ClearPass Guest 3.9

Deployment Guide

Open Source Code

Certain Aruba products include Open Source software code developed by third parties, including software code subject to the GNU General Public License (GPL), GNU Lesser General Public License (LGPL), or other Open Source Licenses. The Open Source code used can be found at this site:

http://www.arubanetworks.com/open_source

Legal Notice

The use of Aruba Networks, Inc. switching platforms and software, by all individuals or corporations, to terminate other vendors' VPN client devices constitutes complete acceptance of liability by that individual or corporation for this action and indemnifies, in full, Aruba Networks, Inc. from any and all legal actions that might be taken against it with respect to infringement of copyright on behalf of those vendors.

Warranty

This hardware product is protected by the standard Aruba warranty of one year parts/labor. For more information, refer to the ARUBACARE SERVICE AND SUPPORT TERMS AND CONDITIONS.

Altering this device (such as painting it) voids the warranty.

www.arubanetworks.com

1344 Crossman Avenue
Sunnyvale, California 94089

Phone: 408.227.4500
Fax 408.227.4550

Contents

Figures

Tables

Collaboration between companies and mobility of staff has never been greater. Distributed workforces, traveling sales staff and a dependence on outsourced contractors and consultants requires efficient management, which can pose problems for network security and operational staff.

With visitors increasingly requiring online access to perform their work, ClearPass Guest provides a simple interface that can quickly create and manage visitor accounts within a pre-defined security profile. The faster and easier staff can connect with visitors, the quicker they can start being productive.

ClearPass Guest provides a simple and personalized user interface through which operational staff can quickly and securely manage visitor network access. With ClearPass Guest, your non-technical staff have 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 customized print receipt with account details or they 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.

Using the built-in customization features, your visitors are also able to self-provision their own guest accounts using the settings you have defined. The registration experience is delivered with a branded and customized Web portal, ensuring a streamlined and professional user experience. Visitors may also be asked to complete additional survey questions during the self-registration process, with the collected data stored for later analysis by the reporting system to provide additional feedback on your visitors and their usage of the network.

ClearPass Guest integrates with all leading wireless and NAC solutions through its AAA enterprise services interface. This ensures that IT administrators have a standard integration with the network security framework, but gives operational staff the user interface they require.

ClearPass Guest is an effective solution to resolve the ever-growing demand for network access from external visitors, contractors and business partners.

About this Manual

This deployment guide is intended for system administrators and the persons installing and configuring ClearPass Guest. It takes you through the process of installing and configuring ClearPass Guest as your solution for visitor management.

Documentation Conventions

Tab and button names are shown in bold, preceded by the appropriate icon, for example,  **Save Changes**.

Code samples are shown in a fixed-width font; for example:

```
Sample template code or HTML text
```

Command link icons are shown in the margin. These icons are used within the ClearPass Guest user interface to visually identify the different components of the software.

Documentation Overview

Click the context-sensitive **Help** link displayed at the top right of each page to go directly to the relevant section of the deployment guide.

The following quick links may be useful in getting started.

Table 1*Quick Links*

For information about...	Refer to...
What visitor management is and how it works	"Management Overview"
Using the guest management features	"Standard Guest Management Features"
Running reports	"Running and Managing Reports"
Creating new reports	"Creating Reports"
Role-based access control for operators	"Operator Profiles"
Setting up LDAP authentication for operators	"LDAP Operator Authentication"
Guest self-provisioning features	"Self Provisioned Guest Access"
Dynamic authorization extensions	"RFC 3576 Dynamic Authorization"
SMS receipts for guest accounts	"SMS Services"
Email receipts for guest accounts	"SMTP Services"
Network administration of the appliance	"Administrator Tasks"

A brief outline of this deployment guide includes:

- Chapter 2, "Management Overview" provides an overview of the processes and interactions involved in visitor management.
- Chapter 3, "Setup Guide" covers the hardware installation (or virtual appliance deployment) and initial configuration of the ClearPass Guest servcr.
- Chapter 5, "RADIUS Services" provides reference material about implementing network access control using ClearPass Guest's RADIUS services.
- Chapter 6, "Operator Logins" describes how to define operator profiles and operator logins for ClearPass Guest, including integrating operator logins with an LDAP directory server.
- Chapter 7, "Guest Management" explains the built-in guest management features and the customization options for provisioning guest accounts, including setting up guest self-provisioning and defining new SMS or email receipts.
- Chapter 8, "Report Management" covers the use of the built-in reports and explains how to create new reports to summarize visitor account information and network usage accounting data.
- Chapter 9, "Administrator Tasks" describes the configuration and maintenance tools used by network administrators to manage ClearPass Guest.
- Chapter 10, "Hotspot Manager" introduces the optional features that may be used to deploy a commercial hotspot and enable visitors to purchase self-provisioned network access.

- Chapter 11, "High Availability Services" describes the optional high availability services that may be used to deploy a cluster of appliances in a fault-tolerant configuration.
- Chapter 12, "Reference" contains technical reference information about many of the built-in features of the appliance.

Getting Support

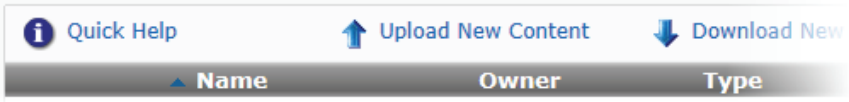
Field Help

The ClearPass Guest user interface has **field help** built into every form.

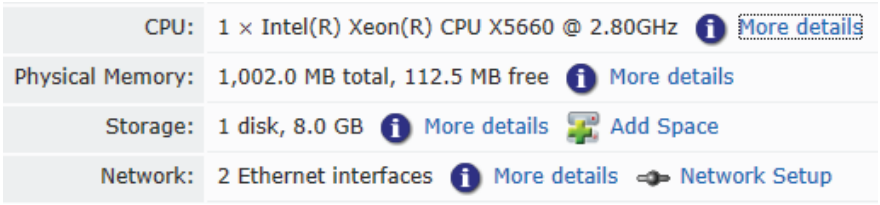
The field help provides a short summary of the purpose of each field at the point you need it most. In many cases this is sufficient to use the application without further assistance or training.

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.

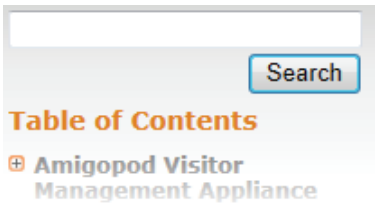


Context-Sensitive Help

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 will open a new browser window showing the relevant section of this deployment guide.

Searching Help

The deployment guide may be searched using the Search box in the top left 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”).

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 Deployment 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.

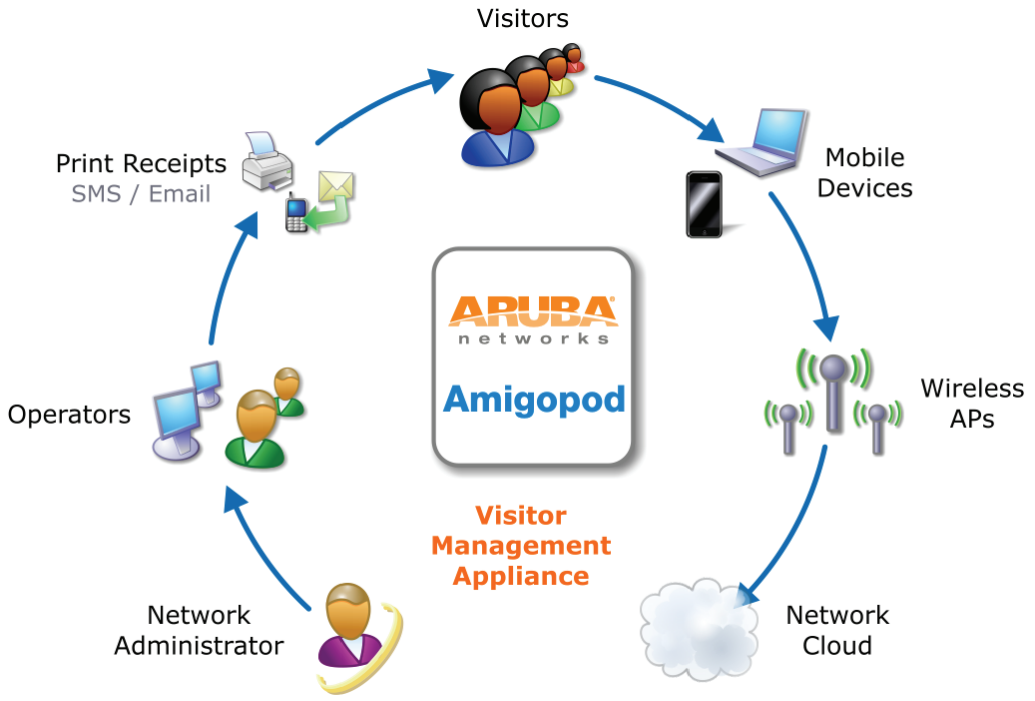
If you still need information, refer to the **Web Resources** command available under Support Services in the ClearPass Guest user interface.

This section explains the terms, concepts, processes, and equipment involved in managing visitor access to a network. The content here 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. Reading this section will enable you to become familiar with the terminology used in this guide and understand how ClearPass Guest can be successfully integrated into your network infrastructure.

Visitor Access Scenarios

The following figure shows a high-level representation of a typical visitor access scenario. **See Figure 1.**

Figure 1 *Visitor access using ClearPass Guest*



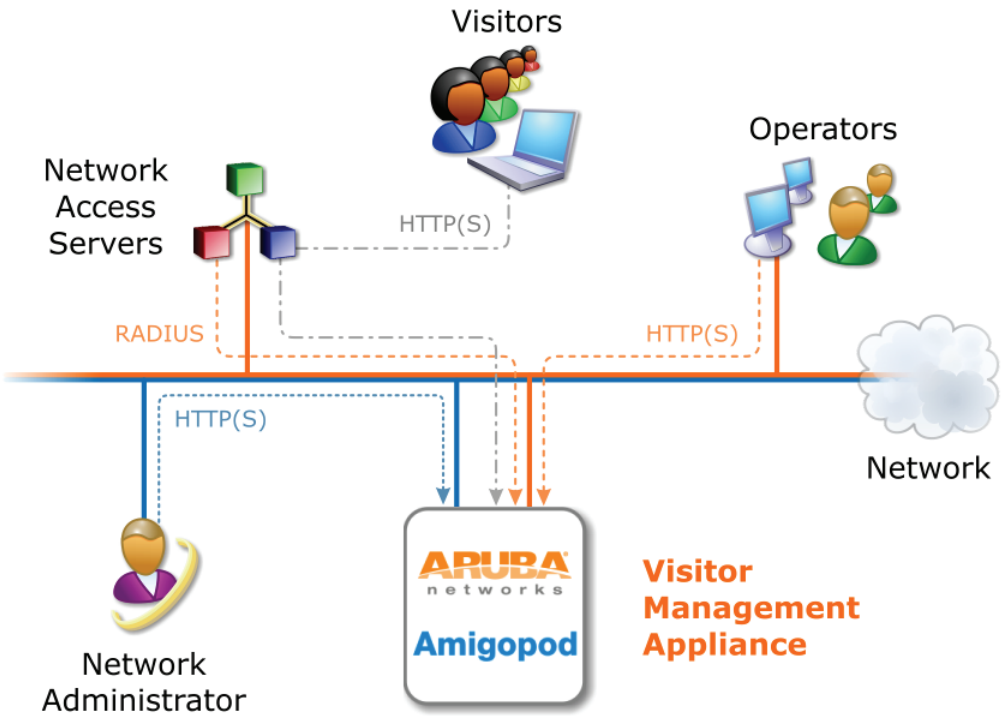
In this scenario, visitors are using their own mobile devices to access a corporate wireless network. Because access to the network is restricted, visitors must first obtain a username and password. A guest account may be provisioned by a corporate operator such as a receptionist, who can then give the 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. **See Figure 2.**

Figure 2 *Reference network diagram for visitor access*

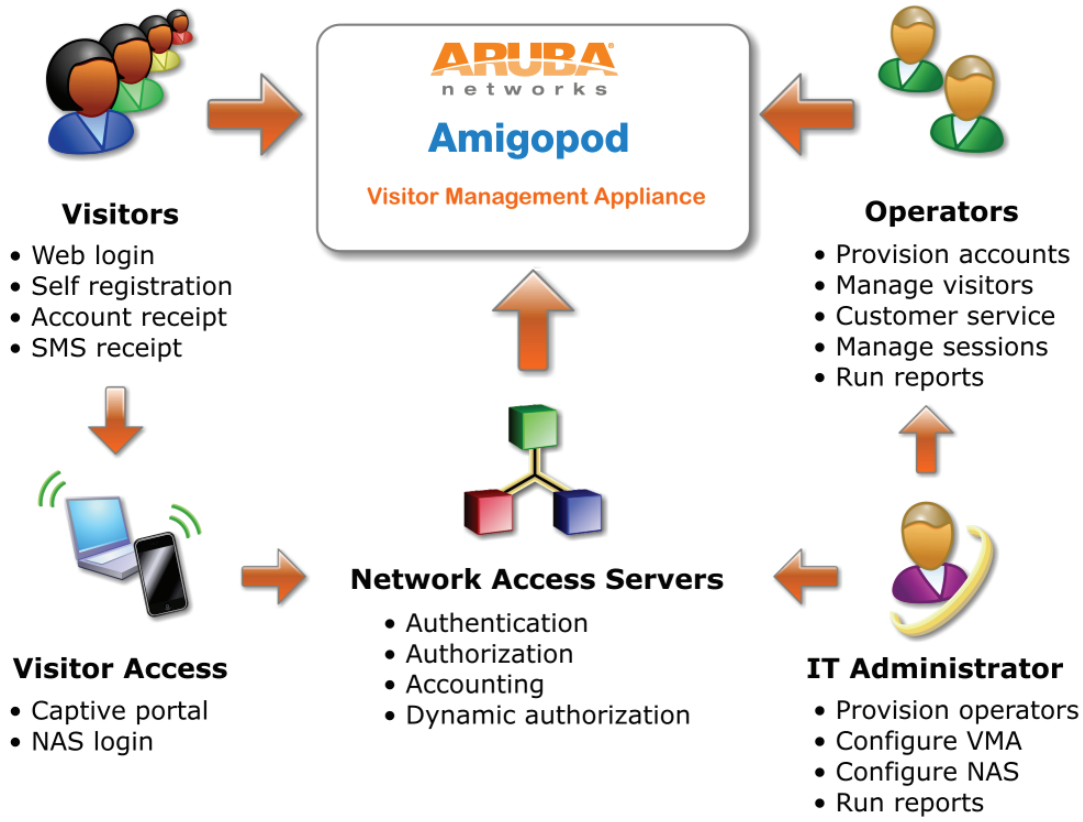


The network administrator, operators and visitors may use different network interfaces to access the visitor management features. The exact topology of the network and the connections made to it will depend on the type of network access offered to visitors and the geographical layout of the access points.

Key Interactions

The following figure shows the key interactions between ClearPass Guest and the people and other components involved in providing guest access. **See Figure 3.**

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 Guest 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.

Authorized access uses the concept of roles. Each visitor is assigned a role, which consists of a group of RADIUS attributes. These attributes are used to control every aspect of the guest's network session, effectively defining a security policy that controls what the guest is permitted to do on the network. Vendor-specific attributes may be used to configure the finer details of the NAS security policy.

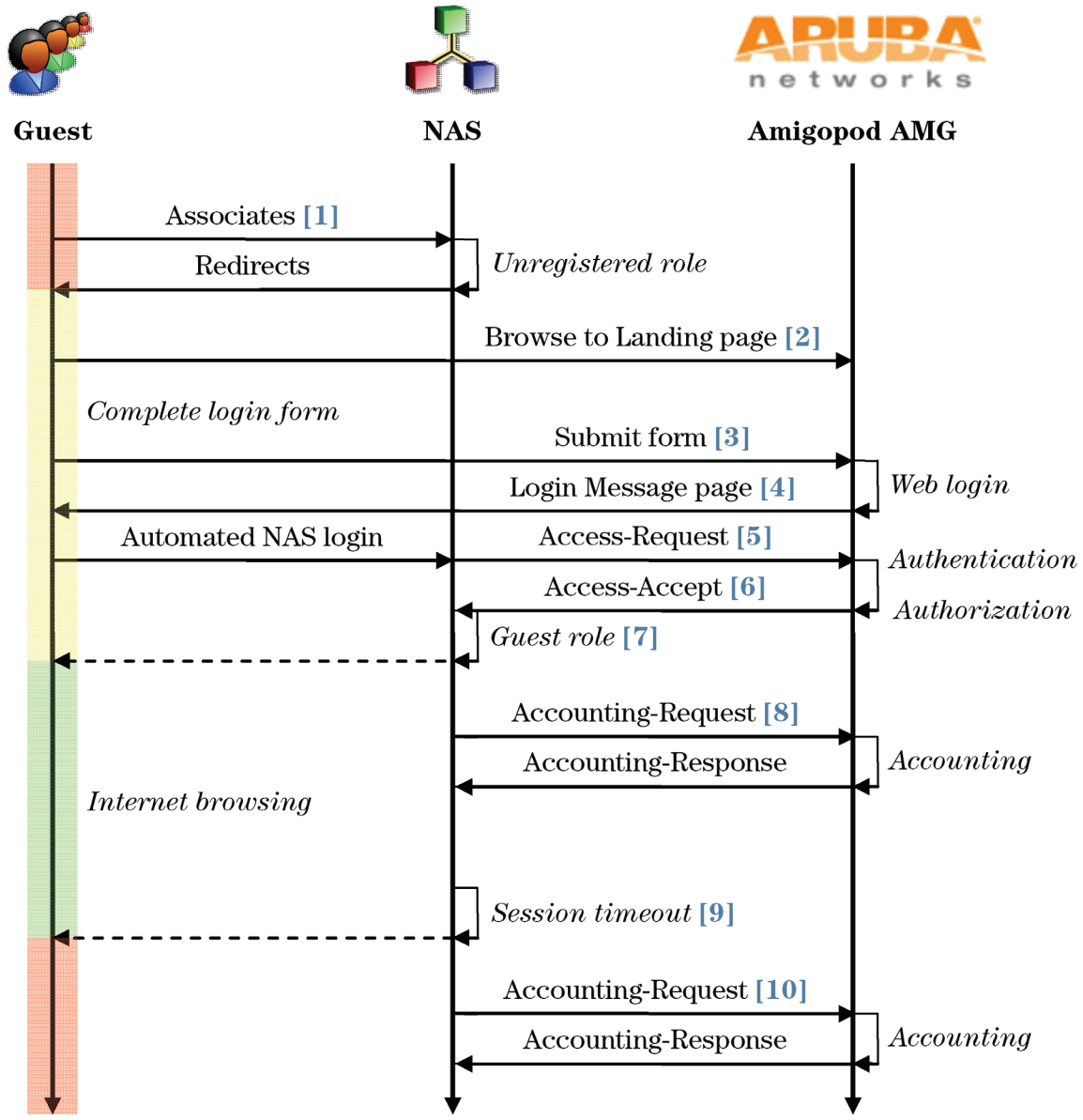
The network usage of authorized guests is monitored by the NAS and reported in summary form to ClearPass Guest using RADIUS accounting, which allows administrators to generate network usage reports.

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. See Figure 4.

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 into 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 Guest 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 [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 Guest server.
- The NAS reports details about the user's session to the ClearPass Guest 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 deployment guide.

Table 2 *List of Key features*

Feature	Refer to…
Visitor Access	
RADIUS server providing authentication, authorization, and accounting (AAA) features	"RADIUS Services"
▪ Support for 802.1X authentication	"EAP and 802.1X Authentication and Certificate Management"
▪ Support for external authentication servers, including Microsoft Active Directory and LDAP	"External Authentication Servers (EAS)"
Web server providing content delivery for guests	"Content Manager"
Guest self-registration	"Customizing Self Provisioned Access"
Web login portal	"Web Logins"
Visitor Management	
Create and manage visitor accounts, individually or in groups	"Standard Guest Management Features"
Manage active RADIUS sessions using RFC 3576 dynamic authorization support	"Active Sessions Management"
Import and export visitor accounts	"Importing Guest Accounts"
Create guest self-registration forms	"Creating a Self-Registration Page"
Configure a self-service portal for guests	"Self-Service Portal Properties"
Paid access via Hotspot Manager	"Hotspot Manager"
Run reports on all aspects of visitor access	"Running and Managing Reports"
Local printer, SMS or email delivery of account receipts	"Editing Guest Receipt Page Properties"
Role based access control for visitor accounts	"User Roles"
Configure NAS equipment with vendor-specific attributes per visitor role	"Adding Role Attributes"

Table 2 *List of Key features (Continued)*

Visitor Account Features	
Independent activation time, expiration time, and maximum usage time	"Business Logic for Account Creation"
Disable or delete at account expiration	"Account Expiration Types"
Logout at account expiration	"Account Expiration Types"
Define unlimited custom fields	"Customization of Fields"
Username up to 64 characters	"GuestManager Standard Fields"
Customization Features	
Create new fields and forms for visitor management	"Customization of Forms and Views"
Use built-in data validation to implement visitor survey forms	"Form Validation Properties"
Create print templates for visitor account receipts	"Editing Guest Receipt Page Properties"
Create new Web login pages for visitor NAS access	"Web Logins"
Create new reports	"Creating Reports"
Administrative Management Features	
Operators defined and authenticated locally	"Local Operator Authentication"
Operators authenticated via LDAP	"LDAP Operator Authentication"
Restrict operator logins by IP address ranges	"Creating a VLAN Interface"
Role based access control for operators	"Operator Profiles"
Configure network interfaces and run diagnostic checks	"Network Setup"
Integrated backup and restore	"Backup and Restore"
Scheduled backup to FTP or SMB server	"Scheduling Automatic Backups"
Secure Web access with HTTPS	"SSL Certificate"
Plugin based application update service (Web service)	"Plugin Manager"
Perform a security audit of the system	"Security Manager"
Synchronize server time automatically with NTP	"Server Time"
Syslog support	"Exporting the System Log"
SNMP support	"SNMP Configuration"

Table 2 *List of Key features (Continued)*

Advanced RADIUS modules for custom configuration	"Server Configuration"
Customize RADIUS dictionary	"Dictionary"
User Interface Features	
Context-sensitive help with searchable online documentation	Documentation Overview

Visitor Management Terminology

The following tables describes the common terms used in this guide. See Table 3.

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	AControls 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.
Netw ork 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.
Ope rator Profile	Characteristics assigned to a class of operators, such as the permissions granted to those operators.
Ope rator/Operator Login	User of ClearPass Guest to create guest accounts, run reports or perform system administration.
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.

Table 3 *Common Terms (Continued)*

Web Login/NAS Login	Login page displayed to a guest user.

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

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?

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

Deploying 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?

This section covers the initial deployment and configuration of ClearPass Guest.

If you have a hardware appliance, **See "Hardware Appliance Setup"** in this chapter. If you are using ClearPass Guest in a virtual machine, See "Setting Up the Virtual Appliance" in this chapter.

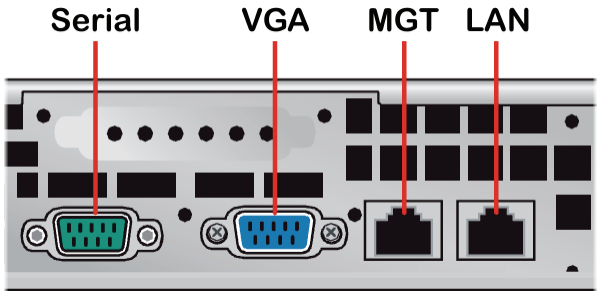
Hardware Appliance Setup

Refer to the Hardware Setup Guide sheet included in the box with the appliance for detailed installation information for the chassis and rack assembly.

Default Network Configuration

The AMG-HW-100 and AMG-HW-2500 appliances have two gigabit Ethernet network ports on the rear of the chassis. **See Figure 5**.

Figure 5 *Rear port configuration for AMG-HW-100/-2500 appliances*



The factory default network configuration for these ports is:

Table 5 *Default port configurations*

Item	MGT Port	LAN Port
Configuration Method	Static	DHCP
IP Address	192.168.88.88	–
Netmask	255.255.255.0	–
Gateway	192.168.88.1	–
DNS	–	–
Adapter Name	eth0	eth1
Hostname	clearpass-guest.localdomain	

Setting Up the Virtual Appliance

VMware Workstation or VMware Player

The virtual appliance is packaged as a zip file containing a directory with the files for the virtual machine.

To install the virtual appliance:

1. Extract the contents of the zip file to a new directory.
2. Double-click the .vmx file to start the appliance.

The configuration for the VMware Player virtual machine includes two virtual Ethernet adapters. The initial network configuration of these adapters is:

Table 6 *Ethernet adapter configuration*

Item	Network Adapter	Network Adapter 2
Adapter Type	NAT	Bridged
Configuration Method	DHCP	DHCP
IP Address	–	–
Netmask	–	–
Gateway	–	–
DNS	–	–
Adapter Name	eth0	eth1
Hostname	clearpass-guest.localdomain	

VMware ESXi

The virtual appliance is packaged as a zip file containing a directory with the files for the virtual machine. An OVF file specifies the details of the virtual machine.

To install the virtual appliance:

1. Extract the contents of the zip file to a new directory.
2. Start the VMware vSphere Client.
3. Use the **File > Deploy OVF Template** command to create a new virtual machine from the files in the virtual appliance directory.

In version 3.5 of VMware ESXi, the management console is called VMware Infrastructure Client. In this software, use the **File > Virtual Appliance > Import** command to create a new virtual machine from the files in the virtual appliance directory.

The configuration for the virtual machine includes one virtual Ethernet adapter. The initial network configuration of this adapter is:

Table 7 *Virtual ethernet adapter configuration*

Item	Network Adapter
Configuration Method	DHCP
IP Address	–
Netmask	–
Gateway	–
DNS	–
Adapter Name	eth0
Hostname	clearpass-guest.localdomain

Accessing the Console User Interface

The appliance's console user interface can be used to perform basic administrative functions such as changing the network configuration or viewing the appliance's MAC address details. It is also possible to recover a forgotten administrator password, or reset the appliance to its factory default settings.

For hardware appliances, you may access the console using a null modem cable connected to the serial port on the rear of the chassis. Use serial port settings of 9600 baud, 8 data bits, no parity, and 1 stop bit. Flow control is not required.

Both hardware and virtual appliances support command-line access directly at the console, and remotely via SSH. The following table summarizes the methods that you may use to access the console user interface.

Table 8 *Console access methods*

Access Method	Hardware Appliance	Virtual Appliance
Serial	Yes 9600, 8-N-1	No
VGA Console	Yes Use VGA display and a PS/2 or USB keyboard	Yes Use host's virtual console
SSH	Yes	Yes

Console Login

To access the console user interface:

- Log in with the username **admin** and the appliance's root password. This is **admin** by default, but is changed during the initial setup wizard.

When the administrator password is set during the setup wizard, the root password for the system will also be set to this password. However, once you have set the initial root password, future changes to the administrator password will not change the appliance's root password. The username to access the console user interface is always admin and cannot be changed.

Console User Interface Functions

When you log in to the console user interface, the following menu options are presented.

- To make a selection, type its corresponding number.

Table 9 *Console user interface functions*

#	Option	Description
1	Change network settings	Allows for interactive configuration of the appliance's network settings.
2	Restart services	Restarts major system services.
3	Reinitialize database	Destroys the entire configuration of the appliance and resets to the factory default state. All guest accounts, operator logins, RADIUS accounting records, application configuration, and customization will be lost.
4	Change shell password	Sets the new shell password used to access the console user interface.
5	Reset admin Web password to default	Recovers a forgotten Web administration password by restoring the default setting of admin.
6	Reboot appliance	Shuts down and restarts the appliance.
7	Reset network settings to default	Restores the original factory default network configuration for the appliance.
8	Display physical address information	Displays the MAC addresses of the appliance's network adapters.
9	Logout	Exits the console user interface.
10	Shut down appliance	Shuts down and powers off the appliance.

Accessing the Graphical User Interface

After you start ClearPass Guest, the initial startup screen is displayed in the console.

```
----------------------------------------

Aruba Amigopod Appliance
Copyright (C) 2011 Aruba Networks, Inc.
----------------------------------------

     /\    NOTICE: THIS IS LICENSED
    /!!\   COMPUTER SOFTWARE AND IS
   /_!!_\  PROTECTED BY COPYRIGHT.
----------------------------------------

Amigopod web interface is available at:
http://127.0.0.1
----------------------------------------

Aruba Amigopod OS release 3.1
Kernel 2.6.18-194.26.1.el5 on an x86_64

amigopod login: _
```

To open the ClearPass Guest graphical user interface (GUI):

- Either type or copy and paste the displayed URL into your Web browser.


NOTE

The default login settings for new installations require https: to access the graphical user interface. However, if you use https: to access the setup wizard, you may receive a warning message from your browser about the default self-signed SSL certificate that is installed on the appliance. **See "SSL Certificate"** in the Administrator Tasks chapter for information about installing a new SSL certificate.

Initial Configuraton Using the Setup Wizard

When you first log in to the appliance using the graphical user interface, you will be guided through an initial configuration process, which is explained in more detail below.

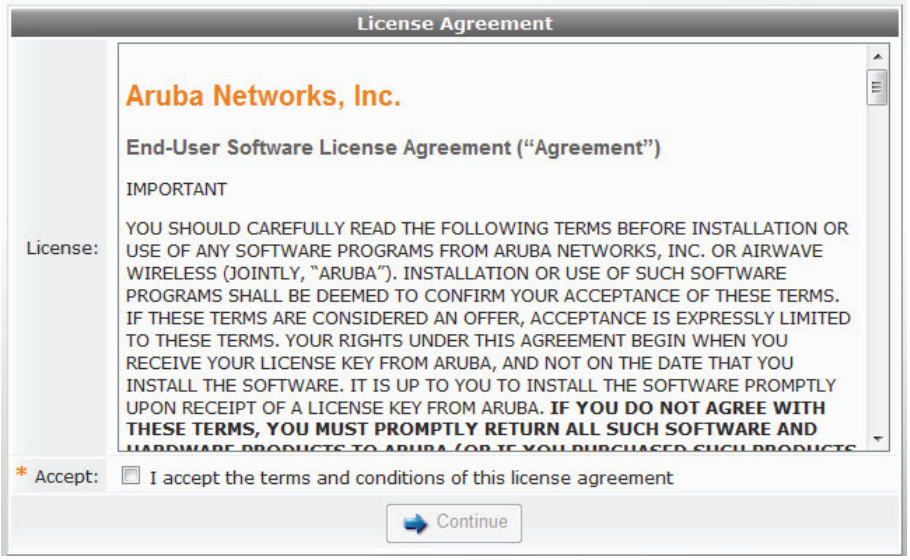
Logging In

To start the setup wizard:

- Enter the default username and password. When you log in for the first time, the default username is **admin**, and the default password is **admin**.
- Click the **Log In** button.

Accepting the ClearPass Guest License Agreement

The first time you log in, you are prompted to accept the license agreement.



To accept the agreement and continue the insatallation:

1. Review the software license agreement.
2. Mark the **Accept** check box, then click **Continue**.

If you have any questions about the license agreement, contact Aruba support using the Web site http://support.arubanetworks.com.

Setting the Administrator Password

After you review and accept the software license agreement, you will be prompted to set the password for the administrator account. This account has full access to all settings and areas in the graphical user interface.

To create a new password for the administrator account:

1. (Optional) For enhanced security, you may choose to change the **Operator Username** of the administrative account. Changing the username of the administrator account does not change the username for logging in to the console user interface.
2. In the **Operator Password** field, enter the new password. Passwords must be at least eight characters long and must include at least one uppercase letter, one lowercase letter, one digit, and one symbol.
3. (Optional) In the **Email** field, you may provide an email address for the administrator. While this step is not required, it is recommended. ClearPass Guest sends notification emails to this address for various system events.

When the administrator password is set for the first time, the root password for the system will also be set to this password. The root password is required to log in to the console user interface. **See "Console Login"** in this chapter for a description of how to do this. However, once you have set the initial root password, future changes to the administrator password will **not** change the appliance's root password.

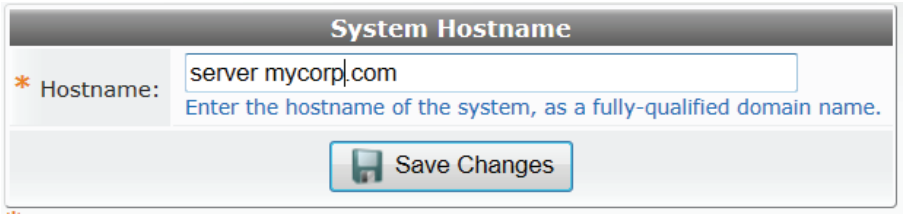
See "Resetting the Root Password" in the Administrator's Tasks chapter for details on resetting the appliance's root password.

Setting the System Hostname

The system hostname is a fully-qualified domain name. By default, this is set to **clearpass-guest.localdomain**, but you may specify another valid domain name.

To change the system hostname:

1. Go to **Administrator > Network Setup > System Hostname**.



2. In the **Hostname** field, enter the new name. A valid hostname is a domain name that contains two or more components separated by a period (.).

   Hostname parameters are:

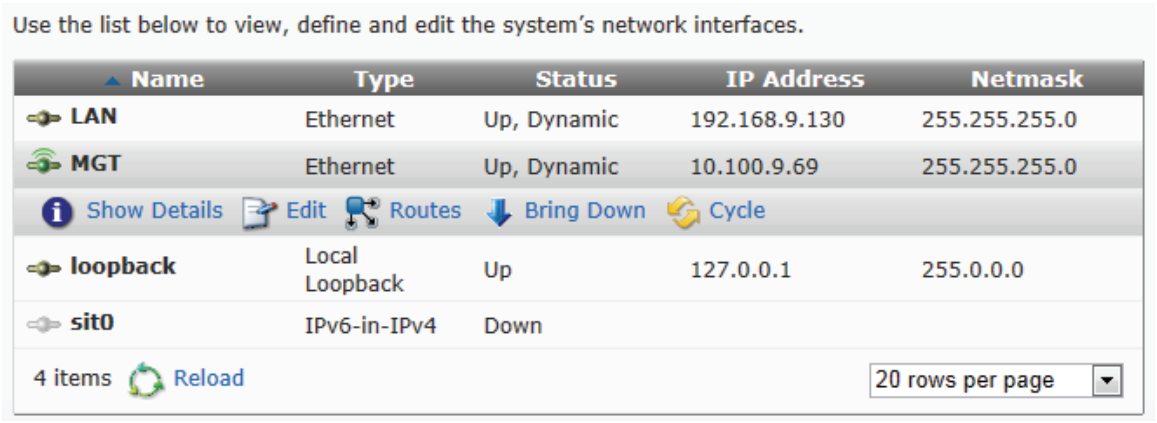
   - Each component of the hostname must not exceed 63 characters
   - The total length of the hostname must not exceed 255 characters
   - Only letters, numbers, and the hyphen (-) and period (.) characters are allowed
   - Hostnames may start with numbers, and may contain only numbers

Configuring Network Interfaces

The Network Interfaces List lets you view details and configure settings for the system's network interfaces.

To configure network interface settings:

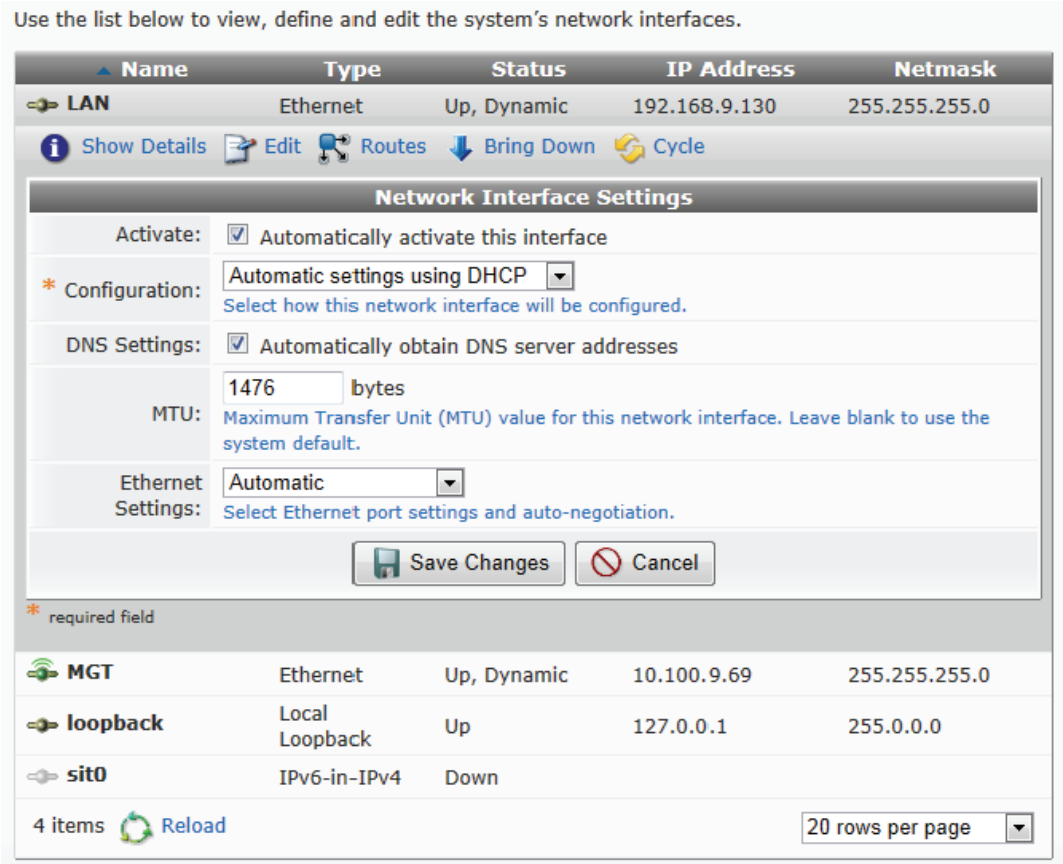
1. Go to **Administrator > Network Setup > Network Interfaces**.



   The results of an automated network diagnostic test are displayed at the top of the page. For more details about the network diagnostics, see Automatic Network Diagnostics in the Administrator Tasks chapter.

2. To change the configuration of a network interface, click the network interface's row in the list, then click the **Edit** command. The row expands to provide configuration options.

   LAN and MGT network interfaces may be configured for automatic settings using DHCP or BOOTP, or can be manually configured for an IP address. When you choose one of these settings from the Configuration drop-down list, additional options are displayed.



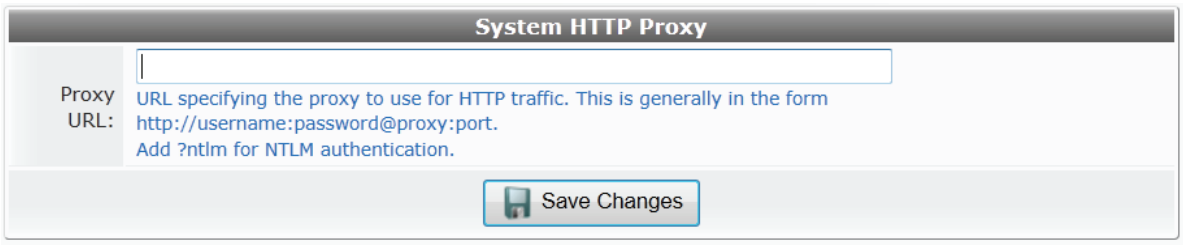
ClearPass Guest must be configured appropriately for your organization's relevant network infrastructure. For details on how to configure your network interface, see Changing Network Interface Settings in the Administrator Tasks chapter.

Configuring HTTP Proxy Settings

If you do not need to configure an HTTP proxy, click **Skip to Mail Settings** to continue with setup.

To configure HTTP proxy settings:

1. Go to **Administrator > Network Setup > HTTP Proxy**.



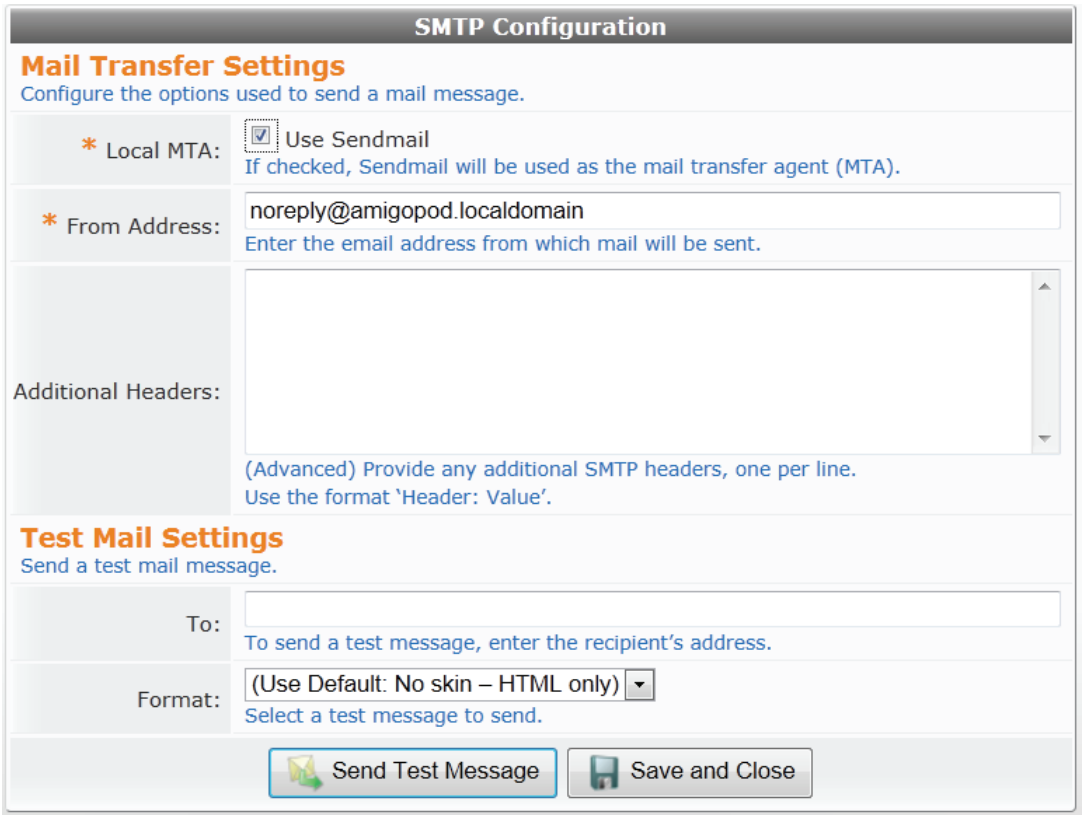
2. If your network configuration requires the use of an HTTP proxy to access the Internet, enter the details for the proxy in the Proxy URL field, then click **Save Changes**. If your HTTP proxy requires authentication, supply the username and password in the URL, as shown in the field help.

For details on HTTP proxy settings, See "Automatic Network Diagnostics" in the Administrator Tasks chapter.

Configuring SMTP Mail Settings

To configure SMTP settings:

1. Go to **Administrator > Network Setup > SMTP Configuration**.



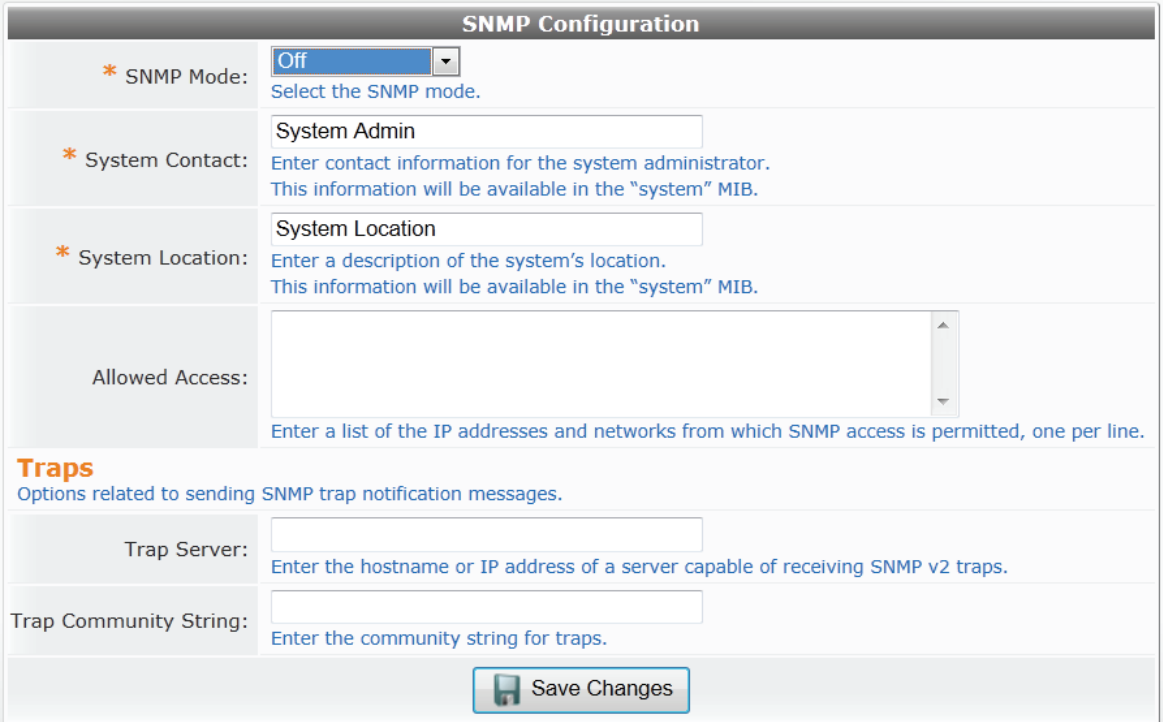
2. For details on how to complete the SMTP configuration, see "SNMP Configuration" in the Administrator Tasks chapter.
3. When you have completed the fields on this form, click the **Send Test Message** button to send an email to a test email address. The test email is in the selected format, and is used to verify the SMTP configuration and check the delivery of HTML formatted emails.
4. Click the **Save and Close** button to save the updated SMTP configuration.

