployment and Provisioning > Provisioning Settings** and click the **Supported Devices** tab.

**Figure 489** *Provisioning Settings, Supported Devices Tab, Chromebook Area*



2. In the **Chromebook Devices** row, select the **Enable Chromebook device provisioning** check box.
3. In the **Chromebook Token** row, select the hardware token to store certificates against. Options include:
  - **User-Specific**
  - **System-Wide**
4. Click **Save Changes**. Configuration fields for Chromebook are added to the **Instructions & Messages** tab.

For more information, see "Configuring Provisioning Settings for Supported Devices" on page 227.

## Configure Instructions and Messages

1. After you enable Chromebook on the **Supported Devices** tab, click the **Instructions & Messages** tab. The text displayed on the device provisioning page for Chromebook devices can be customized here.

**Figure 490** Provisioning Settings, Instructions & Messages Tab, Chromebook Area

|  <b>Chromebook Instructions</b><br><small>These options control messages shown during Chromebook device provisioning.</small> |                                                                                                                                                    |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| * Pre-Login:                                                                                                                                                                                                   | <input type="text" value="Use default message"/> ▾<br><small>Instructions shown to the user before they log in using an Chromebook device.</small> |
| * Plugin Launch:                                                                                                                                                                                               | <input type="text" value="Use default message"/> ▾<br><small>Instructions shown to the user when asked to launch the Chromebook plugin.</small>    |
| * Installing Profile:                                                                                                                                                                                          | <input type="text" value="Use default message"/> ▾<br><small>Instructions shown to the user while the Chromebook certificate installs.</small>     |
| * Complete:                                                                                                                                                                                                    | <input type="text" value="Use default message"/> ▾<br><small>Instructions shown to the user when Chromebook provisioning is complete.</small>      |
| * Link Text:                                                                                                                                                                                                   | <input type="text" value="Use default labels"/> ▾<br><small>Controls the labels shown on download links during Chromebook provisioning.</small>    |

2. Make the appropriate selections in the **Provisioning Instructions, Device Status, and Chromebook Instructions** areas. For more information, see "Configuring Provisioning Settings for Instructions and Messages" on page 238.
3. Click **Save Changes**.
4. Use the other tabs in the **Provisioning Settings** form to complete the configuration for the provisioning setting, and save the configuration. For more information, see "About Configuring Provisioning Settings" on page 221.

## Google Admin Configuration for Chromebook

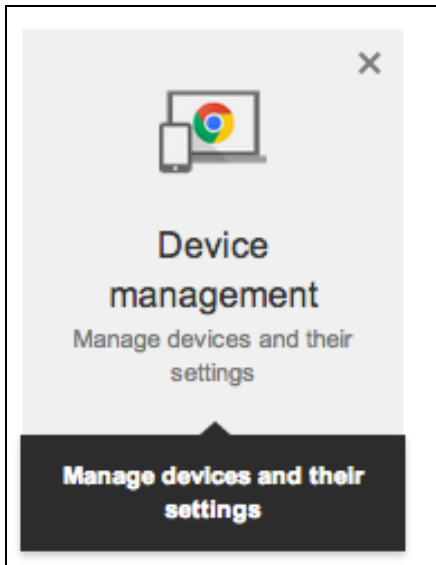
This section describes Google Admin configuration for Chromebook in Onboard.

To begin, log in to the Google admin console at <https://admin.google.com/>.

### Configuring the Chrome extension

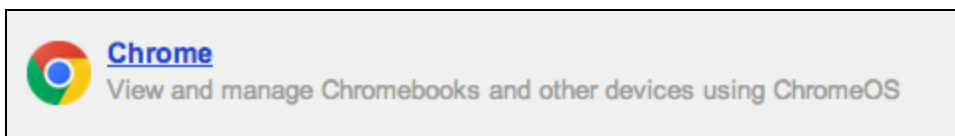
1. In the Google Admin console, select the **Device Management** option.

**Figure 491** *The Device Management Option in the Google Admin Console*



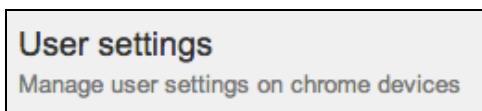
2. Select the **Chrome** option.

**Figure 492** *The Chrome Option*



3. Go to **User Settings**.

**Figure 493** *The User Settings Option*

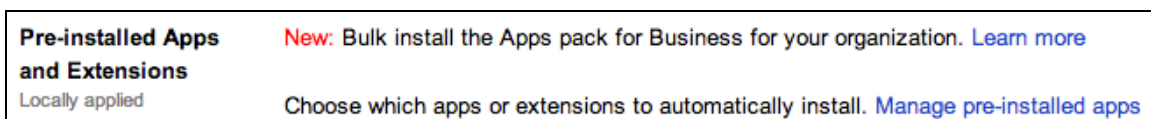


---

If you have multiple organizational units or levels, be sure to select the appropriate organizational unit or level before you make changes to the settings.

---

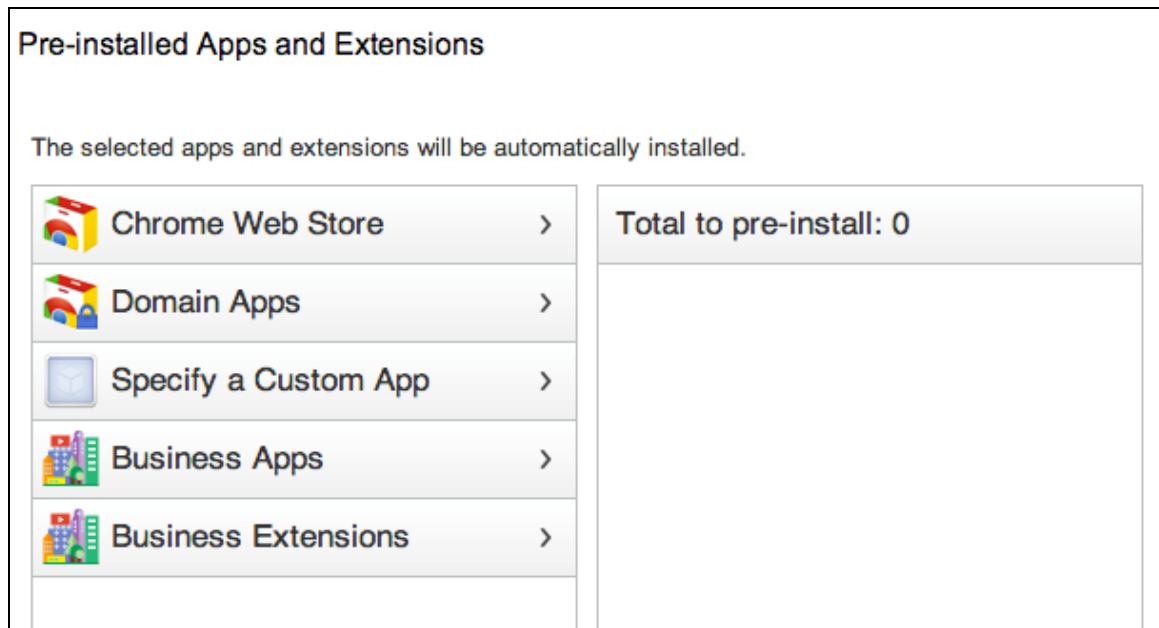
4. In the user settings, find the **Pre-installed Apps and Extensions** section, and then click the **Manage pre-installed apps** link.



5. Select **Specify a Custom App**.

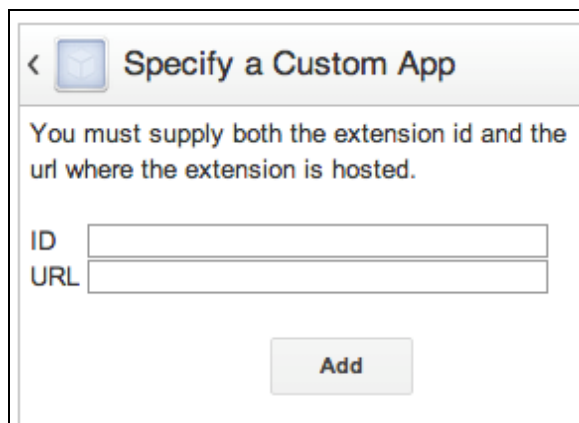


**Figure 494** Pre-Installed Apps and Extensions, Specify a Custom App



6. Enter the **ID** and **URL** of the Onboard Chromebook extension and then click **Add**.

**Figure 495** Specify a Custom App, ID and URL



The ID and URL information is available on the **Onboard > Deployment and Provisioning > Provisioning Settings > Chromebook** tab.



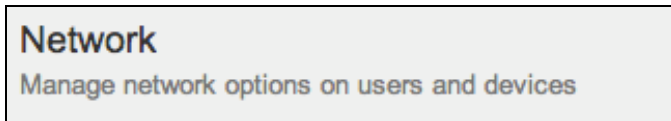
If you have a cluster environment, the URL may be modified to refer to any subscriber node.

7. Verify that the extension is listed in the **Pre-installed Apps and Extensions** list, and then click **Save**.
8. Remember to save your changes using the **Save changes** button at the bottom left of the page.

## Configuring Network Settings

1. From the **Chrome Management** page, go to **Network**.

**Figure 496** *The Network Option*



2. You should see the **For Users** tab selected. Click the **Add Wi-Fi** button on the right.

**Figure 497** *The For Users Tab*



3. Specify a **Name** and **SSID** for the network, and select the **Automatically Connect** option.
4. Change the **Security Type** to **WPA/WPA2 Enterprise (802.1X)**,
5. Under **Extensible Authentication Protocol**, select **EAP-TLS**.
6. The **Username** can be set as a fixed value (for example, anonymous), or it can take the variables **\${LOGIN\_ID}** (for example, johndoe) or **\${LOGIN\_EMAIL}** (for example, johndoe@mydomain.com).
7. If your RADIUS server doesn't have a commercially issued certificate, then you might need to use the **Add new certificate...** option for **Server Certificate Authority** to upload the signer of the RADIUS certificate.



---

Be sure to use the **Root CA** and not the **Signer CA**.

---

If you already have an appropriate certificate in the list, then it can be selected directly.

Figure 498 The Add Wi-Fi Network Form

**Add Wi-Fi network** X

**Name** Help

MyEDU-Secured

**Service set identifier (SSID)**

MyEDU-Secured

This SSID is not broadcast

Automatically connect

**Security type**

WPA/WPA2 Enterprise (802.1X) ▾

**Extensible Authentication Protocol**

EAP-TLS ▾

**Username**

`\${LOGIN\_ID}`

**Server Certificate Authority**

ClearPass Onboard Local Certificate Authority ▾

Issued by: ClearPass Onboard Local Certificate Authority, Aruba Networks  
Issued to: ClearPass Onboard Local Certificate Authority, Aruba Networks  
Issued on: Jul 14, 2014      Expires on: Jul 14, 2024

**Client enrollment URL**

**Save** **Cancel**

8. For **Client enrollment URL**, provide the URL of the Onboard captive portal page—for example, `https://server/onboard/device_provisioning.php`.
9. You should also specify the **Common Name** of the Onboard CA's issuing certificate in **Issuer pattern > Common name**—for example, "ClearPass Onboard Local Certificate Authority (Signing)".
10. Click **Save** to save the network settings, and remember to click **Save changes** to commit.



---

**\$criteria**

Array that consists of one or more criteria on which to perform a data-based search. This array is used for advanced cases where predefined helper functions do not provide required flexibility.

**802.1X**

IEEE standard for port-based network access control, designed to enhance 802.11 WLAN security. 802.1X provides an authentication framework that allows a user to be authenticated by a central authority. The actual algorithm that is used to determine whether a user is authentic is left open, and multiple algorithms are possible.

**AAA**

Authentication, Authorization, and Accounting. Security architecture for distributed systems that provides control over who can access services and that tracks the resources they use. - Authentication: Verification of a user's credentials. Typically accomplished with a username and password, a one-time token, or a digital signature. - Authorization: Controls the type of access an authenticated user is permitted to have based on the user's authentication type. - Accounting: Process of recording summary information about network access by users and devices. Tracks network resource consumption and records events such as authentication failures.

**access point**

Device that serves as a point of connection between the WLAN and a wired network, and which connects devices within the network. The number of access points a WLAN needs is determined by the number of users and the size of the network.

**Access-Accept**

Response from RADIUS server indicating successful authentication, and containing authorization information.

**Access-Reject**

Response from RADIUS server indicating a user is not authorized.

**Access-Request**

RADIUS packet sent to a RADIUS server requesting authorization.

**accounting**

Process of recording summary information about network access by users and devices.

**accounting session time**

Length of time the guest has been using the network.

**Accounting-Request**

RADIUS packet type sent to a RADIUS server containing accounting summary information.

**Accounting-Response**

RADIUS packet sent by the RADIUS server to acknowledge receipt of an Accounting-Request.

---

## **Active Directory**

Microsoft Active Directory. Directory server that stores information about a variety of things, such as organizations, sites, systems, users, shares, and other network objects or components. It also provides authentication and authorization mechanisms, and a framework within which related services can be deployed.

## **ActiveSync**

Mobile data synchronization app developed by Microsoft that allows a mobile device to be synchronized with either a desktop or a server running compatible software products.

## **AD**

Microsoft Active Directory. Directory server that stores information about a variety of things, such as organizations, sites, systems, users, shares, and other network objects or components. It also provides authentication and authorization mechanisms, and a framework within which related services can be deployed.

## **AES**

Advanced Encryption Standard. Used to encrypt and protect electronic data, AES encrypts and decrypts data in blocks of 128 bits (16 bytes), and can use keys of 128, 192, and 256 bits.

## **agent**

Agents such as persistent agents, dissolvable agents, or the ClearPass OnGuard Unified Agent perform device fingerprinting, posture assessments, and health checks. See also dissolvable agent, persistent agent, native agent, and OnGuard.

## **AirGroup**

ClearPass application that allows end users to register their personal mobile devices on a local network and define a group of friends or associates who are allowed to share them. Primarily designed for colleges and other institutions. AirGroup uses zero configuration networking to allow Apple mobile devices, such as the AirPrint wireless printer service and the AirPlay mirroring service, to communicate over a complex access network topology.

## **Amigopod**

Original name of the ClearPass Guest application. No longer used, but still appears in some syntax.

## **app**

Application. This shortened form of the word is used for mobile devices.

## **application identifier**

Unique identifier generated when a provisioning profile is created. In combination with the approved domain, it allows app distribution.

## **audit server**

Evaluates the health of clients that do not have an installed agent, or that cannot respond to Policy Manager interactions. Audit servers typically operate in lieu of authentication methods, authentication sources, or internal posture policies and posture servers.

## **authentication**

Verification of a user's credentials, typically a username and password.

---

## **authentication source**

Identity repository against which Policy Manager verifies identity. ClearPass supports the following authentication source types: Microsoft Active Directory, LDAP-compliant directories, RSA or other RADIUS-based token servers, and SQL database, as well as Static Host lists for MAC-based authentication.

## **authorization**

Authorization controls the type of access that an authenticated user is permitted to have.

## **authorization source**

Collects attributes for use in role-mapping rules. You specify the attributes you want to collect when you configure the authentication source. CPPM supports the following authorization source types: Microsoft Active Directory, any LDAP compliant directory, RSA or other RADIUS-based token servers, and SQL database, including the local user store.

## **bounce**

To shut down and restart a service or port.

## **BYOD**

Bring your own device. Refers to using personal mobile devices within an employer's enterprise network infrastructure, and the associated network and resource management challenges.

## **CA**

Certificate Authority. Entity in a public key infrastructure system that issues certificates to clients. A certificate signing request received by the CA is converted into a certificate when the CA adds a signature that is generated with the CA's private key. See digital certificate, private key, and public key infrastructure.

## **captive portal**

Implemented by NAS. Provides access to the network only to authorized users.