Configuring SNMP Settings

The SNMP Setup form is used to configure the system's SNMP server and enable SNMP access.

To configure SNMP settings:

1. Go to **Administrator > Network Setup > SNMP Configuration**.



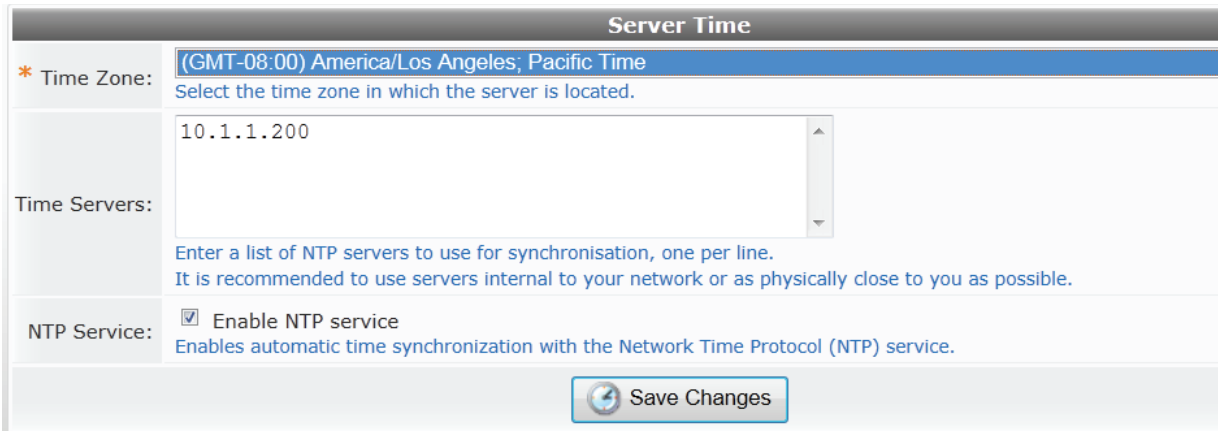
2. For details on how to complete the SNMP configuration, see "SNMP Configuration" in the Administrator Tasks chapter.
3. Click the **Save Changes** button to apply the SNMP configuration.

Configuring Server Time and Time Zone

To ensure that authentication, authorization and accounting (AAA) is performed correctly, it is vital that the server maintains the correct time of day at all times.

To configure the server's time and time zone:

1. Go to **Administrator > Server Time**.



2. In the **Time Zone** field, select the server's time zone.
3. It is strongly recommended that you configure one or more NTP servers to automatically synchronize the server's time. In the **Time Servers** field, enter the list of NTP servers to use for synchronization.

   If available, it is recommended that you use an NTP server that is available on your local network. This will improve timekeeping and will eliminate the need for additional Internet traffic for the time server.

To use a public NTP server, enter the following hostnames:

0.pool.ntp.org
1.pool.ntp.org
2.pool.ntp.org

You can also use NTP pool servers located in your region. For more information, refer to the NTP Pool Project Web site: http://www.pool.ntp.org.

NOTE

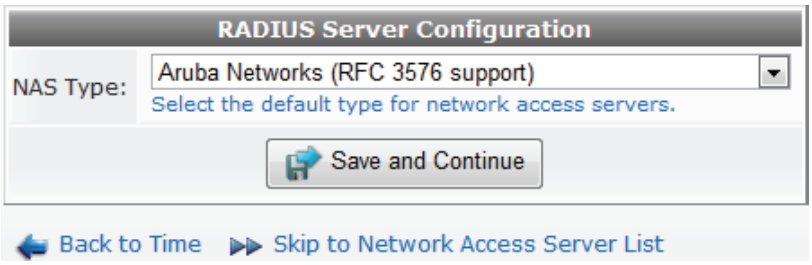
NTP can interfere with timekeeping in virtual machines. The default virtual machine configuration will automatically synchronize its time with the host server, so you should not configure NTP within the virtual machine. However, make sure that the host is configured to keep its clock in sync with a suitable time source.

4. To enable automatic time synchronization with NTP, mark the check box in the **NTP Service** row.
5. Click **Save and Continue** to apply the server's time configuration and continue with setup.

Configuring the Default RADIUS NAS Vendor Type

NOTE

If you do not need to configure the default NAS vendor type, click **Skip to Network Access Server List** to continue with setup.

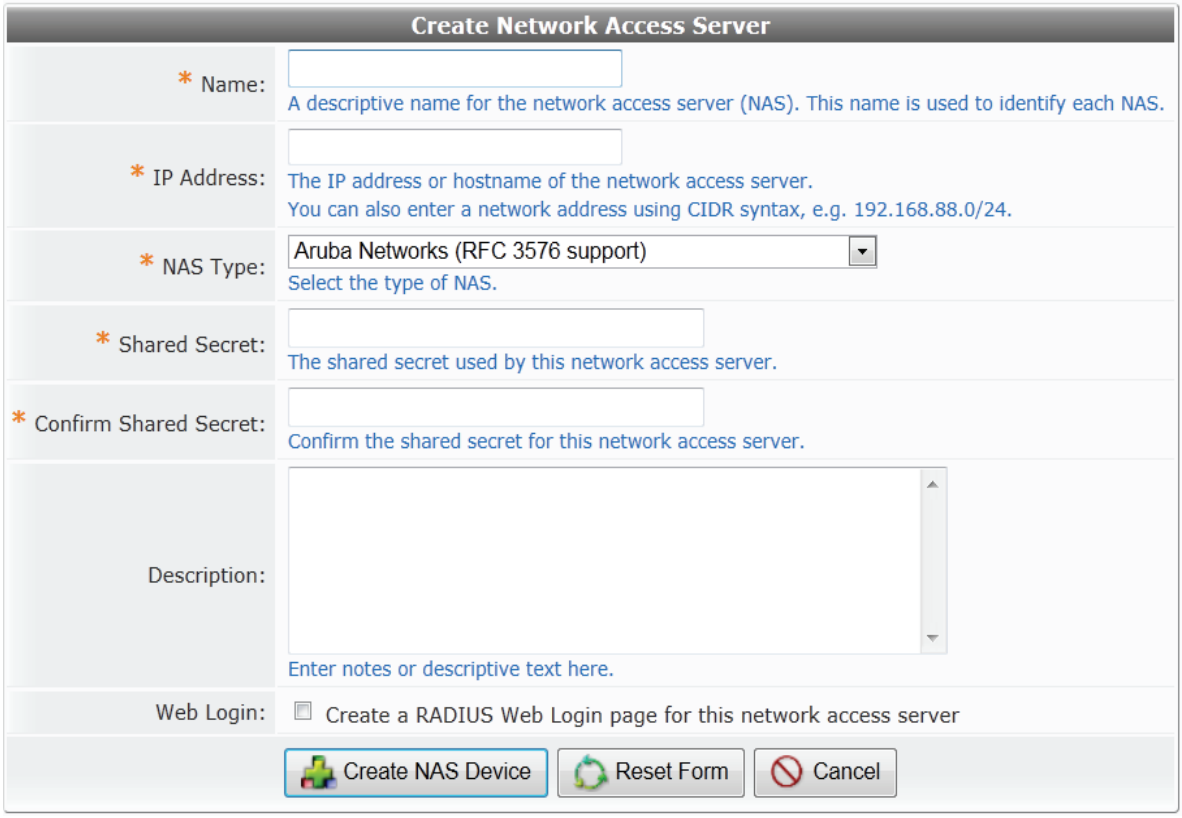


To configure the default Network Access Services (NAS) vendor type:

1. In the **NAS Type** drop-down list, if your deployment uses only one type of NAS, choose the default NAS vendor type to use when defining RADIUS clients or creating RADIUS Web Login pages that have vendor-specific settings.
2. Click **Save and Continue** to apply the RADIUS server configuration,.

Defining RADIUS Network Access Servers

A network access server (NAS) is a RADIUS client, and must be predefined in order to access the RADIUS server. For security, each NAS device must also have a shared secret which is known only to the device and the RADIUS server. Use the Network Access Servers list view to define the NAS devices for this server and to make changes to existing NAS devices.



To define the RADIUS network access servers:

1. In the **Name** field, enter a descriptive name to identify the first NAS server.
2. For details on how to complete the rest of the fields for defining the NAS entry, see **"Creating a Network Access Server Entry"** in the RADIUS Services chapter.
3. Click **Create NAS Device**.

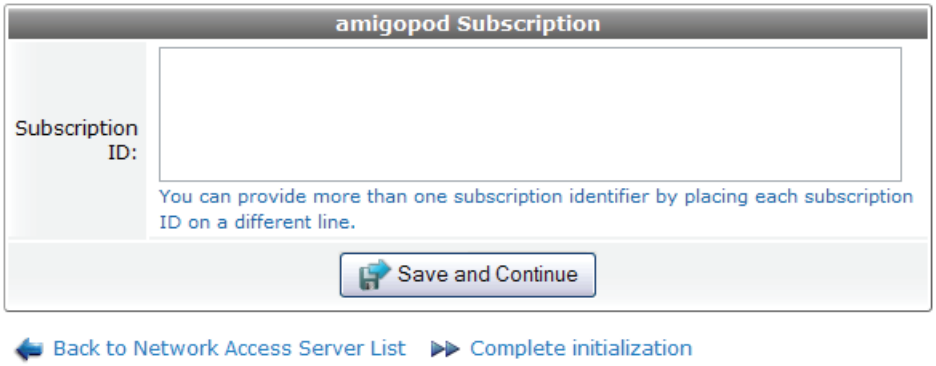
To define additional NAS entries for the RADIUS server, you can click the **Create** tab above the form.

Configuring the ClearPass Guest Subscription ID

Both hardware and software appliances are shipped with a restricted default license. This default license permits each guest account to have only a limited lifetime, as well as restricting other capabilities of the software.

If you have purchased ClearPass Guest, you will have one or more subscription IDs that enable particular modules of functionality that you have purchased. These subscription IDs will have been provided to you by your reseller at the time of purchase. To enable all functionality for your subscription, you need to provide your subscription ID information.

If you are evaluating the application and do not have a subscription ID, click **Complete initialization** link below the form to continue with setup.



To provide your subscription information:

1. In the **Subscription ID** field, enter your subscription ID or IDs.

   A subscription ID consists of number and letter groups separated with hyphens. A typical subscription ID might look like this:
   xn2ncr-gyjyd4-mxlx2s-fv9gcy-rwy7n6

   Incorrectly-formatted subscription IDs cannot be entered in this form. A form validation error is displayed if an incorrect value is entered.

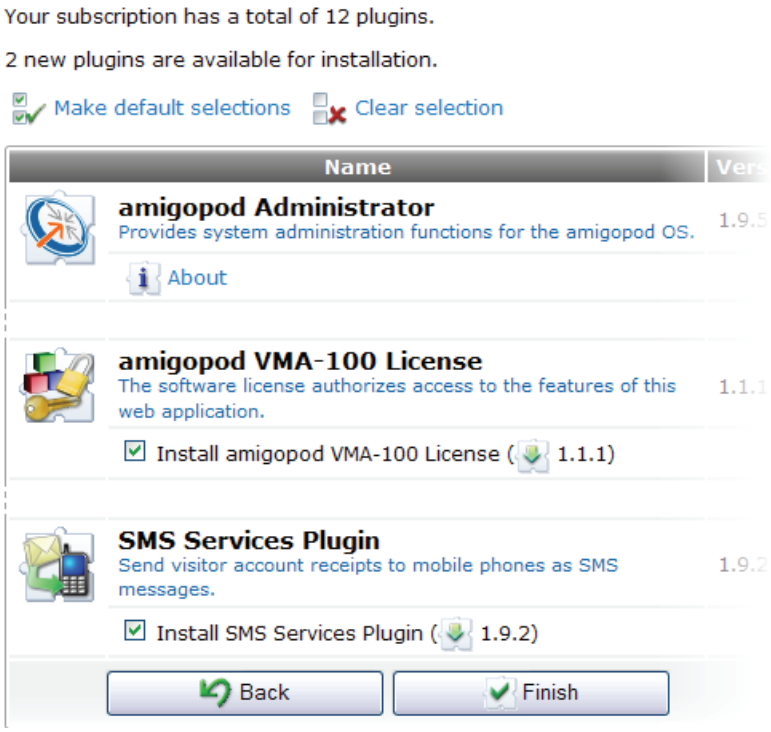
2. You can also attach a description to each subscription ID. To do this, write the description and follow it with the corresponding subscription ID in parentheses. For example:
   ClearPass Guest Subscription (xn2ncr-gyjyd4-mxlx2s-fv9gcy-rwy7n6)

3. Click **Save and Continue** once you have entered your subscription IDs.

If your subscription includes SMS capabilities, an SMS gateway is automatically created based on your subscription ID.

Installing Subscription Updates

If you have entered any subscription IDs, the software checks for available software updates and new plugins that are part of your subscription. This may include components such as a license plugin, custom skin, or new software modules, as well as any available updates to the software that was on your application when it was shipped. The default selections include all new plugins and any updated plugins that are available.

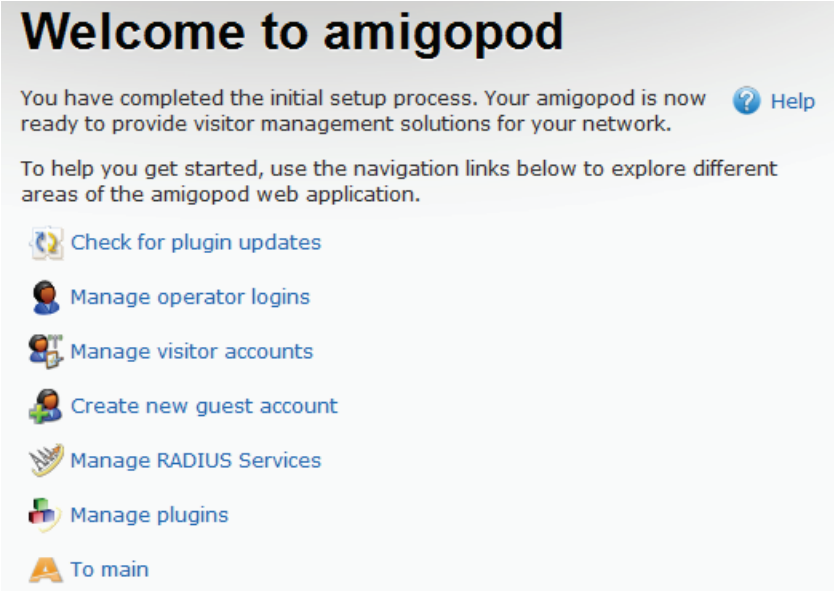


To install the default selections:

- You do not need to make any selections; the system has already determined what you need. Simply click the **Finish** button to download and install the selected plugins.

Setup Completion

After downloading and installing the available plugin updates, the setup process is complete. and the Welcome screen is displayed. You may begin using ClearPass Guest.



Context-sensitive help is available throughout the application. For more detailed information about the area of the application you are using, click the **Help** link displayed at the top right of the page. This opens a the relevant section of this deployment guide in a new browser window.

Operator logins are the login accounts used for administration and management of ClearPass Guest. The default administrative operator account is configured during the setup process. See "About Operator Logins" in the Operator Logins chapter for more details on configuring operator logins.

Visitor accounts are the user accounts for which ClearPass Guest performs authentication, authorization and accounting (AAA) functions. Visitor accounts are managed by operators using the Guest Manager component of the software. See "Guest Management" chapter for more details on setting up visitor account provisioning.

RADIUS Services is for system administrator use, and provides fine-grained control over the AAA functions of the application. See "RADIUS Services" chapter for more details on setting up the RADIUS server to perform authentication, authorization and accounting according to your network security policies.

Chapter 4

Onboard

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—Windows, Mac OS X, iOS and Android—across wired, wireless and 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.
- Leverages ClearPass profiling to identify device type, manufacturer, and model.

About ClearPass Onboard

This section provides important information about ClearPass Onboard.

Onboard Deployment Checklist

Use the following checklist to complete your Onboard deployment.

Table 10 *Onboard Deployment Checklist*

Deployment Step	Reference
Planning and Preparation	
Review the Onboard feature list to identify the major areas of interest for your deployment.	See "Onboard Feature List"
Review the list of platforms supported by Onboard, and identify the platforms of interest for your deployment.	See "Supported Platforms"
Review the Onboard public key infrastructure, and identify any certificate authorities that will be needed during the deployment.	See "Public Key Infrastructure for Onboard"
Review the network requirements and the network architecture diagrams to determine how and where to deploy the Onboard solution.	See "Network Requirements for Onboard"and "Network Architecture for Onboard"
Configuration	
Configure the hostname and networking properties of the Onboard provisioning server. • DNS is required for SSL. • Ensure that hostname resolution will work for devices being provisioned.	See "Network Setup"in the Administrator Tasks chapter

Table 10 *Onboard Deployment Checklist*

Deployment Step	Reference
Configure SSL certificate for the Onboard provisioning server. A commercial SSL certificate is required to enable secure device provisioning for iOS devices.	See "SSL Certificate"in the Administrator Tasks chapter
Configure the Onboard certificate authority. • Decide whether to use the Root CA or Intermediate CA mode of operation. Create the certificate for the certificate authority.	See "Configuring the Certificate Authority "
Configure the data retention policy for the certificate authority.	See "Configuring Data Retention Policy for Certificates"
Configure ClearPass integration. • Set Policy Manager connection and authentication details. Set Profiler options, if required.	See "Configuring ClearPass Servers for Device Provisioning"
Configure device provisioning settings. • Select certificate options for device provisioning. Select which device types should be supported.	See "Configuring Provisioning Settings"
Configure network settings for device provisioning. • Set network properties. • Upload 802.1X server certificates. Set device-specific networking settings.	See "Configuring Network Settings for Device Provisioning"
Configure networking equipment for non-provisioned devices. • Set authentication for the provisioning SSID, if required. Ensure the captive portal redirects non-provisioned devices to the device provisioning page.	See "Network Requirements for Onboard"
Configure networking equipment to authenticate provisioned devices. • 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.	See "Network Requirements for Onboard"
Configure the user interface for device provisioning. • Set display options for iOS devices. • Set user interface options for other Onboard devices. Setup the device provisioning Web login page.	See "Configuring the User Interface for Device Provisioning"
Testing and Verification	
Test device provisioning. • 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. • 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 11 *Onboard Features*

Feature	Uses
Automatic configuration of network settings for wired and wireless endpoints.	• 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.	• 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.	• 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.	• 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	• Exchange ActiveSync • Passcode policy • VPN settings

Supported Platforms

The platforms supported by ClearPass Onboard and the version requirements for each platform are summarized in Table 12.

Table 12 *Platforms Supported by ClearPass Onboard*

Platform	Example Devices	Version Required for Onboard Support	Notes
Apple iOS	iPhone iPad iPod Touch	iOS 4 iOS 5	1, 3

Table 12 *Platforms Supported by ClearPass Onboard*

Platform	Example Devices	Version Required for Onboard Support	Notes
Apple Mac OS X	MacBook Pro MacBook Air	Mac OS X 10.8 “Mountain Lion” Mac OS X 10.7 “Lion”	1
		Mac OS X 10.6 “Snow Leopard” Mac OS X 10.5 “Leopard”	2
Android	Samsung Galaxy S Samsung Galaxy Tab Motorola Droid	Android 2.2 (or higher)	2
Microsoft Windows	Laptop Netbook	Windows XP with Service Pack 2 Windows Vista with Service Pack 2 Windows 7	2

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.

Public Key Infrastructure for Onboard

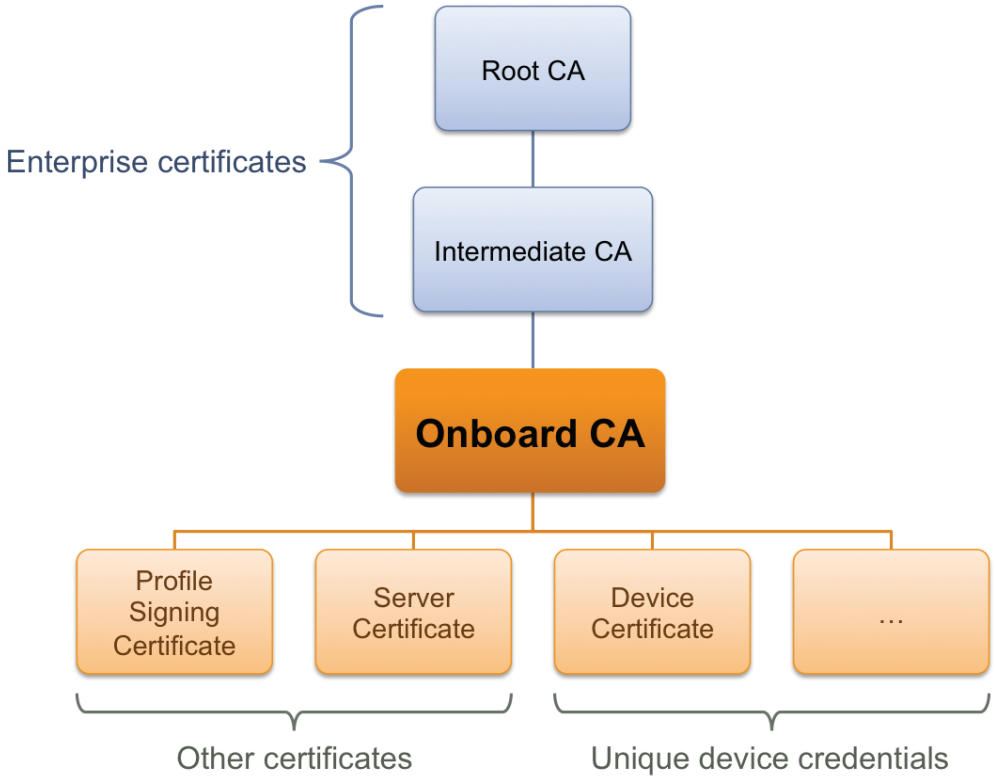
During the device provisioning process, one or more digital certificates are issued to the device. These are used as the unique credentials for a device.

To issue the certificate, ClearPass Onboard must operate as a certificate authority. 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. See Figure 6.

Figure 6 *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 "Configuring the Certificate Authority ".

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"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.

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".

Note: 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 also prevent the device from being re-provisioned.

This is necessary to prevent the user from simply re-provisioning and obtaining a new certificate. To re-provision the device, the revoked certificate must be deleted.

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.

Note: 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.

Note: OCSP and CRL are not used when using PEAP unique device credentials. The 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.

If the TLS client certificate has been revoked, then the device will not be permitted to re-provision. The revoked certificate must be deleted before the device is able to be provisioned.

Network Requirements for Onboard

For complete functionality to be achieved, 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 the Same SSID for the 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 a Different SSID for the 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 the Online Certificate Status Protocol for the Provisioned Network

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/mdps_ocsp.php/1.

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

Configuring a Certificate Revocation List (CRL) for the Provisioned Network

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.

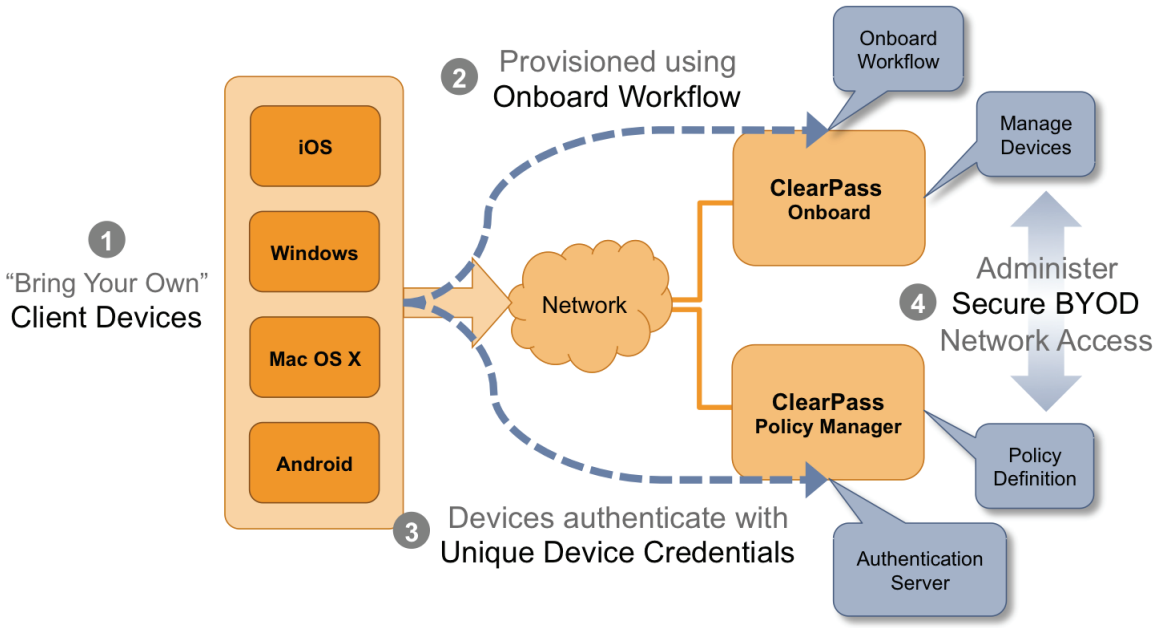
For example, if the Onboard server's hostname is onboard.example.com, the location of the CRL is: http://onboard.example.com/mdps_crl.php?id=1.

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

Network Architecture for Onboard

The high-level network architecture for the Onboard solution is shown in Figure 7.

Figure 7 *ClearPass Onboard Network Architecture*

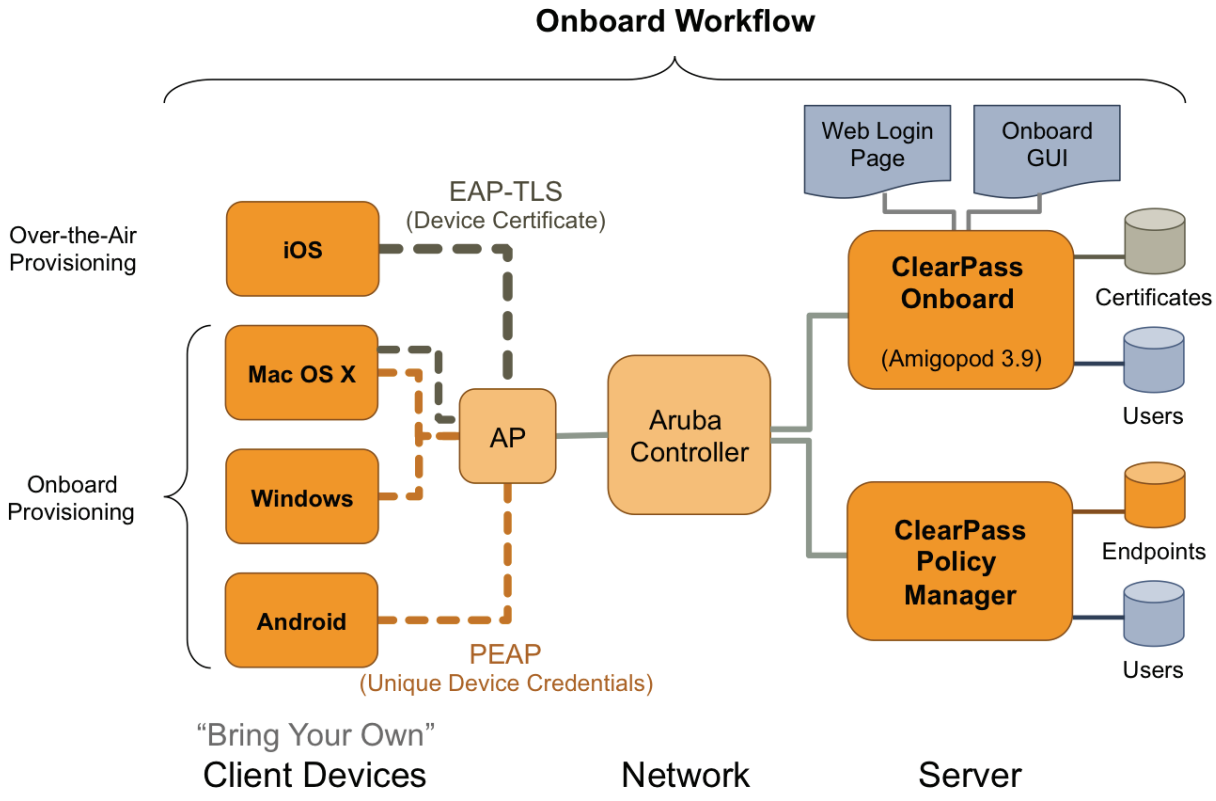


The sequence of events shown in Figure 7 is:

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. Once 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 8 on page 57 below. 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 8 *Detailed View of the ClearPass Onboard Network Architecture*



The components shown in Figure 8 are:

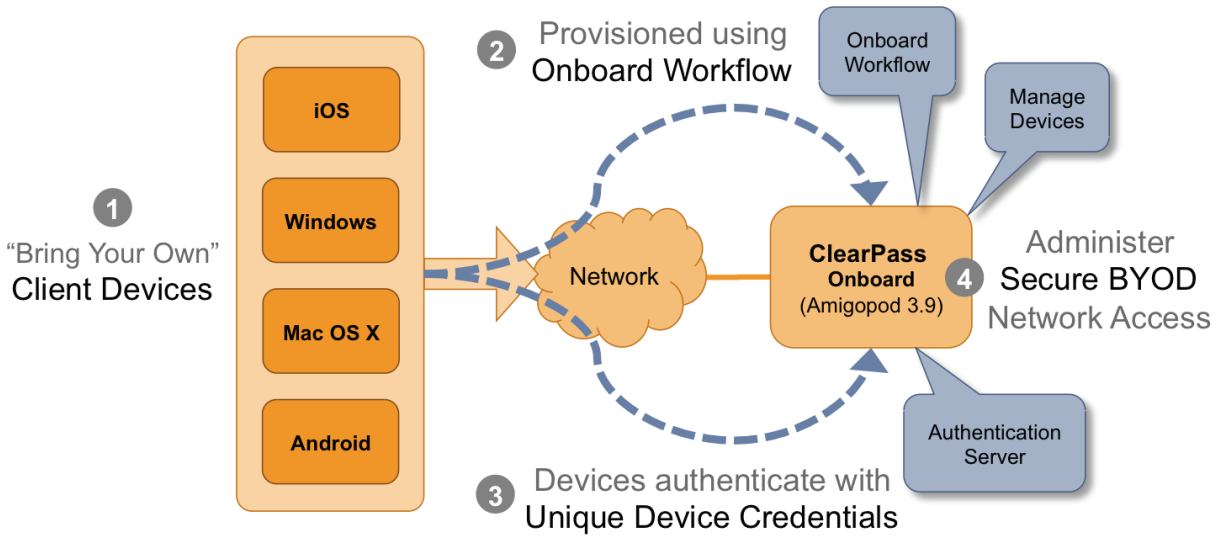
1. Users bring different kinds of client device with them. Onboard supports "smart devices" that use the iOS or Android operating systems, such as smartphones and personal tablets. Onboard also supports the most common versions of Windows and Mac OS X operating systems found on desktop computers, laptops 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. Once provisioned, client devices use 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 9 on page 58 shows the high-level network architecture for the Onboard solution when using ClearPass Guest as the provisioning and authentication server.

Figure 9 *ClearPass Onboard Network Architecture when Using ClearPass Guest*



The user experience for device provisioning is the same in Figure 9 and Figure 7 on page 56, however there are implementation differences between these approaches:

- When using the ClearPass Guest RADIUS server for provisioning and authentication, EAP-TLS and PEAP authentication must be configured.

  Navigate to **RADIUS > Authentication > EAP & 802.1X** to configure a server certificate and the appropriate EAP types for the ClearPass Guest RADIUS server.
- ClearPass Policy Manager supports a rich policy definition framework. If you have complex policies to enforce, multiple authentication or authorization sources that define user accounts, or you need features beyond those available in the ClearPass Guest RADIUS server, you should deploy Policy Manager for authentication.

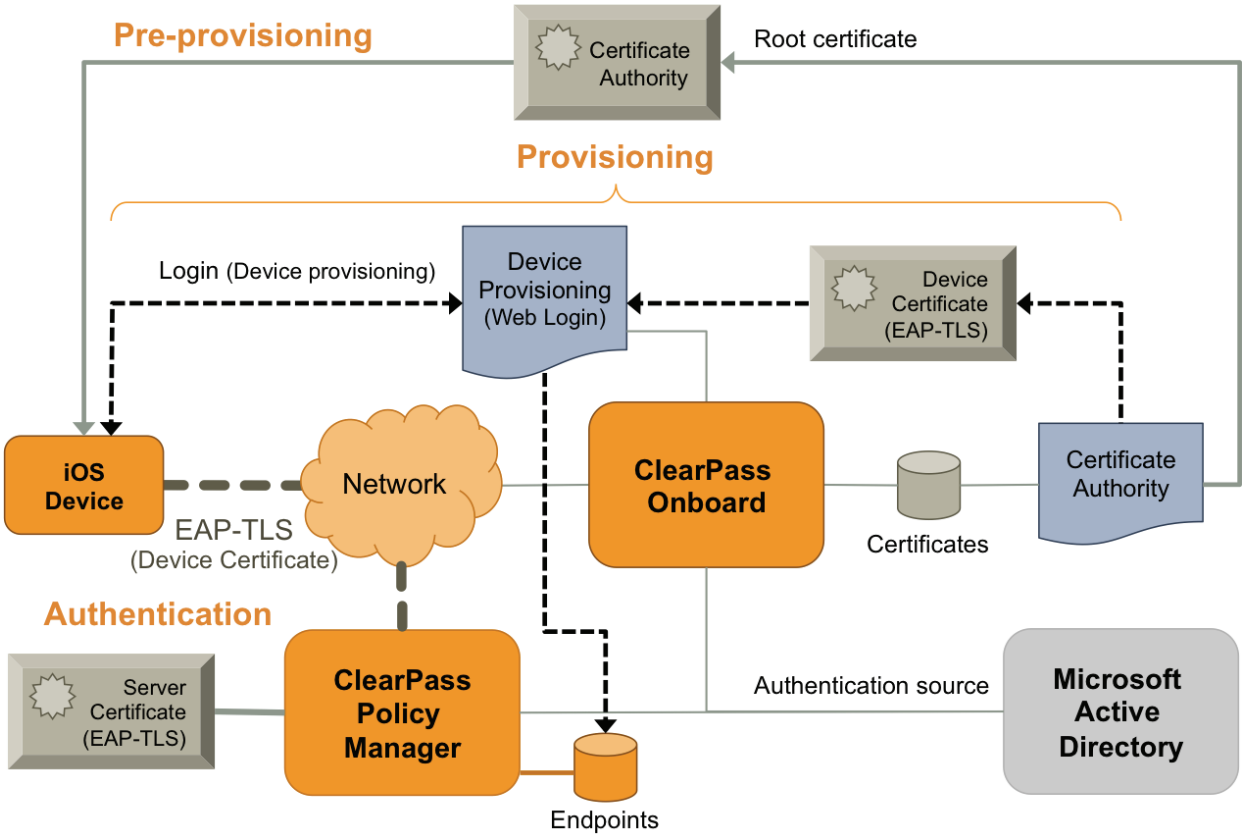
The ClearPass Onboard Process

Devices Supporting Over-the-Air Provisioning

ClearPass Onboard supports secure device provisioning for iOS 4, iOS 5, 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 10 on page 59.

Figure 10 *ClearPass Onboard Process for iOS Devices*

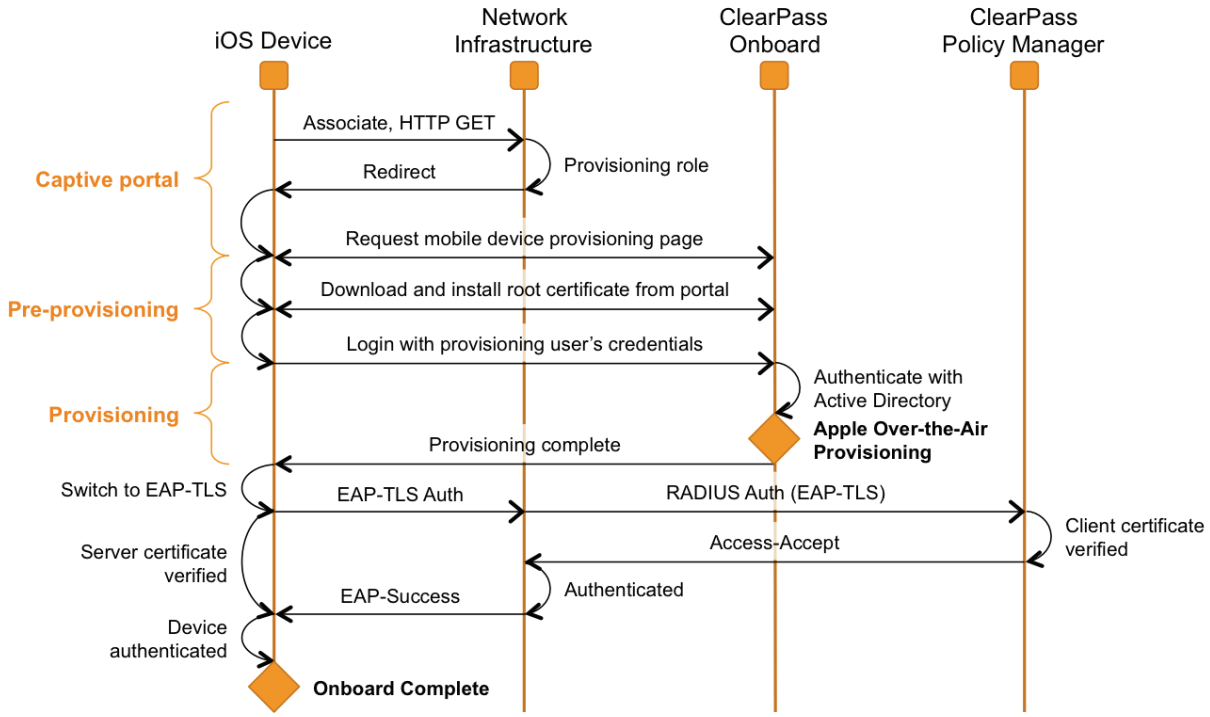


The Onboard process is divided into three stages:

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**. Once 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 11 on page 60.

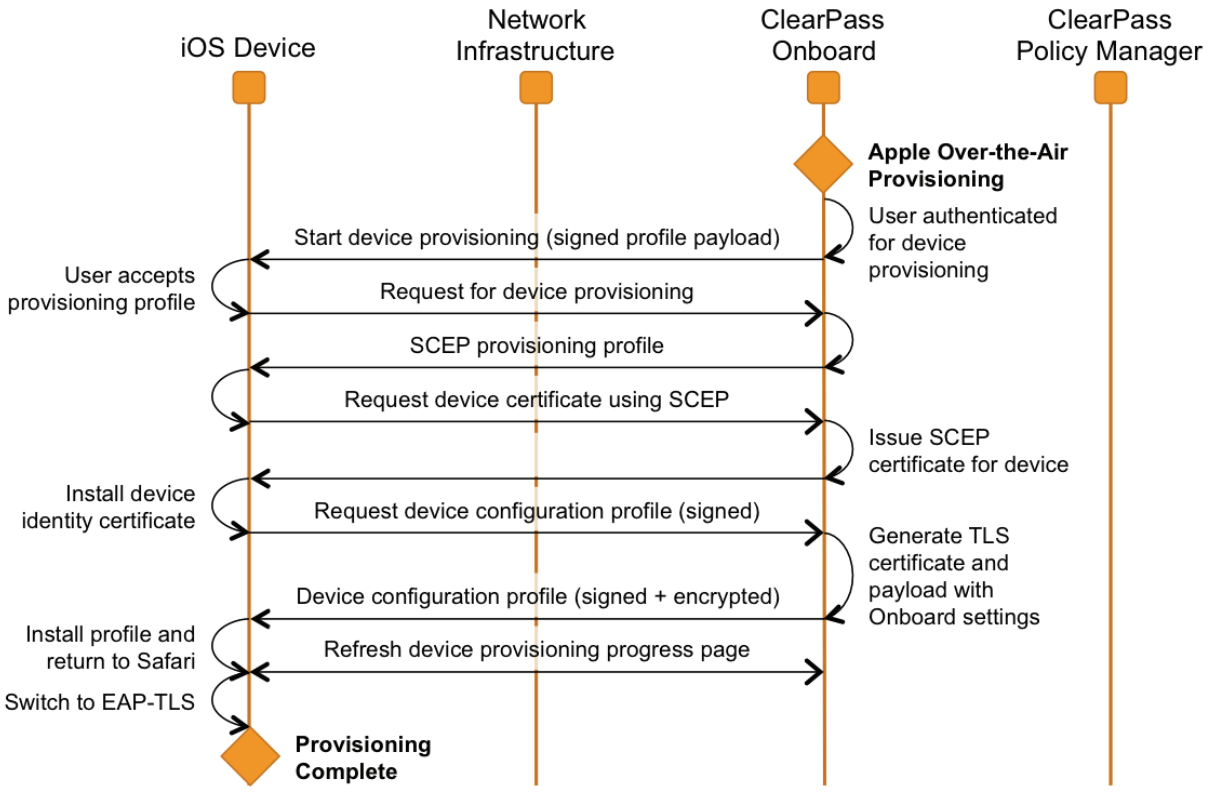
Figure 11 *Sequence Diagram for the Onboard Workflow on iOS Platform*



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 12 on page 61, 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 onboard 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 12 on page 61 shows a sequence diagram that explains the steps involved in this workflow.

Figure 12 *Over-the-Air Provisioning Workflow for iOS Platform*



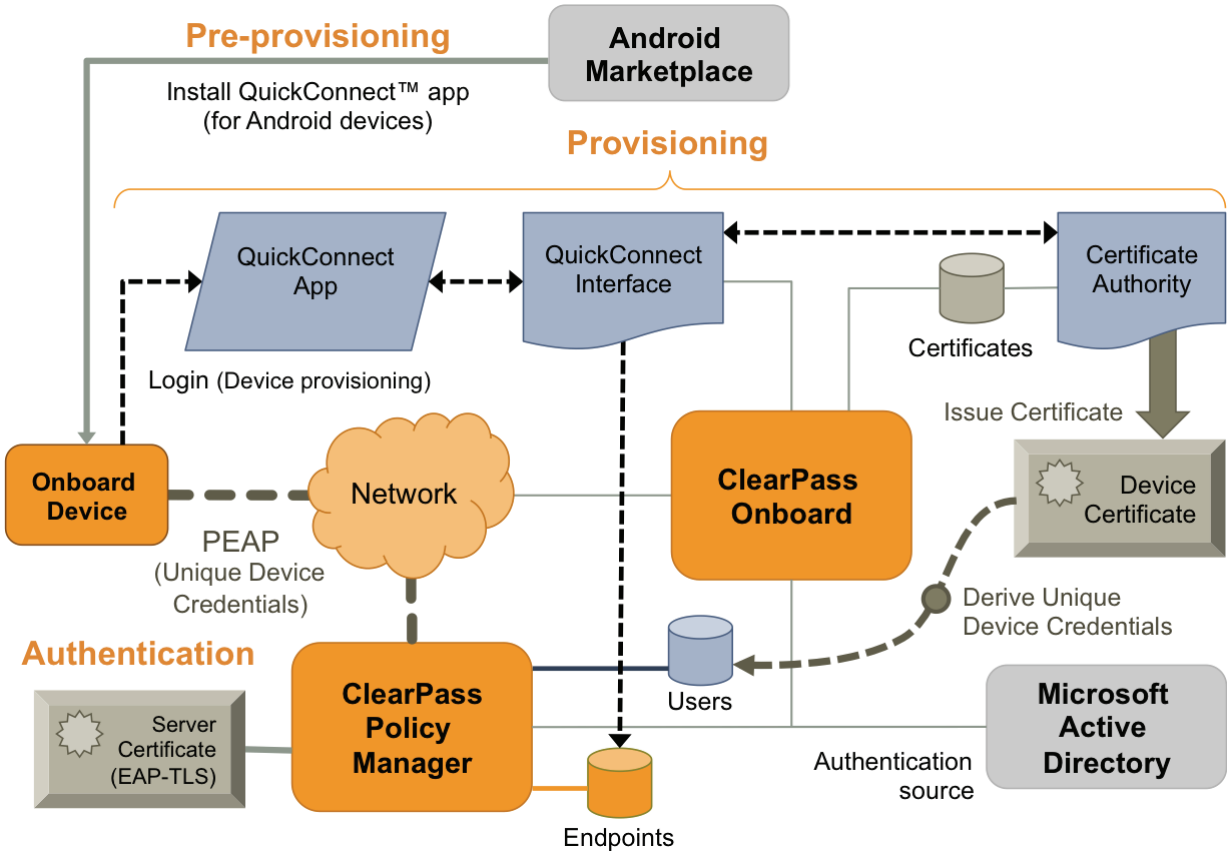
1. The only user interaction required is to accept the provisioning profile. This profile is signed by the Onboard server, so that the user can be assured of its authenticity.
2. An iOS device will have two certificates after over-the-air provisioning is complete:
   a. A Simple Certificate Enrollment 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 XP (service pack 2 and later), 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 13.