## **Certificate Authority**

Entity in a public key infrastructure system that issues certificates to clients. A certificate signing request received by the Certificate Authority (CA) is converted into a certificate when the CA adds a signature that is generated with the CA's private key. See digital certificate, private key, and public key infrastructure.

## **CHAP**

Challenge-Handshake Authentication Protocol. Authentication scheme used by Point to Point Protocol (PPP) servers to validate the identity of remote clients.

## **ClearPass**

Access Management System for creating and enforcing policies across a network to all devices and applications. The ClearPass integrated platform includes Policy Manager, Guest, Onboard, OnGuard, Insight, Profile, AirGroup, MACTrac, and QuickConnect.

## **ClearPass Guest**

Configurable ClearPass application for secure visitor network access management. Access permissions to ClearPass Guest features are controlled through an operator profile that can be integrated with an LDAP server or Active Directory login. The ClearPass Guest application can be accessed either directly or through Policy Manager.

---

**cluster**

Group of independent servers connected through a dedicated network that act as a single system, allowing high availability and load balancing. Resources in a cluster are dynamically assigned. See also publisher, subscriber.

**CNA**

Apple Captive Network Assistant. Pop-up browser shown when joining a network that has a captive portal.

**CoA**

Change of Authorization.

**collector**

Network elements providing data for profiling endpoints. The following collectors send endpoint attributes to Profiler: DHCP, Onboard, HTTP User Agent, MAC OUI, ActiveSync plugin, OnGuard, SNMP, and Subnet Scanner.

**common name**

See distinguished name.

**CRL**

Certificate Revocation List. List of revoked certificates maintained by a Certificate Authority and regularly updated.

**cryptobinding**

Short for cryptographic binding. Procedure in a tunneled EAP method that binds together the tunnel protocol and the tunneled authentication method(s), ensuring the relationship between a collection of data assets and protecting authentication protocol negotiation against man-in-the-middle attacks. Cryptographic binding focuses on protecting the server; mutual cryptographic binding protects both peer and server.

**CSR**

Certificate Signing Request.

**CSV**

Comma-separated values.

**device category**

Classification describing a device's type—for example, computer, smartdevice, printer, access point, and so on. One of three hierarchical elements in a device profile.

**device family**

Within the device category, a classification based on the type of operating system or vendor—for example, if the device category is Computer, the value for device family might be Windows, Linux, or Mac OS. One of three hierarchical elements in a device profile.

**device fingerprint**

Information collected about a device for the purpose of identification. Fingerprints can fully or partially identify individual users or devices even when cookies are turned off.



---

**device name**

Within the device family, a classification based on granular details such as OS version—for example, if the device family is Windows, the value for device name might be Windows 7 or Windows 2008 Server. One of three hierarchical elements in a device profile.

**device provisioning**

Process of preparing a device for use on an enterprise network, by creating the appropriate access credentials and setting up the network connection parameters. Same as onboarding.

**DHCP**

Dynamic Host Configuration Protocol. An auto-configuration protocol used on IP networks. Computers or any network peripherals that are connected to IP networks must be configured before they can communicate with other computers on the network. DHCP allows a computer to be configured automatically, eliminating the need for a network administrator. DHCP also provides a central database to keep track of computers connected to the network; this database helps prevent any two computers from being configured with the same IP address.

**digital certificate**

Contains identification data (see distinguished name) and the public key portion of a public/private key pair, and a signature that is generated by a Certificate Authority. The signature ensures the integrity of the data in the certificate (only the Certificate Authority can create valid certificates).

**Disconnect-Ack**

NAS response packet to a Disconnect-Request, indicating that the session was disconnected.

**Disconnect-Nak**

NAS response packet to a Disconnect-Request, indicating that the session could not be disconnected.

**Disconnect-Request**

RADIUS packet type sent to a NAS requesting that a user or session be disconnected.

**dissolvable agent**

Functionality within ClearPass OnGuard that performs device fingerprinting, posture assessments, and health checks. Performs a one-time check at login to ensure policy compliance. Dissolvable agents cannot perform remediation; devices not meeting compliance can be redirected to a captive portal for manual remediation. Dissolvable agents are browser-based and are not installed on the endpoint. They are temporary: when the browser page used during authentication is closed, the dissolvable agent is removed, leaving no trace. The Web-based dissolvable agent is ideal for personal, non IT-issued devices that connect via a captive portal and do not allow agents to be permanently installed. See also persistent agent, native agent, and OnGuard.

**distinguished name**

(DN) Series of fields in a digital certificate that, taken together, constitute the unique identity of the person or device that owns the digital certificate. Common fields in a distinguished name include country, state, locality, organization, organizational unit, and the “common name”, which is the primary name used to identify the certificate.

**DN**

See Distinguished Name.

---

**EAP**

Extensible Authentication Protocol. An authentication framework that supports multiple authentication methods, such as token cards, smart cards, certificates, one-time passwords, and public key encryption authentication. In tunneled EAP methods, authentication and posture credential exchanges occur inside of a protected outer tunnel.

**EAP-FAST**

EAP Flexible Authentication Secure Tunnel. (tunneled)

**EAP-GTC**

EAP Generic Token Card. (non-tunneled)

**EAP-MD5**

EAP Method Digest 5. (non-tunneled)

**EAP-MSCHAP**

EAP Microsoft Challenge Handshake Authentication Protocol. EAP-MSCHAP is version 1 and EAP-MSCHAPv2 is version 2. (non-tunneled)

**EAP-MSCHAPv2**

EAP Microsoft Challenge Handshake Authentication Protocol. EAP-MSCHAP is version 1 and EAP-MSCHAPv2 is version 2. (non-tunneled)

**EAPoUDP**

EAP over UDP. See also UDP.

**EAP-PEAP**

Protected EAP. Widely-used protocol for securely transporting authentication data across a network. (tunneled)

**EAP-TLS**

EAP Transport Layer Security. Certificate-based authentication method supporting mutual authentication, integrity-protected ciphersuite negotiation, and key exchange between two endpoints.

**EAP-TTLS**

EAP Tunneled Transport Layer Security. Certificate-based authentication method supporting mutual authentication, integrity-protected ciphersuite negotiation, and key exchange between two endpoints. It is designed to be as strong as EAP-TLS but does not require that each user be issued a certificate, instead issuing certificates only to the authentication servers.

**field**

In a database or a user interface, a single item of information; attribute.

**form**

Interactive page in the application where users can provide or modify data.

**FQLN**

Fully Qualified Location Name. A device location identifier in the format: APname.Floor.Building.Campus.

---

**GET**

HTTP request method that submits data to be processed to a specified resource.

**guest**

Someone who is permitted to access the Internet through your Network Access Server.

**Guest**

Configurable ClearPass application for secure visitor network access management. Access permissions to ClearPass Guest features are controlled through an operator profile that can be integrated with an LDAP server or Active Directory login. The ClearPass Guest application can be accessed either directly or through Policy Manager.

**Identity Provider**

Service that authenticates a user or client identity and issues security tokens for ACS.

**IdP**

Service that authenticates a user or client identity and issues security tokens for ACS.

**Insight**

ClearPass analytics and reporting application.

**intermediate CA**

Certificate Authority with a certificate that was issued by another Certificate Authority. See trust chain.

**iOS**

Operating system from Apple, Inc. for mobile devices, including the iPhone, iPad, and iPod Touch.

**jailbroken**

Condition of an iOS device that has been modified in order to download applications, extensions, or themes not authorized by Apple. The term is also sometimes used to describe similar activity on non-Apple devices. The legal implications of jailbreaking a device vary by country and by device.

**JSON**

JavaScript Object Notation. An open-standard, language-independent, lightweight data-interchange format used to transmit data objects consisting of attribute–value pairs. JSON uses a "self-describing" text format that is easy for humans to read and write, and that can be used as a data format by any programming language.

**keepalive**

Signal sent at periodic intervals from one device to another to verify that the link between the two devices is working. If no reply is received, data will be sent by a different path until the link is restored. A keepalive can also be used to indicate that the connection should be preserved so that the receiving device does not consider it timed out and drop it.