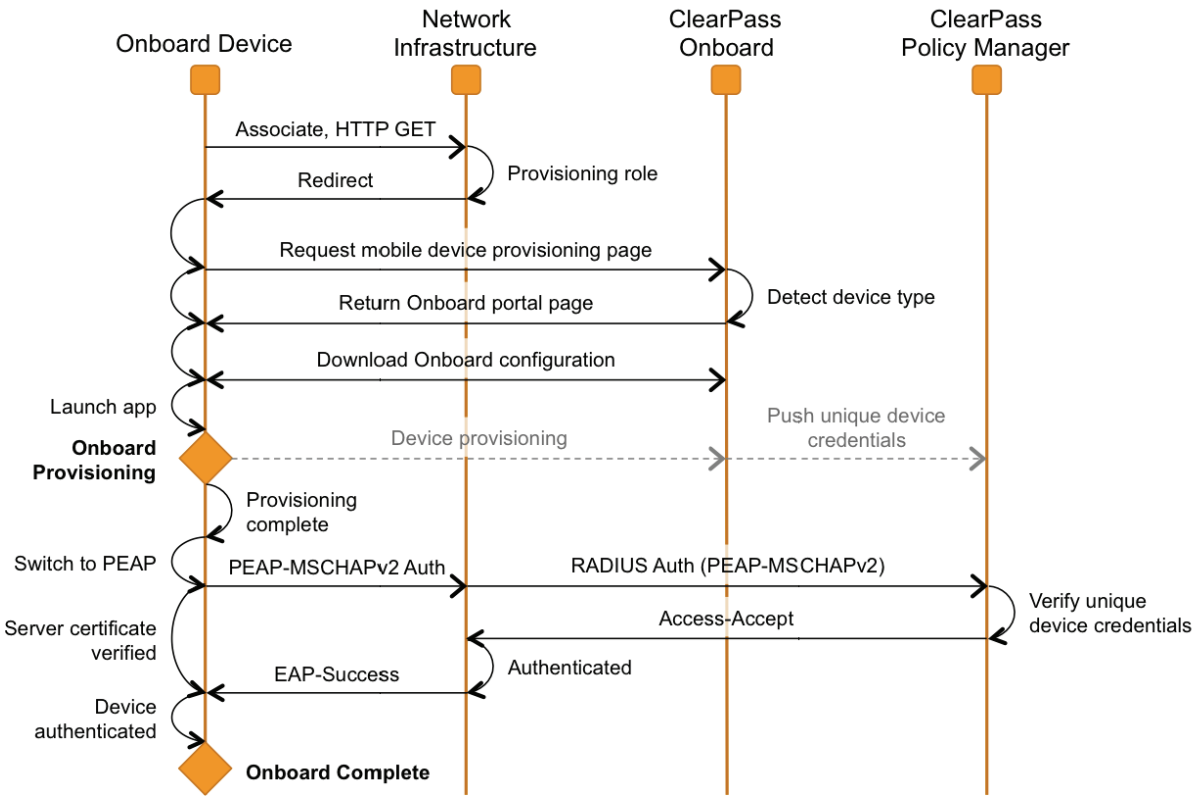
Figure 13 *ClearPass Onboard Process for Onboard-Capable Devices*



The Onboard process is divided into three stages:

1. **Pre-provisioning.** This step is only required for Android devices; the Aruba Networks 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 14 on page 63 for details.
3. **Authentication**. Once configuration is complete, the user switches to the secure network and is authenticated using PEAP-MSCHAPv2 unique device credentials.

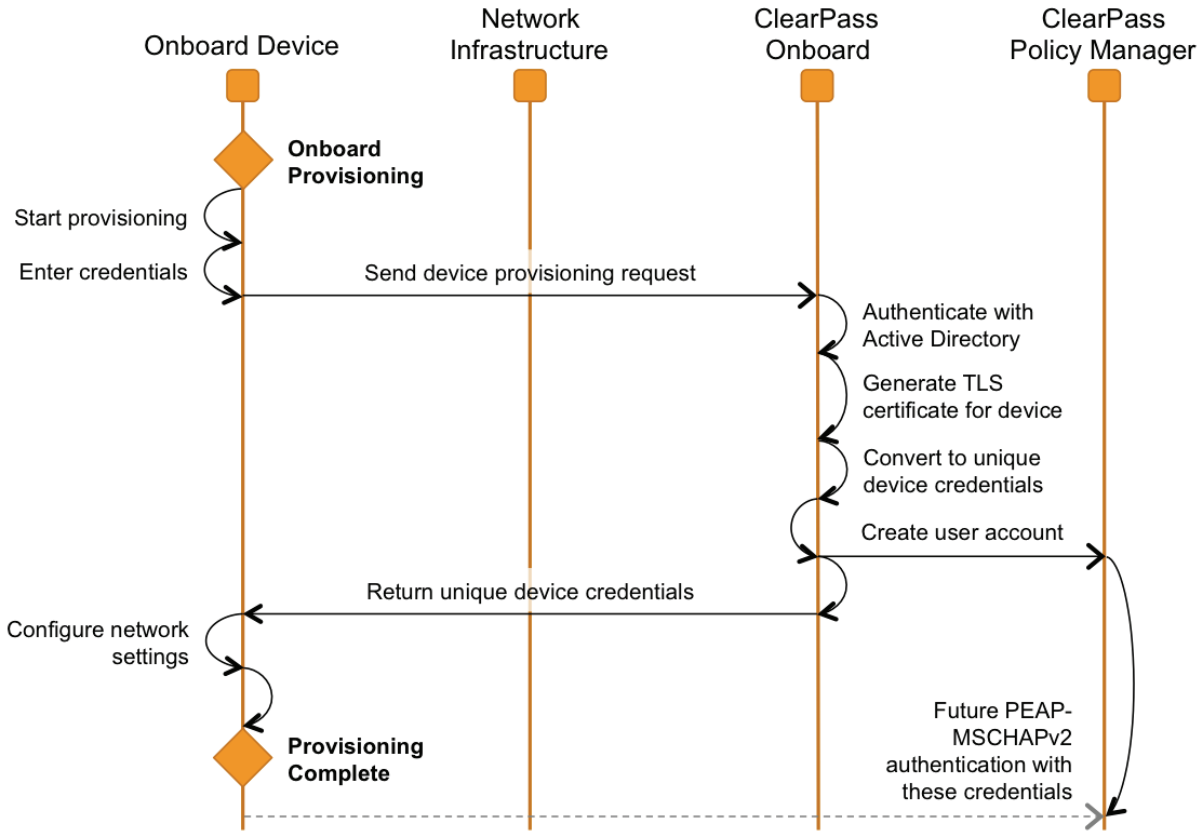
Figure 14 *Sequence Diagram for the Onboard Workflow on Android Platform*



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 onboard 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 15 on page 64 shows a sequence diagram that explains the steps involved in this workflow.

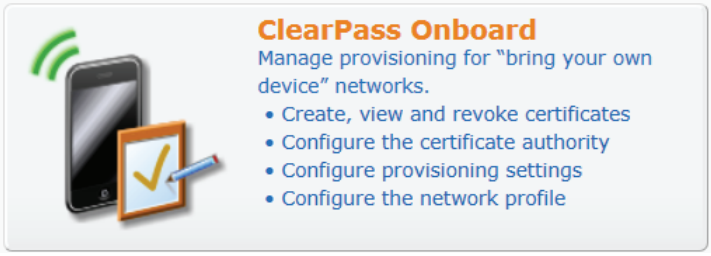
Figure 15 *Onboard Provisioning Workflow in the QuickConnect App*



Accessing Onboard

To access ClearPass Onboard:

- From the Home page, click the **ClearPass Onboard** command link. Alternatively, use the **Onboard** link at the top level of the left navigation to go directly to any of the features within Onboard.



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 "Customizing the Device Provisioning Web Login Page"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"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 Provisioning Settings for Mac OS X, Windows, and Android Devices" to make changes to the user interface.

Customizing the Device Provisioning Web Login Page

Onboard creates a default Web login page that is used to start the device provisioning process.

To edit this page, navigate to **Customization > Web Logins**, click to expand the **Onboard Provisioning** row in the list, and then click **Edit**. The RADIUS Web Logins Editor form opens. Scroll to the **Onboard Device Provisioning** rows of the form. (For details about the rest of this form, see "Creating a Web Login Page" in the RADIUS Services chapter.

The Onboard-specific settings required for a device provisioning page are described below:

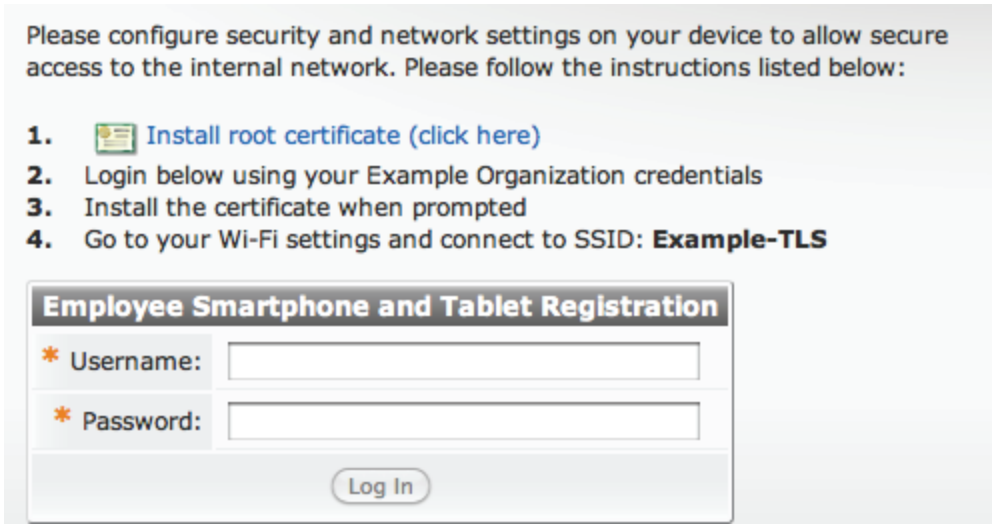
Mark the **Enable device provisioning** check box to activate the Onboard features for this Web login page.

Note: If this check box is not marked, device provisioning will be inoperative.

Select the appropriate Onboard configuration from the **Configuration** drop-down list.

To modify the instructions provided to users on the device provisioning page, edit the contents of the **Header HTML** text area.

The default instructions are displayed to the user as:



This corresponds to the following text prepopulated in the Header HTML text area:

```
<p>
Please configure security and network settings on your device to allow secure<br>
access to the internal network. Please follow the instructions listed below:<br>
```

```
<br>
<strong>1.</strong>    {nwa_iconlink icon="images/icon-
certificate22.png" text="Install root certificate (click here)"}{nwa_mdps_config
name=root_cert}{/nwa_iconlink}<br>
<strong>2.</strong>    Login below using your {nwa_mdps_config
name=organization_name} credentials<br>
<strong>3.</strong>    Install the certificate when prompted<br>
<strong>4.</strong>    Go to your Wi-Fi settings and connect to
SSID: <strong>{nwa_mdps_config name=wifi_ssid}</strong>
<br>
</p>
```

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 13 on page 66.

Table 13 *Properties Available for Use with the* `(nwa_mdps_ocnfig)` *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:
	`<a href="{nwa_mdps_config name=root_cert}">`
	`  Install Onboard root certificate`
	`</a>`

wifi_ssid	Name of the wireless network. See “Configuring Basic Network Access Settings”. Example: Connect to the network named `{nwa_mdps_config name=wifi_ssid}`

organization_name	The organization name. See “Configuring Basic Provisioning Settings”.
	Example:
	`<h2>`
	`  Welcome to {nwa_mdps_config name=organization_name}`
	`</h2>`

Configuring ClearPass Servers for Device Provisioning

To configure ClearPass servers for device provisioning, navigate to **Administrator > Network Setup > ClearPass**, or click the **ClearPass** command link. The Manage ClearPass Servers form opens.

The first part of the form is used to specify the connection details for the ClearPass Policy Manager.

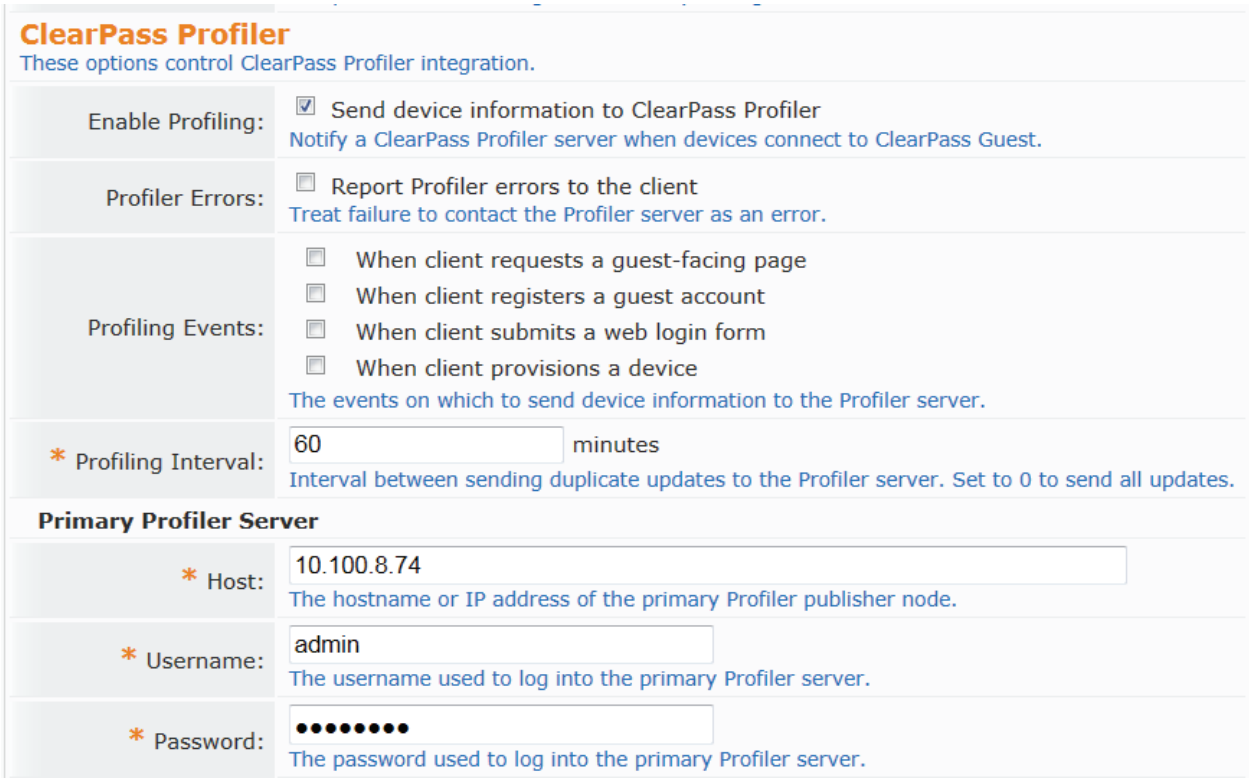
Mark the **Send device information to ClearPass Policy Manager** check box when you will use Policy Manager as the authentication server for devices provisioned with Onboard.

Specify the hostname or IP address of the Policy Manager publisher node in the **Host** text field.

You must provide a valid username and password for the Policy Manager. This account should have “Super Administrator” privileges.

Note: Onboard requires only the ability to create guest user accounts, Onboard accounts, and endpoint records. No other configuration changes are made using these credentials.

The second part of the form specifies options for ClearPass Profiler.



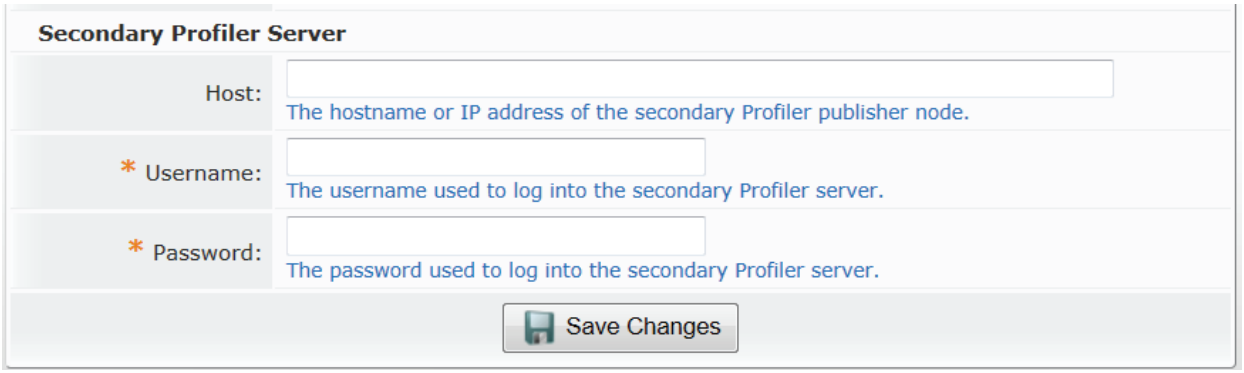
Mark the **Send device information to ClearPass Profiler** check box when you will use Profiler to collect device information.

Select the events of interest in the **Profiling Events** checklist:

- **When client requests a guest-facing page** – Device information is sent to Profiler as soon as a guest-facing page (such as a Web login page, guest self-registration page, or device provisioning captive portal page) is requested.
- Note: Selecting this option may collect information about devices that are not actively using the network, i.e. devices that are not logged in.
- **When client registers a guest account** – Device information is sent to Profiler when a guest self-registration form is completed and a guest account is created or updated.
- **When client submits a Web login form** – Device information is sent to Profiler when a Web login form is submitted, indicating a login attempt has been made.
- **When client provisions a device** – Device information is sent to Profiler when a valid device provisioning request has been received.

The **Profiling Interval** text field may be used to limit the rate of repeated updates for the same client. This option can be used to reduce the load on the Profiler server, especially if the "When client requests a guest-facing page" profiling event is enabled.

A primary Profiler server must be configured. Specify the hostname or IP address of the Profiler server in the **Host** text field. You must also provide a valid username and password for the Profiler.



A secondary Profiler server may also be configured. This server will be used if the primary Profiler server is unreachable.

Click the **Save Changes** button to apply the new configuration settings.

Configuring the Certificate Authority

To configure certificate authority settings, Navigate to **Onboard > Certificate Authority Settings**, or click the **Certificate Authority Settings** command link.

The Certificate Authority Settings form opens.

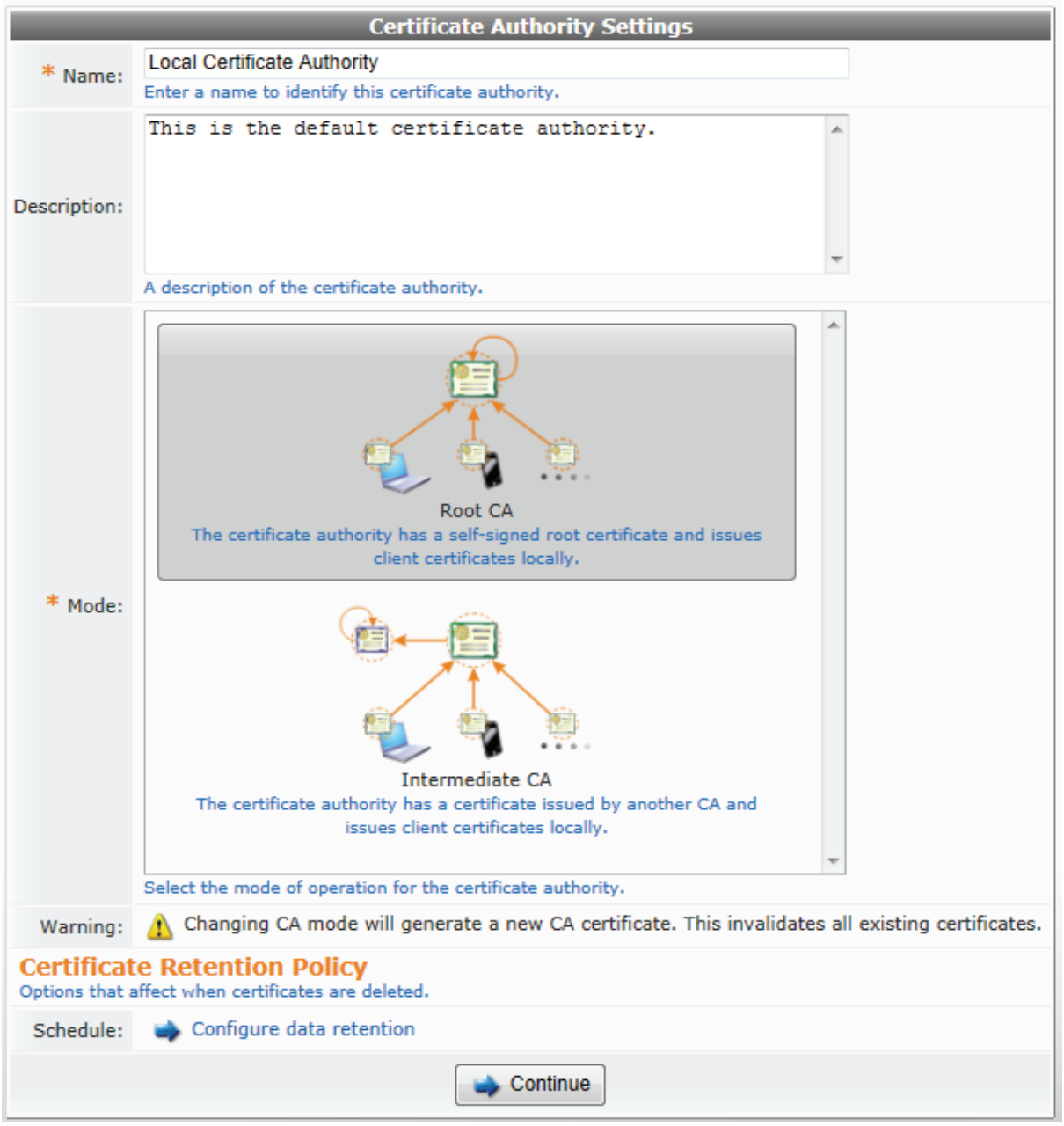
This page is used to configure the Onboard certificate authority and to perform maintenance tasks for the CA.:

- Set up a root or intermediate certificate authority (See "Setting Up the Certificate Authority")

- Determine the OCSP URL for the certificate authority
- View the trust chain for the certificate authority (See "Viewing the Certificate Authority's Trust Chain")
- Renew the certificate authority's certificate (See "Renewing the Certificate Authority's Certificate")
- Configure the data retention policy applied to certificates issued by the authority (See "Configuring Data Retention Policy for Certificates")

Setting Up the Certificate Authority

The Certificate Authority Settings form is used to set up the mode of operation for the certificate authority.



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.

Select the appropriate mode for the certificate authority:

- **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.

Click the ➡Continue button to proceed to the second step. See "Setting Up a Root Certificate Authority".

- **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.

Click the ➡Continue button to proceed to the second step. See "Setting Up an Intermediate Certificate Authority".

Setting Up a Root Certificate Authority

If you already have a certificate and private key for the certificate authority, see "Installing a Certificate Authority's Certificate".

The Root Certificate Settings form is used to configure the distinguished name and properties for the certificate authority's root (self-signed) certificate.

Note: If you intend to change any of the root certificate's distinguished name properties, and you have previously created any client or server certificates or performed device provisioning using the existing root certificate, these certificates will be invalidated and deleted as the root certificate's distinguished name has changed.

To avoid the complication of revoking and reissuing certificates, it is recommended that you configure the certificate authority before any device provisioning or other configuration is done.

In the **Identity** section of the form:

- Enter values in the **Country**, **State**, **Locality**, **Organization,** and **Organizational Unit** text fields that correspond to your organization. These values form part of the distinguished name for the root certificate.
- Enter a descriptive name for the root certificate in the **Common Name** text field. This value will be used to identify the root certificate as the issuer of other certificates, notably the signing certificate.
- Enter a descriptive name for the signing certificate in the **Signing Common Name** text field. This value will be 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.
- Enter a contact email address in the **Email Address** text field. This email address will be included in the root and signing certificates, and provides a way for users of the certificate authority to contact your organization.

In the **Private Key** section:

- Mark the **Generate a new private key** check box to create a new private key for the root certificate. This is only necessary if you are recreating the entire certificate authority from the beginning.

  Note: If you have previously created any client or server certificates or performed device provisioning using the existing root certificate, these certificates will be invalidated when changing the root certificate's private key.

- The **Key Type** drop-down list specifies the type of private key that should be created for the certificate. You can select one of these options:
  - **1024-bit RSA** – not recommended for a root certificate
  - **2048-bit RSA** – recommended for general use
  - **4096-bit RSA** – higher security

In the **Self-Signed Certificate** section:

- Use the **CA Expiration** field to specify the lifetime of the root certificate in days. The default value of 3653 days is a 10-year lifetime.
- The **Clock Skew Allowance** field adds a small amount of time to the start and end of the root 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.
- The **Digest Algorithm** drop-down list allows you to specify which hash algorithm should be used.

  Note: MD5 is not recommended for use with root certificates.

Mark the **Generate CA certificate and invalidate all other certificates** check box to confirm the changes.

Click the **Create Root Certificate** button to save the settings and generate a new root certificate.

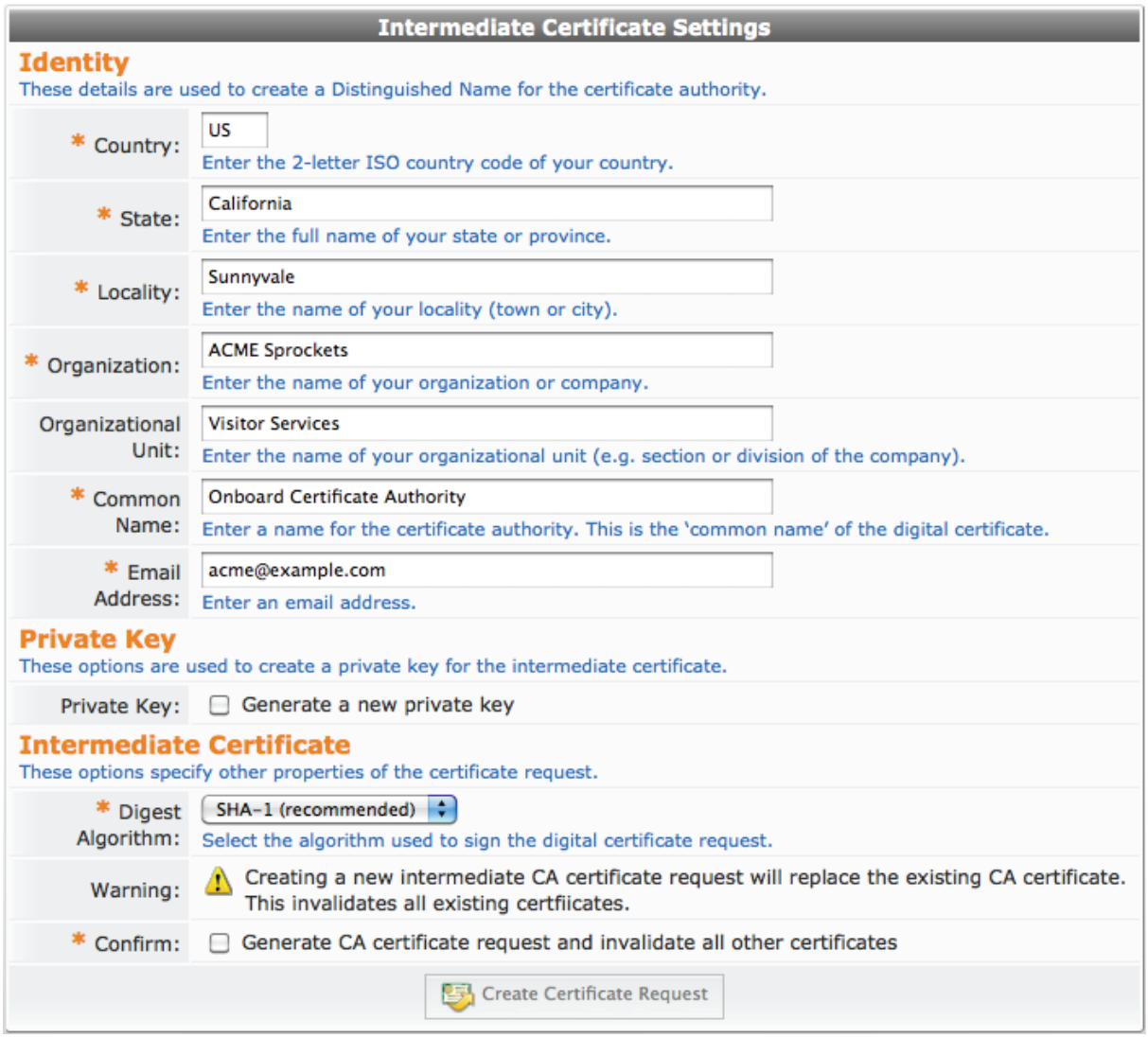
Setting Up an Intermediate Certificate Authority

The Intermediate Certificate Settings form is used to configure the distinguished name and properties for the certificate authority's certificate, which will be issued by an external certificate authority.

Note: If you intend to change any of the intermediate certificate's distinguished name properties, and you have previously created any client or server certificates or performed device provisioning using the existing intermediate certificate, these certificates will be invalidated as the intermediate certificate's distinguished name has changed.

In this case, you should use the Reset to Factory Defaults form (see "Resetting Onboard Certificates and Configuration") to delete all client certificates and re-provision all devices. You will also need to reissue any server or subordinate CA certificates.

To avoid the complication of revoking and reissuing certificates, it is recommended that you configure the certificate authority before any device provisioning or other configuration is done.



In the **Identity** section of the form:

- Enter values in the **Country**, **State**, **Locality**, **Organization,** and **Organizational Unit** text fields that correspond to your organization. These values form part of the distinguished name for the certificate authority.
- Enter a descriptive name for the certificate authority in the **Common Name** text field. This value will be used to identify the intermediate certificate as the issuer of client and server certificates from this certificate authority.
- Enter a contact email address in the **Email Address** text field. This email address will be included in the certificate authority's certificate, and provides a way for users of the certificate authority to contact your organization.

In the **Private Key** section:

- Mark the **Generate a new private key** check box to create a new private key for the intermediate certificate. This is only necessary if you are recreating the entire certificate authority from the beginning.

  Note: If you have previously created any client or server certificates or performed device provisioning using the existing intermediate CA certificate, these certificates will be invalidated when changing the intermediate CA's private key.

- The **Key Type** drop-down list specifies the type of private key that should be created for the certificate. You can select one of these options:
  - **1024-bit RSA** – not recommended for a certificate authority
  - **2048-bit RSA** – recommended for general use
  - **4096-bit RSA** – higher security

In the **Intermediate Certificate** section:

- The **Digest Algorithm** drop-down list allows you to specify which hash algorithm should be used.

  Note: MD5 is not recommended for use with certificate authority certificates.

Mark the **Generate CA certificate request and invalidate all other certificates** check box to confirm the changes.

Click the **Create Certificate Request** button to save the settings and generate a new certificate signing request.

Obtaining a Certificate for the Certificate Authority

The Intermediate Certificate Request page displays the certificate signing request for the certificate authority's intermediate certificate. This page is also used to renew the certificate authority's intermediate certificate when it is close to expiring.

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.

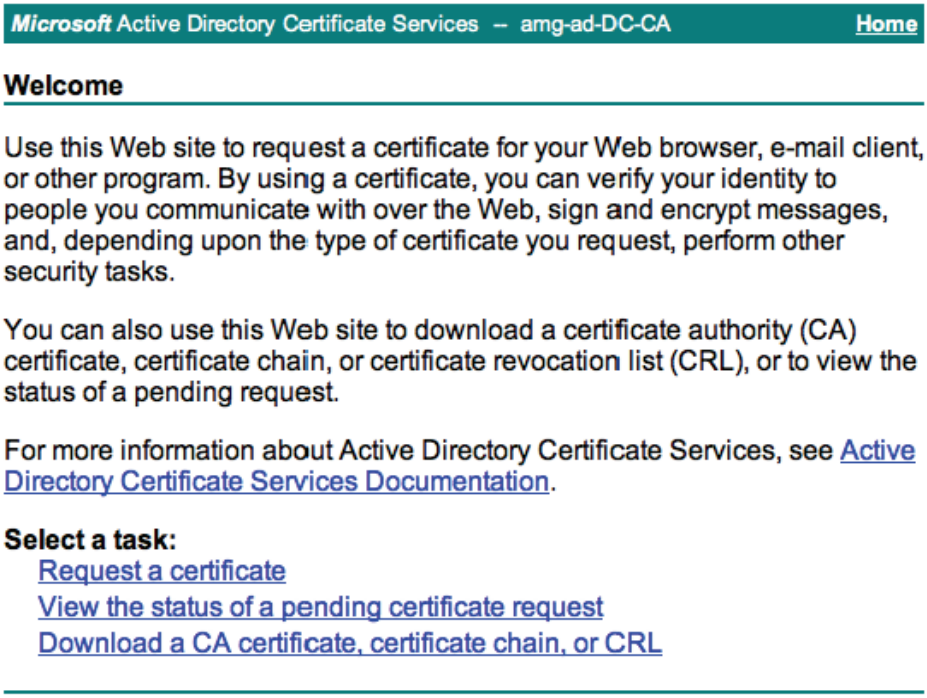
Once you have obtained the certificate, click the Install a signed certificate link to continue configuring the intermediate certificate authority. See "Installing a Certificate Authority's Certificate".

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.

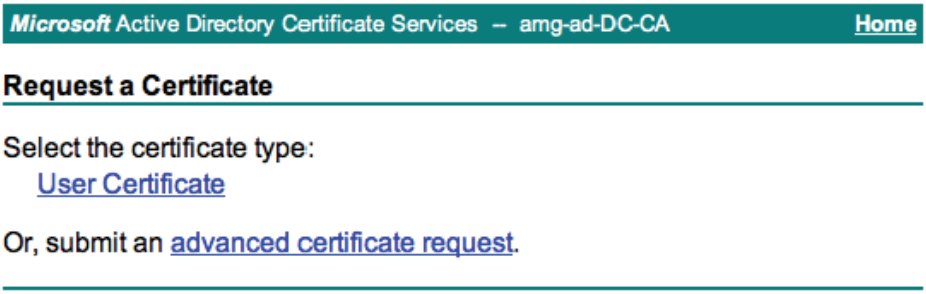
Using Microsoft Active Directory Certificate Services

Navigate to the Microsoft Active Directory Certificate Services Web page. This page is typically found at https://yourdomain/certsrv/.

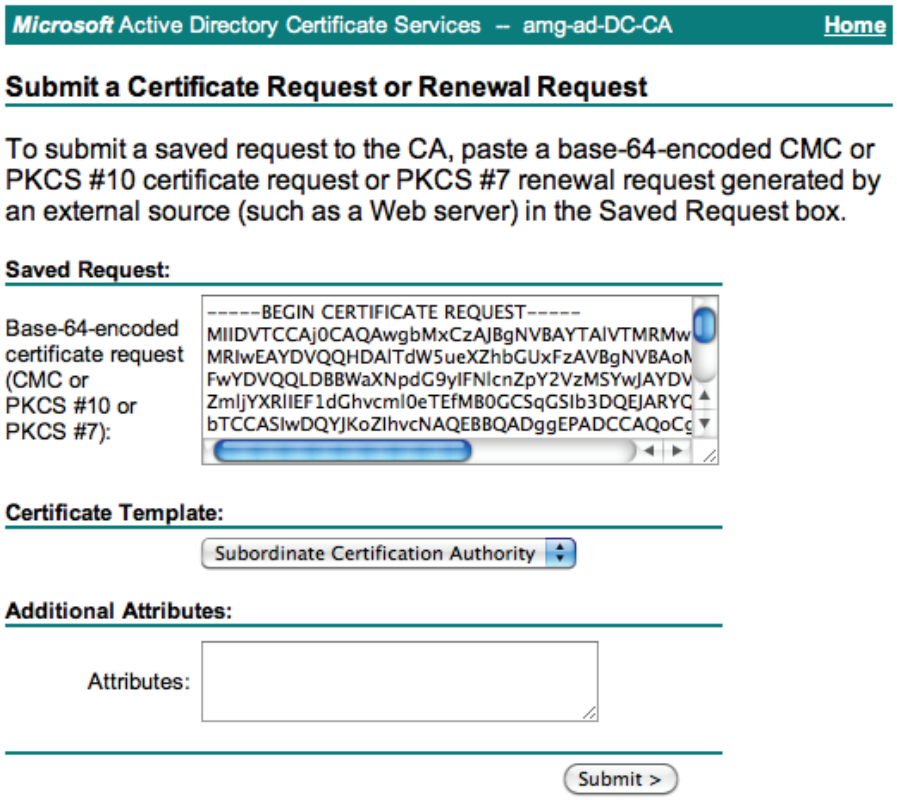
The Welcome page is displayed.



Click the **Request a Certificate** link on this page. The Request a Certificate page is displayed.



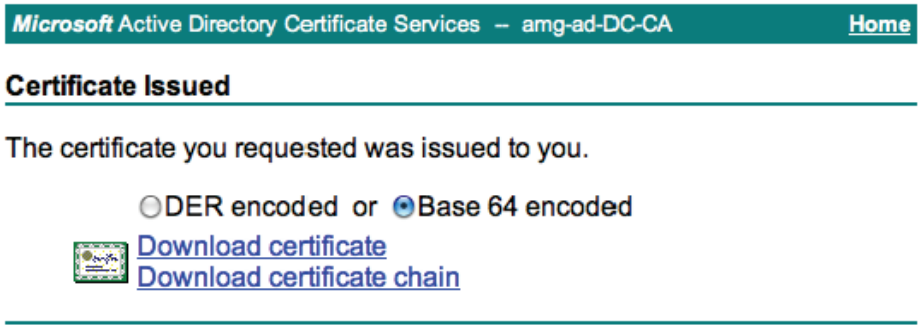
Click the link to submit an advanced certificate request. The Submit a Certificate Request or Renewal Request page is displayed.



Copy and paste the certificate signing request text into the **Saved Request** text field.

Because this certificate is for a certificate authority, select the "Subordinate Certificate Authority" in the **Certificate Template** drop-down list.

Click the **Submit** button to issue the certificate. 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.

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

Installing a Certificate Authority's Certificate

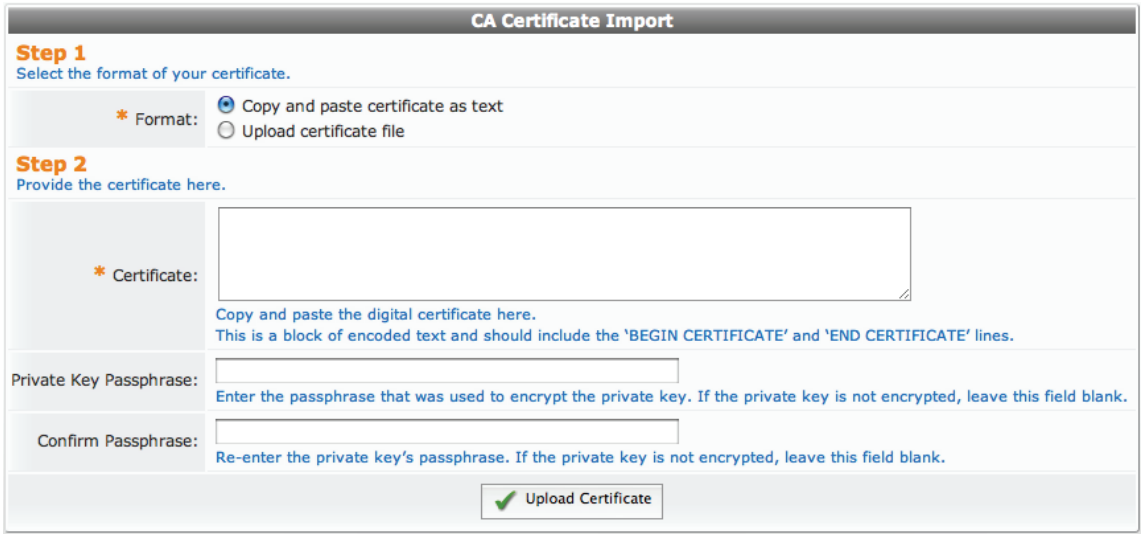
The CA Certificate Import page may be used to:

- 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.

Note: This form may be used multiple times, 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.

In the **Step 1** section of the form, select one of the following options in the **Format** radio buttons:

- **Copy and paste certificate as text**. The form expands to include the Step 2 fields.



  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.

- **Upload certificate file** – Step 2 and Step 3 are displayed on the CA Certificate Import form.

Choose the file to upload in the **Certificate** field.

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.

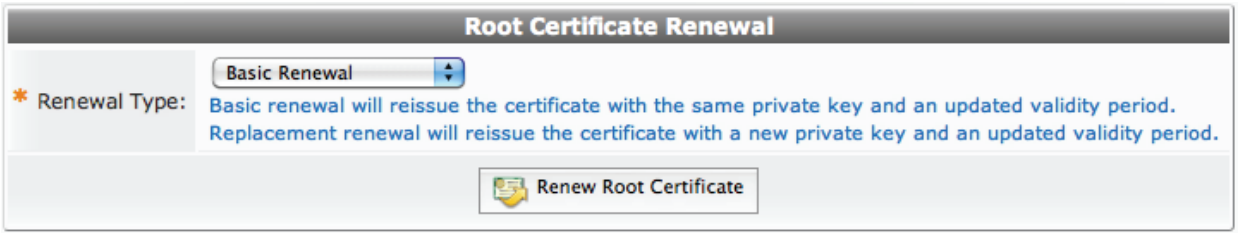
Click the ✔**Upload Certificate** button to save your changes.

- 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.

Renewing the Certificate Authority's Certificate

When a root certificate is close to expiration, it must be renewed.

Navigate to **Onboard** > **Certificate Authority Settings** and click the **Renew Root Certificate** link. The Root Certificate Renewal form is displayed.



Select an option in the **Renewal Type** drop-down list:

- **Basic Renewal** – Uses the same private key for the root certificate, but reissues the root CA certificate with an updated validity period. Use this option to maintain the validity of all certificates issued by the CA.

- **Replacement Renewal** – Generates a new private key for the root certificate, and reissues the root CA certificate with an updated validity period. Use this option if the root certificate has been compromised, or if you want to invalidate all certificate that were previously issued by the CA.

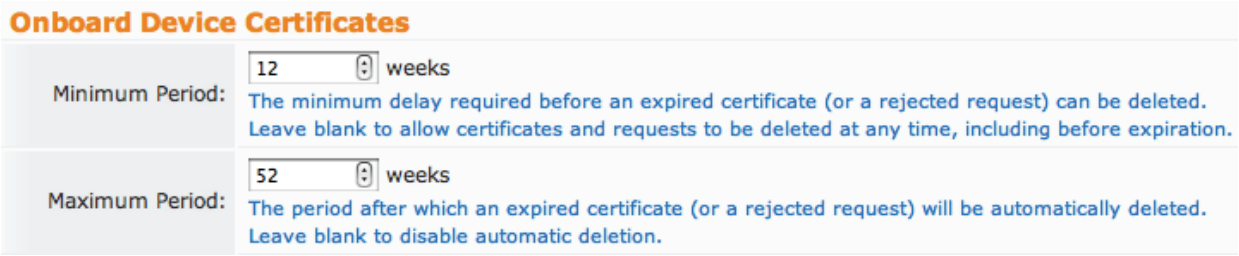
Whether you renew or replace the root certificate, you should distribute a new copy of the root certificate to all users of that certificate.

Click the **Renew Root Certificate** button to perform the renewal action.

Configuring Data Retention Policy for Certificates

The data retention policy for certificates and certificate requests can be configured by navigating to **Onboard > Certificate Authority Settings** and clicking the **Configure data retention** link.

The Manage Data Retention form is displayed.



In the Onboard Device Certificates section of the form, specify a value in the **Minimum Period** and **Maximum Period** fields that is appropriate for your organization's retention policy.

Note: Use a blank value for Minimum Period to enable the **Delete Certificate** and **Delete Request** actions in the Certificate Management list view. This is useful for testing and initial deployment.

The default data retention policy specifies the values:

- Minimum Period of 12 weeks
- Maximum Period of 52 weeks

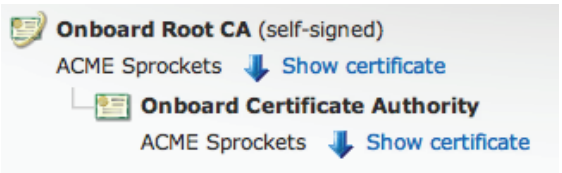
Uploading Certificates for the Certificate Authority

This 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 Certificate Authority's Trust Chain

Navigate to **Onboard** > **Certificate Authority Settings** and click the **View CA Certificate** link.

The Certificate Authority Trust Chain page is displayed. This page shows a graphical representation of the certificates that make up the trust chain.



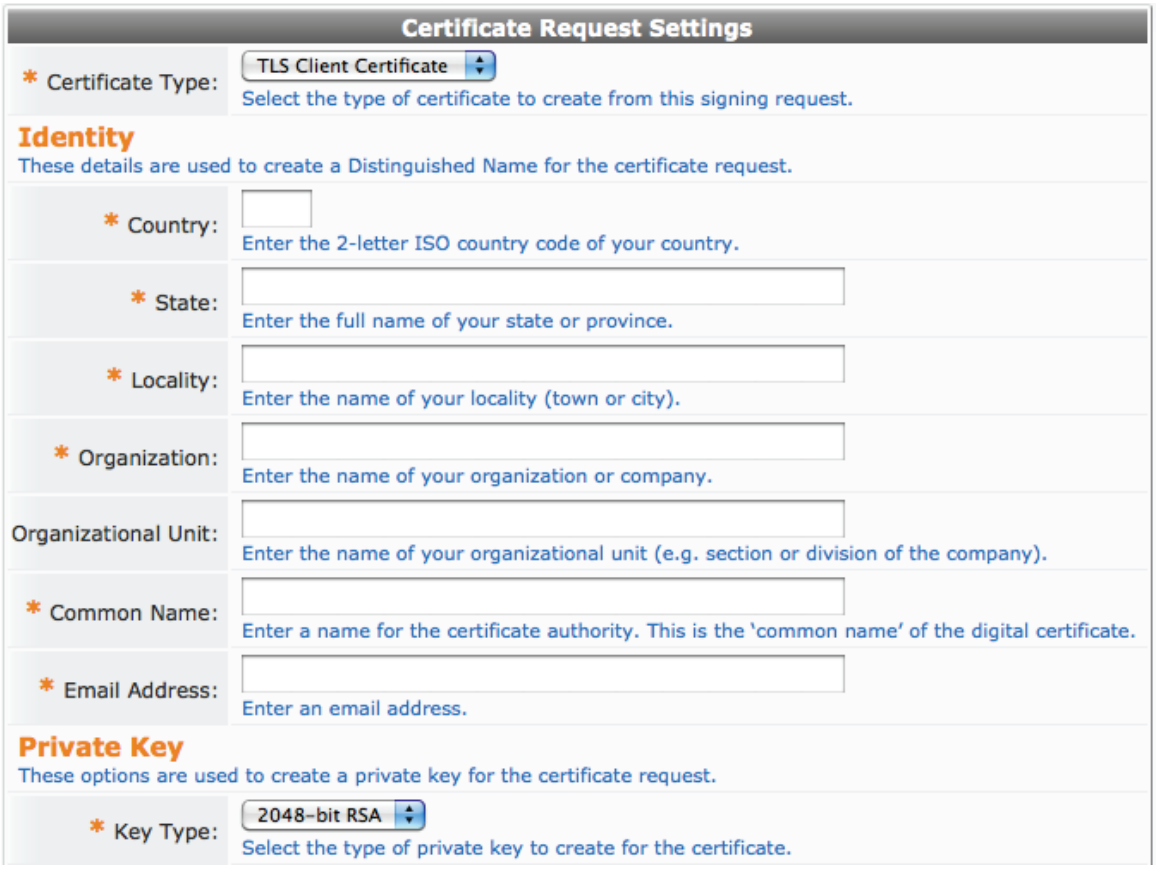
The first certificate listed is the root certificate. Root certificates are always self-signed and are explicitly trusted by clients.

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.

Click the **Show certificate** link to view the properties of a certificate in the trust chain.

Creating a Certificate

From the Certificate Management page, click the **Generate a new certificate signing request** link to access the Certificate Request form.



To create a new certificate or certificate signing request, first select the type of certificate you want to create from the **Certificate Type** drop-down list:

- **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.
- **TLS Server 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.
- **Certificate Authority** – Use this option when the certificate is for an 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".

Specifying the Identity of the Certificate Subject

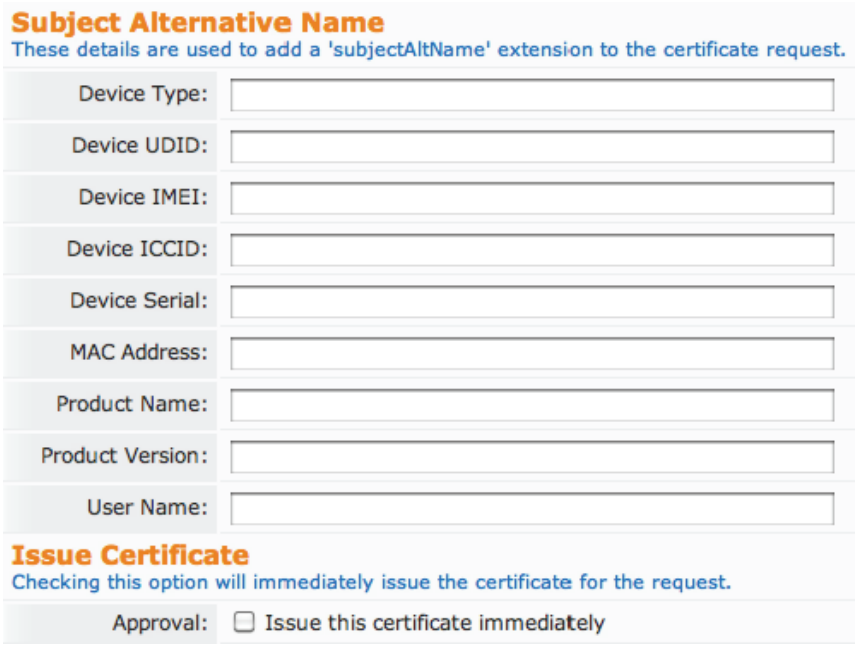
In the first part of the form, provide the identity of the person or device for which the certificate is to be issued (the “subject” of the certificate). Together, these fields are collectively known as a distinguished name, or “DN”.

- Country
- State
- Locality
- Organization
- Organizational Unit
- Common Name – this is the primary name used to identify the certificate
- Email Address

The **Key Type** drop-down list specifies the type of private key that should be created for the certificate. You can select one of these options:

- **1024-bit RSA** – lower security
- **2048-bit RSA** – recommended for general use
- **4096-bit RSA** – higher security

Note: 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.



If you have selected **TLS Client** as the certificate type, the Subject Alternative Name section is also shown. 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 subjectAltName extension with the specified values.

Table 14 on page 82 explains the fields that may be included as part of the subject alternative name.

Table 14 *Subject Alternative Name Fields Supported When Creating a TLS Client Certificate Signing Request*

Name	Desctiption
Device Type	Type of device, such as “iOS”, “Android”, etc.
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.

Issuing the Certificate Request

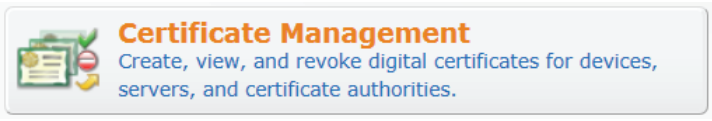
Mark the **Issue this certificate immediately** check box to automatically create the certificate.

Click the **Create Certificate Request** button 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.

Managing Certificates

To view the list of certificates and work with them, go to **Onboard > Certificate Management**, or click the **Certificate Management** command link.



This list view displays all of the certificates and certificate requests in the Onboard system. Table 15 on page 83 lists the types of certificate that are displayed in this list.

Table 15 *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
	Profile signing certificate	profile-signing	Issued by the certificate authority
	Certificate signing request	tls-client or tls-server	The type shown depends on the kind of certificate requested
	Rejected certificate signing request	tls-client or tls-server	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 user's device
	Server certificate	tls-server	Identity certificate issued to a server
	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

Searching for Certificates

The **Filter** field can be used to quickly search for a matching certificate. Type a username into this field to locate all certificates matching that username quickly.

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.

Note: 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

Click on a certificate to select it. You can then select from one of these actions:

- **View certificate** – Displays the properties of the certificate. Click the **Cancel** button to close the certificate properties.
- **Export certificate** – Displays 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:

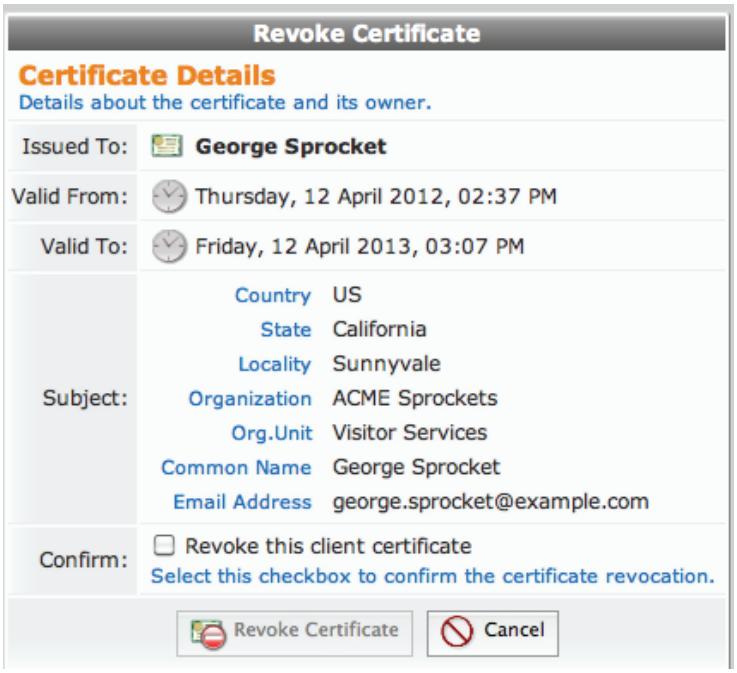
- **PKCS#7 Certificates (.p7b)** – Exports the certificate, and optionally the other certificates forming the trust chain for the certificate, as a PKCS#7 container.
- **Base-64 Encoded (.pem)** – Exports the certificate as a base-64 encoded text file. This is also known as "PEM format".
- **Binary Certificate (.crt)** – Exports the certificate as a binary file. This is also known as "DER format".
- **PKCS#12 Certificate & Key (.p12)** – Exports the certificate and its associated private key, and optionally any other certificates required to establish the trust chain for the certificate, as a PKCS#12 container. This option is only available if the private key for the certificate is available to the server.

If you selected the PKCS#12 format, you must enter a passphrase to protect the private key stored in the file.

Note: 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 the **Export Certificate** button to download the certificate file in the selected format.

- **Revoke certificate** – Displays the Revoke Certificate form.



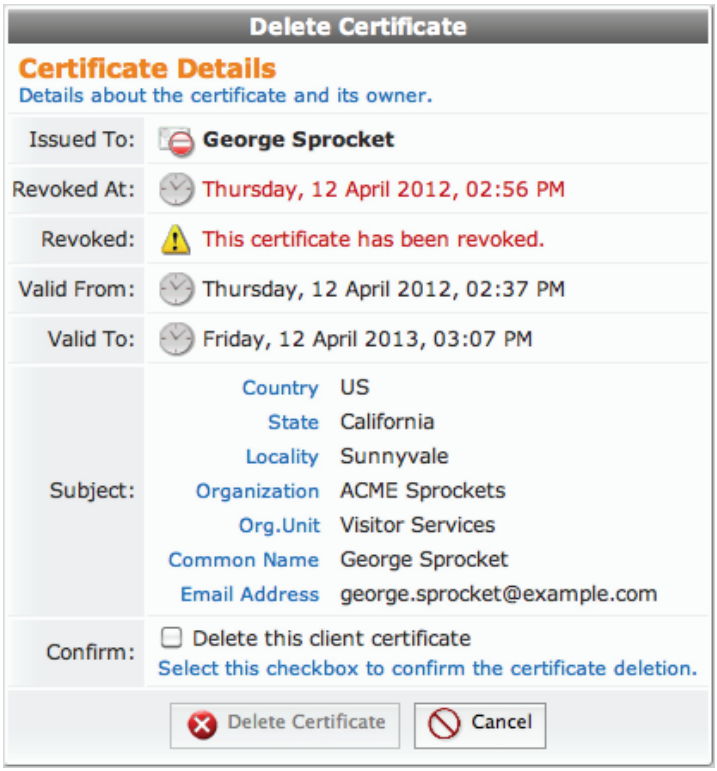
Mark the **Revoke this client certificate** check box to confirm that the certificate should be revoked, and then click the **Revoke Certificate** button.

Once 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.

Note: 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.

Note: Revoking a device's certificate will also prevent the device from being re-provisioned. This is necessary to prevent the user from simply re-provisioning and obtaining a new certificate. To re-provision the device, the revoked certificate must be deleted.

- **Delete certificate** – Removes the certificate from the list. This option is only available if the data retention policy is configured to permit the certificate's deletion. See "Configuring Data Retention Policy for Certificates".



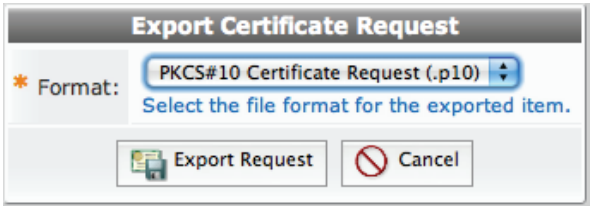
The Delete Certificate form is displayed. Mark the **Delete this client certificate** check box to confirm the certificate's deletion, and then click the **Delete Certificate** button.

Working with Certificate Signing Requests

Certificate signing requests can be managed through the Certificate Management list view. This allows for server certificates, subordinate certificate authorities, and other client certificates not associated with a device to be issued by the Onboard certificate authority.

Click on a certificate request to select it. You can then select from one of these actions:

- **View request** – Displays the properties of the certificate request. Click the **Cancel** button to close the certificate request properties.
- **Export request** – Displays the Export Certificate Request form.



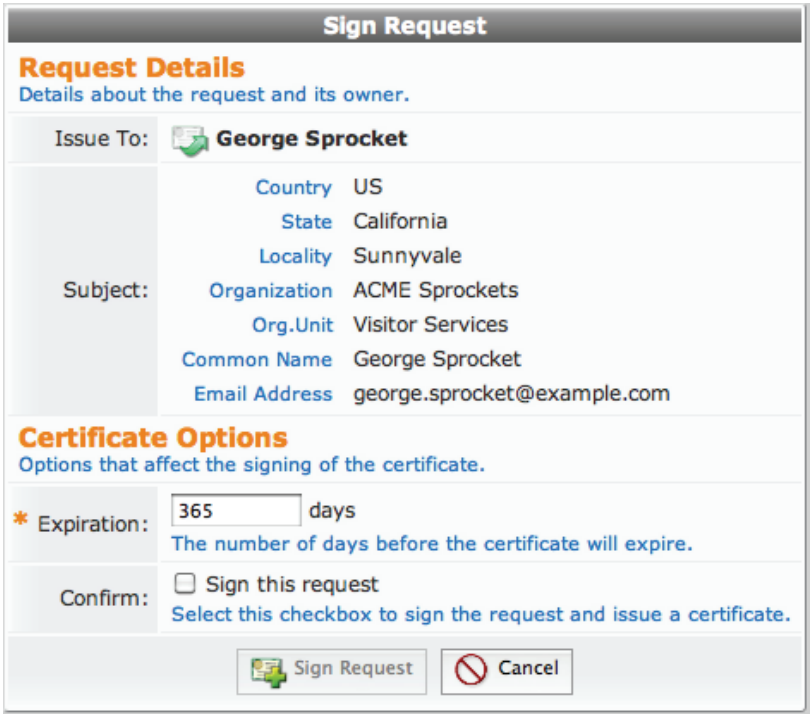
Use the **Format** drop-down list to select the format in which the certificate signing request should be exported. The following formats are supported:

- **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 the **Export Certificate** button.

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

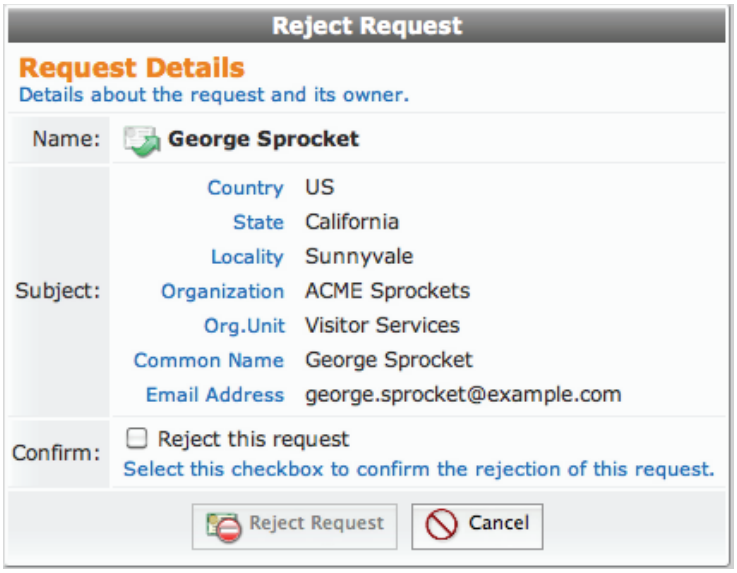
- **Sign request** – Displays the Sign Request form. Use this action to approve the request for a certificate and issue the certificate.



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 the **Sign Request** button. The certificate will be issued and will then replace the certificate signing request in the list view.

- **Reject request** – Displays 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.



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** – Removes the certificate signing request from the list. This option is only available if the data retention policy is configured to permit the certificate signing requests's deletion. See "Configuring Data Retention Policy for Certificates".

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

Requesting a Certificate

From the Certificate Management page, click the **Upload a certificate signing request** link to access the Certificate Signing Request form.

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.

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-----
MIIB7DCCAVUCAQAwgasxCzAJBgNVBAYTAlVTMRMwEQYDVQQIEwpDYWxpZm9ybmlh
MRIwEAYDVQQHEwlTdW5ueXZhbGUxFzAVBgNVBAoTDkFDTUUgU3Byb2NrZXRzMRkw
FwYDVQQLExBWaXNpdG9yIFNlcnZpY2VzMR4wHAYDVQQDExVBdXRoZW50aWNhdGlv
biBTZXJ2ZXIxHzAdBgkqhkiG9w0BCQEWEGluZm9AZXhhbXBsZS5jb20wgZ8wDQYJ
KoZIhvcNAQEBBQADgY0AMIGJAoGBALR4wRSH26wlcf3OEPEIh34iXRQIUrnYnDfo
+ZezeB/i4NZUhRvLMvhPW7DcLpiZJ17ILj3aPPUXWDBYYiiuOkmuFX3dG7eKCLMH
Z4E9z1ozK5Znm8cWIj56kg69le7QrAZBYrd5QaBTMxEe0F9CGFsYbFx1viMUMxN6
EJILaCTBAgMBAAGgADANBgkqhkiG9w0BAQUFAAOBgQB8/So9KU5BS3oxjyxftIwF
dWvNP2CNruKyQaba5RQ1ixdHAsPE+3uYIHNvlqqIpSzBlfYkr21S4DdR3SSC3bXy
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.

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

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

Specifying Certificate Properties

Select the type of certificate from the **Certificate Type** drop-down list. Choose from one of the following options:

- **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.
- **TLS Server 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.
- **Certificate Authority** – Use this option when the certificate is for an 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".

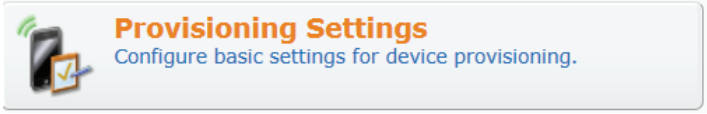
Mark the **Issue this certificate immediately** check box to automatically issue the certificate.

Click the **Submit Certificate Signing Request** button 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.

Configuring Provisioning Settings

To configure basic device provisioning settings, go to **Onboard > Provisioning Settings**, or click the **Provisioning Settings** command link. The Device Provisioning Settings page opens.

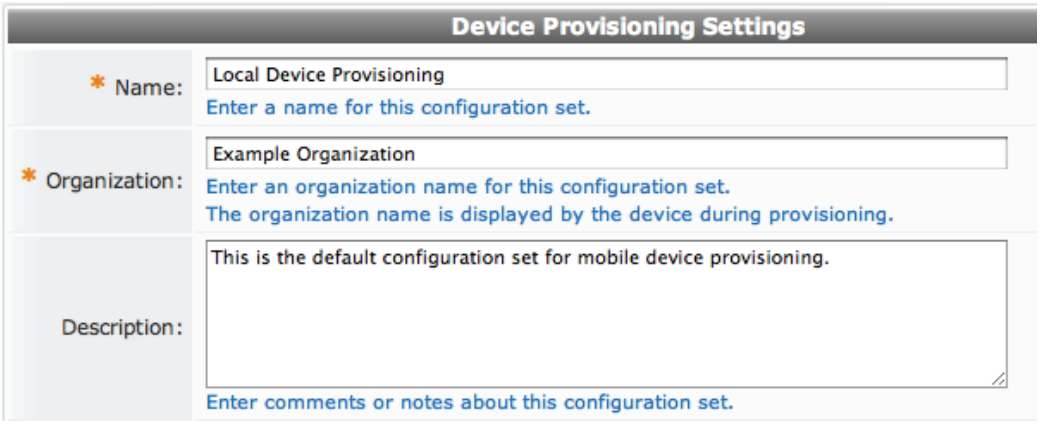


This page is used to configure the settings for ClearPass Onboard device provisioning, including:

- The organization name displayed during device provisioning
- Properties for the certificates issued to devices when they are provisioned
- Which operating systems should be supported
- Authorization properties – the number of devices that a user may provision

Configuring Basic Provisioning Settings

The first part of the Device Provisioning Settings form is used to specify basic information about the Onboard provisioning.

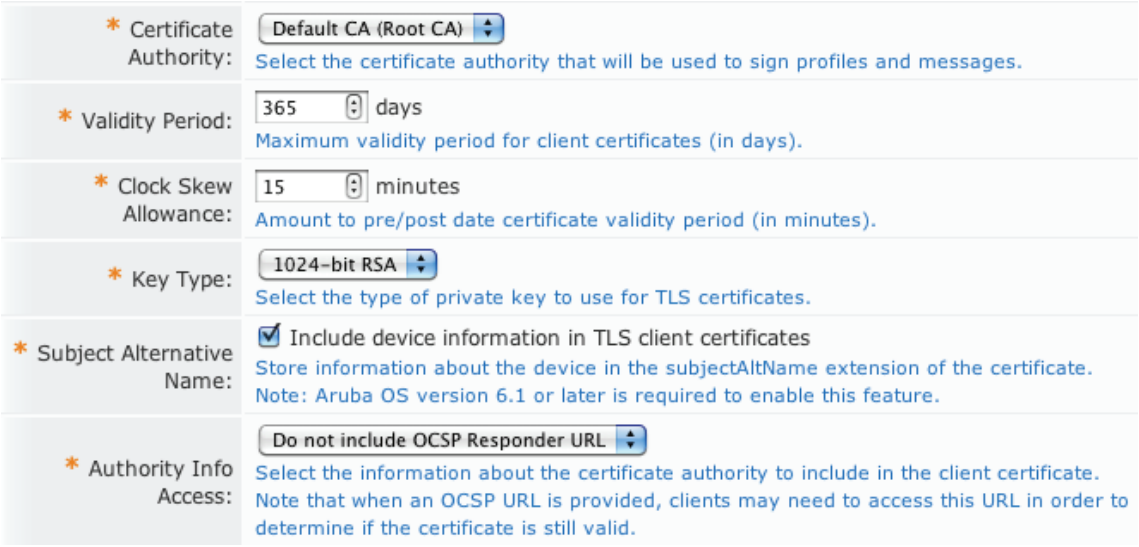


The **Name** and **Description** fields are used internally to identify this set of Onboard settings for the network administrator. These values are never displayed to the user during device provisioning.

Use the **Organization** field to provide the name of your organization; this will be displayed to the user during the device provisioning process.

Configuring Certificate Properties for Device Provisioning

The second part of the Device Provisioning Settings form is used to specify the properties for certificates issued to devices.



The **Certificate Authority** drop-down list can be used to select a different certificate authority. By default, there is only a single certificate authority.

Use the **Validity Period** text field to specify the maximum length of time for which a client certificate issued during device provisioning will remain valid.

The **Clock Skew Allowance** text field 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.

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.

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.

When issuing a certificate, the certificate's validity period is determined as follows:

- 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:
  - 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.

The **Key Type** drop-down list specifies the type of private key that should be created when issuing a new certificate. You can select one of these options:

- **1024-bit RSA** – lower security
- **2048-bit RSA** – recommended for general use
- **4096-bit RSA** – higher security

Note: 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.

Mark the **Include device information in TLS client certificates** check box to include additional fields in the TLS client certificate issued for a device. These fields are stored in the subject alternative name (subjectAltName) of the certificate. Refer to Table 16 on page 92 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.

Note: If you are using an Aruba Controller to perform EAP-TLS authentication using these client certificates, you must have Aruba OS 6.1 or later to enable this option.

Table 16 *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)

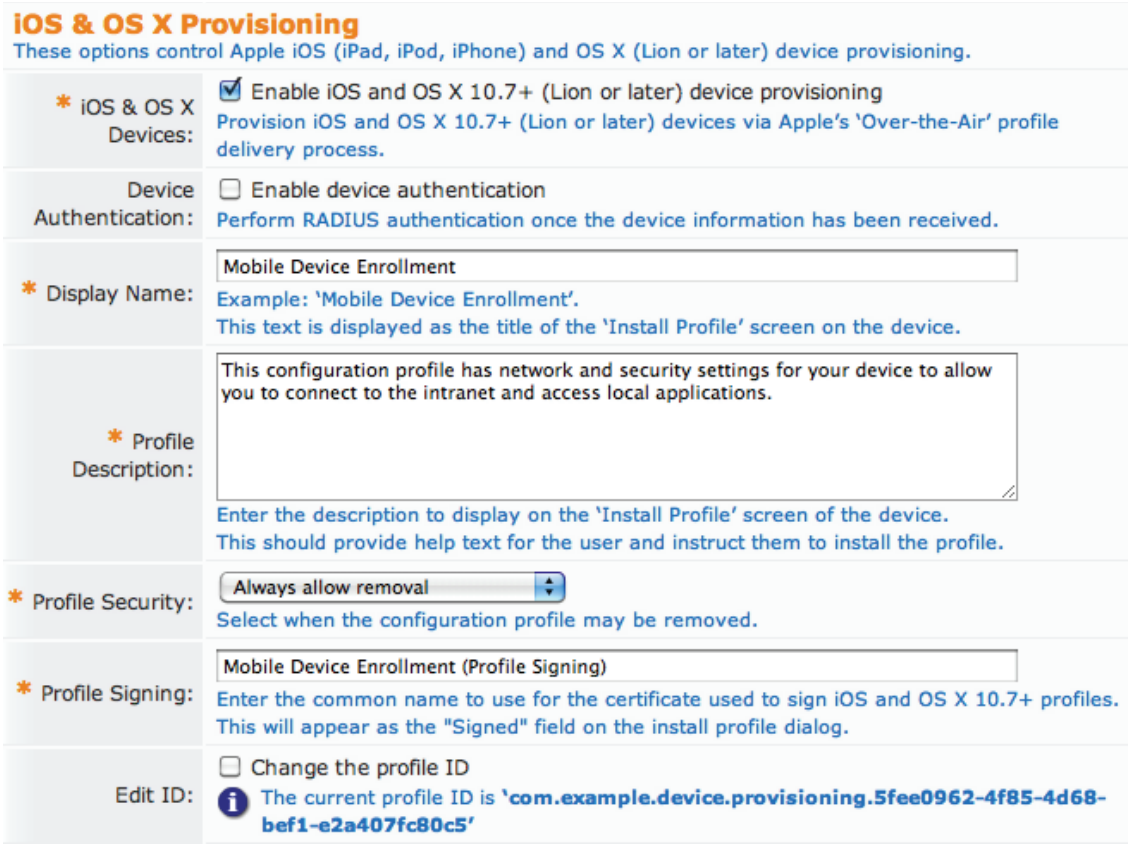
Note: Object Identifier. These OIDs are relative to the ClearPass Guest base OID, which is 1.3.6.1.4.1.14823.1.5.1.

Specify one of the following options in the **Authority Info Access** drop-down list to control automatic certificate revocation checks:

- **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.

Configuring Provisioning Settings for iOS and OS X

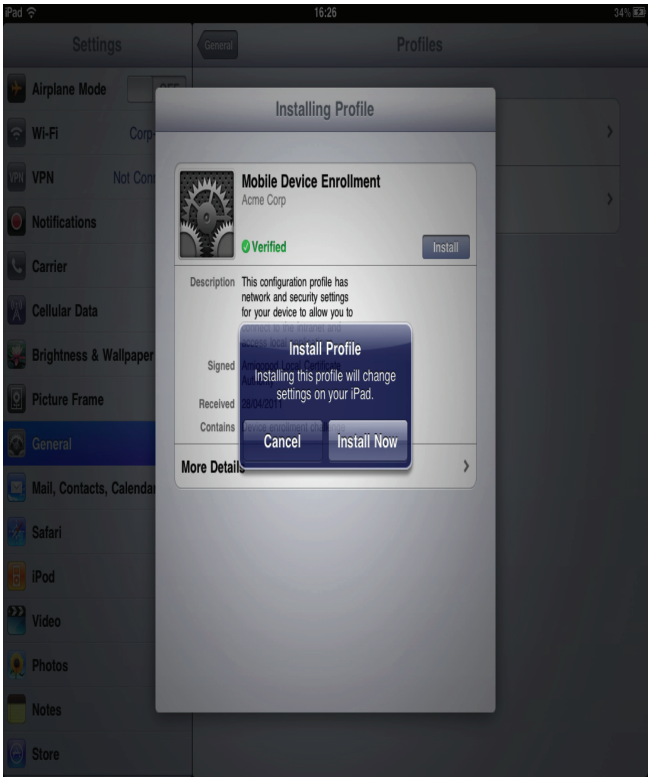
The third part of the Device Provisioning Settings form is used to specify provisioning settings related to iOS devices.



Mark the **Enable iOS and OS X 10.7+ (Lion or later) device provisioning** check box to enable provisioning for these devices.

Mark the **Enable device authentication** check box to enable an additional authorization step to be performed during device provisioning. See "Advanced: Device Authentication During Provisioning" for details about this process.

Use the **Display Name** and **Profile Description** text fields to control the user interface displayed during device provisioning.



Select one of the following options in the Profile Security drop-down list to control how a device provisioning profile may be removed:

- **Always allow removal** – The user may remove the device provisioning 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 device provisioning 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 device provisioning 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.

Use the **Profile Signing** text field to specify 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 "Sign**ed" field on the device when the user authorizes the device provisioning.**

Mark the Change the profile ID check box to change the unique value associated with the configuration profile. This value is used to identify the configuration settings as being from a particular source, and should be globally unique.

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.

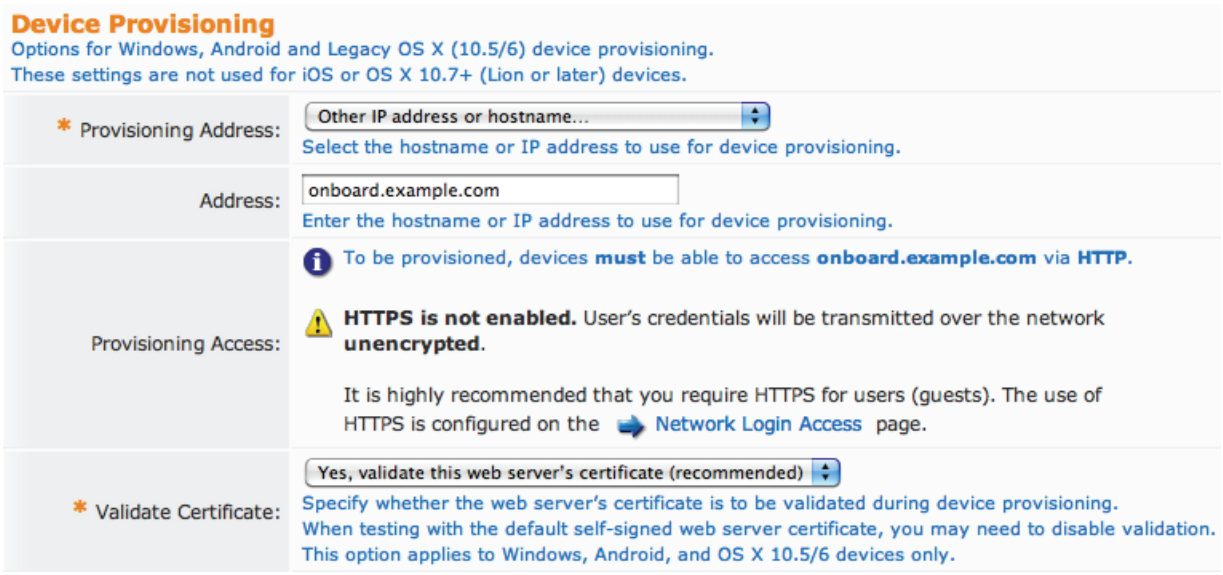
Note: Changing the profile ID will affect any device that has already been provisioned with the existing profile ID. The default value is automatically generated and is globally unique. You should only change this value during initial configuration of device provisioning.

Configuring Provisioning Settings for Mac OS X, Windows, and Android Devices

The fourth part of the Device Provisioning Settings form is used to specify provisioning settings related to Onboard-capable devices.

Mark the appropriate check boxes here to enable device provisioning on the respective platforms:

- Enable OS X 10.5 (Leopard) and 10.6 (Snow Leopard) device provisioning
- Enable Windows XP, Vista and 7 (or later) device provisioning
- Enable Android device provisioning



Select one of the options in the **Provisioning Address** drop-down list to control where a device is directed to during provisioning:

- **The system's hostname (requires DNS resolution)** – Select this option to use the system hostname for device provisioning.

  Note that this option requires that the device be able to resolve the listed hostname at the time the device is provisioned.
- **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.

  Use this option when special DNS or NAT conditions apply to devices that are in a provisioning role.

The Provisioning Access 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.

Note: 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".

The **Validate Certificate** drop-down list is used to specify whether the SSL server's certificate should be validated as trusted. When this option is set to "Yes, validate this web server's certificate (recommended)", a certificate validation failure on the client device will cause device provisioning to fail. This is the default option.

You should change this option to "No, do not validate this web server's certificate" only during testing, or if you are waiting for a commercial SSL certificate.

Configuring User Interface Options for Mac OS X, Windows, and Android Devices

The Device Provisioning section of the Device Provisioning Settings form allows you to customize the user interface displayed by the QuickConnect app.

To display your enterprise's logo, select an image from the list in the **Logo Image** field. Navigate to **Administrator** > **Content Manager** to upload new images for 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.

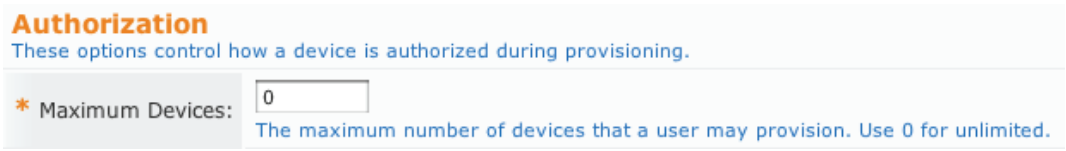
The **Wizard Title** text field may be used to specify the text displayed to users when they launch the QuickConnect app to provision their device.

If provided, the **Password Recovery URL** and **Helpdesk URL** fields may be used to provide additional resources to users who encounter trouble in provisioning their devices.

Note: Ensure that users in the provisioning role can access these URLs.

Configuring Authorization Settings for Device Provisioning

The fifth part of the Device Provisioning Settings form is used to specify authorization settings for device provisioning.



Enter a number in the **Maximum Devices** field to limit the maximum number of devices that each user may provision.

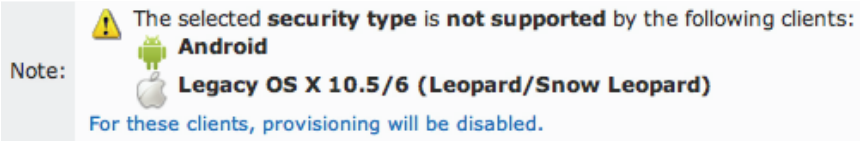
Devices are recognized as unique when they have a different MAC address, or a different device identifier (when the MAC address is not available).

Configuring Network Settings for Device Provisioning

To configure the network settings that will be sent to a provisioned device, go to **Onboard > Network Settings**, or click the **Network Settings** command link. The Network Settings page opens.

This page is used to configure the network settings that will be provisioned to devices.

Note: Some devices do not support all possible combinations of network settings. If you make a selection that is incompatible with a certain type of device, a message will be displayed in the Onboard user interface.



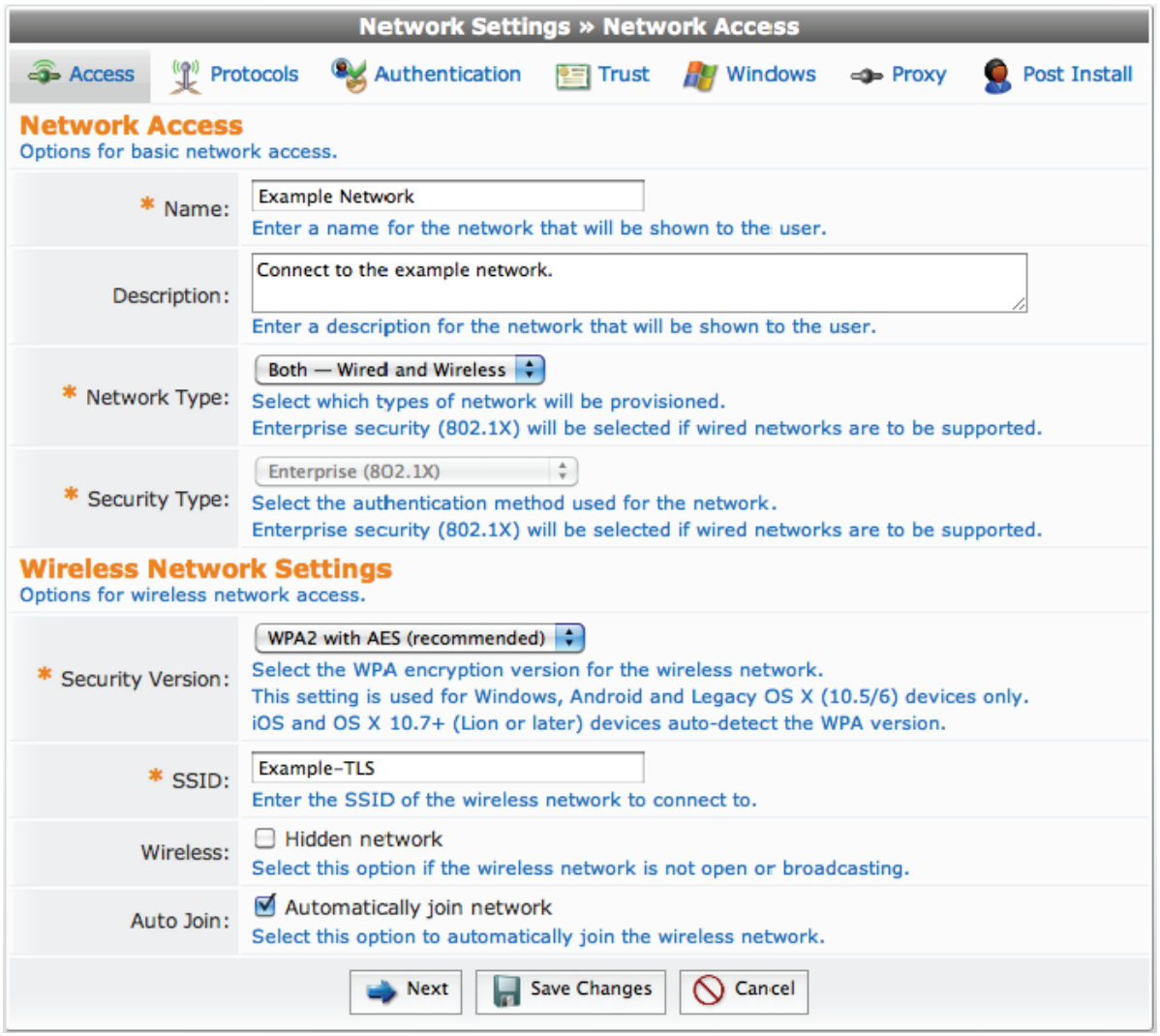
The Network Access form is divided into several tabs:

- Access – Specifies basic network properties, such as the name of the wireless network and the type of security that is used. See "Configuring Basic Network Access Settings".
- Protocols – Specifies the 802.1X authentication protocols that are used by the network. See "Configuring 802.1X Authentication Network Settings".
- Authentication – Specifies the type of device authentication to be used for the network. See "Configuring Device Authentication Settings".
- Trust – Specifies options related to mutual authentication. See "Configuring Mutual Authentication Settings".
- Windows – Specifies networking options used only by devices using the Windows operating system. See "Configuring Windows-Specific Network Settings".
- Proxy – Specifies a proxy server to be used by devices connecting to the network. See "Configuring Proxy Settings".
- Post Install – Specifies additional information and instructions to users after the network is configured. See "Configuring Post-Installation Instructions".

Note: Navigating between different tabs will save the changes you have made. The modified settings are indicated with a "#" marker in the tab. The settings used for device provisioning are not modified until you click the **Save Changes** button.

Configuring Basic Network Access Settings

Click the **Access** tab to display the Network Access form.



The options available in the Network Type drop-down list are:

- **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.
- **Wireless only** – Configures only wireless network adapters.
- **Wired only** – Configures only wired (Ethernet) network adapters.

The options available in the **Security Type** drop-down list are:

- **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”.

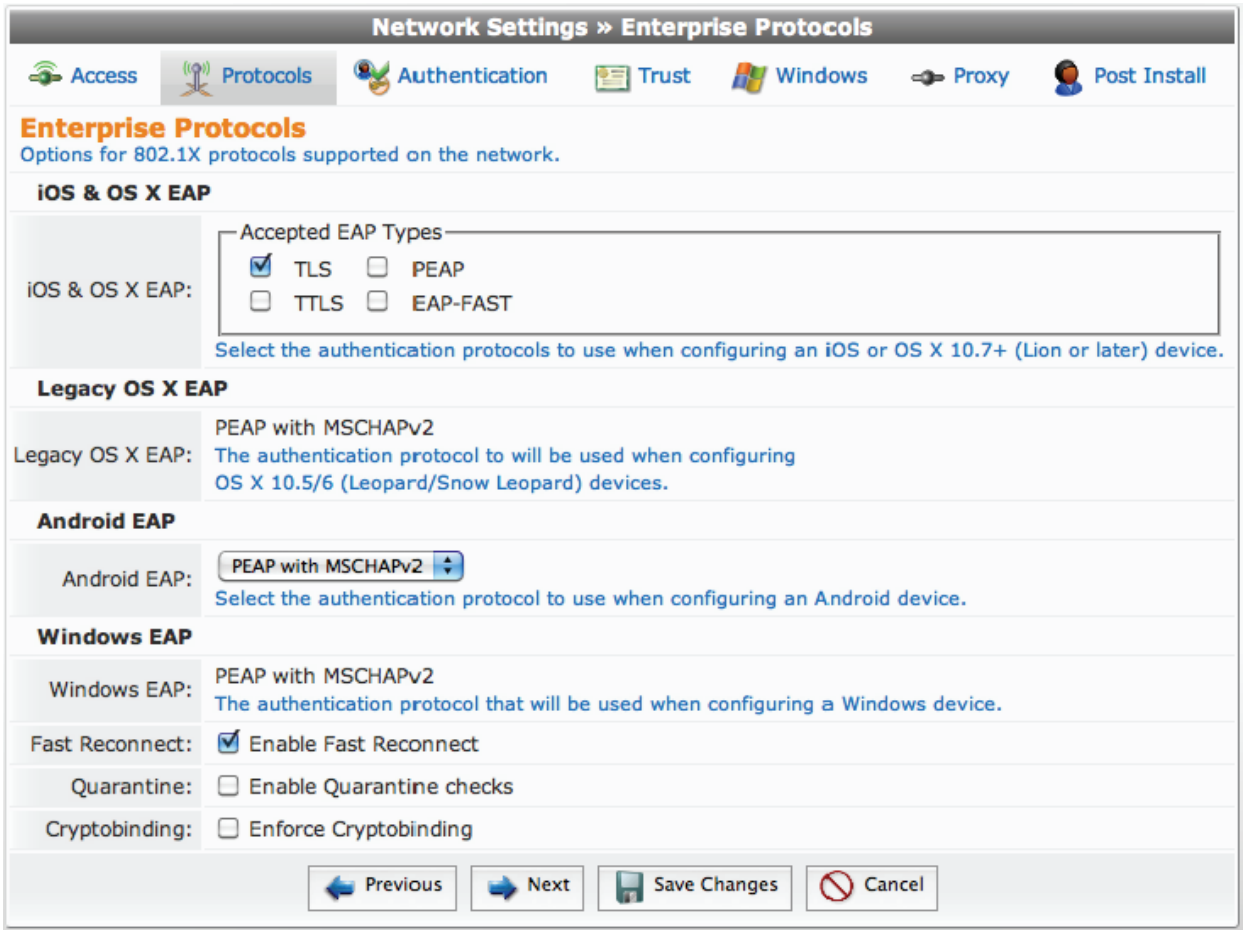
The **Security Type** field lets you set the encryption version for the wireless network to **WPA** or **WPA2**.