**landing page**

Login page displayed to a visitor.

**LDAP**

Lightweight Directory Access Protocol. Communications protocol used to maintain and access distributed directory information about users and other objects over a network.

---

**MAC address**

Media Access Control Address. Unique identifier assigned to network interfaces for communications on a network. A device may have a wired network address and a wireless network address.

**MAC auth**

MAC Authentication Method. Authenticates devices based on their MAC address. MAC authentication might be the only method of client authentication or clients may also be required to authenticate themselves using other methods, depending on the network privileges required.

**MAC OUI**

The OUI, or Organizationally Unique Identifier, is the first half of a MAC address. It can be useful in some cases for better identifying endpoints, or for profiling devices like printers that might be configured with static IP addresses. See also OUI.

**MACTrac**

Application that allows end users to register their personal mobile devices on a local network. Each device registered by an operator is automatically shared with all of that operator's registered devices. There is no limit to the number of device accounts an operator can create, and no expiration time is set on device accounts. MACTrac operators are created in Policy Manager, and can then log in through ClearPass Guest to register and manage their devices.

**MAM**

Mobile Application Management. The employee owns the mobile device used for work, and the company provides and manages the features.

**MDM**

Mobile Device Management. The company owns and manages the mobile device the employee uses for work. A company-issued laptop is actually an MDM device, but MDM features in ClearPass allow company management to be applied to a variety of devices.

**MFA**

See multi-factor authentication.

**MIB**

Management Information Base. Hierarchical database used by SNMP to manage the devices being monitored.

**multi-factor authentication**

Multi-factor authentication (MFA) lets you require multiple factors, or proofs of identity, when authenticating a user. Policy configurations define how often multi-factor authentication will be required, or conditions that will trigger it.

**NAD**

Network Access Device. The device that automatically connects the user to the preferred network; for example, an AP or an Ethernet switch.

**NAK**

Negative Acknowledgement code. Response indicating that a transmitted message was received with errors or corrupted, or that the receiving end is not ready to accept transmissions.

---

**NAP**

Network Access Protection. Functionality in the Windows Server that allows network administrators to define specific levels of network access based on identity, groups, and policy compliance. The NAP Agent is a service that collects and manages health information for NAP client computers. If a client is not compliant, NAP provides a mechanism to automatically bring the client back into compliance and then dynamically increase its level of network access.

**NAS**

Network Access Server. Device -- such as a wireless access point, network switch, or dial-in terminal server -- that provides network access to users. When a user connects to the NAS device, a RADIUS user authentication request (Access-Request) is generated by the NAS.

**native agent**

Browser-based dissolvable agent that uses a separate binary file for each operating system. See also dissolvable agent, persistent agent, and OnGuard.

**NetBIOS**

Network Basic Input/Output System. Program that lets applications on different computers communicate within a local area network (LAN).

**Network Access Server**

(NAS) Device that provides network access to users, such as a wireless access point, network switch, or dial-in terminal server. When a user connects to the NAS device, a RADIUS user authentication request (Access-Request) is generated by the NAS.

**nMAP**

Network Mapper. Open source utility for network discovery and security auditing. Nmap uses IP packets to determine such things as the hosts available on a network and their services, operating systems and versions, types of packet filters/firewalls, and so on.

**NTP**

Network Time Protocol. Protocol for synchronizing the clocks of computers over a network.

**OCSP**

Online certificate status protocol (RFC 2560). Protocol used to determine the current status of a digital certificate without requiring CRLs.

**Onboard**

ClearPass application for automating 802.1x configuration and provisioning for “bring your own device” (BYOD) and IT-managed devices across wired, wireless, and virtual private networks (VPNs). Information Onboard collects during device onboarding is sent to Profile and used for device category, family, and name classification. ClearPass Onboard features are part of the Onboard module in the ClearPass Guest application.

**onboard provisioning**

Process used to securely provision a device and configure it with network settings.

**onboard-capable**

Device supported by the QuickConnect application.

---

**onboarding**

Process of preparing a device for use on an enterprise network, by creating the appropriate access credentials and setting up the network connection parameters. Same as device provisioning.

**OnGuard**

Functionality within ClearPass that uses persistent and dissolvable agents to perform endpoint protection, posture assessments, and health checks, ensuring compliance is met before devices connect. See also persistent agent, dissolvable agent, and native agent.

**OnGuard Unified Agent**

Combination of OnGuard and Aruba VIA.

**operator**

Person who uses ClearPass Guest to create guest accounts or perform system administration. Operators act as sponsors for visitor access.

**operator login**

Configuration defining a ClearPass Guest operator's roles and access privileges.

**operator profile**

Characteristics assigned to a class of operators, such as the permissions granted to those operators.

**OS X**

Operating system from Apple, Inc. for desktop and laptop computers.

**OUI**

Organizationally Unique Identifier. Synonymous with Company ID or Vendor ID, an OUI is a 24-bit, globally-unique assigned number referenced by various standards. The OUI is used as the first half of a MAC address.

**over-the-air provisioning**

Process used to securely provision a device and configure it with network settings; applies to iOS and OS X 10.7+ only.

**PANW**

Palo Alto Networks. Network security company whose products include a firewall with which ClearPass integrates, exchanging user context related to posture assessments.

**PAP**

Password Authentication Protocol. Validates users by password, PAP does not encrypt passwords for transmission and is thus considered insecure.

**PEAP**

Protected EAP. See EAP-PEAP.

**persistent agent**

Functionality within ClearPass OnGuard that performs device fingerprinting, posture assessments, and health checks. Provides nonstop monitoring and automatic remediation and control, and supports automatic and manual remediation. When running persistent OnGuard agents, ClearPass can centrally send system-wide notifications and alerts, and allow or deny network access. Persistent agents are OS-based. They are installed

---

on the endpoint; a user must have admin privileges in order to install them. Persistent agents are typically used for corporate-owned and managed devices. See also dissolvable agent, native agent, and OnGuard.

**ping**

Test network connectivity using an ICMP echo request (“ping”).

**PKCS#n**

Public-key cryptography standard N. Refers to a numbered standard related to topics in cryptography, including private keys (PKCS#1), digital certificates (PKCS#7), certificate signing requests (PKCS#10), and secure storage of keys and certificates (PKCS#12).

**PKI**

See public-key infrastructure.

**Policy Manager**

ClearPass Policy Manager is the main application of the ClearPass access management platform, and is used to create and enforce policies across a network for all devices and applications. Policy Manager also includes links to Guest, Insight, and Onboard. OnGuard and Profile features and some AirGroup configuration items are included within the Policy Manager user interface.

**POST**

HTTP request method that requests data from a specified resource.

**posture**

Set of characteristics describing the health of an endpoint device seeking access to the network. These may include such things as device type, operating system, or antivirus software. Posture assessment or posture validation: Using rules to evaluate and provide a security assessment for the endpoint and its user, assuring they are compliant. Posture token: Health status of the endpoint.

**posture policy**

Internal posture policies test requests against internal posture rules to assess health. Posture rule conditions can contain attributes present in vendor-specific posture dictionaries.

**posture server**

Evaluates client health based on specified vendor-specific posture credentials, typically posture credentials that cannot be evaluated internally by Policy Manager (that is, not by internal posture policies). Currently, Policy Manager supports two forms of posture server interfaces: RADIUS posture servers and GAMEv2 posture servers.

**Pre-Shared Key**

See PSK.

**print template**

Defines the format and appearance of a guest account receipt.

**private key**

The part of a public/private key pair that is always kept private. The private key is used to encrypt a message's signature to authenticate the sender (only the sender knows the private key). The private key is also used to decrypt a message that was encrypted with the sender's public key (only the sender can decrypt it). See also public key.

---

**Profiler**

Functionality within ClearPass that automatically classifies endpoints, using attributes obtained from collectors. It associates an endpoint with a specific user or location, secures access for devices like printers and IP cameras, and can be used to implement BYOD flows where access is controlled based on the type of the device and the identity of the user.

**provisioning**

Process used to securely provision a device and configure it with network settings.

**PSK**

Pre-shared Key. Shared secret that was previously shared between the two parties using a secure channel before it needed to be used.

**public key**

The part of a public/private key pair that is made public. The public key is used to encrypt a message; the recipient's private key is required to decrypt the message. A large part of a digital certificate is the certificate owner's public key. See also private key.

**public-key infrastructure**

Security technology based on digital certificates and the assurances provided by strong cryptography. See also Certificate Authority, digital certificate, public key, private key.

**publisher**

Required server in a cluster. Each cluster can have only one publisher; it is the first server installed on the cluster. The publisher provides database services to the subscribers in the cluster. See also cluster, subscriber.

**push certificates**

Enable the server to work with the Apple Push Notification Service (APNS) and Apple iOS devices connected to an MDM account.

**QC**

See QuickConnect.

**QuickConnect**

Functionality within ClearPass used to securely provision an Android, Windows, Linux, or OS X device and configure it with network settings. QuickConnect's functionality is incorporated within Onboard.

**RADIUS**

Remote Authentication Dial-In User Service. Network access-control protocol for verifying and authenticating users; provides AAA management. A RADIUS transaction might be 802.1X, MAC-Auth, or generic RADIUS.

**Registration Authority**

Type of Certificate Authority that processes certificate requests. The Registration Authority (RA) verifies that requests are valid and comply with certificate policy, and authenticates the user's identity. The RA then forwards the request to the Certificate Authority to sign and issue the certificate.

**RFC**

Request For Comments; a commonly-used format for Internet standards documents.



---

## **RFC 3576 Dynamic Authorization**

Dynamic authorization describes the ability to make changes to a visitor account's session while it is in progress. This might include disconnecting a session or updating some aspect of the authorization for the session.

### **role**

Type of access being granted. ClearPass lets you define multiple roles. Such roles could include employee, guest, team member, or press. Roles are used for both guest access (user role) and operator access to ClearPass. See operator profile.

### **root CA**

Certificate Authority that signs its own certificate (a self-signed certificate), and must be explicitly trusted by users of the CA.

### **SAML**

Security Assertion Markup Language. XML-based framework for communicating user authentication, entitlement, and attribute information. SAML enables single sign-on by allowing users to authenticate at an identity provider and then access service providers without additional authentication.

### **SAN**

Subject Alternative Name. SANs let you specify a list of host names to be protected by a single SSL certificate. Multiple domain names are secured by adding them to the Subject Alternative Name (SAN) field during enrollment. The common name, or primary domain name, on the certificate must be a registered fully qualified domain name.

### **SCEP**

Simple certificate enrollment protocol. Protocol for requesting and managing digital certificates.

### **SCP**

Secure copy; SCP Protocol. Network protocol that supports file transfers between hosts on a network.

### **self-signed certificate**

See root CA.

### **session**

Service provided by a NAS to an authorized user.

### **skin**

A Web site's visual appearance, or "look and feel." It can be thought of as a container that holds the application, its layout, style sheet (font size and color for example), header and footer, and so forth.

### **Smarty**

Template engine for PHP, facilitating the separation of presentation (HTML/CSS) from application logic.

### **SMS**

Short Message System; a method for delivering short messages (up to 140 characters) to mobile phones.

### **SNMP**

Simple Network Management Protocol. A TCP/IP standard protocol for managing devices on IP networks. Network administrators use SNMP to monitor and map network availability, and facilitate the exchange of

---

information between network devices.

### **SOAP Web Services**

SOAP Web services provide a way of transferring data across the Internet to integrate Web-based applications. Web services let businesses share data and processes programmatically, and can be added to a user interface to provide functionality. The SOAP interface is available to third-party applications that will integrate with the ClearPass Guest Visitor Management Appliance. The API provides direct access to the underlying functionality of the ClearPass Guest Visitor Management Appliance. Developers wishing to provide integrated applications can use the API to programmatically perform actions that would otherwise require manual operation of the user interface.

### **SoH**

Statement of Health.

### **sponsor**

See operator.

### **SSID**

Service Set Identifier. Unique identifier attached to the header of packets sent over a WLAN, and which acts as a password when a mobile device tries to connect to the basic service set (BSS).

### **SSO**

Single Sign-On. Access-control property that lets a user log in once to access multiple related but independent applications or systems to which they have privileges. The process authenticates the user across all allowed resources during their session, eliminating additional login prompts.

### **static host**

A hostname; a relationship between a name and an IP address. A static host list is a named list of MAC or IP addresses.

### **subscriber**

Server in a cluster that “subscribes” to the publisher to receive updated database information. As redundant servers, subscribers improve performance through load balancing, and provide failover and high availability. Sometimes referred to as a node. See also cluster, publisher.

### **TACACS**

Terminal Access Controller Access Control System. Family of protocols that handle remote authentication and related services for network access control through a centralized server.

### **TLS**

See EAP-TLS.

### **trust chain**

Sequence of certificates, starting at a trusted root certificate, that establishes the identity of each certificate in the chain.

### **trusted root**

See root CA.

---

**TSV**

Tab-separated values.

**TTY**

TTY-enabled devices allow telephones to transmit text communications for people who are deaf or hard of hearing as well as transmitting voice communication.

**UAM**

Universal Access Method. Used by Wi-Fi operators to allow access to a wireless network, or to allow access to another network while roaming. For roaming, a Web browser is used to access a login page on a captive portal.

**UDID**

Unique Device Identifier for an iOS device.

**UDP**

User Datagram Protocol. Part of the TCP/IP family of protocols used for data transfer. UDP is typically used for streaming media, and is a "stateless" protocol, meaning it does not acknowledge that the packets being sent have been received.

**unique device credentials**

Network authentication credentials that uniquely identify the device and user and enable management of provisioned devices. May be a username and password or a TLS client certificate, depending on the type of device.

**user database**

Database of the guests on the system.

**UUID**

Universally Unique Identifier. Unique identifier generated when a provisioning profile is created, allowing proper app distribution permissions.

**VA**

Virtual appliance.

**VIA**

Aruba's Virtual Intranet Access client. Provides secure remote network connectivity for Android, Apple iOS, Mac OS X, and Windows mobile devices and laptops. Automatically scans and selects the best secure connection to the corporate network.

**view**

Page in the application that displays data but does not contain interactive fields the user can modify. Usually a table listing things like accounts or other sets of data and providing links to related actions or forms.

**VIP**

Virtual IP address.

**visitor**

Someone who is permitted to access the Internet through your Network Access Server. Also referred to as a guest.

---

**VMA**

Visitor Management Appliance. Refers to the ClearPass Guest application.

**VPN**

Virtual Private Network. Enables secure access to a corporate network when located remotely. It allows a computer to send and receive data across shared or public networks as if it were directly connected to the private network, while benefiting from the functionality, security, and management policies of the private network. This is done by establishing a virtual point-to-point connection through the use of dedicated connections, encryption, or a combination of the two.

**VSA**

Vendor-specific attribute.

**walled garden**

Defined set of internet or network resources that can or cannot be accessed by unauthorized users through the captive portal.

**Web Auth**

User-authentication system for Web pages and Web applications. Web authentication transactions through the dissolvable agent in OnGuard.

**Web login**

Login page displayed to a visitor.

**Wi-Fi**

Technology that allows devices to connect to a Wireless LAN (WLAN) network, mainly using the 2.4 gigahertz and 5 gigahertz radio bands.

**WLAN**

Wireless Local Area Network. Local Area Network (LAN) that users access through a wireless connection. 802.11 standards specify WLAN technologies. WLANs, in most cases, are some portion of a wired LAN.

**WPA2**

Wi-Fi Protected Access II. Certified interoperable version of the full IEEE 802.11i specification. WPA2 supports IEEE 802.1X/EAP authentication or PSK technology, but includes an advanced encryption mechanism using Counter-Mode/CBC-MAC Protocol (CCMP) called the Advanced Encryption Standard (AES).