If you have selected the **Personal (PSK)** security type, you must provide the pre-shared key in the **Password** field. Selecting this security type will hide the **Protocols**, **Authentication**, and **Trust** tabs.

Click the **Next** button to continue to the **Protocols** tab. Click the **Save Changes** button to make the new network configuration settings take effect. Click the **Cancel** button to discard your changes and return to the main Onboard configuration user interface.

Configuring 802.1X Authentication Network Settings

Click the **Protocols** tab to display the Enterprise Protocols form.



Use this form to specify the authentication methods required by your network infrastructure.

- The **Legacy OS X EAP** option supports only PEAP with MSCHAPv2.
- The **Windows EAP** option supports only PEAP with MSCHAPv2.

These best practices are recommended when choosing the 802.1X authentication methods to provision:

- Configure PEAP with MSCHAPv2 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.

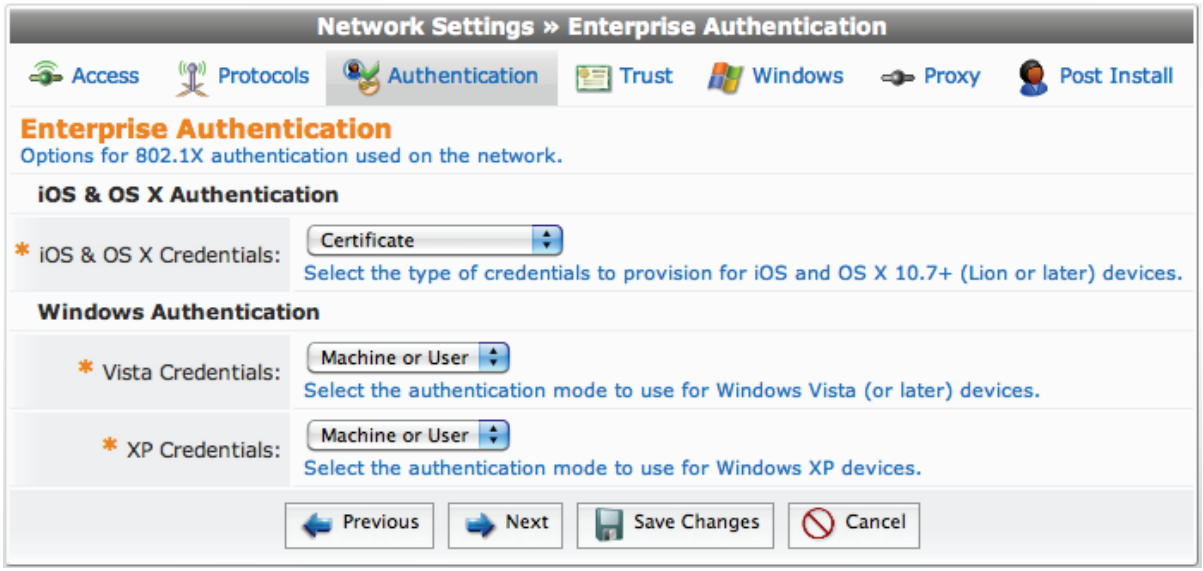
The **Windows EAP** options that may be specified include:

- **Enable Fast Reconnect** – 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.
- **Enable Quarantine Checks** – Enable this option to obtain a system statement-of-health (SSoH) from the OnGuard or Microsoft NAP Agent and send it to the authentication server during the 802.1X authentication process. Use this option to enforce network access control (NAC) protections on the network.
- **Enforce Cryptobinding** – 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.

Click the **Previous** button to return to the Access tab. Click the **Next** button to continue to the **Authentication** tab. Click the **Save Changes** button to make the new network configuration settings take effect. Click the **Cancel** button to discard your changes and return to the main Onboard configuration user interface.

Configuring Device Authentication Settings

Click the **Authentication** tab to display the Enterprise Authentication form.



Select one of these options in the **iOS & OS X Credentials** drop-down list:

- **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.

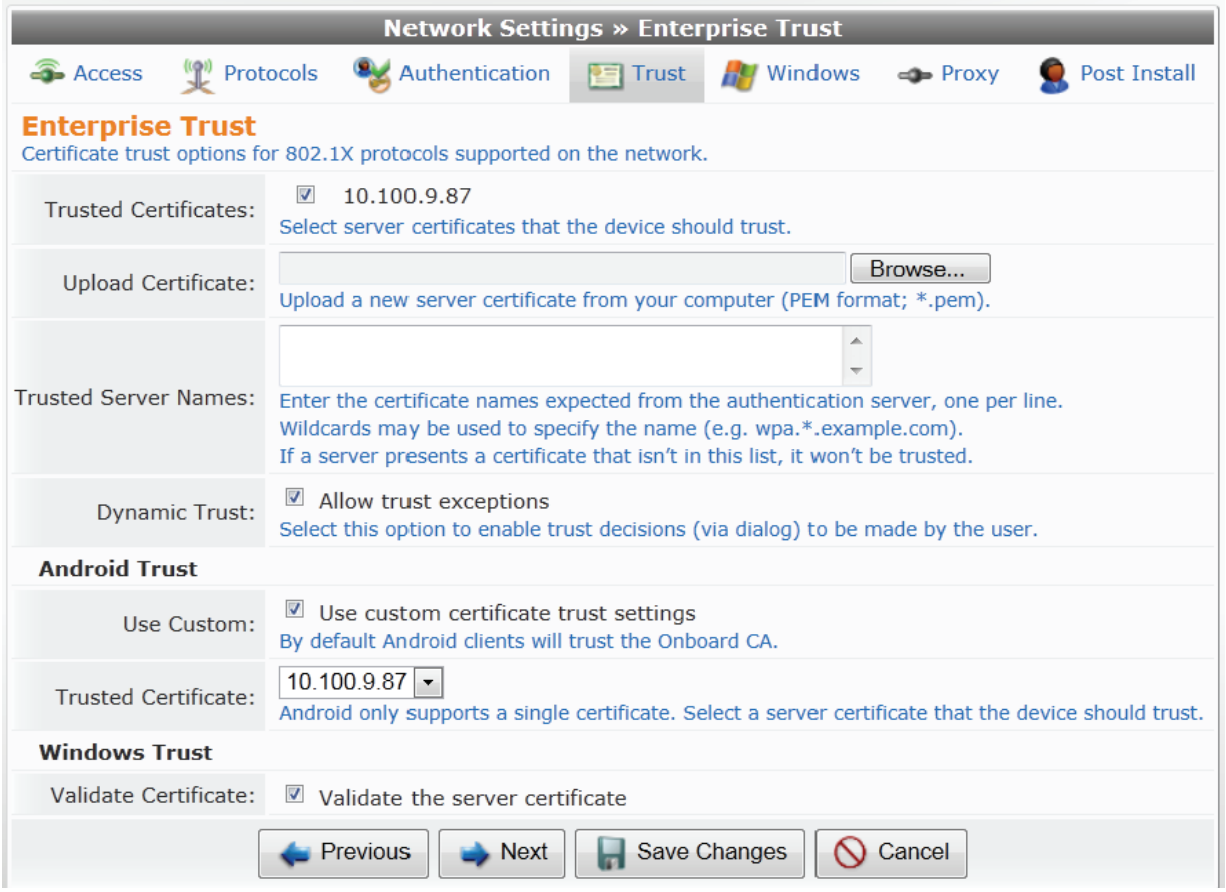
The **Windows Authentication** options that may be selected are:

- **Machine Only** – Use computer-only credentials.
- **User Only** – Use user-only credentials
- **Machine Or User** – Use computer-only credentials or user-only credentials. When a user is logged on, the user's credentials are used for authentication. When no user is logged on, computer-only credentials are used for authentication.
- **Guest –** Use guest-only credentials.

Click the **Previous** button to return to the Protocols tab. Click the **Next** button to continue to the Trust tab. Click the **Save Changes** button to make the new network configuration settings take effect. Click the **Cancel** button to discard your changes and return to the main Onboard configuration user interface.

Configuring Mutual Authentication Settings

Click the **Trust** tab to display the Enterprise Trust form.



In the **Trusted Certificates** row, mark the check box for each server certificate that the client should trust.

Use the **Upload Certificate** field to upload additional server certificates. These certificates will be displayed in the certificate management list view with the type "tls-server".

These best practices are recommended for enterprise trust options:

- Provide the certificate for each authentication server that a provisioned device will use, and select it in the **Trusted Certificates** list.
- 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.
- Mark the **Validate the server certificate** check box for Windows. This ensures that the provisioned device will check the server certificate is valid before using the server for authentication.

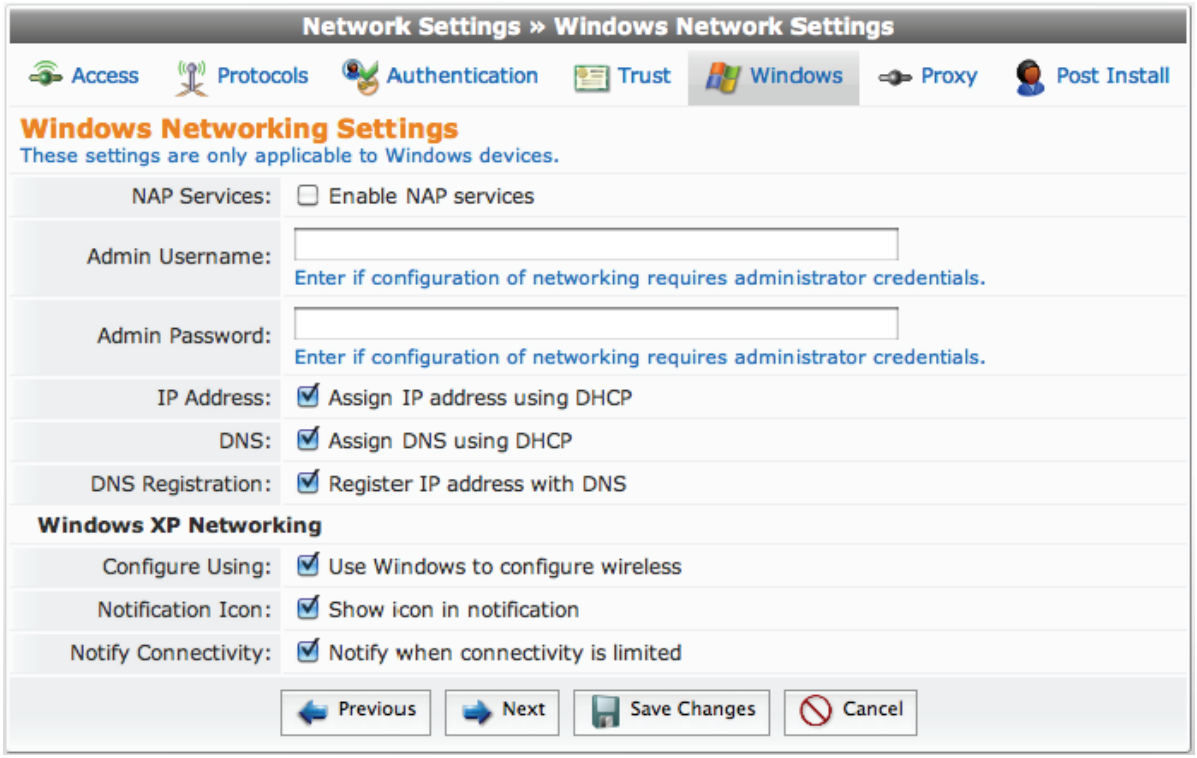
In the **Android Trust** row, the default setting is for Android devices to automatically provision Onboard's Root CA certificate to the device. You can choose to provision a custom certificate instead. To provision a custom certificate for an Android device, mark the **Use custom certificate trust settings** check box. The form expands to include the Trusted Certificate row. In the drop-down list, choose the certificate the device should trust.

Click the **Previous** button to return to the Authentication tab. Click the **Next** button to continue to the Windows tab. Click the **Save Changes** button to make the new network configuration settings

take effect. Click the **Cancel** button to discard your changes and return to the main Onboard configuration user interface.

Configuring Windows-Specific Network Settings

Click the **Windows** tab to display the Windows Network Settings form.



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.

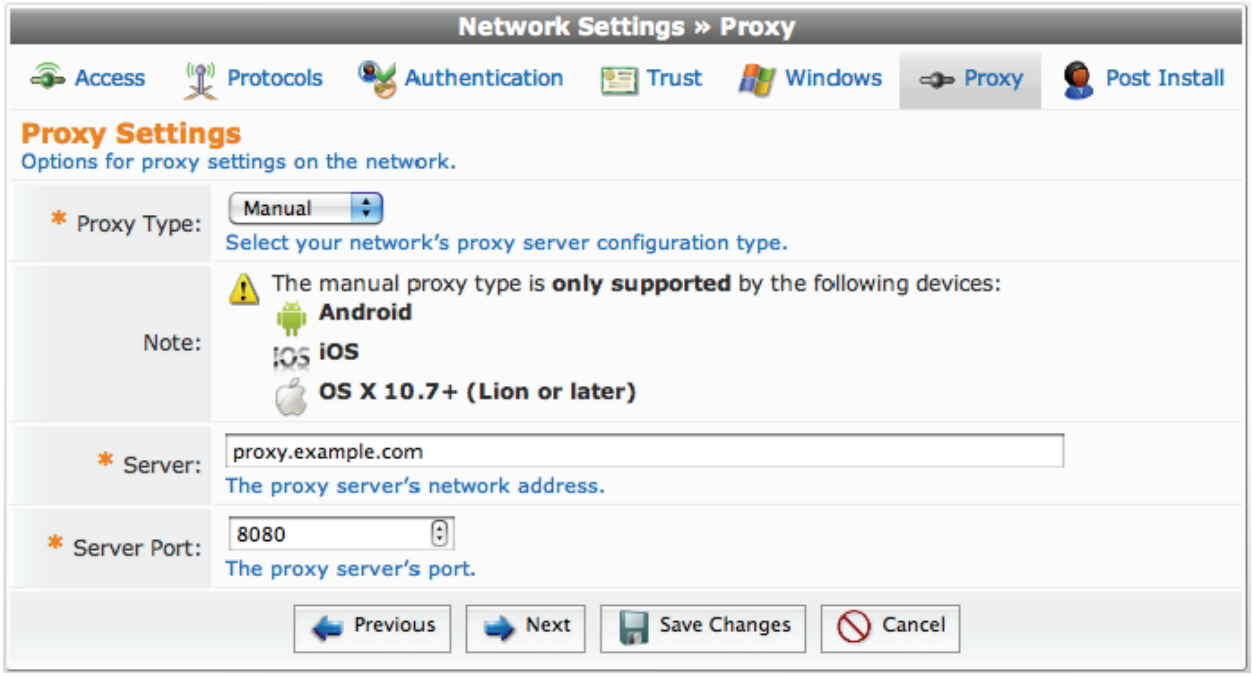
Deploying NAP requires a NAP-compatible authentication server, so that appropriate policies may be implemented based on the statement of health provided by the NAP client.

To enable NAP for Microsoft Windows clients, mark the **Enable NAP services** check box on this tab. You will also need to mark the **Enable Quarantine Checks** check box on the **Protocols** tab.

Click the **Previous** button to return to the Trust tab. Click the **Next** button to continue to the Proxy tab. Click the **Save Changes** button to make the new network configuration settings take effect. Click the **Cancel** button to discard your changes and return to the main Onboard configuration user interface.

Configuring Proxy Settings

Click the **Proxy** tab to display the Proxy Settings form.



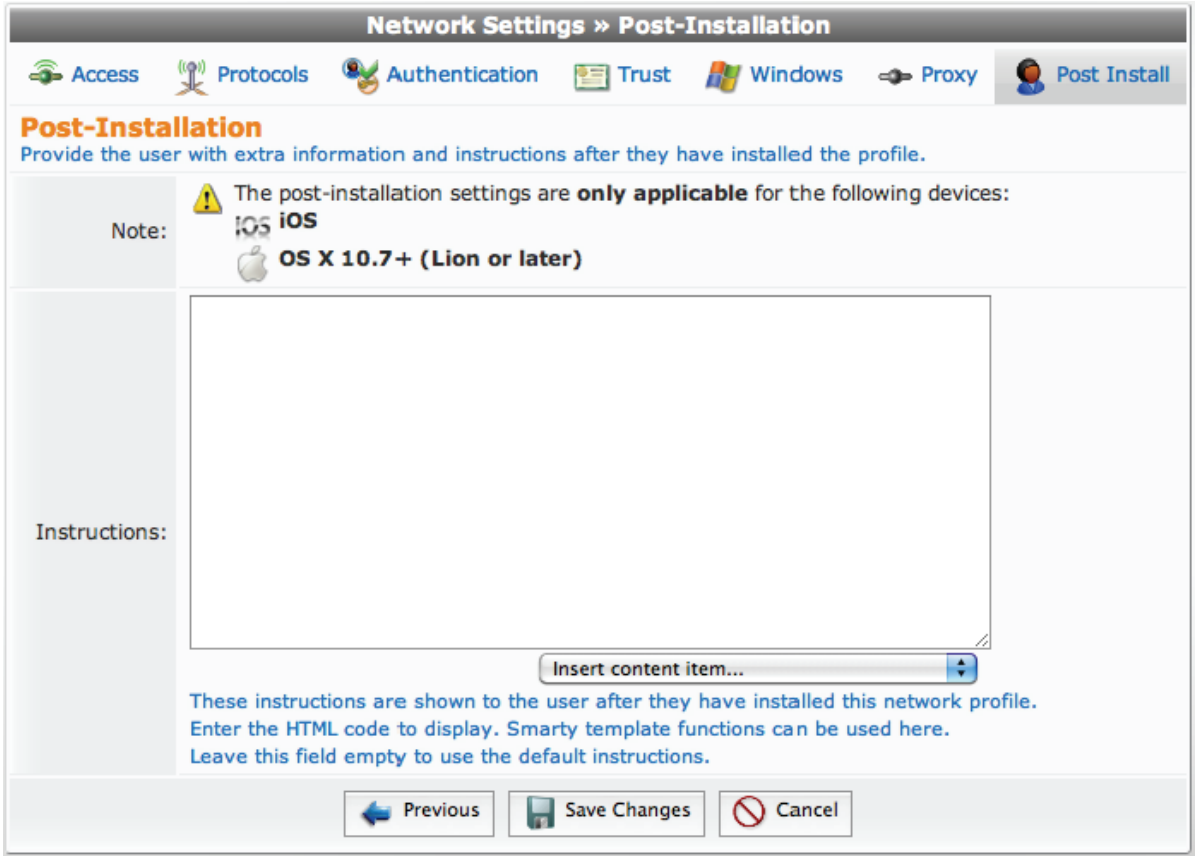
Select one of these options in the **Proxy Type** drop-down list:

- **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.

Click the **Previous** button to return to the Windows tab. Click the **Next** button to continue to the Post Install tab. Click the **Save Changes** button to make the new network configuration settings take effect. Click the **Cancel** button to discard your changes and return to the main Onboard configuration user interface.

Configuring Post-Installation Instructions

Click the **Post Install** tab to display the Post-Installation form.



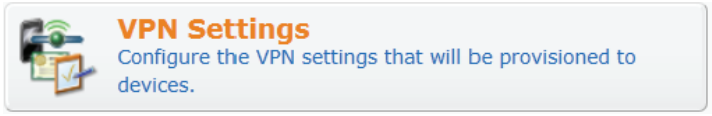
The **Instructions** text field can be used to provide more information or instructions to an iOS or OS X user immediately after device provisioning has completed.

For example, if you have provisioned Wi-Fi network settings for an SSID that is separate from the initial provisioning SSID, you could add a message requesting that the user now switch to the new SSID in order to complete setup.

Click the **Previous** button to return to the Proxy tab. Click the **Save Changes** button to make the new network configuration settings take effect. Click the **Cancel** button to discard your changes and return to the main Onboard configuration user interface.

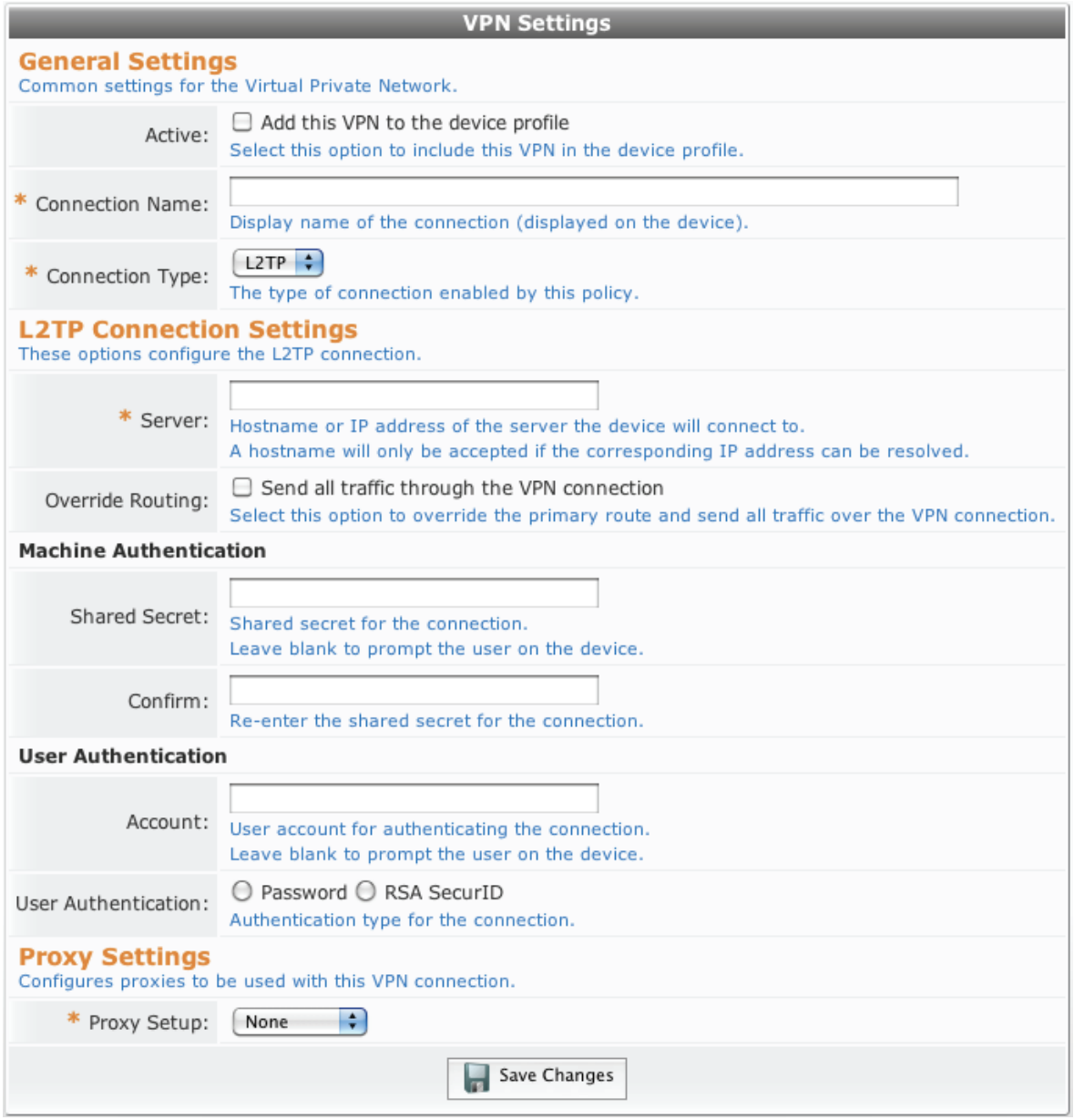
Configuring an iOS Device VPN Connection

To configure the VPN settings that will be sent to a device, go to **Onboard > VPN Settings**, or click the **VPN Settings** command link. The VPN Settings page opens.



This page is used to automatically configure virtual private networking (VPN) settings on the iOS device. Use this option when you have deployed a VPN infrastructure and want to automatically provide the secure connection settings to users at the time of device provisioning.

Note: Onboard VPN settings can only be used with iOS 4 and iOS 5 devices. Other platforms are not supported.



Mark the **Add this VPN to the device profile** check box to enable provisioning of VPN settings.

The **Display Name** text field specifies the name for this VPN connection. This will be displayed on the device in the Settings app. To help the user identify the connection easily, include your organization's name in the Display Name field. For example, use "ACME Sprockets VPN".

Select the appropriate **Connection Type** from the drop-down list:

- **L2TP** – Connection uses the Layer 2 Tunneling Protocol. Complete the fields shown in the L2TP Connection Settings section of the form.
- **PPTP** – Connection uses the Point-to-Point Tunneling Protocol. Complete the fields shown in the PPTP Connection Settings section of the form.
- **IPSec** – Connection uses the Internet Protocol with security extensions. Complete the fields shown in the IPSec Connection Settings section of the form.

  The **Authentication Type** drop-down list provides these options when configuring an IPSec VPN:

  - **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.

The Proxy Settings section of the form specifies a proxy server that is used when the VPN connection is active. Select one of these options in the **Proxy Setup** drop-down list:

- **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** fields.

  If authentication is required to access this proxy, you may specify the username and password using the **Authentication** and **Password** text fields.
- **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** text field.

Click the **Save Changes** button to save the VPN connection profile and return to the main Onboard configuration user interface.

Configuring an iOS Device Email Account

To configure the Exchange ActiveSync settings that will be sent to a device, go to **Onboard > Exchange ActiveSync**, or click the **Exchange ActiveSync** command link. The Exchange ActiveSync Settings page opens.

This page is used to automatically configure an email account on the iOS device. Use this option when you have an Exchange mail server and want to automatically provide the email settings to users provisioning their mobile devices.

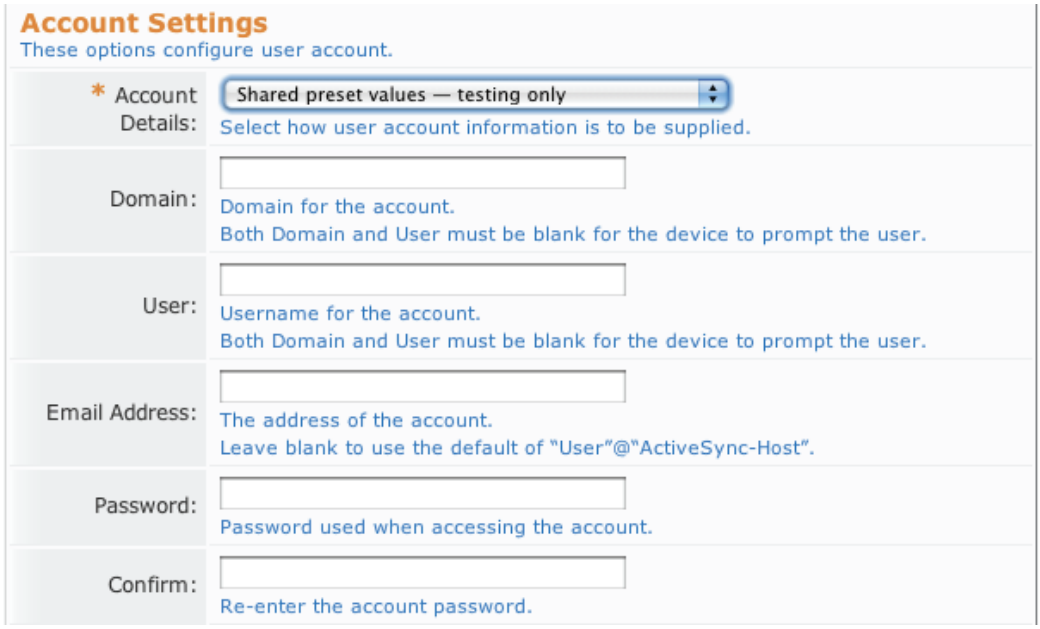
Note: Onboard Exchange ActiveSync settings can only be used with iOS 4 and iOS 5 devices. Other platforms are not supported.

Mark the **Add this ActiveSync configuration to the device profile** check box to enable email account provisioning.

The **Account Name** text field specifies the name for this email account. This will be displayed on the device in the Settings app, and also within the Mail app to identify the mailbox. To help the user identify this mailbox easily, include your organization's name in the Account Name field. For example, use "ACME Sprockets Mail".

In the **Account Settings** group, choose one of the following options from the **Account Details** drop-down list:

- **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.
- **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.



In the **Sync Settings** group, choose one of the following options from the **Days of Mail** drop-down list:

- No Limit
- 1 day
- 3 days
- 1 week
- 2 weeks
- 1 month

Click the **Save Changes** button to save the Exchange ActiveSync profile and return to the main Onboard configuration user interface.

Configuring an iOS Device Passcode Policy

To make changes to the Passcode Policy configuration that will be sent to a device, go to **Onboard > Passcode Policy**, or click the **Passcode Policy** command link. The Passcode Policy Settings page opens.

This page is used to configure a passcode policy that is applied to iOS devices when provisioned.

Typically, you would enable this policy when provisioning a corporate-owned device, or if you are allowing a user to access sensitive information remotely.

NOTE: Onboard Passcode Policy settings can only be used with iOS 4 and iOS 5 devices. Other platforms are not supported.

To enable the passcode policy on all iOS devices, mark the **Enable passcode policy** check box and configure the remaining options according to your enterprise's security requirements.

Click the **Save Changes** button to save the passcode policy settings and return to the main Onboard configuration user interface.

Resetting Onboard Certificates and Configuration

To delete certificates, re-create the Onboard Web login page, or reset configuration to factory default settings, go to **Onboard > Reset to Factory Defaults**, or click the **Reset to Factory Defaults** command link. The Reset to Factory Defaults page opens.

This page is used to delete certificates, or restore the default configuration for Onboard. These options are useful while trialing the Onboard workflow with a set of test devices.

Select one of the following options in the **Reset Type** drop-down list:

- **Delete all client certificates** – Removes all client certificates from Certificate Management. The certificate authority's root certificate, intermediate certificate, profile signing certificate, and any server certificates are not affected. The provisioning settings for iOS and Onboard-capable devices are not modified.
- **Delete all certificates** – Removes all certificates from Certificate Management, including the certificate authority's root certificate, intermediate certificate, profile signing certificate, and any server certificates. The default certificate authority certificate will be recreated. The provisioning settings for iOS and Onboard-capable devices are not modified.
- **Re-create the Onboard weblogin page** – Select this option to create the default device_provisioning Web login page, if it has been deleted or has been modified and no longer functions correctly. All certificates and settings are left unmodified.
- **Delete all certificates and reset configuration to factory defaults** – Removes all certificates from Certificate Management, including the certificate authority's root certificate, intermediate certificate, profile signing certificate, and any server certificates. The provisioning settings for iOS and Onboard-capable devices are restored to the default settings. The default certificate authority will be recreated.

Mark the **Reset the specified items** check box to indicate that the reset operation should be performed, and then click **Reset to Factory Defaults** to perform the operation.

Advanced: Device Authentication During Provisioning

When the **Enable device authentication** check box is marked, a RADIUS request is performed during the device provisioning step.

The local RADIUS server is always used for this request.

The attributes sent with the RADIUS request are listed in Table 17 on page 111.

Table 17 *RADIUS Attributes Included with a Device Authentication Request.*

RADIUS Attribute	Value
User-Name (1)	The username for the current device provisioning process.
User-Password (2)	Password credentials supplied by the user during device provisioning.
Calling-Station-Id (31)	MAC address of the device being provisioned. This attribute is omitted if the MAC address information is unavailable. If multiple MAC addresses are available, only the first MAC address will be included in the RADIUS request.
Framed-IP-Address (8)	IPv4 address of the device being provisioned.
NAS-IP-Address (4)	Always set to “127.0.0.1”.
NAS-Identifier (32)	Set to the hostname of the Onboard server.
NAS-Port (5)	Always set to “0”.
NAS-Port-Type (61)	Always set to “Ethernet” (15).
Service-Type (6)	Always set to “Authorize-Only” (17).
Event-Timestamp (55)	Set to a value indicating the current time.
Mdps-Device-Name1 (19)	Type of device, such as “iOS”, “Android”, etc.
Mdps-Device-Product1 (20)	Product string identifying the device and often including the hardware version information.
Mdps-Device-Version1 (21)	Software version number for the device.
Mdps-Device-Udid1 (15)	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).
Mdps-Device-Imei1 (16)	International Mobile Equipment Identity (IMEI) number allocated to this device.
Mdps-Device-Iccid1 (17)	Integrated Circuit Card Identifier (ICCID) number from the Subscriber Identity Module (SIM) card present in the device.
Mdps-Device-Serial1 (22)	Serial number of the device.

Note: This is a vendor-specific attribute with vendor ID 14823.

If the RADIUS server responds with an Access-Reject, then the device provisioning will fail. The value of the Reply-Message attribute, if one was included in the Access-Reject message, will be used to construct the error message.

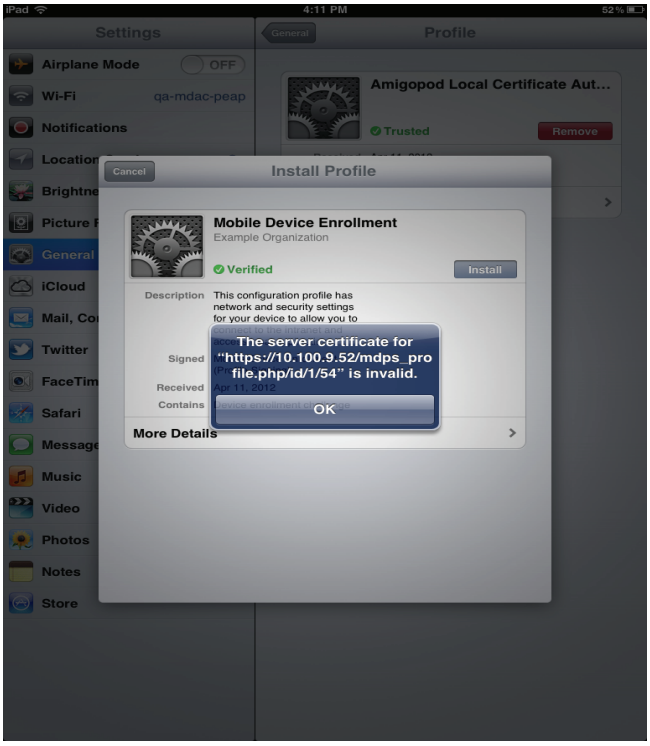
If the RADIUS server responds with an Access-Accept message, then the device provisioning proceeds as normal.

Onboard Troubleshooting

If you encounter a problem that is not listed here, refer to the “Onboard Deployment Checklist” 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”.



Resolution: 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”.

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.

RADIUS is a network access-control protocol that verifies and authenticates users. The framework around which RADIUS is built is known as the AAA process, consisting of authentication, authorization, and accounting.

RADIUS authenticates a guest user's session by checking that the guest's password matches the guest's login details stored in the RADIUS database. Guest access is authorized by assigning a user role to the guest account. The properties of the role determine the authorization for each guest session. Dynamic authorization extensions to RADIUS allow for sessions to be disconnected, or for changes in authorization to be made while a guest is connected. Lastly, the RADIUS database records summarized accounting information about each guest session. This allows you to generate reports about guest network usage.

Accessing RADIUS Services

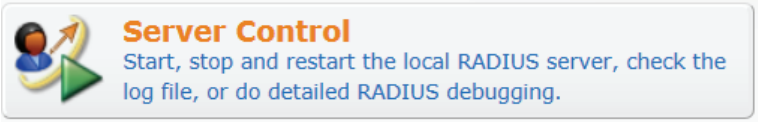
To access RADIUS Services:

- From the Home page, click the **RADIUS Services** command link. Alternatively, use the **RADIUS** link at the top level of the left navigation menu to jump directly to any of the features within RADIUS Services.

Server Control

To restart, stop, or debug the RADIUS server:

- Go to **RADIUS > Server Control**.



The Restart RADIUS Server and Stop RADIUS Server commands take effect the moment either one is clicked. You are not presented with any confirmation windows.

RADIUS Log Snapshot

The latest entries in the RADIUS server log are displayed on the Server Control page in reverse chronological order.

Log entries that are displayed include both successful and unsuccessful authentication attempts, the details about any authentication or authorization failures, and server configuration messages when the RADIUS server is started.

Debug RADIUS Server

The AAA Debug option on the RADIUS Server Configuration page enables additional debugging messages logged during the handling of RADIUS packets. The default setting is “No debugging.” This option might be of use when setting up or troubleshooting advanced authorization methods, and you can refer to the application log to view the AAA debug messages. However, for performance reasons, this option should be disabled in a production environment. If you do enable it for troubleshooting, remember to disable it when you are through.

In debugging mode, the detailed log output from the local RADIUS server is redirected to your browser. This can greatly assist in troubleshooting the exact cause of an authentication, authorization or accounting (AAA) problem.

Normally, the RADIUS server runs in the background, processing AAA requests from incoming clients and generating responses. However, if you are troubleshooting an authentication problem, sometimes it is convenient to see exactly what is being sent and received by the RADIUS server. This can help track down configuration problems in NAS clients (such as an incorrect shared secret, or an invalid request attribute), user roles (wrong reply attributes or values), and other problems.

To view this output, the RADIUS server is stopped and restarted in a diagnostic mode. The output generated on each request is redirected to your Web browser.


NOTE

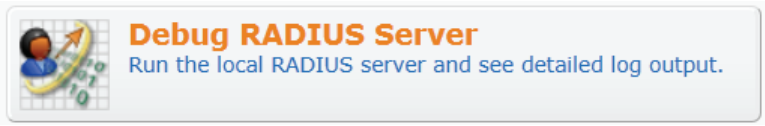
You can resize the log output area by clicking and dragging the border.

When you stop the debugger, the normal background operation of the RADIUS server is resumed. No further output will be received once the debugger has been stopped.

During the starting and stopping of the server, there may be brief periods of time during which the RADIUS server is unreachable. RADIUS clients should cope with this outage by retrying their RADIUS requests. However, on a busy network some traffic may still be lost.

To enter debugging mode:

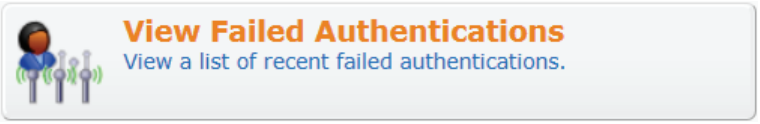
Go to **RADIUS > Server Control > Debug RADIUS Server**.



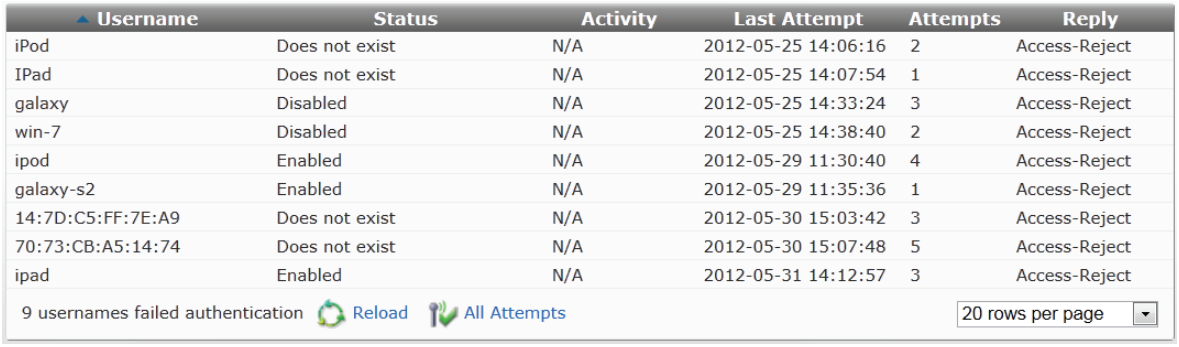
Viewing Failed Authentications

To view a list of recent authentication failures:

- Go to **RADIUS > Server Control > View Failed Authentications**.



The RADIUS Failed Authentications list is displayed.



Username	Status	Activity	Last Attempt	Attempts	Reply
iPod	Does not exist	N/A	2012-05-25 14:06:16	2	Access-Reject
IPad	Does not exist	N/A	2012-05-25 14:07:54	1	Access-Reject
galaxy	Disabled	N/A	2012-05-25 14:33:24	3	Access-Reject
win-7	Disabled	N/A	2012-05-25 14:38:40	2	Access-Reject
ipod	Enabled	N/A	2012-05-29 11:30:40	4	Access-Reject
galaxy-s2	Enabled	N/A	2012-05-29 11:35:36	1	Access-Reject
14:7D:C5:FF:7E:A9	Does not exist	N/A	2012-05-30 15:03:42	3	Access-Reject
70:73:CB:A5:14:74	Does not exist	N/A	2012-05-30 15:07:48	5	Access-Reject
ipad	Enabled	N/A	2012-05-31 14:12:57	3	Access-Reject

Each row in the table groups together authentication attempts based on the username (that is, the User-Name attribute provided to the RADIUS server in the Access-Request).

The Status column displays one of the following messages for each authentication record, explaining the current state of the user account in the system:

- **Does not exist** – The user account could not be found.
- **Deleted** – The user account no longer exists.
- **Disabled** – The user account is disabled.

Additionally, if all authentication attempts are displayed, the following status messages may be displayed:

- **Expires:** *date* – The user account is enabled and has the specified expiration time.
- **Enabled** – The user account is enabled.

The Activity column displays one of the following messages for each authentication record, indicating the recent session activity for the corresponding account:

- **Never** – The user has never logged in and no sessions have been recorded.
- **Logged Out** – The user has previously logged in, but there is no current active session for this user. To view the start and stop times for the user's most recent session, hover over the text .
- **Logged In** – The user is currently logged in. To view the start time for the user's most recent active session, hover over the text .
- **Stale** – The user has an active accounting session, but no updates have been received recently; the session might be "stale." To view the start time and duration for this session, hover over the text.

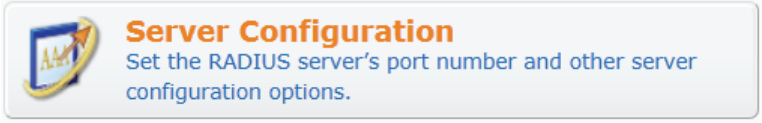
The Last Attempt and Attempts columns display the time at which the most recent authentication was recorded for the user, and the total number of authentication attempts.

The Reply column displays the RADIUS server's response. This may be either Access-Accept to indicate a successful authentication, or Access-Reject to indicate the authentication attempt failed.

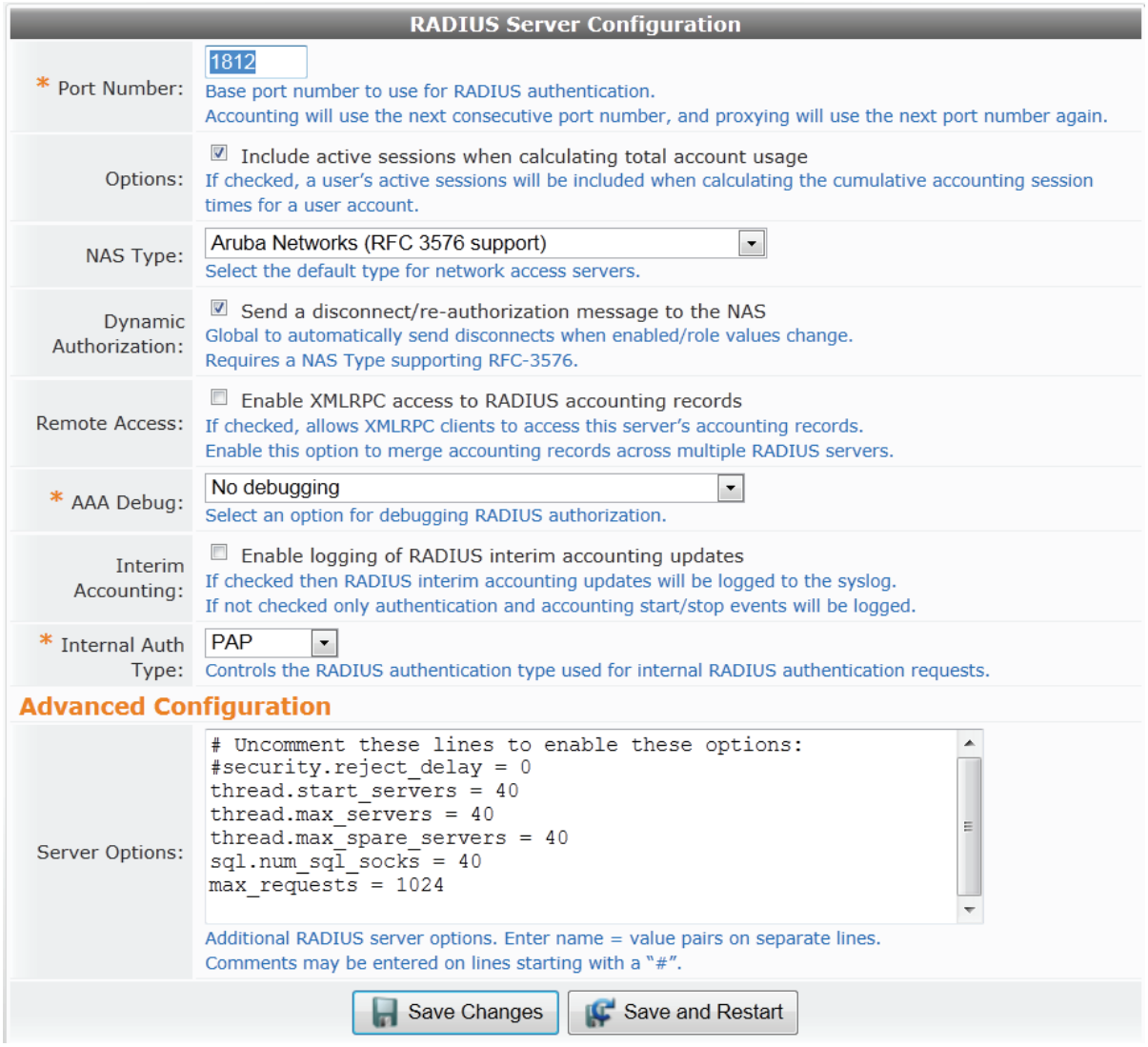
Server Configuration

To modify the advanced configuration options for the RADIUS server:

- Go to **RADIUS > Server Configuration**.