**WSDL**

Web Service Description Language. An XML-based interface definition language used to describe the functionality provided by a Web service.

**X.509**

Standard defining the format and contents of digital certificates.

**XML-RPC**

XML Remote Procedure Call. Protocol that uses XML to encode its calls and HTTP as a transport mechanism. The XML-RPC interface is available to third-party applications that will integrate with the ClearPass Guest Visitor Management Appliance. The ClearPass Guest XML-RPC API provides direct access to the underlying functionality of the ClearPass Guest Visitor Management Appliance. Developers wishing to provide integrated

---

applications can use the API to programmatically perform actions that would otherwise require manual operation of the user interface.



**1**

1024-bit RSA 224

**2**

2048-bit RSA 224

**A**

AAA 23

access

configuring 164

access control, print templates 451

account filters, creating 675

accounting 22-23, 25

accounts

changing guest account role 44, 69, 78, 372

passwords, multiple 332

visitor account 26

Active Directory

LDAP authentication 681

active sessions 35, 37

administration 537, 662

plugin management 635

Administration module 537

advertising 473

campaigns 492

rank and weight 496

interstitial ads 486

labels 501

materials 502

nwa\_adspace Smarty template tag 481

pages 476

process overview 474

promotions 496

rank 486

services 473

spaces 484

tutorial 474

AirGroup

authenticating users via LDAP 545

configuration summary 28

configuring fields 302

configuring operator device limit 679

creating groups 79

creating users 680

defining controller 542, 638

enabling dynamic notifications 542, 638

LDAP user search, configuring 545

personal devices 82

registering devices 78

shared locations 80

shared roles 80

tag=value pair 80

time-based sharing 89

time-based sharing syntax reference 88

time-based sharing, examples 85

time fencing 90

AirPlay 181

AirPrint 183

alerts, SMS 39

API See also XML-RPC API

configuring plugin 639

SOAP Web services 570

XML-RPC 597

API clients 560

API documentation 564

API Explorer 564

API privileges 565

API services 560

- APN 184
- app sets 214
- app, registering for OAuth 567
- application log 663
  - filtering 664
  - searching 663
  - viewing 663
- authentication 22-23, 25, 35, 91
  - configuring 170
  - multi-factor 236, 409
- authorization 23, 25, 35
  - access, role-based 22
  - dynamic 37
- authorization servers 567
- B**
- Base-64 encoded 147
- binary certificate 147
- C**
- caching, CSV 720
- CalDAV 185
- calendar 185
- CAPTCHA security code 311
- captive portal 25, 347
  - hotspot 508
- CardDAV 187
- carrier
  - selecting 456
- certificate authorities 116
  - creating 117
  - editing 122
  - installing certificate 128
  - Microsoft Active Directory Certificate Services 133
  - requesting a certificate 128
- certificate management 144
- certificates
  - code-signing 153
  - creating 155
  - deleting 149
  - exporting 147
  - formats 147
  - importing 154
  - iOS certificate considerations 133
  - requesting 159
  - revoking 148
  - searching for 146
  - signing requests 149
  - trust chain 130
  - usage counts 162
- character set encoding 61
- Chromebook 751
  - configuring for Onboard 754
  - configuring Google Admin 755
  - network architecture 751
  - requirements 752
- client applications 567
- client credentials grant type 569
- client ID, OAuth 567
- client secret, OAuth 567
- closed session 37
- closing session 39
- code-signing certificate 153
- Configuration module 271
- configuration profiles 216-217
- configuring
  - access 164
  - AirGroup Services plugin 542, 638
  - AirPlay 181
  - AirPrint 183
  - API Framework plugin 639
  - APN 184
  - app sets 215
  - authentication 170
  - calendar (CalDAV) 185
  - Chromebook for Onboard 754



- configuration profiles 216-217
- contacts (CardDAV) 187
- device limit in AirGroup 679
- device provisioning 113
- Device Restrictions 189
- email 197
- Exchange ActiveSync 178
- Google Admin for Chromebook 755
- GuestManager plugin 277, 644
- iOS settings 177
- IP Phone Services plugin 650
- IPSec connection 209
- Kernel plugin 651
- LDAP user search for AirGroup 545
- MAC Authentication plugin 91, 653
- Onboard deployment and provisioning 216
- operator logins 668
- pages 294
- passcode policy 200
- Platform Services plugin 654
- plugins 636
- protocol settings 167
- provisioning settings 220-221
- proxy 175
- receipts 419, 462
- self-service portal, display functions 745
- shared\_location field 302
- shared\_role field 302
- Skin plugin 641
- SMS services 453
- SMS Services plugin 654
- SMTP Services plugin 657
- SOAP Web Services plugin 661
- subscribed calendar 203
- Translation Assistant plugin 659
- trust 171
- VIA connection 205
- VPN 204, 209
- Web Analytics plugin 660
- Web clips 213
- Web logins 397
- Web pages 418
- Windows-specific network settings 174
- contacting support 665
- contacts 187
- content
  - directory, creating 276
  - management 273
  - private files 274
  - public files 274
  - uploading 275
- creating
  - account filter 675
  - AirGroup administrator 680
  - AirGroup groups 79
  - AirGroup operator 680
  - certificate authority 117
  - configuration profiles 217
  - content directory 276
  - device accounts 45
  - field 295
  - guest account 41
  - hotspot plan 512
  - LDAP server 683
  - LDAP translation rule 690
  - multiple guest accounts 50, 58
  - operator 680
  - operator profile 673
  - operator profiles 673
  - print template 445
  - self registration 348
  - session filter 675
  - SMS gateway 454
  - Web logins 397
  - Web pages 418
- credits, SMS 460

## CSV

  caching 720

  parsing 722

customer support 665

## customizing

  content 273

  email receipt 438

  fields 294

  Guest Manager 277

  hotspot invoice 524

  hotspot receipt 533

  hotspot selection interface 527, 530, 533

  login message 377

  login page 373-374

  login page, Onboard enrollment 378

  receipt actions 358

  receipt page 357

  Register Shared Device 302

  registration form 355

  registration page 353

  self-service portal 386

  view fields 337

## D

data retention 97, 622

databases, user 26

default skin 643

## deleting

  certificate 149

  field 295

  SMS gateways 453

  SMTP carrier 462

## deployment

  network provisioning 26

  operational issues 26

  overview 26

  security policy 28

  site checklist 27

device management 136, 141

Device Restrictions 189

device type 144

  detection override 228

devices 69

  creating accounts 45

  editing 84

  filtering 70

  importing 93

  list 136, 141

  paired accounts 49

  personal, AirGroup 82

  provisioning configuration 221

  shared 79

  viewing 84

digital passes 420

  Apple Passbook certificates 423

  creating and editing a template 427

  images 434

  managing 427

  process overview 423

  template code variables 433

  templates 422

  viewing certificates 424

## disabling

  SMTP carrier 462

disconnecting session 35, 37

documentation, viewing 666

## duplicating

  SMS gateways 453

dynamic authorization 35, 37

## E

### editing

  base field 309, 338, 356

  certificate authorities 122

  devices 84

  expiration time, guest account 66

  fields 295

  form fields 309

- forms 306, 308
- guest account role 44, 69, 78, 372
- guest accounts 687
- guest self-registration 347
- hotspot plans 512
- print templates 451
- receipt pages 357
- self-registration 355
- SMS gateway 454
- SMS gateways 453
- views 306, 337
- Web logins 397
- Web pages 418
- email 197
  - guest self-registration receipts 361
  - receipts 44, 435
  - receipts, customizing 438
  - SMTP services 435
- enabling
  - SMTP carrier 462
- encoding 61
- encryption key, in guest receipt 283, 649
- Exchange ActiveSync 178
- expiration
  - guest accounts, editing 66
- exporting
  - certificates 147
  - guest accounts 58
- F**
- fields 25, 284
  - account\_activation 725
  - address 733
  - auto\_send\_sms 734
  - auto\_send\_smtp 734
  - auto\_update\_account 285, 725
  - captcha 725
  - card\_code 733
  - card\_expiry 733
  - card\_name 733
  - card\_number 733
  - change\_of\_authorization 725
  - city 733
  - country 733
  - create\_time 725
  - creating 295
  - creator\_accept\_terms 285, 725
  - creator\_name 726
  - customizing 294
  - Delete 295
  - deleting 295
  - do\_expire 287, 726
  - do\_schedule 286
  - dynamic\_expire\_time 726
  - dynamic\_is\_authorized 726
  - dynamic\_is\_expired 726
  - dynamic\_session\_time 726
  - Edit 295
  - email 285, 726
  - enabled 286, 726
  - expiration\_time 726
  - expire\_after 287
  - expire\_postlogin 287
  - expire\_time 287, 727
  - expire\_timezone 727
  - expire\_usage 287, 727
  - first\_name 733
  - hotspot\_plan\_id 733
  - hotspot\_plan\_name 733
  - http\_user\_agent 727
  - id 727
  - importing matching 62
  - ip\_address 727
  - last\_name 733
  - modify\_expire\_postlogin 727
  - modify\_expire\_time 287, 727
  - modify\_expire\_usage 728