The RADIUS Server Configuration form opens.



The **NAS Type** list may be used to select a default type for network access servers. Use this option if you have a deployment that uses only one type of NAS.

The **AAA Debug** option on the RADIUS Server Configuration page enables additional debugging messages logged during the handling of RADIUS packets. The default setting is "No debugging." This option might be of use when setting up or troubleshooting advanced authorization methods, and you can refer to the application log to view the AAA debug messages. However, for performance reasons, this option should be disabled in a production environment. If you do enable it for troubleshooting, remember to disable it when you are through.

Logging interim accounting updates is optional, and is disabled by default. You can use the check box in the **Interim Accounting** row to enable or disable logging of RADIUS interim accounting updates.

The **Internal Auth Type** option lets the administrator specify the authentication method to use for internally-generated RADIUS requests, such as Web login page authentication or device provisioning requests. You can select PAP, CHAP, or MSCHAP.

The **Server Options** field is a text field that accepts multiple **name = value** pairs. You can also add comments by entering lines starting with a **#** character. For available parameters that can be configured with the Server Options field, see "RADIUS Server Options" in the Reference chapter.

Example: Removing a User-Name Suffix

Some NAS equipment always appends a realm in the form '@domain.com' to a RADIUS User-Name attribute in the Access-Request message sent to the RADIUS server. It is possible to configure the RADIUS server to strip off this additional text, using the attr_rewrite module.

Use the following Server Configuration entries to perform this modification:

```
module.attr_rewrite.consentry.attribute = User-Name
module.attr_rewrite.consentry.searchin = packet
module.attr_rewrite.consentry.searchfor = "@consentry.com$"
module.attr_rewrite.consentry.replacewith = ""
authorize.after_preprocess.0.name = consentry
```

Here, an instance of the **attr_rewrite** module is created, named "consentry". Any trailing text that matches the pattern "@consentry.com" in the User-Name attribute will be removed before the RADIUS server attempts authentication.

Removing a Variable-Length Suffix

The Consentry NAS limits username fields to 32 characters. Many email addresses are longer than this, especially when an additional @realm is appended, so the suffix string might be truncated at an arbitrary point.

The following server configuration option can be used in this situation:

```
module.attr_rewrite.consentry.searchfor =
"@consentry\\.com$|@consentry\\.co$|@consentry\\.c$|@consentry\\.$|@consentry$|@cons
entr$|@consent$|@consen$|@conse$|@cons$|@con$|@co$|@c$|@$"
```

Example: Correcting the NAS-IP-Address Attribute

Some NAS equipment (notably Chillispot) will send a NAS-IP-Address of 0.0.0.0 in accounting records, which renders the active sessions list view useless as well as any attempt to perform RFC 3576 management such as a session disconnect.

This can be fixed by using the Client-IP-Address internal attribute and rewriting the accounting packet so that the actual IP address the packet is received from is recorded:

```
# Fix incoming NAS-IP-Address of 0.0.0.0
module.attr_rewrite.fix_nas_ip.attribute = NAS-IP-Address
module.attr_rewrite.fix_nas_ip.searchin = packet
module.attr_rewrite.fix_nas_ip.searchfor = "^0.0.0.0$"
module.attr_rewrite.fix_nas_ip.replacewith = "%{Client-IP-Address}"
preacct.after_preprocess.0.name = "fix_nas_ip"
```

Example: Adding a Reply-Message to an Access-Reject Packet

The **postauth.reject.append** configuration item can be used to define attribute rewriting specific to the Access-Reject packet:

```
# adding Reply-Message to an Access-Reject
module.attr_rewrite.reject_message.attribute = Reply-Message
module.attr_rewrite.reject_message.searchin = reply
module.attr_rewrite.reject_message.new_attribute = yes
module.attr_rewrite.reject_message.replacewith = "Authorization failed"
postauth.reject.append.0.name = reject_message
```

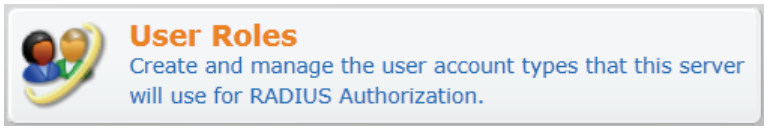
User Roles

Each user in the RADIUS database is assigned a role. A user role is a group of RADIUS attributes and rules that define when those attributes should be applied.

User roles can be used to apply different security policies to different classes of guest user accounts. For example, guest users, employees, and contractors might all have differing network security policies. The RADIUS attributes defined by a user role can then specify what each class of user is authorized to do.

To create and configure user roles for the server to use for RADIUS authorization:

- Go to **RADIUS > User Roles**.



The User Roles list view defines the user roles for the RADIUS server and allows you to make changes to existing user roles.

Each role is identified by a unique number. The ID is shown in the list view. When creating visitor accounts, the **role_id** field should contain the ID of one of the user roles defined in the RADIUS server.

The RADIUS attributes for each role are shown in the list view. The icon displayed with each attribute indicates the type of condition attached to it:

- ✔ The attribute is enabled and will always be included in a RADIUS Access-Accept message.
- ✖ The attribute is disabled and will never be included in a RADIUS Access-Accept message.
- The attribute has a condition expression that will determine if it is included in the RADIUS server's response.

Creating a User Role

To create a role that will be assigned to guest users:

1. Go to **RADIUS > User Roles**, then click the **Create a new role** link. The RADIUS Role Editor form opens.

Figure 16 *RADIUS Role Editor page*

2. In the **Role Name** field, enter a brief descriptive name for the role—for example, if you are creating a role for the guest users in your network, you might choose 'Guest' or "Visitor" as the role name.
3. (Optional) You may enter a description of the role in the **Description** field. This can be useful, as it appears in the list of user roles.
4. If you wish to prevent users within this role from receiving any session warnings, mark the check box in the **Session Warnings** row. This option only applies if session warnings have been enabled at **Customization > Guest Manager**.

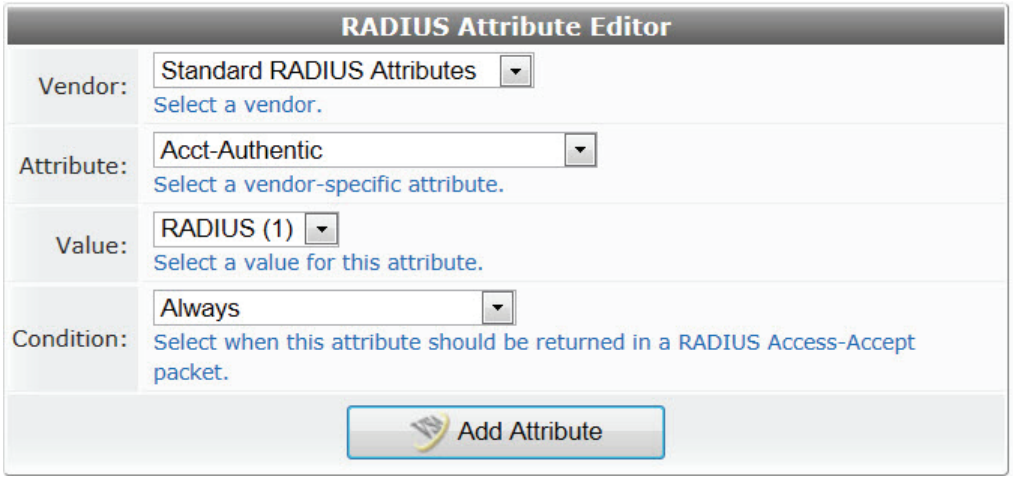
Attributes are used to define the security policies to be applied to guest sessions. The Add Attributes tab lets you configure attributes for the user role you're creating. , click the **Add Attribute** tab. The row expands to include the RADIUS Attribute Editor form. To configure attributes for a role, see "Adding Role Attributes".

Adding Role Attributes

RADIUS attributes form the heart of the role-based access control system. Different user roles may have different attributes associated with them, which allows you to control the behavior of network access devices that authenticate users with the RADIUS server. Furthermore, you can associate a set of rules called a *condition* with each RADIUS attribute. This allows you to make adjustments to the precise definition of a role depending on what kind of access is being requested.

To open the RADIUS Attribute Editor:

1. Do one of the following:
   - To add or edit attributes for an existing role, go to **RADIUS > User Roles**. Click the role's name in the list, then click its **Edit** link. The RADIUS Role Editor opens.
   - To add attributes when you create the role, go to **RADIUS > User Roles**, then click the **Create a new role** link. The RADIUS Role Editor form opens.
2. In the **RADIUS Attributes** row, click the **Add Attribute** tab. The row expands to include the RADIUS Attribute Editor.



You can choose to use either the Standard RADIUS attributes that are applicable to all vendors or to use the attributes particular to your vendor.

If you want to use the vendor specific attributes, select the vendor from the drop down list. The available attributes for the selected vendor will be displayed in the drop-down list for the **Attribute** field.

Additional vendors and attributes may be defined in the RADIUS Dictionary. See "Dictionary" for more information in this chapter.

Enter a value for this attribute in the **Value** field. For integer enumerated attributes, choose an appropriate value from the **Value** drop-down list. To calculate the value of the attribute using an expression, See "Dictionary" in this chapter.

Additional attributes can be added by clicking the **Add Attribute** button at the bottom of the window.

When all the attributes have been added, click the **Save Changes** button to create this user role.

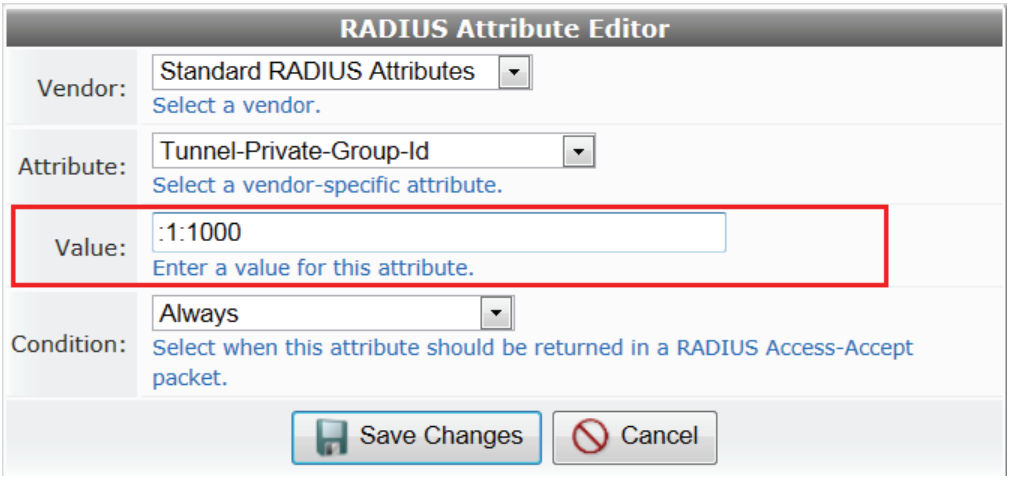
NOTE

You must click the **Save Changes** button before any of the changes you have made will take effect in the user role. A warning message will be displayed if you attempt to navigate away from the RADIUS Role Editor page while there are unsaved changes.

Defining Attribute Tags

Certain attributes, principally those defined in RFC 2868, have a "tag" value associated with them. The tag value is a small number (1 to 31).

To define a tag value for these attributes, prefix the value with the tag number surrounded by colons (**:**). For example, to set the Tunnel-Private-Group-Id attribute to 1000 with a tag of 1, type **:1:1000** into the Value field.



Adding Authorization Conditions to Attribute Definitions

You are able to attach authorization conditions to attribute definitions. The choices for an attribute condition are:

- **Always** – the attribute will always be included in the RADIUS server's response.
- **Never** – the attribute is never included in the response. This option can be used to disable an attribute without deleting it.
- **Enter condition expression…** – the attribute will be included in the response only if the expression is true. See "Example: Time of Day Conditions" and **"Example: Time-Based Authorization"** in this chapter.

Expressions must be entered as PHP code.

Use condition expressions to perform authorization decisions at the time a RADIUS access request is performed. For example, you can alter the authorization for a user role depending on the time of day. It is also possible to refuse access when a certain condition is met.

Several functions are available for use in attribute conditions. See "Standard RADIUS Request Functions" in the Reference chapter for detailed documentation about these functions.

Example: Time of Day Conditions

In this example, the Reply-Message attribute will be modified to provide a greeting to the guest that changes depending on the time of day.

1. Create a new role named **Sample role.**
2. Click the **Add Attribute** tab.
3. Select the Reply-Message attribute from the drop-down list and enter the string value **Good morning, guest.**
4. Select **Enter condition expression...** from the Condition drop-down list and enter the following code in the Expression text field:

   ```
   return date('a') == 'am';
   ```
5. Click the **Add Attribute** tab.
6. Repeat the above steps, but use the string value **Good afternoon, guest** and the following code in the Expression text field:

   ```
   return date('a') == 'pm';
   ```
7. Click the **Save Changes** button to apply the new settings to the role.

Explanation: PHP's **date()** function returns the current time and date; http://www.php.net/date for full details. The 'a' argument will cause the function to return either 'am' or 'pm' depending on the server's current time of day. Finally, the result of the `==` equality comparison is used with the `return` statement to determine which attribute value is included in the response.

Example: Time-Based Authorization

In this example, users will be authorized to access the network only between the local time of 7:30am and 8:00pm.

1. Create a new role named **Sample role.**
2. Click the **Add Attribute** tab.
3. Select the Reply-Message attribute from the drop-down list. Any attribute can be used for this example, because the attribute will never be included in the response.
4. Select **Enter condition expression...** from the Condition drop-down list and enter the following code in the Expression text field:

   ```
   return (date("Hi") < "0730" || date("Hi") >= "2000") &&
   AccessReject();
   ```
5. Click the **Add Attribute** tab.
6. Click the **Save Changes** button to apply the new settings to the role.

Explanation:

- This expression is evaluated every time an Access-Request is made.
- `date("Hi")` is the RADIUS server's local time as hours and minutes with a 24-hour clock (0000, 0001, ..., 0730, 0731, ... 1959, 2000, ..., 2359).
- If it is before 07.30 (`< "0730"`) or after 20.00 (`>= "2000"`) then an Access-Reject will be generated.
- Otherwise, the parenthesized expression will be false, and the attribute will not be sent (nor will an access-reject be sent).

Example: Accounting-Based Authorization

Authorization decisions can also be made based on the accounting records available to the RADIUS server. In this example, users will be authorized only if their total traffic in the past day does not exceed 10 MB.

1. Create a new role named **Sample role.**

2. Click the **Add Attribute** tab.
3. Select the Reply-Message attribute from the drop-down list. Any attribute can be used for this example, because the attribute will never be included in the response.
4. Select **Enter condition expression...** from the Condition drop-down list and enter the following code in the Expression text field:

   ```
   return GetUserTraffic(86400) > 10485760 && AccessReject();
   ```
5. Click the **Add Attribute** tab.
6. Click the **Save Changes** button to apply the new settings to the role.

The GetUserTraffic() function ("GetUserTraffic()" in the Reference chapter) returns the total traffic for the user's sessions in the past 24 hours (86,400 seconds). If this is greater than 10 MB (10,485,760 bytes), the AccessReject() function causes the user's access request to be rejected. Otherwise, the entire expression will evaluate to false, and the user will be authorized. Note that the attribute will not be included in the response, as the condition expression was evaluated to false.

Calculating Attribute Value Expressions

A PHP expression can also be used to calculate the value that the RADIUS server should return for a particular attribute.

To use this feature, use one of these two possible syntaxes when entering the value for an attribute:

- **<?=** *expression* – The PHP expression is evaluated and used as the value for the attribute.
- **<?*php*** *statement*; – The PHP statement is evaluated. To include a value for the attribute, the statement must be a return statement; that is, `return expression;`

A syntax error in the expression or statement will cause all RADIUS authorization requests to fail with an Access-Reject. To use the RADIUS Debugger feature, **See "Debug RADIUS Server"** in this chapter to diagnose any problems with your code in value expressions.

Several predefined functions and variables are available for use in value expressions. **See "View Display Expression Technical Reference"** in the Reference chapter for details.

Example: Using Request Attributes in a Value Expression

In this example, the Reply-Message attribute will be modified to greet the user with their username.

1. Create a new role named **Sample role.**
2. Click the **Add Attribute** tab.
3. Select the Reply-Message attribute from the drop-down list and enter the following value:

   <?= "*Hello*, " . GetAttr("user-name")
4. Select **Always** from the Condition drop-down list and click the **Add Attribute** tab.
5. Click the **Save Changes** button to apply the new settings to the role .

Explanation: See "GetAttr()" . This function returns the value of an attribute that was supplied to the RADIUS server with the Access-Request. Here, the User-Name attribute is retrieved. PHP's string concatenation operator (.) is used to build a greeting message, which will be used as the value of the attribute returned to the NAS in the Access-Accept packet.

Identical behavior could also be achieved using the following code in the attribute's value:

```
<?php return "Hello, " . GetAttr("user-name");
```

Example: Location-Specific VLAN Assignment

In this example, the value of a vendor-specific VLAN attribute will be modified based on the NAS to which visitors are connecting.

The network has an Aruba wireless controller at 192.168.30.2 which should be configured to place all visitor traffic into VLAN ID 100. There is another Aruba wireless controller at 192.168.40.2 which should be configured to place visitor traffic into VLAN ID 200.

1. Create a new role named **Sample role**
2. Click the **Add Attribute** tab.
3. Select the **Aruba** vendor, and then select **the Aruba-User-Vlan** attribute from the drop-down list. Enter the following value for the attribute:
   ```
   <?= GetAttr('NAS-IP-Address') == '192.168.30.2' ? '100' : '200'
   ```
4. Select **Always** from the Condition drop-down list and click the **Add Attribute** button.
5. Click the **Save Changes** button to apply the new settings to the role.

Explanation: The GetAttr() function returns the value of an attribute that was supplied to the RADIUS server with the Access-Request. Here, the NAS-IP-Address attribute is retrieved, which will contain the IP address of the NAS making the RADIUS request. PHP's ternary operator (`?:`) is used to check if the NAS is 192.168.30.2; if it is, then 100 is returned as the VLAN ID. In all other cases, the value 200 is returned as the VLAN ID.

Multiple ternary statements can be nested in parentheses to allow more than two values to be checked. For example, to check against three values, and return a default value if none of the values are matched, use a PHP expression like the following:

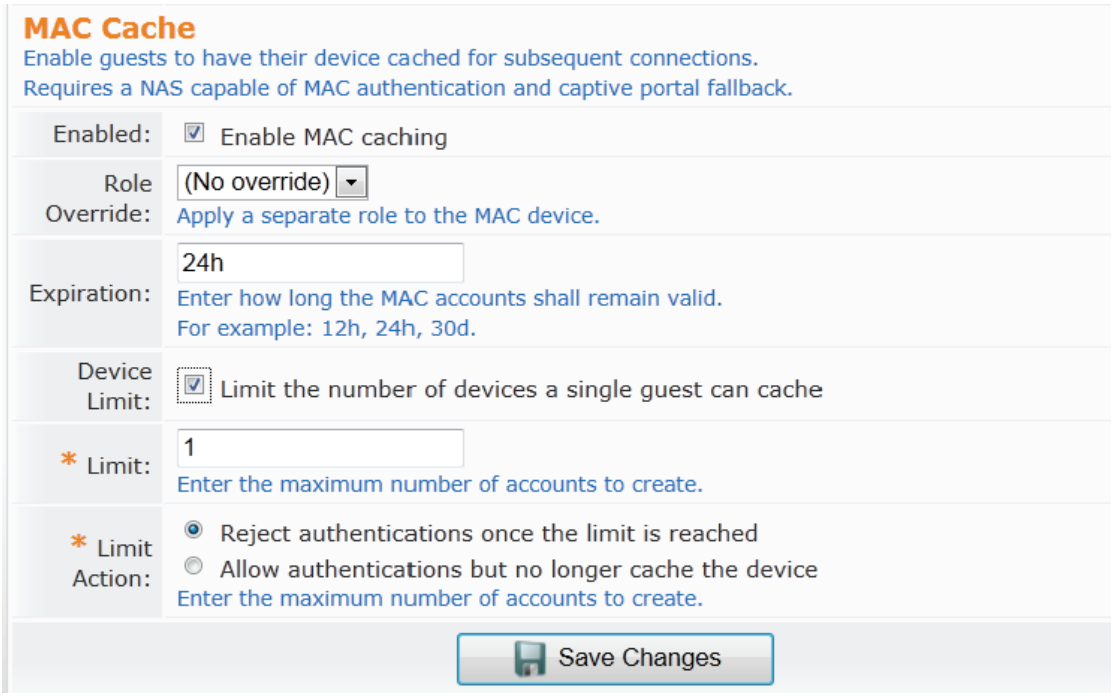
```
(GetAttr('NAS-IP-Address') == 'value1' ? 'result1' : (GetAttr('NAS-IP-Address') ==
'value2' ? 'result2' : (GetAttr('NAS-IP-Address') == 'value3' ? 'result3' :
'default_value')))
```

Configuring MAC Caching During User Authentication

You can control MAC caching during user authentication without having to write complex expressions within the role.

To configure MAC device caching for a role during user authentication:

1. Go to **RADIUS > User Roles** and click the role's row, then click its **Edit** link. The RADIUS Role Editor form opens.
2. In the **MAC Cache** area at the bottom of the form, mark the **Enabled** check box. The form expands to include options for the role override, expiration, and device limit settings.



3. Complete the **Role Override**, **Expiration**, **Device Limit**, account **Limit**, and **Limit Action** fields with the appropriate information, then click **Save Changes**.

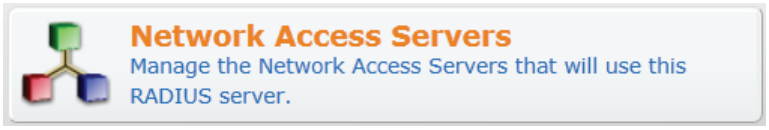
Network Access Servers

A **Network Access Server** (NAS) is a 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 packet) is generated by the NAS.

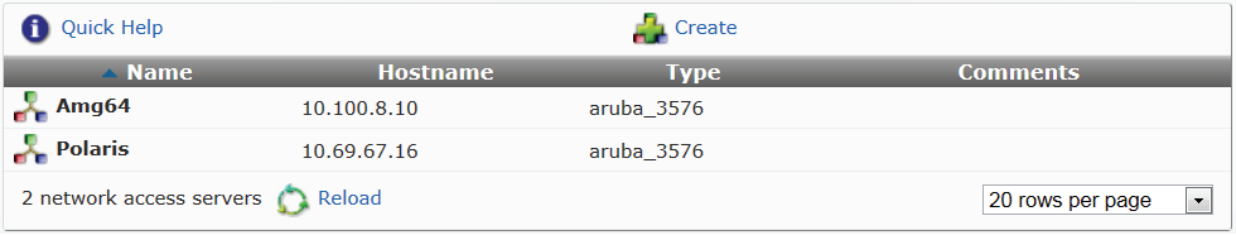
Network access servers are RADIUS clients, and must be predefined in order to access the RADIUS server. For security, each NAS device must also have a shared secret which is known only to the device and the RADIUS server.

To manage network access servers:

- Go to **RADIUS > Network Access Servers**.



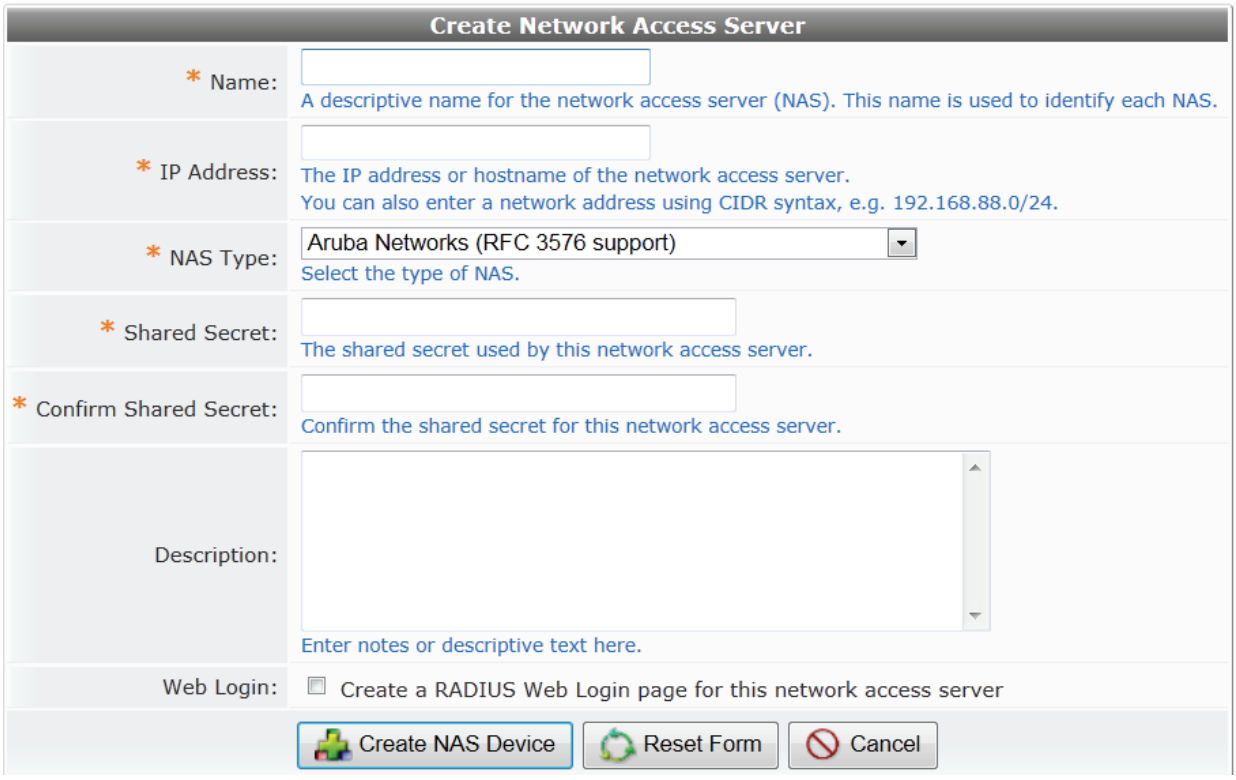
The Network Access Servers list opens.



Use the Network Access Servers list view to define the NAS devices for this server and to make changes to existing NAS devices.

Creating a Network Access Server Entry

A new NAS device is added by clicking on the **Create** tab.



The NAS name is used in the RADIUS server log to identify access requests from NAS servers. This name must be unique.

The NAS type is selected from a drop down list with the following predefined types:

- Other NAS
- RFC 3576 Dynamic Authorization Extensions Compatible
- Aerohive (RFC 3576 support)
- Aruba Networks (RFC 3576 support)
- Aruba Networks
- Bluesocket
- Chillispot (RFC 3576 support)
- Cisco
- Cisco (RFC 3576 support)
- Colubris/HP
- Consentry Networks
- Enterasys
- Extreme Networks
- Extricom
- Infoblox
- Juniper Networks
- Meraki
- Meru Networks

- Motorola (RFC 3576 support)
- Ruckus Networks
- Trapeze Networks (RFC 3576 support)
- Trendnet
- Xirrus

RFC 3576 is used by the RADIUS server to request that a NAS disconnect or reauthorize a session that was previously authorized by the RADIUS server.

If your NAS vendor is not listed, select the "Other NAS" option. If the NAS is known to support RFC 3576, select the "RFC 3576 Dynamic Authorization Extensions Compatible" option. See "RFC 3576 Dynamic Authorization" in the Guest Management chapter for more information about RFC 3576.

The Shared Secret is used to ensure the security of the authentication request to ClearPass Guest. It can be a passphrase or a random set of ASCII characters up to 64 characters in length. The term "shared secret" is used because the same value must be configured on both the RADIUS client and the RADIUS server.

The Web Login check box is displayed when certain vendors are selected. Select this option to automatically create a corresponding RADIUS Web Login page for this NAS. See "Example: Time-Based Authorization" in this chapter for details on customizing this page.

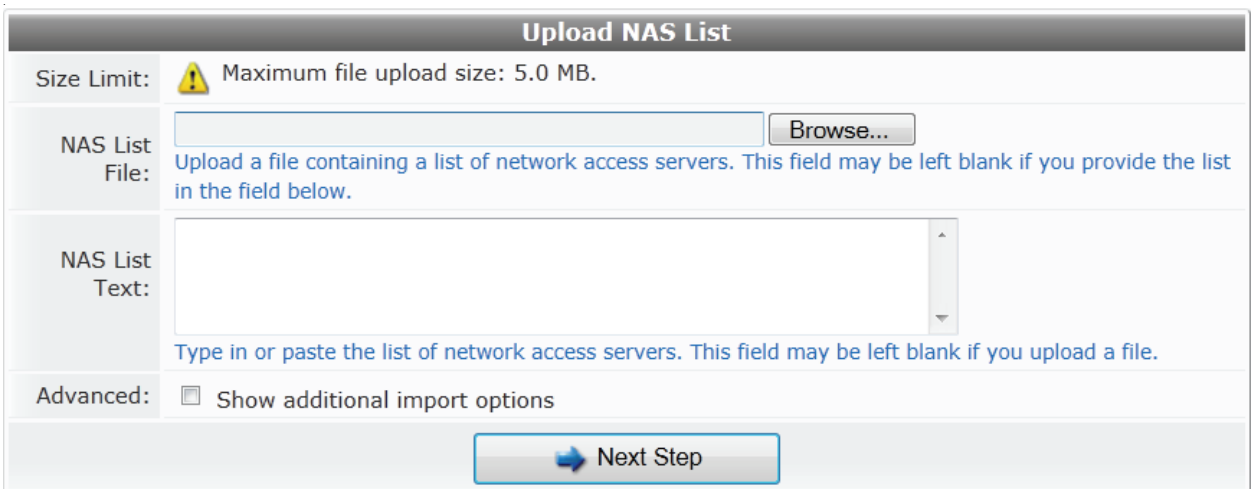
Click the **Create NAS Device** button to create this NAS. If you do not want to proceed, click the **Reset Form** button to cancel your entry.

Once a NAS entry has been created, it can be edited, deleted or pinged by clicking on it.

Importing a List of Network Access Servers

NAS entries may be created from an existing list by uploading the list to ClearPass Guest. Click the **Import a list of network access servers** link on the NAS List page to start the process.

The Upload NAS List form provides you with different options for importing a list of servers



To complete the form, you must either specify a file containing the server information, or type or paste in the NAS information to the NAS List Text area.

Advanced import options may be specified by selecting the **Show additional import options** check box.

ClearPass Guest uses the UTF-8 character set encoding internally to store NAS server properties. If your file is not encoded in UTF-8, the import may fail or produce unexpected results if non-ASCII characters are used. To avoid this, you should specify what character set encoding you are using.

The format of the NAS list file is automatically detected. You may specify a particular encoding if the automatic detection is not suitable for your data.

Select the **Force first row as header row** check box if your data contains a header row that specifies the field names. This option is only required if the header row is not automatically detected.

Click the **Next Step** button to upload the data.

In step 2 of 3, the format of the uploaded data is determined and the appropriate fields are matched to the data. The first few records in the data will be displayed, together with any automatically detected field names.

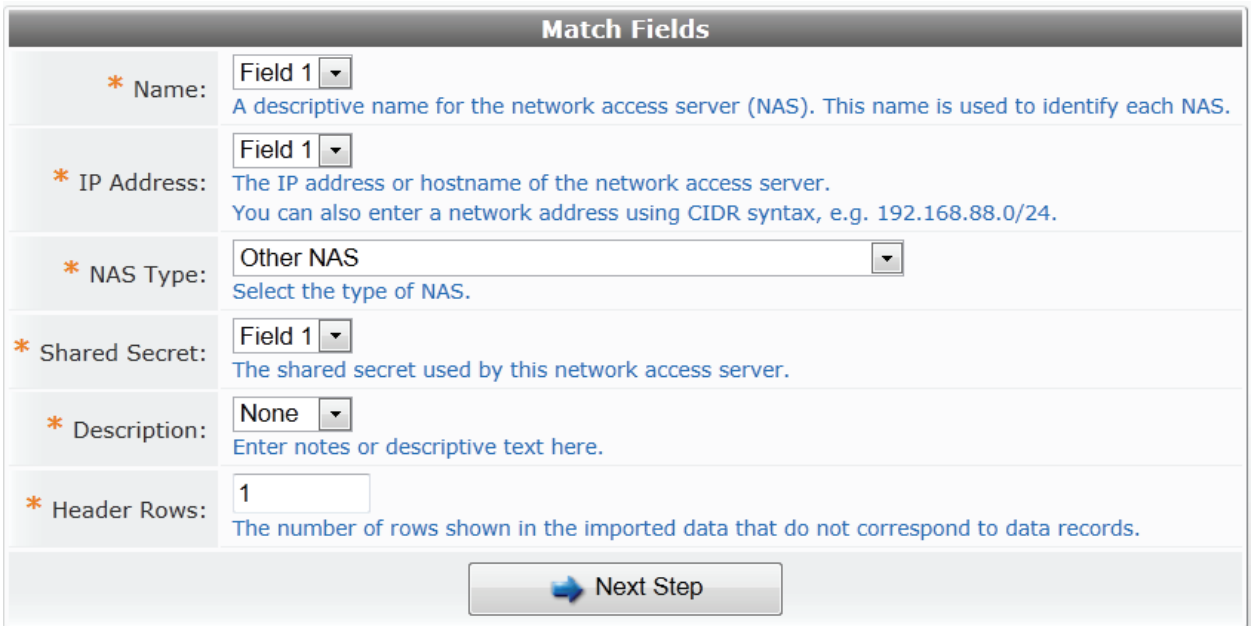
For example, the following data was used:

```
server1,192.168.22.10,Radius_Secret
server2,192.168.22.11,Radius_Secret
server3,192.168.22.12,Radius_Secret
external,10.22.0.10,Rmd*3n2pEfz9
```

Because this data does not include a header row that contains field names, the corresponding fields must be identified in the data:

Record	Field 1	Field 2	Field 3
1	server1	192.168.22.10	Radius_Secret
2	server2	192.168.22.11	Radius_Secret
3	server3	192.168.22.12	Radius_Secret
4	external	10.22.0.10	Rmd*3n2pEfz9

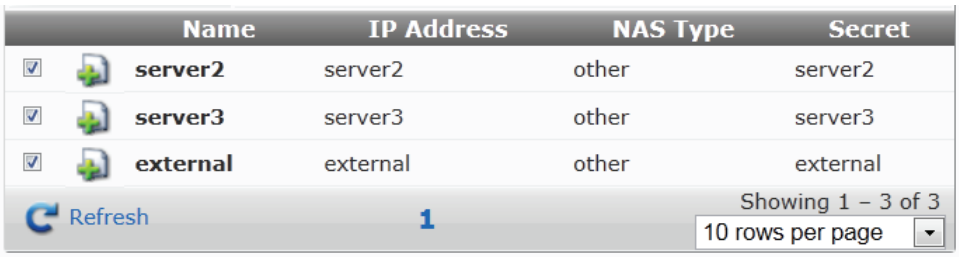
Use the **Match Fields** form to identify which NAS server fields are present in the imported data. You can also specify the values to be used for fields that are not present in the data.



To complete the **Match Fields** form, make a selection from each of the drop-down lists. Choose a column name (Field 1, Field 2, etc.) to use the values from that column when importing the NAS entries, or select one of the other available options to use a fixed value.

Click the **Next Step** button to preview the final result.

In step 3 of 3, a preview of the import operation is displayed. The properties of each NAS are determined, and any conflicts with existing NAS entries are displayed



Select the NAS entries to be created or updated with the imported data. The icon displayed in each row indicates if it is a new entry ( ) or if an existing NAS entry will be updated ( ).

Click the **Update existing entries** check box to select or unselect all existing NAS entries in the list.

Click the **Create Network Access Servers** button to finish the import process. The selected items will be created or updated.

A completion screen is then displayed, showing the results of the import operation.

You must restart the RADIUS server in order for the new NAS entries to be recognized. See "Server Control" in this chapter for more information.

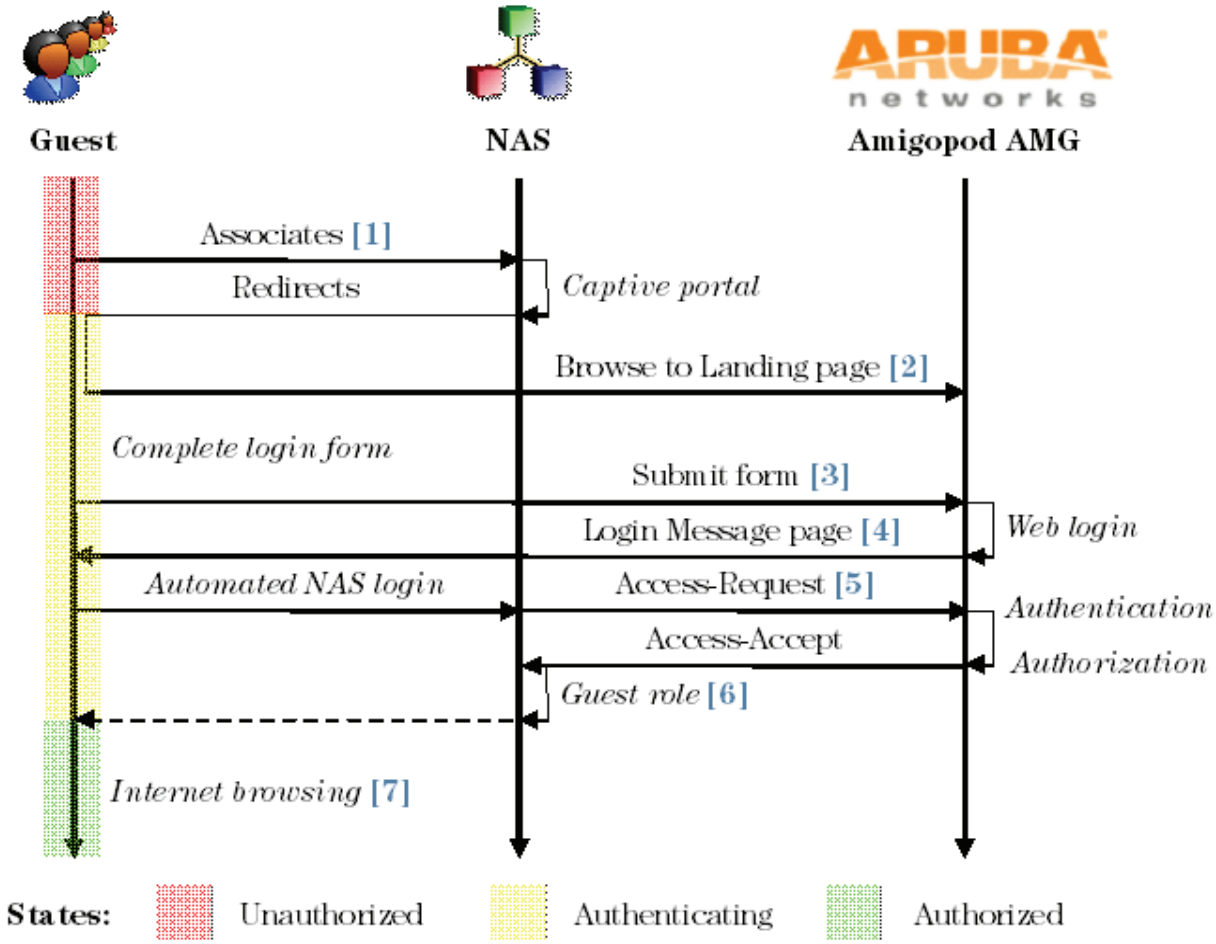
Web Logins

Many NAS devices support Web-based authentication for visitors.

When you use ClearPass Guest to define a Web login page, you can provide a customized login page for visitors who access the network through these NAS devices.

The sequence diagram in Figure 17 shows the login process for guests using a Web login page.

Figure 17 *Sequence diagram for guest captive portal and Web login*



In a typical configuration, you would enable the captive portal functionality of your NAS [1], and use the URL of your custom Web login page as the default portal landing page [2] for unauthorized guests.

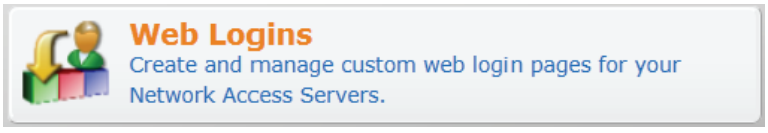
When the login form is submitted [3], the Login Message page is displayed to the visitor [4]. A subsequent automatic redirect to the NAS will perform the actual login [5], which invokes the AAA process. If this is successful, the NAS will apply the appropriate security policy to the visitor's session [6], enabling them to start browsing the Internet [7].

In this way you can provide a branded and customized login page that is integrated with your existing network access devices.

Use this list view to define new Web login pages, and to make changes to existing Web login pages.

Creating a Web Login Page

To create a new Web login page, navigate to **Customization > Web Logins**.

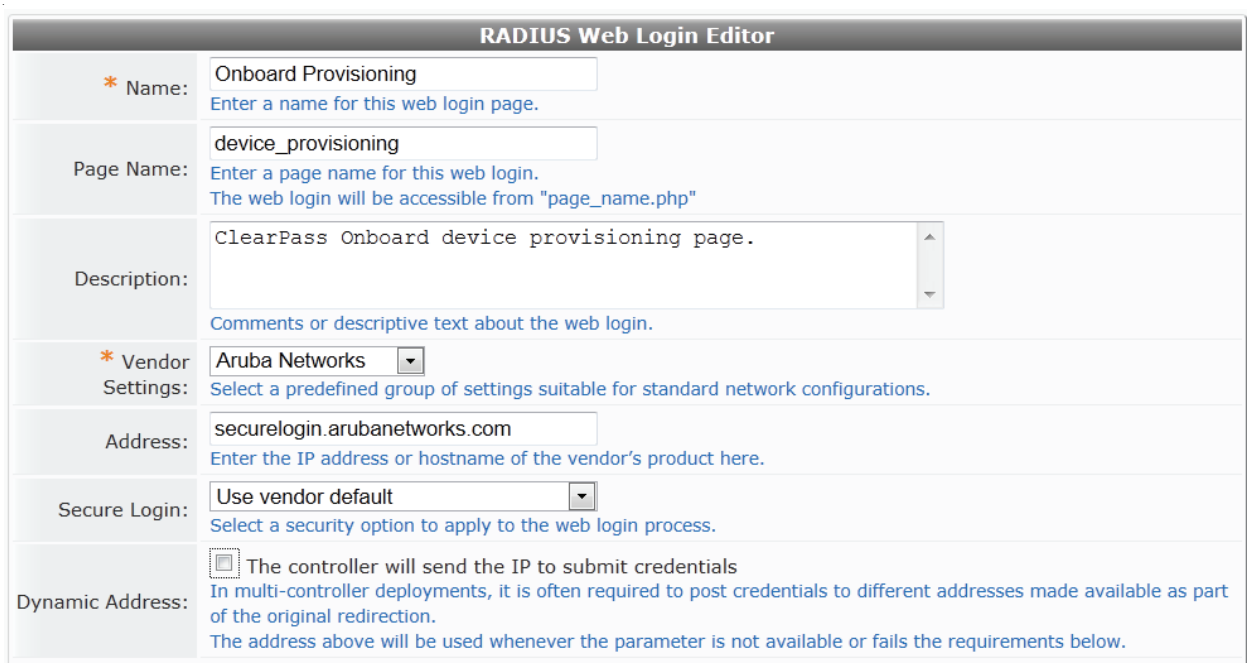


Click **Create a new Web login page** to create a Web login page for your guests.

There are seven sections to this form.

The first section requires that you enter a name for this login page, as well as an optional page name. You can also provide an optional description of the login page.

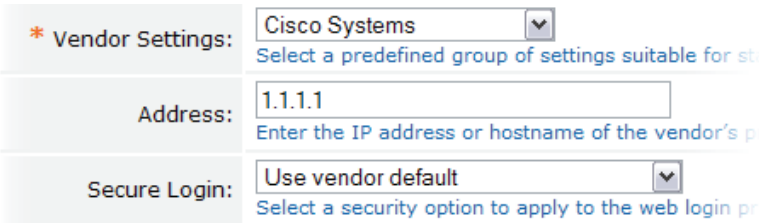
To use predefined network settings for NAS equipment, select the appropriate vendor in the Vendor Settings drop-down list. If your NAS vendor is not listed, or if you would prefer to customize all aspects of the Web login page, choose Custom Settings



NOTE

Changing the vendor settings may overwrite any customizations you have made to the Header HTML and Footer HTML.

If you have chosen a specific vendor, the form will display additional options:



The Address option allows you to set the IP address for the NAS, as it will be visible to the guest network. The Secure Login option controls whether the NAS login should be performed using HTTP or HTTPS.

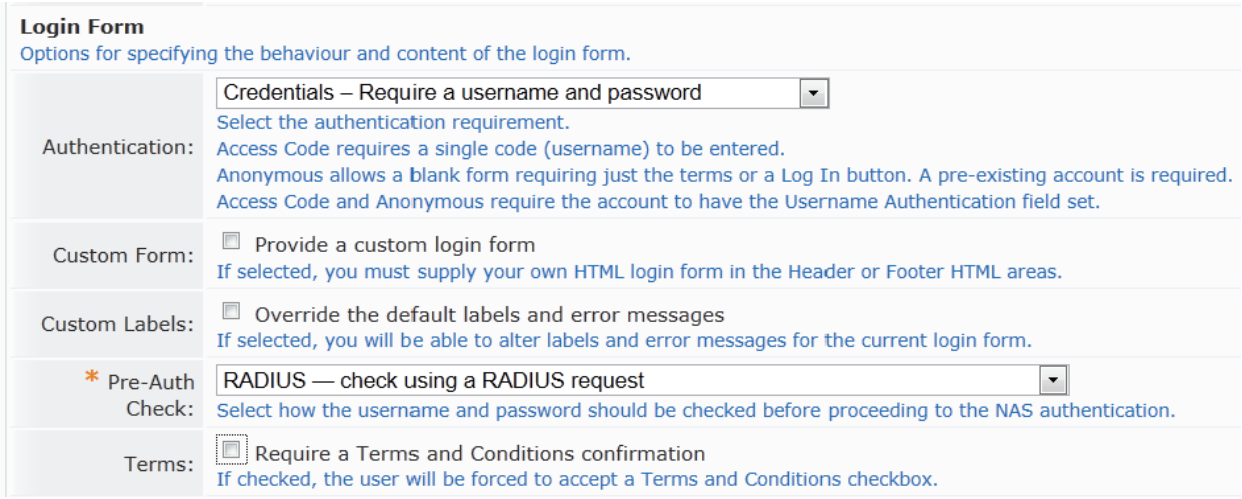
NOTE

The vendor's address or hostname must be available to the guest. The DNS may differ for guests and the operator on the LAN side. If you select Aruba Networks in the Vendor Settings field, then the Aruba controller's IP address (hostname or IP address only) *must* be entered in the Address field as no other entries are supported.

When the Dynamic Address check box is selected, the NAS login can be performed using the controller's IP address as provided to the client. For example, when using an Aruba Networks controller, the controller performing the redirect sends its IP address using the "switchip" parameter. To use this address for the guest login, enable the Dynamic Address check box.

When using this option, the guest's username and password credentials will be sent to a value provided in the URL. As this is a potential security hazard, enter the known IP addresses of the controllers in your network in the Allowed Dynamic and Denied Dynamic fields, to prevent an information leak vulnerability that could be exploited by guest users on your network.

The second section requires you to specify the behavior of the Web login form. There may only be some fields displayed here, depending on which of the Vendor Settings you have chosen.



The Authentication field provides three options:

- **Credentials**—a username and password. The guest is prompted for a username and password to log in to the network.
- **Access Code**—Requires only username for authentication. The guest's password is automatically provided for the login attempt.
- **Anonymous**—This option supports two special usernames: **_mac** and underscore (_).

  When Anonymous is selected, two usernames may be used to enable specific behavior. The guest is not prompted for a username and password; a fixed set of credentials will be used for all guest logins. If you select this option, then the Auto-generate (optional) and Anonymous User (required) fields display.

  - **_mac**: This populates the username and password with the user's MAC if the user is detected on the system. To enable this first navigate to **Administrator > Plugin Manager > MAC Authentication Plugin**. Select the **Configuration** icon to display the MAC Authentication Plugin page. Select the **Allow users to be detected via their MAC address** option and click **Save Configuration**.

    On the RADIUS Web Login page, select **Anonymous** in the **Authentication** field. Check the **Auto-generate the anonymous** account option. Make sure to select the Pre-Auth Check option **Local – match a local account** and save the configuration.
  - **Underscore** (_): Leaves the username and password blank and requires post-processing in the header or footer.

Pre-authentication checks now take place:

- **None — No checks will be made**: No checks are made before redirecting to the NAS login.
- **Local —Match local account:** Checks the entered username and password before redirecting to the NAS login.
- **RADIUS — Check using RADIUS request**: Checks the local database and external authenticationservers for the provided credentials. This provides authentication of the user regardless of where the account is defined.

When the Web login form is submitted, the username and password are submitted to the NAS using the field names specified in Username Field and Password Field:

- The visitor's username is submitted to the NAS, with any suffix provided in Username Suffix appended to the username. If the username suffix is blank, the username is not modified.
- The visitor's password will be submitted to the NAS unmodified if the Password Encryption option No encryption (plaintext password) is selected. Otherwise, See "Universal Access Method (UAM) Password Encryption" in this chapter for details about the supported password encryption methods.


NOTE

When **Local – Match local account** is selected, user accounts defined in Guest Manager will be permitted; user accounts defined in external authentication services will not be permitted to log in

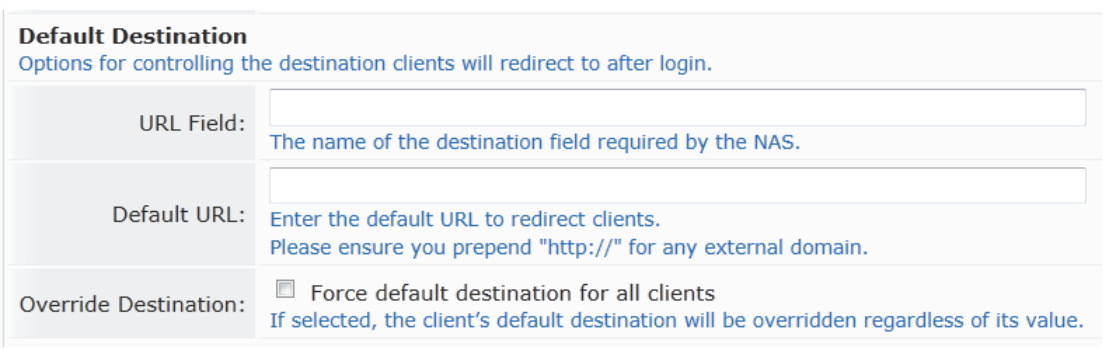
Select the **Require a Terms and Conditions confirmation** check box to add a check box to the login page that indicates the visitor has read and agreed to the terms and conditions of use. If this option has been selected, the check box must be ticked before the login can proceed.

Select the **Override the default labels and error messages** check box to customize the text displayed in the login form. If this option is selected, additional fields will be displayed for the Username Label, Password Label, Login In Label, and the Terms Label, Terms Text and Terms Error if the terms and conditions confirmation option has also been selected. Use these fields to enter text that is appropriate for your deployment.

You can provide extra fields if required by your NAS device, and perform processing on parameters that have been supplied by the NAS during the redirect to the Web login page. See "NAS Redirect Parameters" and **"NAS Login Parameters"** in this chapter for details about these parameters.

The NAS parameters and any extra fields specified are available for use within the Submit URL, which may be a template expression. This allows for complex processing of the input if required. See "Using Web Login Parameters" in this chapter for details about using Web login parameters.

The fourth section allows you to control the destination that clients will be redirected to after login



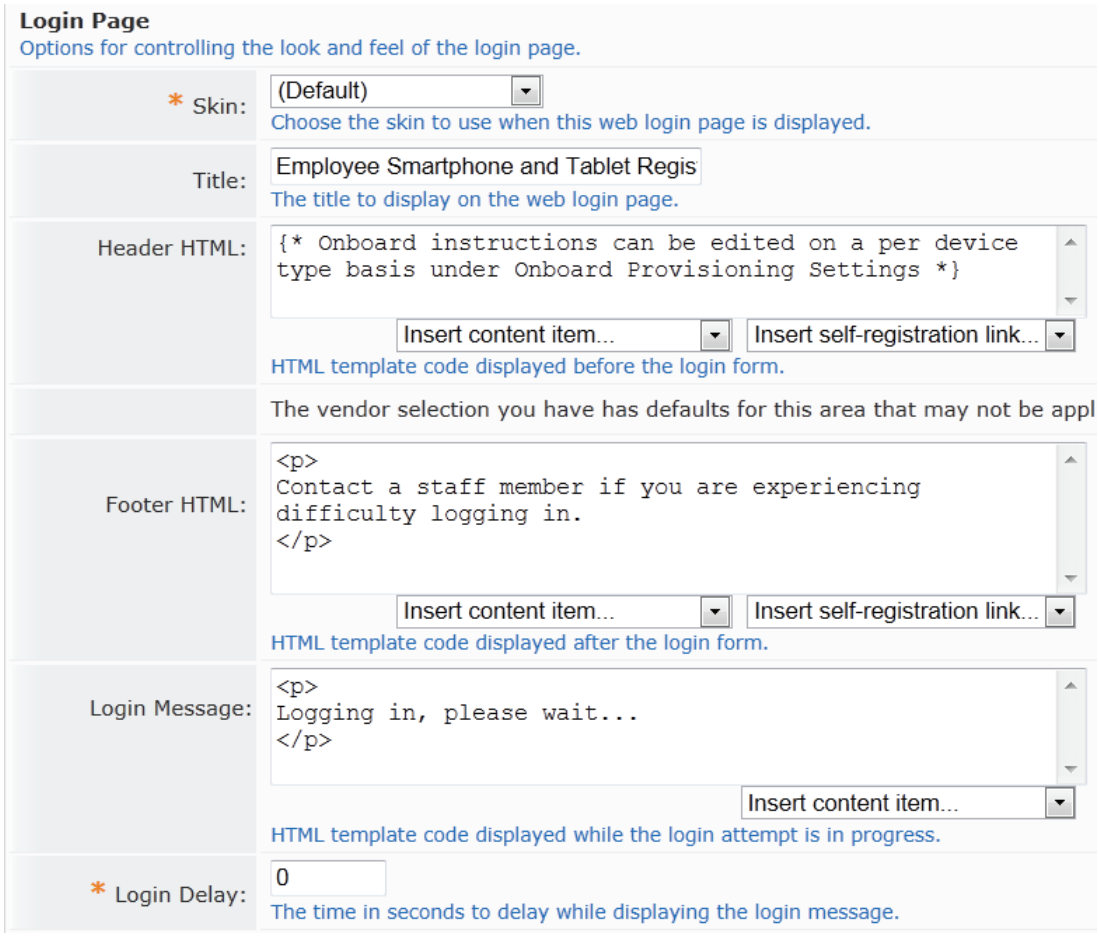
The NAS is responsible for redirecting a visitor to their original destination after a successful login attempt. The URL Field is the name of a parameter supplied to the NAS that contains the visitor's redirection URL.

Normally, this parameter will be provided automatically by the NAS when the visitor is redirected to the Web login page. However, you can use the Default URL field to provide a destination for clients that do not specify a redirection URL. Select the **Force default destination for all clients** check box to cause all visitor access to redirect to the Default URL after login, instead of the visitor's intended access.


NOTE

Be sure to use a fully-qualified URL, such as http://www.example.com. The http:// prefix is an important part of the URL.

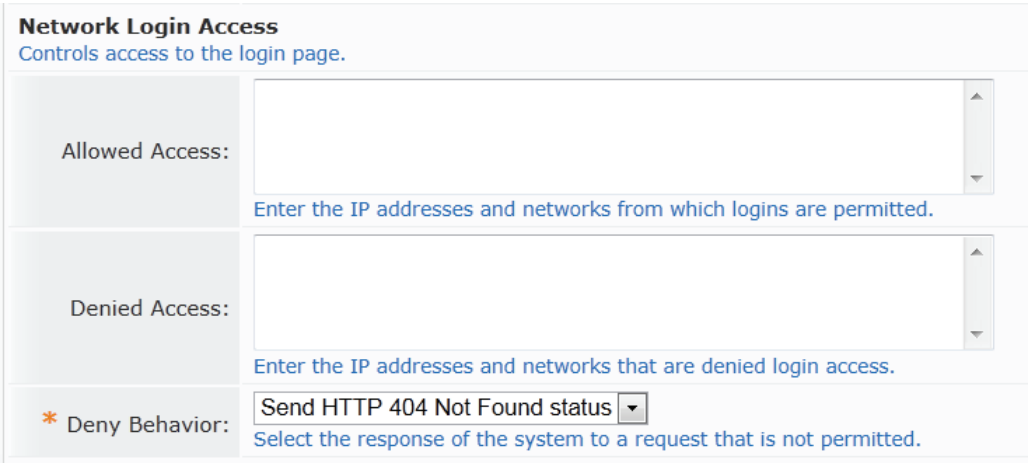
The fifth section allows you to control the look and feel of the login page.



Use the **Insert self-registration link...** drop-down list to insert HTML code that creates a link to an existing guest self-registration page. This may be of use when you are creating a landing page suitable for both registered and unregistered visitors.

You are able to optionally create a login message in this section. This could be used to welcome the guest and outline the terms of usage. The login message is only displayed for the time specified in the Login Delay.

The sixth section allows you to specify access controls for the Web login page.



The 'Allowed Access' and 'Denied Access' fields are access control lists that determine if a client is permitted to access this Web login page. You can specify multiple IP addresses and networks, one per line, using the following syntax:

- **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

The 'Deny Behavior' drop-down list may be used to specify the action to take when access is denied.

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 **0.0.0.0/0**.

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 list, then the client will be denied access. If the matching rule is in the Allowed Access list, then the client will be permitted access.

If the Allowed Access list is empty, all access will be allowed, except to clients with an IP address that matches any of the entries in the Denied Access list. This behavior is equivalent to adding the entry **0.0.0.0/0** to the Allowed Access list.

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 **0.0.0.0/0** to the Denied Access list.

Universal Access Method (UAM) Password Encryption

Two different forms of password encryption are supported for the Web login page. These are:

- **UAM basic** – Equivalent to the Password Authentication Protocol (PAP) scheme.
- **UAM with shared secret** – Equivalent to the Challenge Handshake Authentication Protocol (CHAP) scheme.

When using either of these schemes, the NAS must supply a parameter named **challenge** to the Web login page. This parameter should be a string of hexadecimal digits ("hexadecimal challenge string") encoding a binary value at least 128 bits long ("binary challenge").

The challenge is used to encrypt the user's password as follows:

- **UAM basic** – The user's password is XORed bytewise with the supplied binary challenge. The result is encoded as a string of hexadecimal characters.
- **UAM with shared secret** – The MD5 checksum of the binary challenge followed by the predefined UAM secret is computed ("checksum challenge"). The encrypted password is the hexadecimal MD5 checksum of a stream consisting of a null byte followed by the user's plaintext password and the hexadecimal checksum challenge.

NAS Redirect Parameters

The NAS may supply additional parameters when redirecting the user to the Web login page. These are supported and will be passed back to the NAS along with the variables that are defined as part of the Web login form.

For example, some wireless network equipment will pass a "wlan" parameter that contains the user's ESSID to the login page. This might result in the following redirect URL:

```
http://192.168.88.88/weblogin.php/4?wlan=clearpass-guest
```

This will in turn result in a hidden field included in the Web login form. The field will be named **wlan** and will be set to the value **ClearPass Guest**.

NAS Login Parameters

Extra fields in the **NAS login** form may be defined using **name=value** pairs in the Web login form configuration. This allows you to specify values required by a particular NAS to log in, or to override values supplied by a NAS.

You can also remove a NAS-supplied field from the form. To do this, list only the name of the field in the Extra Fields, without any equals sign or value for the field. By doing this, any value set for the field will be removed when the form is submitted.

To set a value for a field, but only if the NAS did not supply a value for this field, use the syntax **name!=value**. This can be used to provide a default parameter to the NAS, if the user was redirected without the parameter.

To rename a field, specify the old and new names using the syntax **oldname|newname**.

The table below summarizes the syntax that is available in the Web login page extra fields:

Table 18 *Web Login Page Syntax*

Syntax	Meaning
name=value	Sets field to a specific value; will override any NAS-provided value for this field
name={$value|…}	Sets field to a value determined by evaluating the template expression; will override any NAS-provided value for this field
name!=*value*	Sets field to a value, but only if the field was not provided in the redirect to the Web login page. The value may be a template expression.
name	Removes field provided by the NAS; this field will not be submitted to the NAS.
old|new	Renames the field “old” to “new” and keeps its value.
old|new=*value*	Renames the field “old” to “new” and assigns a new value.

Using Web Login Parameters

The parameters passed to the Web login page can be used within the template code. Each parameter is defined as a page variable with the same name. You can use the syntax **{$var}** to display the value of the parameter **var**. More complicated expressions can be built using Smarty template syntax. See “Smarty Template Syntax” in the Reference chapter for details.


NOTE

To display a list of all the parameters available for use on the page, add the following template code to the Footer HTML:

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

The NAS redirect parameters are also automatically stored as the properties of a session variable called **$extra_fields**. You can use this variable to remember the NAS parameters when redirecting the user to a different page that does not include the parameters in the URL.

To access the value of a remembered field called “wlan”, use the syntax:

```
{$extra_fields.wlan}
```

To display all the remembered fields for the current visitor session, use the syntax:

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

Apple Captive Network Assistant Bypass with ClearPass Guest

This section describes the process for leveraging the captive portal to bypass the Captive Network Assistant (Web sheet) that is displayed on iOS devices such as iPhones, iPad, and more recently Mac OS X machines running Lion (10.7).

Based on the suggested configuration in this guide, the combination of an Aruba Wi-Fi network and ClearPass Guest can be used effectively to bypass the Captive Network Assistant technology implemented by Apple in various of their Wi-Fi enabled mobile devices.

The need to bypass this Web sheet solution for prompting users to perform a Web authentication task will largely be driven by the customer design and need to control the user experience as guest or public access users authenticate to the network.

By enabling a full client Web browser based authentication, this solution enables fully customized Web login experience to be developed and presented through the ClearPass Guest portal options.

Some examples of use cases for the browser-based authentication are as follows but certainly not limited to:

- Display of a welcome page to host session statistics, logout button, link to continue to original destination
- Display of an interstitial page for the display of advertising media before being granted access to the Internet
- Based on browser detection, display a promotional link to a mobile device App from associated App Store for retail applications
- Provide mobile device App based Web authentication for transparent Wi-Fi access in retail application
- Mobile Device Access Control (MDAC) environments where the Web authentication process is used to push
- Device configurations and client certificates to mobile devices.

This Web sheet is displayed on iOS devices when a device connects to a Wi-Fi network that has been configured with Open security, such as those typically found in guest access networks or public hotspots.

The benefit of this feature provided by Apple is to automatically prompt users to log in to the detected Captive Portal network without the need to explicitly open a Web browser. This is useful on mobile devices where many of the common applications are not browser based such as email, social networking applications, media streaming and these applications would otherwise fail to connect without the successful browser based authentication.

The Apple operating systems detect the presence of a Captive Portal enabled network by attempting to request a Web page from the Apple public Web site. This HTTP GET process retrieves a simple success.html file from the Apple Web servers and the operating system uses the successful receipt of this file to assume that it is connected to an Open network without the requirement for Captive Portal style authentication.

If the success.html file is not received, the operating system conversely assumes there is a Captive Portal in place and presents the Web sheet automatically to prompt the user to perform a Web authentication task.

Once the Web authentication has successfully completed, the Web sheet window will be automatically closed down and therefore preventing the display of any subsequent welcome pages or redirecting the user to their configured home page.

Also if the user chooses to cancel the Web sheet, the Wi-Fi connection to the Open network will be dropped automatically preventing any further interaction via the full browser or other applications. The following are examples of these Web sheet sessions from a Mac OS X Lion (10.7) laptop, iPad and an iPhone.

Figure 18 *Captive Network Assistant on MacOS X*

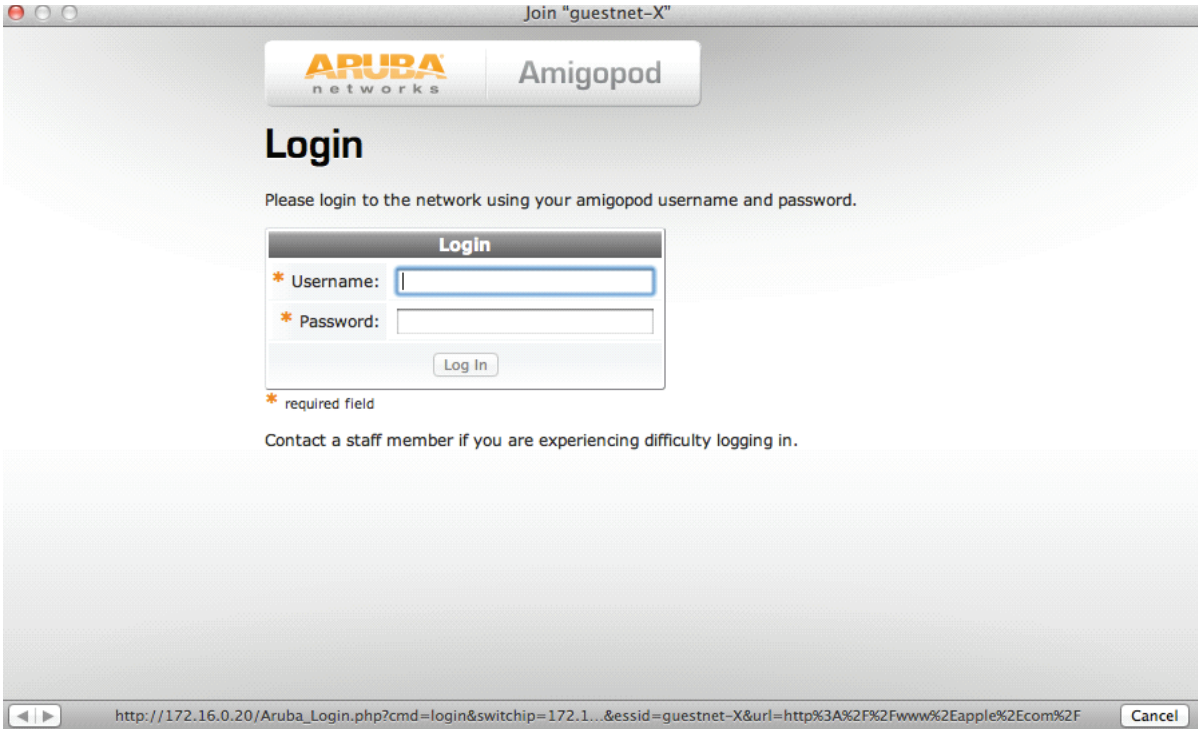


Figure 19 *Captive Network Assistant on iPad*

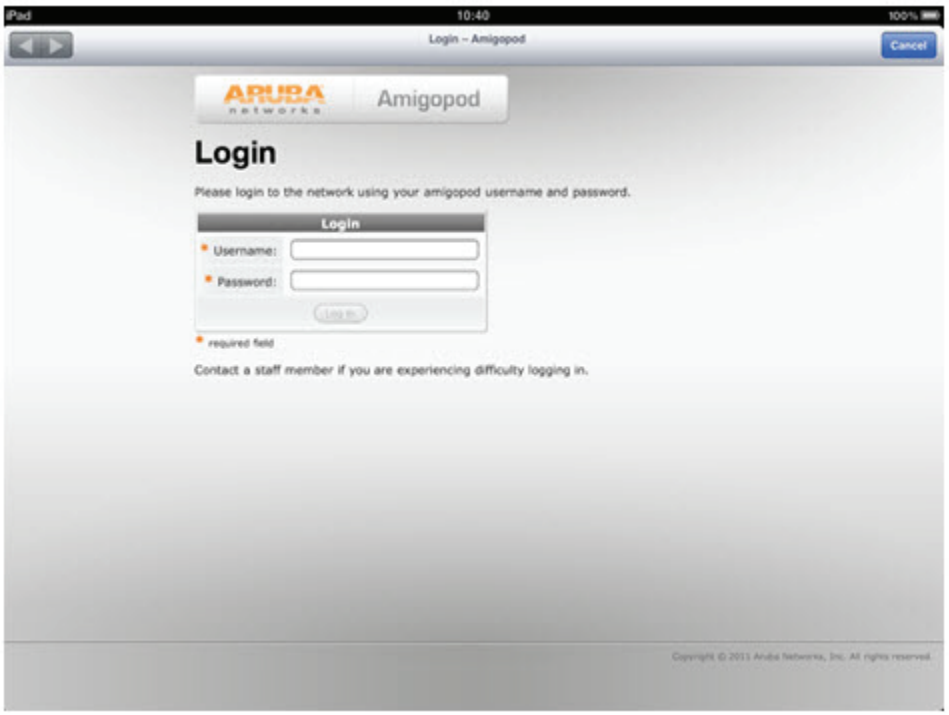
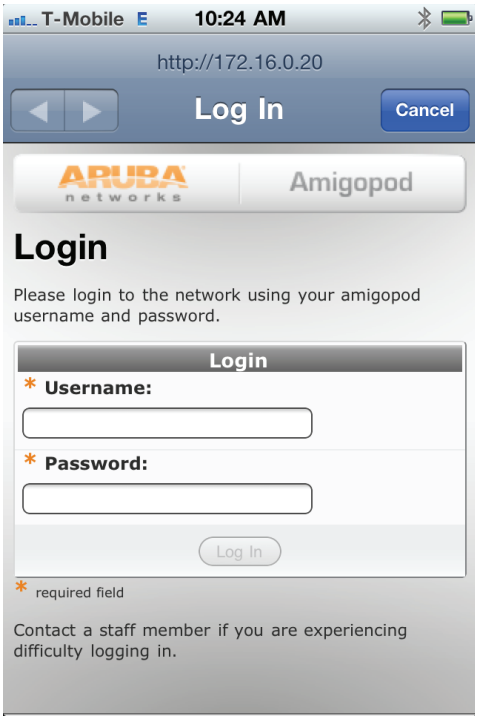


Figure 20 *Captive Network Assistant on iPhone*



The Web sheet can be easily identified by the lack of a URL bar at the top of the screen and typical menu bar items.

For many customers, this behavior of their Apple wireless devices will be acceptable and a great usability enhancement for their user community.

There are, however, particular guest access or public access designs where the use of this Web sheet and the lack of ability to control the entire Web authentication user experience is not desirable.

For these customer scenarios, there is a method of bypassing the display of the Web sheet on the Mac OS X Lion or iOS devices. The main driver for this implementation is to restore the ability to control the user experience and display post authentication welcome pages or redirect the Wi-Fi users to their originally requested Web page.

Alternatively, where SSL secured connections are implemented on both the Aruba controller and ClearPass Guest Web Login pages, testing of the recommended Captive Portal configuration has shown to also prevent the display of the Captive Network Assistant on Apple devices. It appears that the redirect process to the HTTPS hosted Web Login page on ClearPass Guest prevents the display of the Web sheet, and it is assumed that the Captive Network Assistant only supports HTTP. This recommended approach of using HTTPS to avoid user credentials being passed in the clear for guest and public access networks requires the installation of trusted server certificates on both the controller and ClearPass Guest. For some customers where securing these user credentials is not essential (for example in Anonymous login designs) the solution proposed in this guide provides the same desired result using HTTP as the transport for the Web authentication traffic.

Solution Implementation

In a typical deployment integrating with an ArubaOS controller, the Captive Portal profile is configured to redirect all unauthenticated users to the external Captive Portal page hosted on ClearPass Guest.

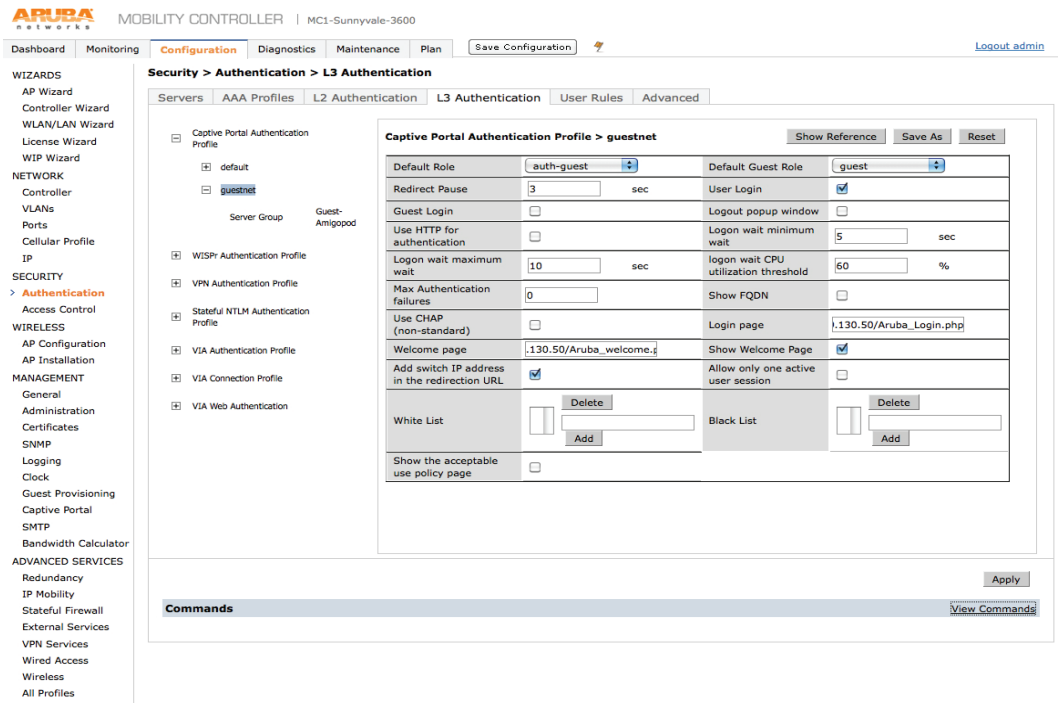
For further details on the recommended configuration of both ClearPass Guest and the ArubaOS controllers, please refer to the Amigopod & ArubaOS Integration Application Note available for download from the following location: http://www.arubanetworks.com/vrd/

The following CLI and WebUI examples show a typical configuration of the Captive Portal profile. The login page is set to point directly to the hosted Web Login page.: http://10.169.130.50/Aruba_Login.php

Captive Portal Profile Configuration

```
aaa authentication captive-portal "guestnet"
   default-role auth-guest
   direct-pause 3
   no logout-popup-window
   login-page http://10.169.130.50/Aruba_Login.php
   welcome-page http://10.169.130.50/Aruba_welcome.php
   switchip-in-redirection-url
```

Figure 21 *Captive Portal Profile Configuration*



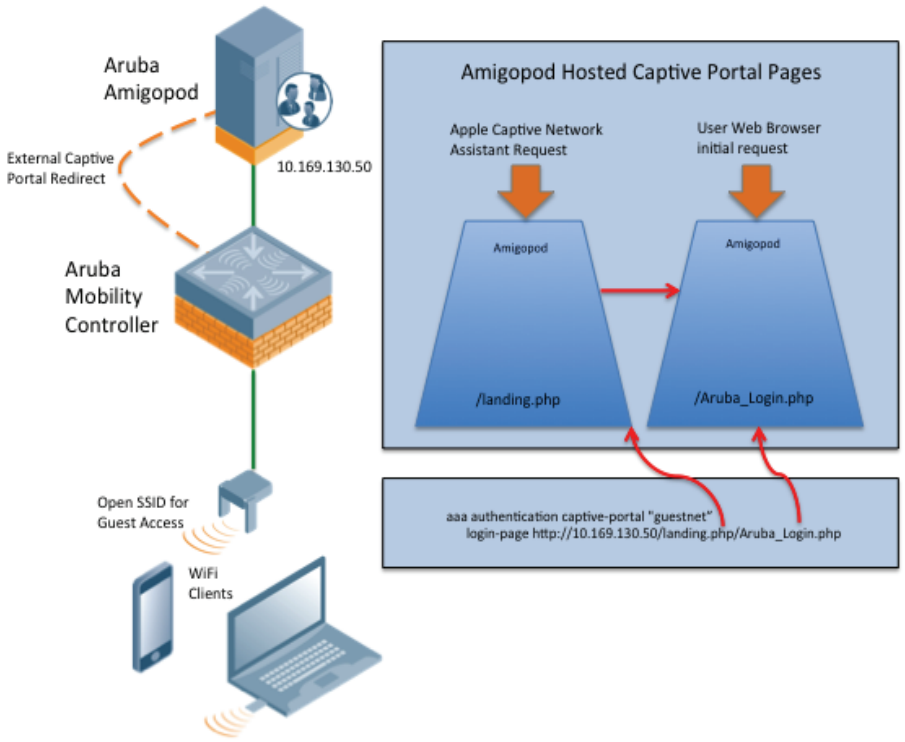
An embedded URL within the portal configuration is designed to address the issue of bypassing the mini browser. This page is available at the following URL: http://<server IP or FQDN>/landing.php/

The Web page includes logic to detect the presence of an iOS device or Mac OS X Lion machine being redirected as part of the Aruba controller Captive Portal configuration. If these devices are detected, their initial request to the Apple Web site will be served locally from the ClearPass Guest server, emulating the environment of an Open connection to the Internet. By emulating the response from the Apple Web site, the iOS device or Mac OS X machine will no longer initiate the Captive Network Assistant and the user can launch their local browser manually as desired.

Now that the devices are able to open the local browser, any subsequent attempt to access the Internet will be redirected to the ClearPass Guest server. This function will then differentiate between this Web browser request and the previous Captive Network Assistant request, and forward the session to the configured ClearPass Guest Web login page.

Because ClearPass Guest can host multiple Web login pages, a simple method is provided to configure the Web login page that should be used. It does not require any additional configuration in ClearPass Guest. This definition of the Web login page can be specified as part of the Captive Portal profile configuration on the Aruba controller.

Figure 22 *Configuring the Web Login page*



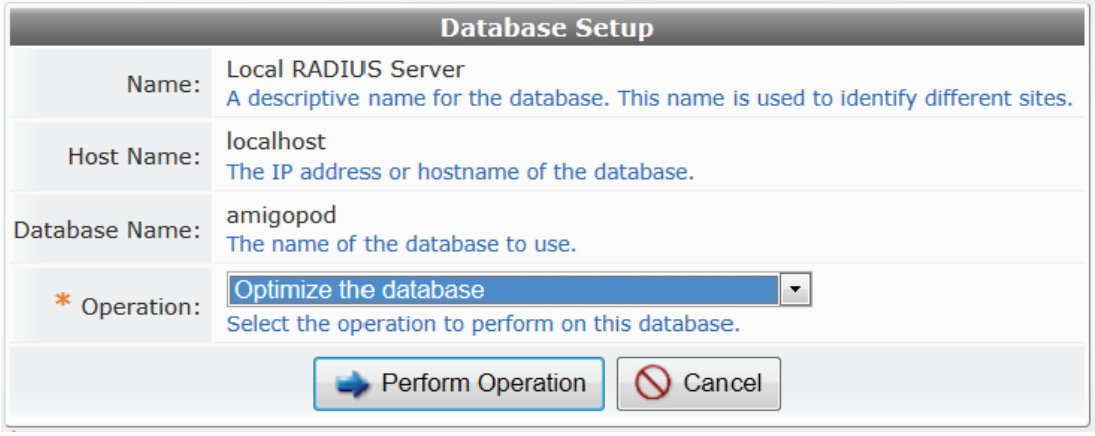
For example, a Captive Portal profile login page configuration like the following sample would link to a hosted Web login page called Aruba_Login: http://<server IP or FQDN>/landing.php/Aruba_Login.php.

Database Lists

This is a list of databases on the NAS server. The ClearPass Guest RADIUS server uses a database to store the user accounts for authentication and other settings for the server.

You can set up as many databases as you like, including databases on other servers. However, exactly one database must be marked as the Active database. This database will be used by the RADIUS server for user authentication. The default configuration for ClearPass Guest includes a pre-configured database. Most deployments will not require more than one database. It is recommended that you leave the default configuration unmodified.

Database Maintenance Tasks



Database optimization and other maintenance tasks can be performed using this form. These tasks are normally carried out automatically and do not require administrative intervention.

Some system updates may require a database schema upgrade. If this is required, it is indicated on the database list with the schema upgrade icon. To upgrade the database schema, select the "Upgrade an existing database schema" operation.

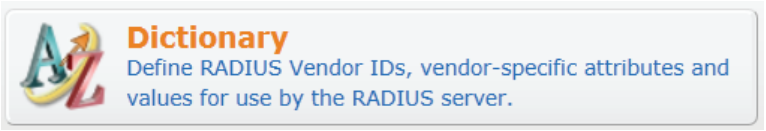
Click the **Perform Operation** button to carry out the specified operation.

Dictionary

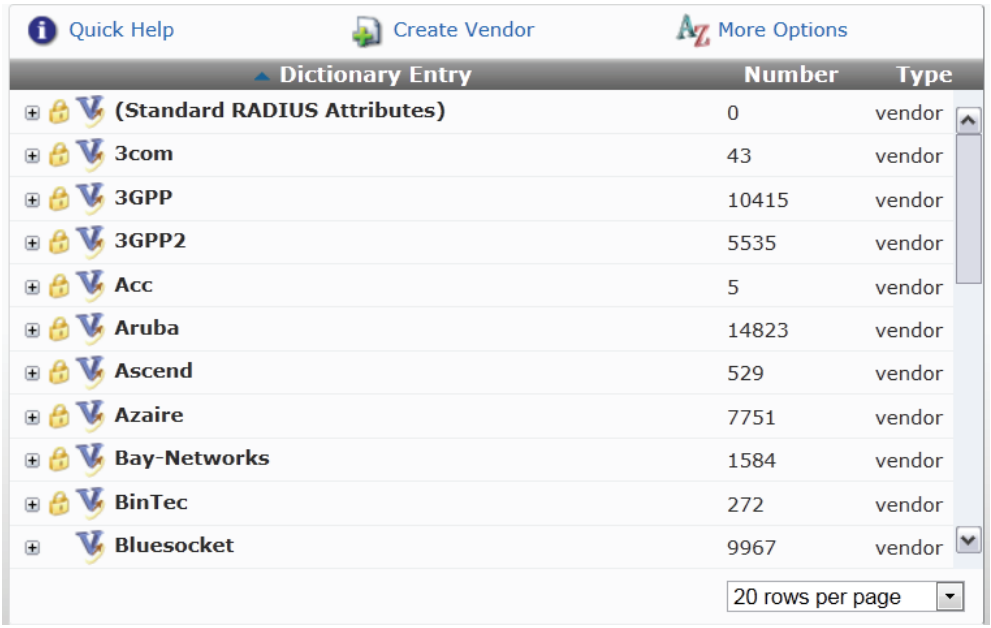
The **RADIUS Dictionary** is a complete list of all the vendor IDs, vendor-specific attributes, and attribute values used in the RADIUS protocol. The dictionary is used to translate between human-readable strings and the underlying numbers used in RADIUS packets.

Many predefined vendor-specific attributes have already been provided in the dictionary. These items are indicated with a lock icon ( ) and cannot be removed from the dictionary.

You can make changes to the predefined vendors and vendor-specific attributes. The new dictionary entry will be shown without a lock icon ( ). To restore the original value of the dictionary entry, simply delete the new entry.



Use this tree view to define a new vendor, create a new vendor-specific attribute, or modify the list of values available for a particular attribute.



The dictionary can be sorted by clicking on a column heading.

Import Dictionary

You are able to import RADIUS dictionary entries from a text file using the **Import Dictionary** command located under the **More Options** tab. These text files can be created by you or you can download them from a manufacturer who is not in the standard list.

Export Dictionary

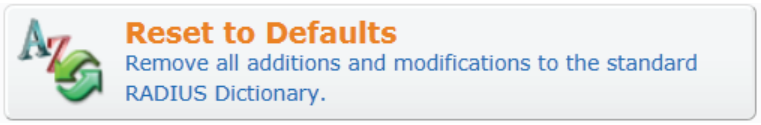
You are able to export the dictionary by clicking on the **More Options** tab and choosing the **Export Dictionary** command. This saves the complete contents of the dictionary as a text file.

Reset Dictionary

You can reset the dictionary to its default set of vendors.

To reset the dictionary:

1. Click the More Options tab above the Dictionary Entry list, then click the **Reset to Defaults** command.



The Reset Dictionary form opens.

2. To permanently delete all additions and modifications to the dictionary, mark the **Confirm** check box. All changes to the vendors, vendor-specific attributes, and attribute values in the dictionary will be lost.

3. Click the **Reset Dictionary** button to have the dictionary reset. This action cannot be undone.

Vendors

Vendors are manufacturers of NAS equipment. ClearPass Guest provides a list of manufacturers but you are able to add to this list.

Vendor-specific attributes as defined in RFC 2865 can be used to configure specific options related to a particular vendor's equipment.

Creating a New Vendor

A new vendor may be added to the dictionary by clicking the **Create Vendor** tab at the top of the Dictionary list view.

You are required to enter the Vendor Name. This name cannot already exist in the dictionary. Spaces are not permitted in the Vendor Name. By convention, hyphens are used in vendor and attribute names instead of spaces.

You are required to enter the Vendor Number. This is the IANA Private Enterprise Code assigned to this vendor. It is unique to this vendor and is used by the RADIUS protocol. For the current mapping of vendor names to IANA Private Enterprise Codes, refer to the IANA Web site: http://www.iana.org/assignments/enterprise-numbers.

The Vendor Number must be less than or equal t.o 65535

Once you have completed the form, click the **Create Vendor** button to add this vendor to the dictionary.

Edit Vendor

You are able to change the Vendor's name or number with the **Ed it Vendor** icon link. This allows you to change the vendor name or number

Delete Vendor

You are able to delete any vendors that you have added to the dictionary. Use the **Delete Vendor** icon link for this. Deleting a vendor will also delete all vendor-specific attributes and attribute values for that vendor.

You will be prompted to confirm the delete operation before it takes place.

Vendors with a lock symbol ( ) next to their name are standard RADIUS dictionary entries and cannot be deleted.

Export Vendor

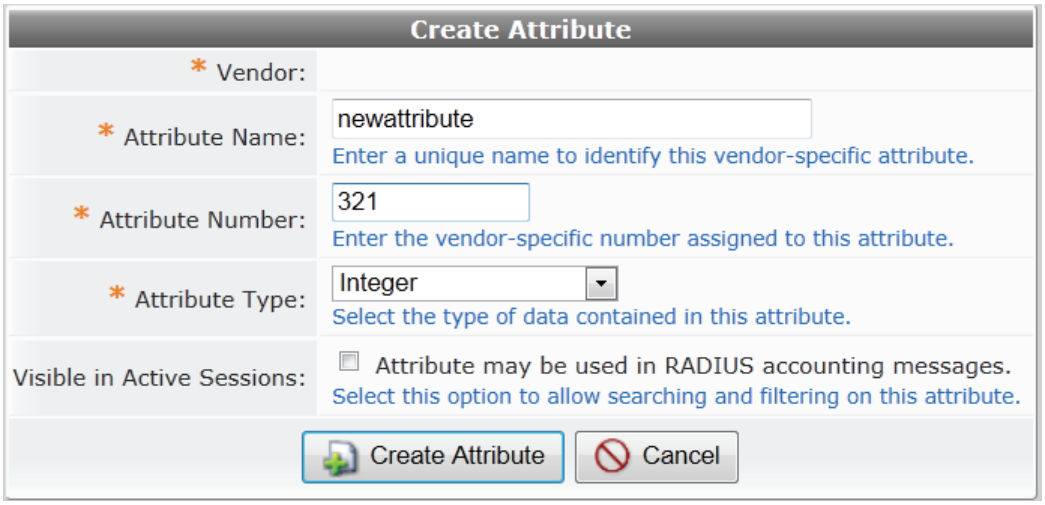
The selected vendor's attributes and values can be exp orted as a text file in RADIUS dictionary format by clicking the **Export Vendor** icon link.

Vendor-Specific Attributes

Vendor-specific attributes identify configuration items specific to that vendor's equipment

Add a Vendor-Specific Attribute (VSA)

A Vendor Specific Attribute (VSA) is a RADIUS attribute defined for a specific vendor. You are able to add vendor-specific attributes to a vendor by clicking the vendor in the RADIUS dictionary list view and then clicking the **Add VSA** icon link.



Each attribute has a name and a unique number specific to that vendor. Refer to your vendor's documentation for the attribute name, number and type settings to use.

The attribute type can be one of:

- Integer
- String
- Binary
- IPv4 Address
- Date/Time
- IPv6 Address
- IPv6 Prefix
- Interface ID (8 octets)
- Ascend Binary Filter

Attribute numbers are normally small decimal numbers in the range 0-255. These may be entered in decimal, or in hexadecimal using the '0x' prefix. Certain vendors in the dictionary have support for larger attribute values.