modify\_password 285, 728  
modify\_schedule\_time 286  
modify\_start\_time 728  
multi\_initial\_sequence 278, 644, 729  
multi\_prefix 278, 644, 729  
netmask 729  
no\_password 729  
no\_portal 729  
no\_warn\_before 729  
notes 729  
num\_accounts 729  
password 280, 285, 450, 646, 729  
password\_action 729  
password\_action\_recur 730  
password\_last\_change 730  
password2 285, 729, 733  
personal\_details 733  
purchase\_amount 733  
purchase\_details 733  
random\_password 285, 730  
random\_password\_length 285-286, 730  
random\_password\_method 285-286, 730  
random\_password\_picture 736  
random\_username\_length 278, 285-286,  
644, 731  
random\_username\_method 278, 285, 644,  
731  
random\_username\_picture 278, 644, 732,  
736  
rank\_ordering 308  
remote\_addr 732  
role\_id 285, 732  
role\_name 285, 450, 732  
schedule\_after 286  
schedule\_time 286  
secret\_answer 395, 732  
secret\_question 395, 732  
Show forms 295  
show\_views 295  
simultaneous\_use 284-285, 650, 732  
sms\_auto\_send\_field 444, 734  
sms\_enabled 443, 734  
sms\_handler\_id 443, 734  
sms\_phone\_field 443, 734  
sms\_template\_id 443, 734  
sms\_warn\_before\_message 734  
smtp\_auto\_send\_field 441, 734  
smtp\_cc\_action 441, 734  
smtp\_cc\_list 441, 735  
smtp\_email\_field 441, 735  
smtp\_enabled 441, 735  
smtp\_receipt\_format 441, 735  
smtp\_subject 441, 735  
smtp\_template\_id 441, 735  
smtp\_warn\_before\_cc\_action 442, 736  
smtp\_warn\_before\_cc\_list 442, 735  
smtp\_warn\_before\_receipt\_format 442, 735  
smtp\_warn\_before\_subject 442, 735  
smtp\_warn\_before\_template\_id 442, 735  
sponsor\_email 732  
sponsor\_name 732  
start\_after 732  
start\_time 732  
state 733  
submit 732  
submit\_free 733  
user\_activity 732  
username 285, 450, 732  
visitor\_accept\_terms 733  
visitor\_carrier 734  
visitor\_company 733  
visitor\_fax 733  
visitor\_name 396, 733  
visitor\_phone 733  
warn\_before\_from 442, 736  
warn\_before\_from\_sponsor 442, 736  
zip 733

- filtering
    - application log 664
    - devices 70
    - guest accounts 65, 77
    - sessions 38
  - form fields
    - advanced properties 331
    - CAPTCHA 311
    - check box 311
    - checklist 312
    - conversion functions 744
    - customizing 305
    - date/time picker 314
    - display functions 308, 745
    - display properties 310
    - drop-down list 315
    - editing 306, 308
    - enable if 336
    - file upload 316
    - form field editor 309
    - group heading 323
    - hidden 316
    - initial value 327
    - multiple selection list 317
    - password 318
    - previewing 309
    - radio buttons 319
    - static text 320
    - static text (options lookup) 322
    - static text (raw value) 321
    - text area 325
    - text field 325
    - validation errors 327
    - validation properties 326
    - validator functions 737
    - value conversion 334
    - value format functions 744
    - value formatter 335
    - visible if 336
  - formats, certificates 147
  - forms 25, 284, 289
    - change\_expiration 289
    - create\_multi 289
    - create\_user 289
    - guest\_edit 289
    - guest\_multi\_form 78, 289
    - guest\_register 289
    - guest\_register\_receipt 289
    - previewing 356
    - reset\_password 289
- G**
- grant types, OAuth 568
  - guest 26
  - guest access
    - business rules 284
    - click to print 283, 649
    - email receipt 435
    - NAS login 341
    - receipt page 341
    - registration page 341
    - roles 22
  - guest access, self-provisioned 35
  - guest accounts
    - activate 67
    - change expiration 66
    - changing role 44, 69, 78, 372
    - creating 41
    - creating multiple 50, 58
    - delete 66
    - disable 66
    - editing expiration 66
    - email receipt 44
    - export 58
    - exporting 58
    - filtering 65, 77
    - importing 60

- list 64
  - paging 65, 77
  - print 68
  - receipts 44
  - reset password 65
  - selection row 77
  - SMS receipt 44
  - view passwords 280, 646
  - XML export 59
  - guest management 33-34
    - custom fields 294
    - customizing 277
    - email receipts 435
    - print template wizard 448
    - print templates 444
    - self provisioned 341
    - sessions 35
    - SMS receipts 40, 461
  - Guest module 33
  - guest self-registration
    - download receipt 359
    - email receipts 361
    - login message 377
    - login page 373-374
    - NAS logins 384
    - Onboard enrollment 378
    - print receipt 360
    - self-service portal 387
    - SMS receipt 364
    - social logins 379
- H**
- help
    - context-sensitive 29
    - field help 30
    - quick help 30
    - searching 29
  - hotspot management 507
    - captive portal 511
    - creating plan 512
    - customer information 524
    - customizing invoice 524
    - customizing receipt 533
    - customizing selection interface 527, 530, 533
    - editing plan 512
    - invoice 524
    - plans 511
  - Hotspot Manager 507
  - HTML
    - Smarty templates 700
    - standard styles 698
    - syntax 697
- I**
- importing
    - certificate, code-signing 153
    - devices 93
    - guest accounts 60
    - matching fields 62
    - trusted certificate 154
  - interstitial ads 486
  - iOS certificate considerations 133
  - iOS settings 177
  - IPSec connection 209
- K**
- key 283, 649
  - key type 224
- L**
- labels, advertising 501
  - language packs 465
  - LDAP
    - authenticating AirGroup users 545
    - custom rules 693
    - matching actions 692
    - matching rules 691
    - operator logins 680

- POSIX-compliant servers 681
- server, creating 683
- standard attributes 748
- translation rules 681
- translation rules, creating 690
- URL syntax 686
- user search for AirGroup, configuring 545

- license counts 162
- local operators 680
- locations, AirGroup 80
- log files 663
- logging
  - passwords 280, 646

## M

### MAC

- address formats 91, 653
- advanced features 93
- authentication 91, 653
- registering devices 92
- message, sending SMS 460
- methods See also XML-RPC API
- Microsoft Active Directory Certificate Services 133

### MMS

- SMS template for 465
- mobile carrier
  - selecting 456
- multi-factor authentication 236, 409, 412

## N

### NAS 35

- login 26
- login, guest self-registration 384
- Network Access Server 25

- network settings 163
  - access 164
  - authentication 170
  - protocols 167

- proxy 175
- trust 171
- Windows-specific 174
- nwa\_radius\_query 705

## O

### OAuth 566

- authorization servers 567
- client applications 567
- client ID 567
- client secret 567
- grant types 568
- redirect URI 567
- registering app 567
- resource owners 566
- resource servers 567
- service accounts 569
- state token 567

### Onboard

- certificate authorities 116
- certificate authority
  - creating 117
  - editing 122
- date retention 97
- deployment checklist 97
- device management 136, 141
- enrollment with registration 378
- management and control 136
- Smarty template functions 114

### Onboard configuration 163

- AirPlay 181
- AirPrint 183
- APN 184
- calendar 185
- Chromebook 754
- configuration profiles 216-217
- contacts 187
- deployment and provisioning 216

- Device Restrictions 189
- email 197
- Exchange ActiveSync 178
- iOS settings 177
- network settings 163
  - access 164
  - authentication 170
  - protocols 167
  - proxy 175
  - trust 171
  - Windows-specific 174
- passcode policy 200
- provisioning settings 220-221
- subscribed calendar 203
- VPN 204
- VPN IPSec connection 209
- VPN VIA connection 205
- Web clips and bookmarks 213
- Windows applications (app sets) 214-215
- Onboard module 95
- Open SSL text format 147
- operator logins 667
  - advanced options 670
  - configuration 668
  - LDAP 680
  - LDAP server, creating 683
  - password options 674
  - user roles 675
- operator profiles 26, 667, 671
  - API privileges 565
  - automatic logout 670
  - creating 673
  - privileges 679
- operators 26
  - creating 680
  - local 680
  - login message 668
  - override device type detection 228
- P**
- pages 414, 418
  - configuring 294
- paired accounts 49
- passcode policy 200
- password grant type 568
- passwords
  - generating 279, 645
  - logging 280, 646
  - multiple accounts 332
  - recovery 264
  - resetting 65
- picture string 736
- PKCS#7 147
- plugin management 635
- plugins
  - configuring 91, 277, 542, 636-638, 641, 644, 650-651, 653-654, 657, 659-661
  - configuring, API Framework 639
  - IP Phone Services 650
  - Plugin Manager 635
  - viewing 635
- POSIX, LDAP 681
- previewing
  - forms 309, 356
- print templates 26, 444
  - creating 445
  - creating using wizard 448
  - custom fields 450
  - editing 451
  - permissions 451
  - SMS receipts 445
- private files, content 274
- programmer's reference 697
- protocol settings
  - configuring 167



- provisioning settings 216, 220-221
  - configuring 221
  - general settings 222
  - instructions and messages 238
  - iOS and OS X profiles 259
  - login form options 229
  - login page options 231
  - multi-factor authentication options 236
  - network login access options 238
  - Onboard client devices 261
  - social logins options 232
  - sponsorship confirmation 265
  - supported devices 227
  - Web login page 229
- proxy
  - configuring 175
- public files, content 274

## R

- RADIUS server 22
  - accounting query 705
  - active sessions 35
  - disconnecting session 35, 37
  - reauthorizing session 35, 38
- reauthorizing
  - session 35, 38
- receipt page 341
  - editing 357
- receipts 40, 461
  - configuring 419, 462
  - email 435
- redirect URI 567
- reference 697
  - basic HTML syntax 697
  - Smarty template syntax 700
    - basic template syntax 700
    - comments 700
    - conditional text blocks 701

- foreach text blocks 701
- modifiers 702
- predefined template functions 703
- repeated text blocks 701
- script blocks 701
- template file inclusion 700
- text substitution 700
- variable assignment 700
- standard HTML styles 698
- time-based sharing syntax 88
- Register page 341
- registering app, OAuth 567
- registering MAC devices 92
- regular expressions 749
- resetting
  - passwords 65, 394
- resource owners 566
- resource servers 567
- revoking certificate 148
- RFC 2255 687-688
- RFC 3576 37
- role-based access 22
- Role-based access control 667
- roles 26
  - changing for guest account 44, 69, 78, 372
  - shared 80
- RSA 224
- S**
- searching
  - application log 663
  - documentation 666
- security policy checklist 27
- selecting
  - mobile carrier 456
- self-registration
  - creating device 48
  - creating page 348

- editing 355
- self-service portal 268, 387
  - accessing 386
  - auto login 388
  - password generation 393
  - resetting passwords 394
  - secret question 395
- sending
  - SMS alert 39
  - SMS message 460
- sequence diagram
  - AAA 23
  - guest self-registration 347
- servers
  - LDAP, creating 683
- service account, OAuth 569
- session filters, creating 675
- sessions
  - active 35, 37
  - closed 37
  - closing 39
  - device 75
  - disconnecting 35, 37
  - filtering 38
  - reauthorizing 35, 38
  - SMS alert 39
  - stale 37
- shared locations 80
- shared roles 80
- skin
  - configuring 641
  - email receipt 439
- Smarty syntax
  - subject line 439
- Smarty template functions 700
  - assign function 700
  - comments 700
  - foreach block 701
  - if block 701
  - include 700
  - literal block 701
  - modifiers 702
  - nwa\_adspace tag 481
  - Onboard 114
  - section block 701
  - variables 700
- SMS
  - alert for session 39
  - alerts 39
  - character limit 445
  - credits 460
  - guest account receipts 44
  - guest self-registration receipts 364
  - guest self-registration sponsorship confirmation 369
  - subject line 439
- SMS gateways
  - creating 454
  - editing 453-454
  - viewing 453
- SMS services 453
  - configuring 453
  - credits available 461
  - guest receipts 40, 461
  - low credit warning 461
  - receipt options 462
  - sending message 460
  - SMS gateways 453
- SMTP services 435
  - customizing receipt 440
  - sending receipt 441
- SOAP Web services 570
- sponsors 26
- sponsorship confirmation
  - SMS receipt 369
- stale session 37

state token, OAuth 567

subject line

    email receipt 436

subscribed calendar 203

support 662, 665

syntax

    time-based sharing, examples 85

    time-based sharing, reference 88

## T

tab-separated values 58, 60

tag=value pair 80

template

    predefined template functions 703

    Web page templates 415

time-based sharing 89

    examples 85

time fencing 90

translation rules 690

translation services 465

    customizing translated user interface  
        text 469

    translation assistant 468

    translation packs 466

        creating and editing 467

troubleshooting

    application integrity check 636

    Onboard 114

trust settings

    configuring 171

TSV 58, 60

## U

uploading

    code-signing certificate 153

    content 275

usage

    certificates 162

    Onboard licenses 162

user database 26

## V

viewing

    application log 663

    devices 84, 136

    documentation 666

    plugins 635

    sessions, device 75

    SMS gateways 453

    SMTP carriers 462

    users 141

views 26, 284, 289

    column format 340

    customization 305

    editing 306, 337

    field editor 339

    guest\_export 59, 289

    guest\_multi 76, 289

    guest\_sessions 37, 289

    guest\_users 64, 289

visitors 26

    account 26

VPN 205, 209

VPN settings 204

## W

Web clips and bookmarks 213

Web logins 26, 396

    advertising services options 404

    creating and editing pages 397

    default destination options 402

    login form options 400

    login page options 403

    multi-factor authentication options 409

    network login access options 411

    post-authentication options 412

    social logins options 405

- Web pages 414
  - creating 418
  - editing 418
  - templates 415
- Windows-specific network settings
  - configuring 174
- Windows applications 214-215
- wizards
  - print template 448
- WPA key 283, 649
- X**
- XML
  - guest account list 59
  - parsing 722
- XML-RPC API 597
  - about 597
  - access control 599
  - accessing the API 600
  - API Symmetry 598
  - architecture overview 597
  - data representation 599
  - data types 599
  - faults 600
  - field customization 599
  - invoking the API 603
  - method
    - amigopod.guest.change.expiration 605
    - method amigopod.guest.create 606
    - method amigopod.guest.delete 607
    - method amigopod.guest.edit 609
    - method amigopod.guest.enable 611
    - method amigopod.guest.get 612
    - method amigopod.guest.list 614
    - method
      - amigopod.guest.reset.password 615
    - method amigopod.mac.create 616
    - method amigopod.mac.edit 618
    - method amigopod.mac.list 621
    - method summary 604
    - parameter names 599
    - parameter validation 599