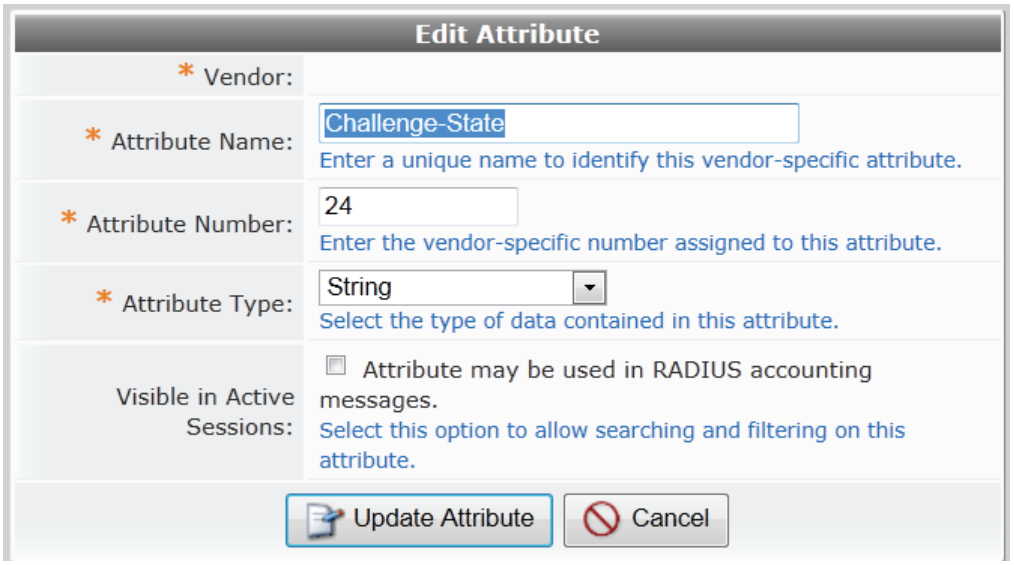
If you want the attribute to appear in the active session views and on RADIUS accounting reports, check the **Visible in Active Sessions** check box. This allows the attribute to be searched and filtered.

Once the data has been entered, click the **Create Attribute** button to complete the creation.

Click the **Cancel** button if you do not want to proceed with creating this vendor attribute.

Edit Vendor-Specific Attribute

You can change the properties of an attribute by clicking on the attribute in the RADIUS dictionary list view and then clicking the **Edit Attribute** icon link.



Once an attribute has been edited, click the **Update Attribute** button to save your changes.

Delete Vendor-Specific Attribute

Attributes can only be deleted from vendors that you have added to the dictionary. Vendor-specific attributes with a lock symbol (🔒) next to their name are standard RADIUS dictionary entries and cannot be deleted.

To delete a vendor-specific attribute, click it in the RADIUS dictionary list view and then click the **Delete Attribute** icon link. You will be prompted to confirm the delete operation before it takes place.

Add Attribute Value

A Value Name with a corresponding numerical value can be created for a selected attribute. These “enumerated” values are used to associate meaningful names with the underlying numerical values of the attribute.

Once an integer attribute has been added to a vendor, you are able to define enumerated values for it.

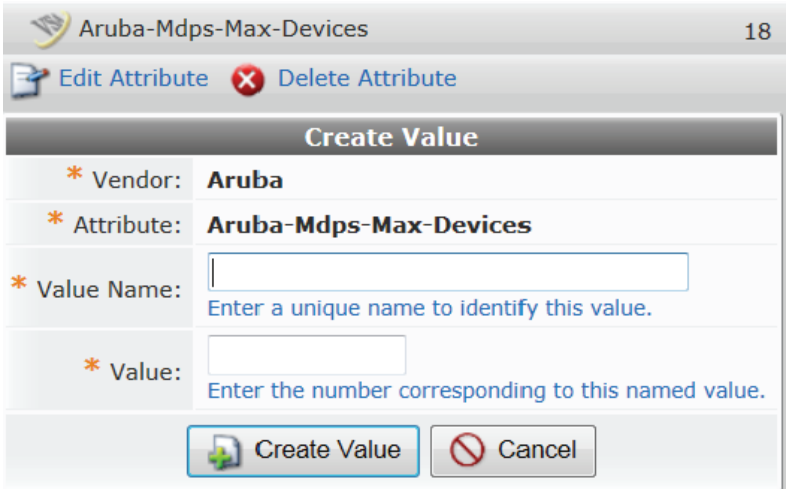
When a vendor-specific attribute is of integer type, this can be used as an explanation of the value, or to specify that the value for an attribute can be only one of a limited number of possibilities.

NOTE

Enumerated values cannot be defined for attributes of string type.

Editing Attribute Value

Enumerated values can be added to an attribute by clicking the attribute in the RADIUS dictionary list view and then clicking the **Add Value** icon link.



You are required to enter the name of the value to be added as well as its value. Values can only be added to attributes that are of integer type.

Deleting Attribute Value

Values that have been added to a vendor-specific attribute can be deleted using the **Delete Value** button.

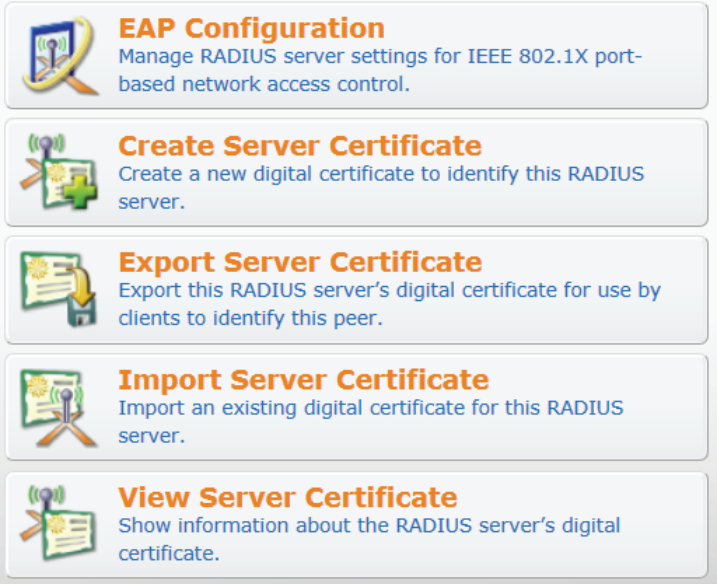
Attribute values with a lock symbol ( ) next to their name are standard RADIUS dictionary entries and cannot be deleted.

EAP and 802.1X Authentication and Certificate Management

The Extensible Authentication Protocol (EAP) supports multiple types of authentication methods, including digital certificates, smart cards, and passwords. This authentication protocol is the basis for the IEEE 802.1X standard, which provides port-based network access control for both wired and wireless networks.

ClearPass Guest supports EAP and 802.1X authentication. This authentication method requires EAP messages to be encapsulated inside RADIUS packets. The RADIUS server must also be configured with the appropriate settings for the EAP types that will be used.

To view or modify a RADIUS server's EAP configuration, go to **RADIUS > Authentication**, then either click **EAP & 802.1X** in the left navigation, or click the **Extensible Authentication Protocol** command. The Extensible Authentication Protocol page opens, and includes command links for EAP configuration and certificate management for the RADIUS server.



To specify supported EAP types and the default type, and to configure OCSP options, see "Specifying Supported EAP Types".

To create a server certificate and self-signed certificate authority, see "Creating a Server Certificate and Self-Signed Certificate Authority".

To request a certificate from another certificate authority, see "Requesting a Certificate from a Certificate Authority".

To import a certificate and its private key, see "Importing a Server Certificate".

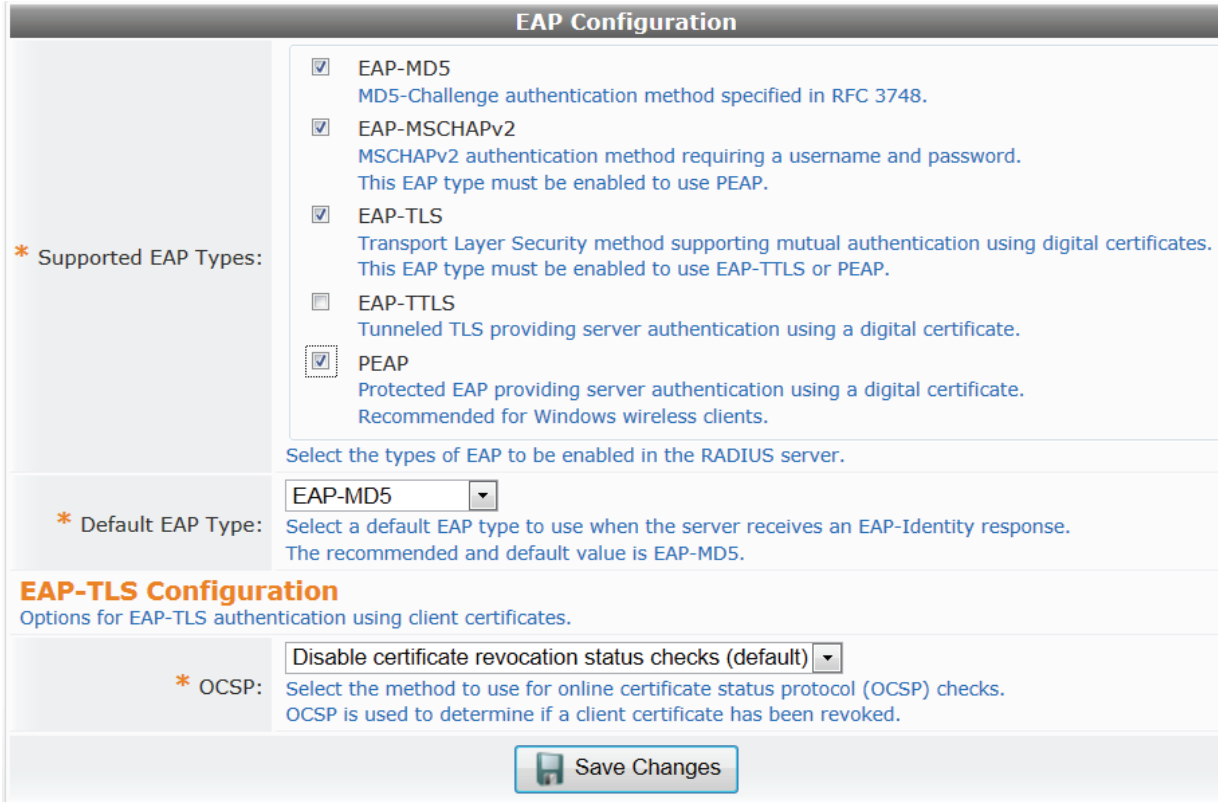
To export a server certificate, see "Exporting Server Certificates".

Specifying Supported EAP Types

To enable the EAP-TLS, EAP-TTLS, and PEAP options on the EAP Configuration form, you must first configure a digital certificate for the RADIUS server. The server certificate is the RADIUS server's identity and will be provided to clients authenticating with these EAP methods. To create and manage the server certificates, see "Creating a Server Certificate and Self-Signed Certificate Authority".

To specify the EAP types the RADIUS server will support and designate the default EAP type:

1. On the Extensible Authentication Protocol page, click the **EAP Configuration** command. The **EAP Configuration** form opens.



2. In the **Supported EAP Types** row, mark the check box for each type the RADIUS server should support. The available types are EAP-MD5, EAP-MSCHAPv2, EAP-TLS, EAP-TTLS, and PEAP. If you select EAP-TLS, the EAP-TLS Configuration area is added at the bottom of the form.
3. In the **Default EAP Type** row, use the drop-down list to select the EAP type to use as the default when the server receives an EAP-Identity response.
4. If you selected EAP-TLS as one of the supported types, use the **EAP-TLS Configuration** area to configure status checks for client certificates. In the drop-down list in the **OCSP** row, select one of the following options:
   - **Disable certificate revocation status checks (default)**—If this option is selected, no OCSP checks are made to determine the client certificate's revocation status.
   - **Automatically check certificate revocation status**—If this option is selected, an OCSP responder defined in the client certificate is used to obtain revocation status. If no OCSP responder is defined in the client certificate, then the local certificate authority is used to check status.
   - **Manually specify OCSP URL for certificate checks**—If this option is selected, the URL specified in the OCSP row of the EAP Configuration form is used to verify revocation status, and any OCSP responder defined in the client certificate is ignored.

   The "Manually specify OCSP URL for certificate checks" option adds the OCSP Responder row to the form.
5. If you chose the manual option for certificate checks, in the **OCSP Responder** row, enter the URL of the service to be used to check certificate status.
6. Click the **Save Changes** button.

Creating a Server Certificate and Self-Signed Certificate Authority

To create a new server certificate and self-signed certificate authority (CA), go to **RADIUS > Authentication > EAP & 802.1X**, then click the **Create Server Certificate** command link. The Create

RADIUS Server Certificate form is displayed. The unique set of identifying details you enter on this form creates the Distinguished Name (DN) for the new certificate.

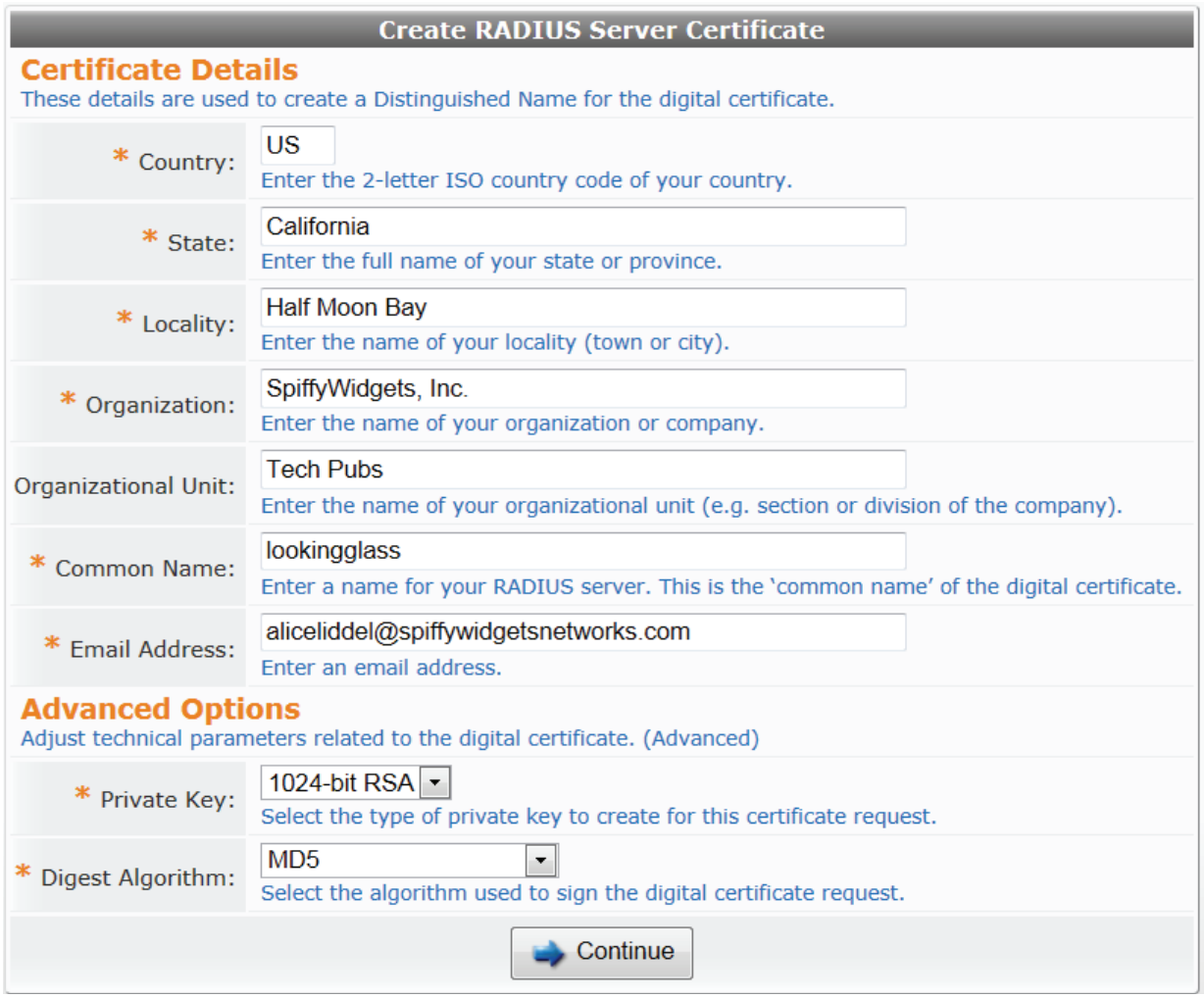
Creating a new server certificate and self-signed CA is a three-step process:

- In step 1, a certificate signing request is created with the identifying details of the Distinguished Name for the RADIUS server's digital certificate.
- In step 2, expiration dates for the certificate and root certificate are specified, and a self-signed certificate authority (CA) is created. This CA is then used to sign the server's certificate request, which produces a valid digital certificate for the server.
- In step 3, the certificate authority and server certificates are installed on the RADIUS server. The CA root certificate is then downloaded for distribution to clients who will use this RADIUS server for authentication.

To create a self-signed certificate authority and issue a server certificate using this CA, use the process described below. If you already have a certificate authority, or are using a third-party CA, See "Requesting a Certificate from a Certificate Authority" in this chapter for details on creating a certificate signing request.

Creating the Certificate Signing Request

The **Create RADIUS Server Certificate** form is used to specify the details of your RADIUS server. The server certificate is the RADIUS server's identity and will be provided to clients authenticating with EAP-TLS, EAP-TTLS, or PEAP.



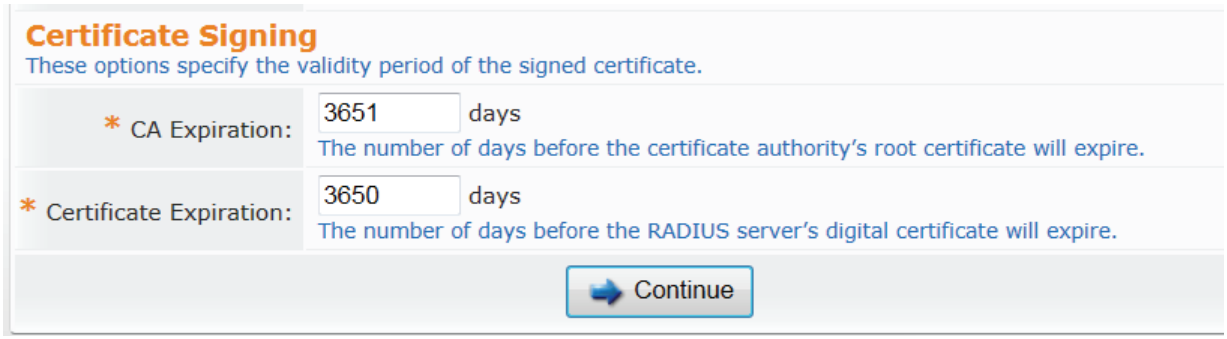
Complete the details for the certificate, and click the **Continue** button to proceed to Step 2.

NOTE

The “Common Name” of the CA certificate will be used to identify it to clients installing it as a trusted CA root. Make sure to choose a sensible name.

Signing RADIUS Server Certificate

For a client to verify that the RADIUS server’s identity is valid, the server’s certificate must be issued by a certificate authority (CA) that is trusted by the client. This authority may be either a trusted third party CA, or a private certificate authority for which the root certificate has been distributed to clients.



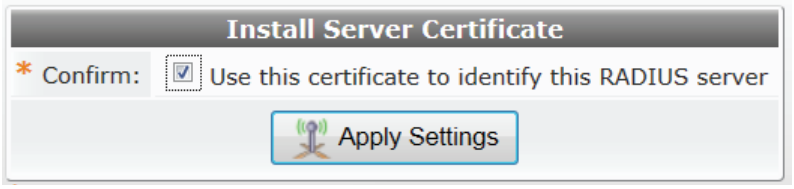
The **Sign RADIUS Server Certificate** form shows the details you entered in the previous step, and includes fields for expiration dates. It is used to create a private certificate authority and sign the RADIUS server’s certificate. By default, the CA certificate’s expiration is set to be 10 years in the future.

1. If you need to edit any of the identifying information for the certificate, you may do so on this form.
2. To change the default expiration settings for the certificate authority and the certificate, enter the number of days in the **CA Expiration** and **Certificate Expiration** fields.
3. Click the **Continue** button to proceed to step 3.

Installing the Self-Signed RADIUS Server Certificate

On the Certificate Details form, the details of the RADIUS server certificate and its issuer, and the certificate’s validity period, are displayed for review. The Install Server Certificate form is included.

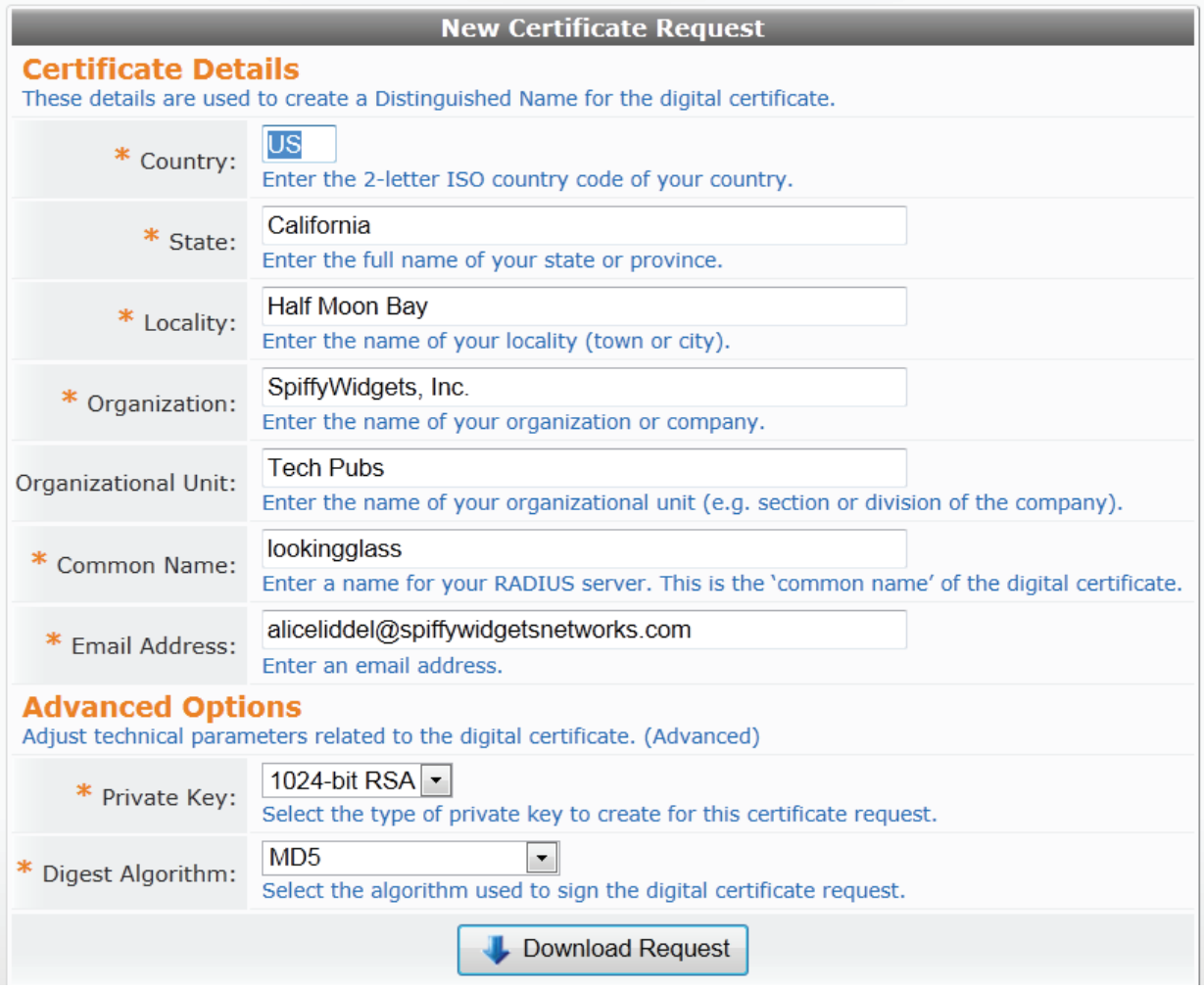
To confirm the certificate’s information and complete the process, mark the **Use this certificate to identify this RADIUS server** check box in the **Confirm** row, then click the **Apply Settings** button to configure the EAP server certificate.



After installing the certificate, the RADIUS server will need to be restarted to complete the changes.

Requesting a Certificate from a Certificate Authority

To create a certificate request to obtain a certificate from a recognized certificate authority (CA), go to **RADIUS > Authentication > EAP & 802.1X**, click the **Create Server Certificate** command link, then click the **Request a certificate from another certificate authority** link. The Server Certificate Request page opens.



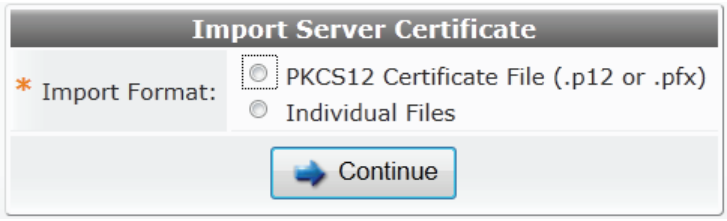
Complete the details for the certificate, and click the **Download Request** button to save the certificate signing request.

This signing request should be submitted to your certificate authority (CA). The CA signs the request to create the server's digital certificate.

Once you have the certificate, you need to import it to set it up for use with EAP. See "Importing a Server Certificate".

Importing a Server Certificate

To import a digital certificate and its private key, go to **RADIUS > Authentication > EAP & 802.1X** and click the **Import Server Certificate** command link. The Import Server Certificate form opens.



A digital certificate may be imported from either the PKCS#12 format, which is a single file containing one or more certificates and an encrypted private key, or from three individual files for the certificate, private key (optionally encrypted with a passphrase), and the root certificate authority.

Complete the form with the details for your certificate, and click **Continue** to proceed to Step 2.

Installing a Server Certificate from a Certificate Authority

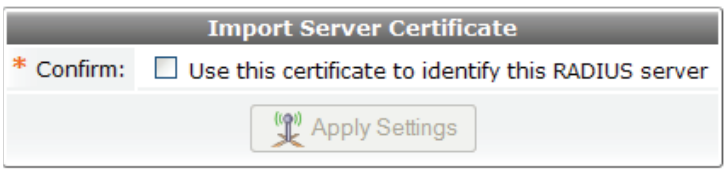
The **Install Server Certificate** form is used to install a digital certificate you have obtained from a third-party certificate authority. This certificate should correspond to a certificate signing request that you previously created using the **New Certificate Request** form.

Select the certificate file and the certificate authority's root certificate, and click the **Upload Certificate** button.

Installing an Imported Server Certificate

In step 2, the details of the imported RADIUS server certificate and its issuer are shown, including the certificate's validity period.

Select the **Use this certificate to identify this RADIUS server** check box and click the **Apply Settings** button to complete the import process and configure the EAP server certificate



After importing the certificate, the RADIUS server will need to be restarted to complete the changes.

Exporting Server Certificates

The **Export Server Certificate** form is used to export the RADIUS server's digital certificate, or the certificate authority's root certificate, in several different formats.

Select one of these options to export a certificate file:

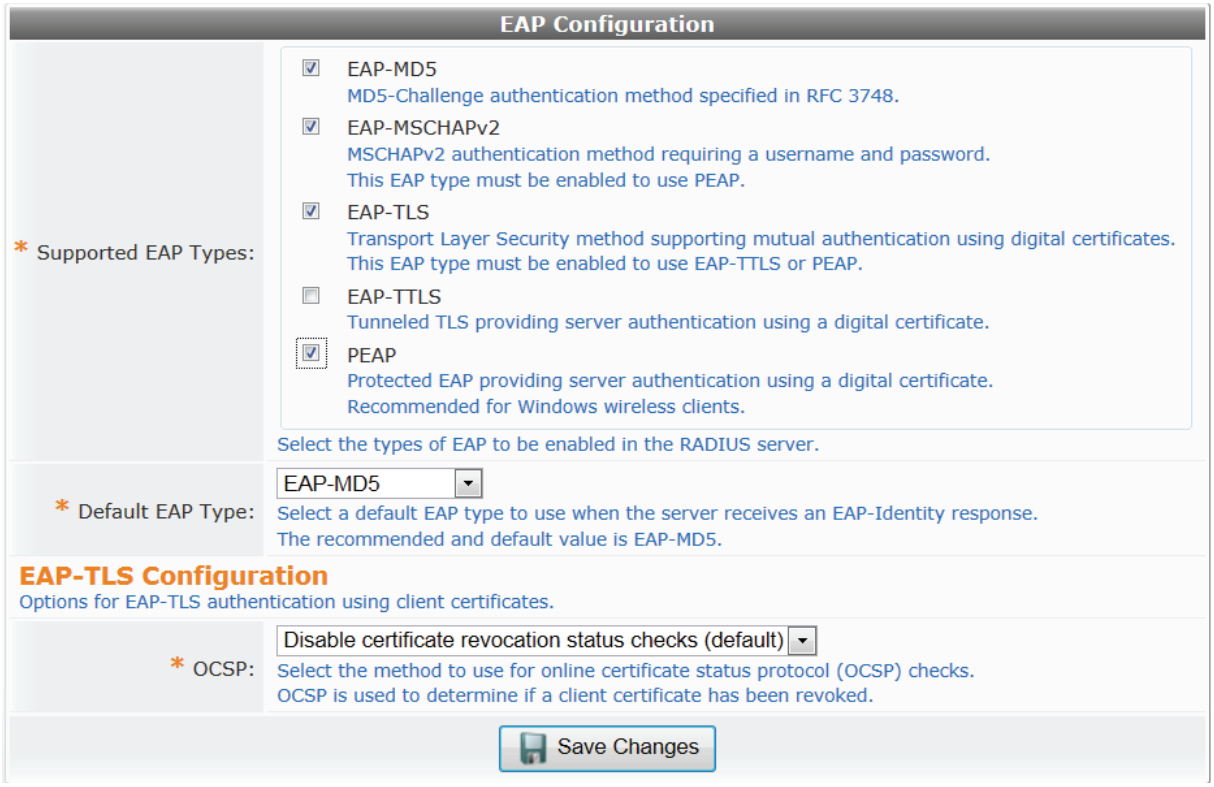
- **Server certificate and CA issuer certificate (PKCS#7)** – use this option to download a file containing the certificates for the CA and the server.
- **Server certificate chain including private key (PKCS#12)** – use this option if you are backing up the server's certificate, or moving it to another server. A passphrase is strongly recommended to protect the private key.
- **Server certificate only** – use this option to download just the RADIUS server's certificate, in either PKCS#7, Base-64 encoded (PEM), or binary (DER) formats.
- **CA issuer certificate only** – use this option to download the root certificate for the certificate authority.

PEAP Sample Configuration

To enable the common case of PEAPv0/MS-CHAPv2 (broadly supported by all wireless clients that implement 802.1X), follow the process described below:

1. Create or import a RADIUS server certificate. See "Creating a Server Certificate and Self-Signed Certificate Authority" and **"Importing a Server Certificate"** in this chapter for details.

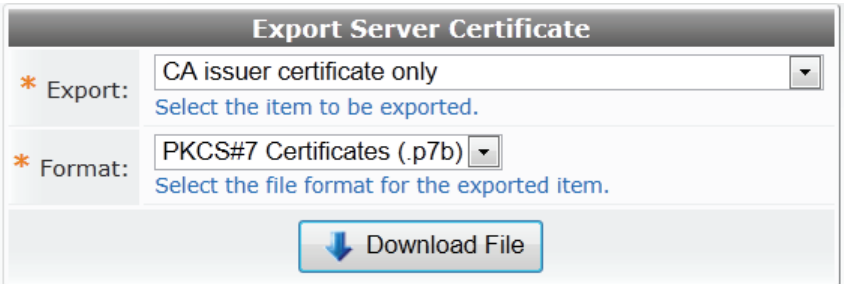
2. Select the appropriate PEAP options in the **EAP Configuration** form, as shown below:



3. Click the **Save Changes** button, and restart the RADIUS Server to apply the configuration.
4. You may verify that the EAP configuration is loaded by checking for a certain startup message on the **RADIUS Server Control** screen:

```
Tue Nov 17 01:04:05 2009 : Info: rlm_eap_tls: Loading the certificate file as a chain
```

5. The certificate authority used to issue the server's certificate must be exported. To do this, click the **Export Server Certificate** command link. In the **Export Server Certificate** form, select "CA issuer certificate only" and use the default PKCS#7 container format.

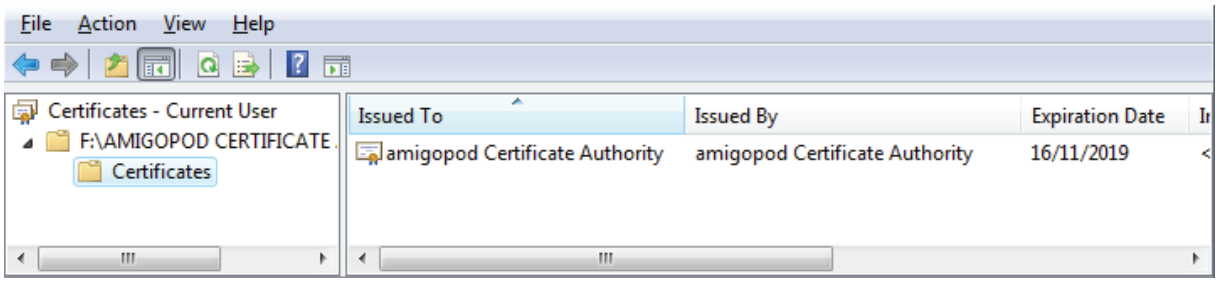


6. Click the **Download File** button and a file named **Guest Certificate Authority.p7b** will be downloaded (the precise name depends on the common name for the CA certificate).
7. This file must be imported as a trusted root certification authority on any client wishing to authenticate using this RADIUS Server. The reason for this is that the server's identity must be established via a trusted root CA in order for authentication to proceed. When using a well-known third party CA, this step does not need to be performed as the necessary trust relationship already exists in most clients.

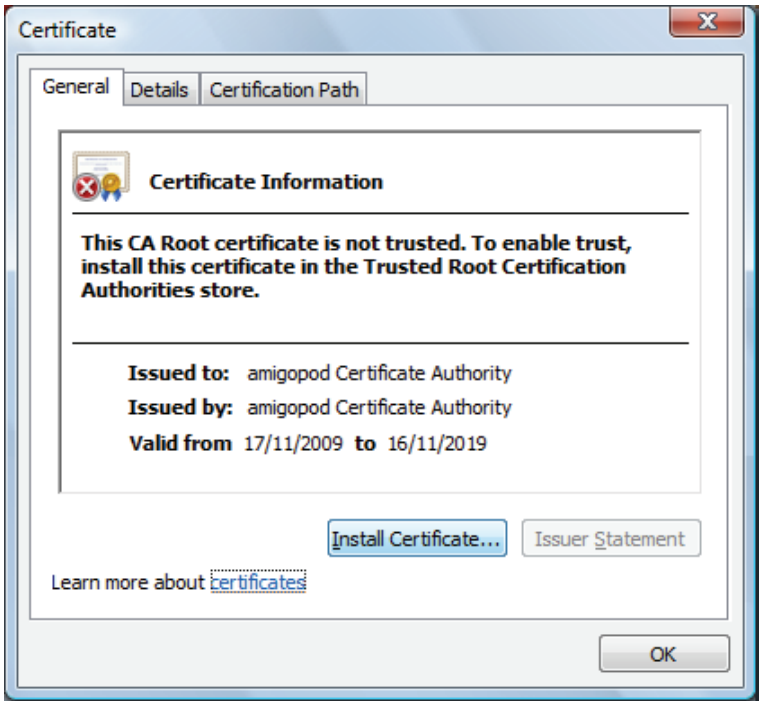
Importing a Root Certificate – Windows Vista and Windows 7

The following steps may be used to import a root certificate on Windows Vista or Windows 7 from a ".p7b" file exported using the **Export Server Certificate** form:

1. Open the .p7b file from Windows Explorer:



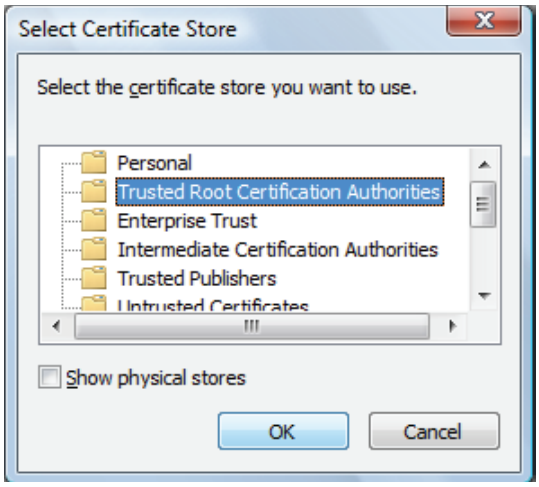
2. Select the certificate in the list. Right-click it and choose **Open**. The Certificate Information dialog opens.



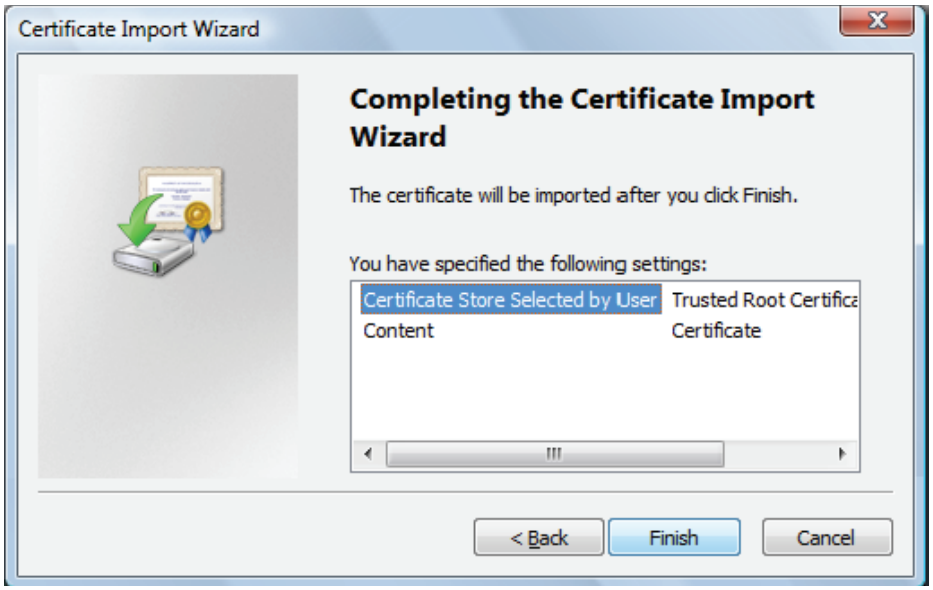
3. Click the **Install Certificate** button. The Certificate Import Wizard opens.

4. Click **Next**. The **Certificate Store** form opens.

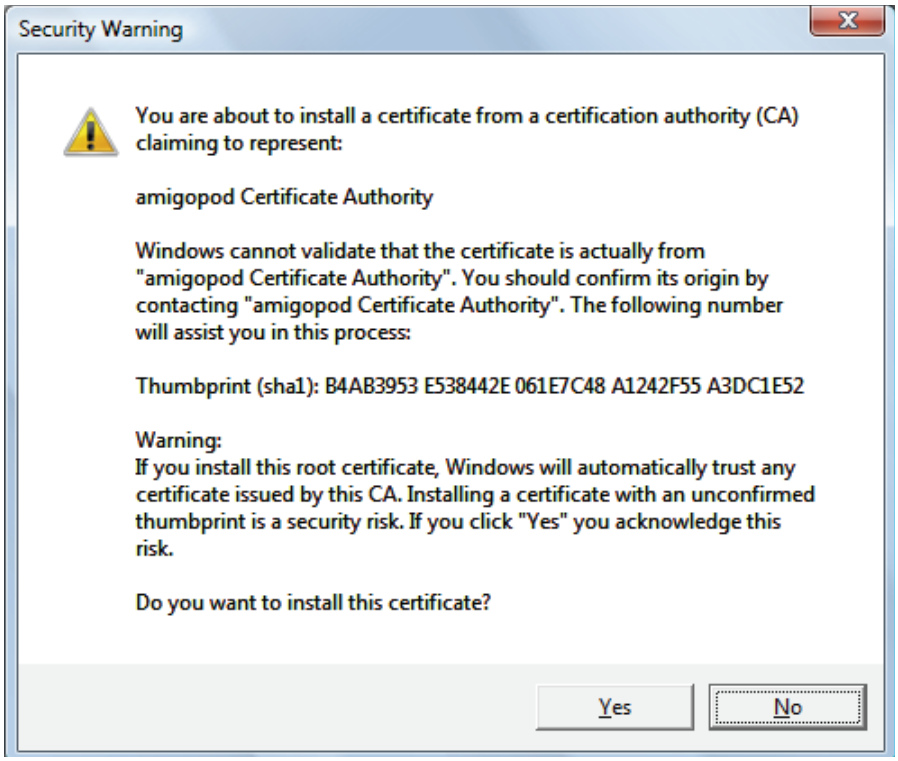
5. Click the **Browse** button to select the **Trusted Root Certification Authorities** store.



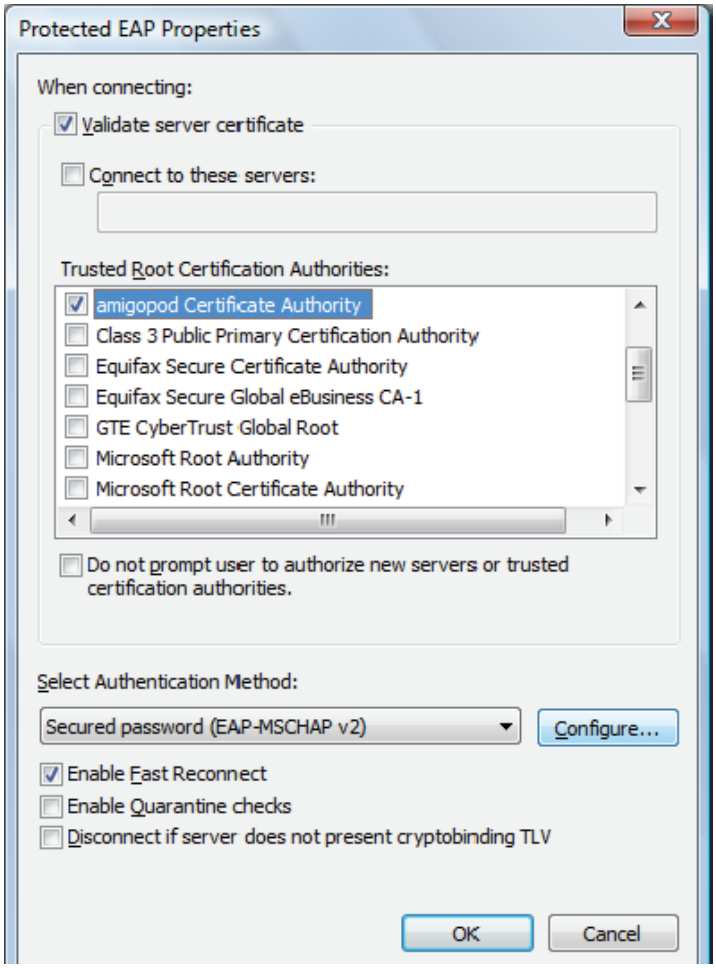
6. Click **OK**, and then click **Next**. The last page of the Certificate Import Wizard is displayed.



7. Click **Finish**. A security warning reminds you that if you install the certificate, all future certificates from this certificate authority will automatically be trusted.



8. To make use of the imported root certificate, make sure that the CA is specified as a Trusted Root Certification Authority for the wireless network connection that is using PEAP. Click **Yes** to confirm and accept the certificate.

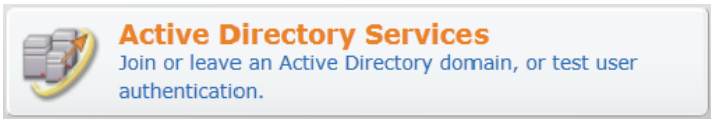


Active Directory Domain Services

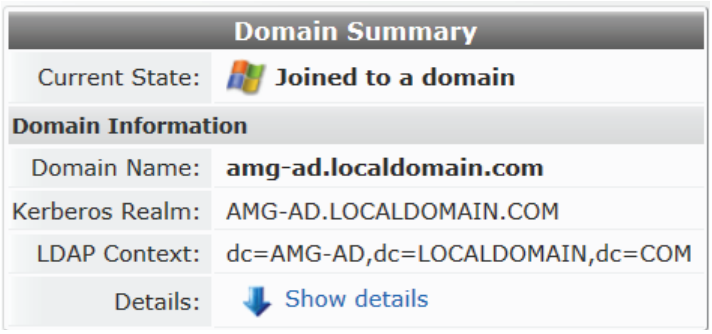
To perform certain types of user authentication, such as using the MS-CHAPv2 protocol to verify a username and password, the RADIUS server must first be joined to an Active Directory domain.

For information on Proxy RADIUS, LDAP, and local certifiacate authority external authentication servers, see External Authentication Servers (EAS).

To view the current domain information, join or leave a domain, or perform authentication tests for user accounts in the domain, use the **Active Directory Services** command link on the **RADIUS > Authentication** page.

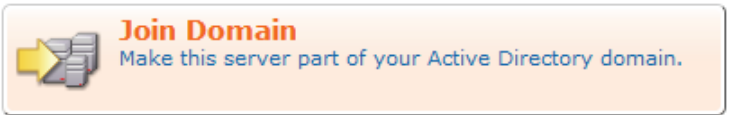


The Domain Summary table shows the current domain settings. Click the **Show details** link to see advanced information about the domain.

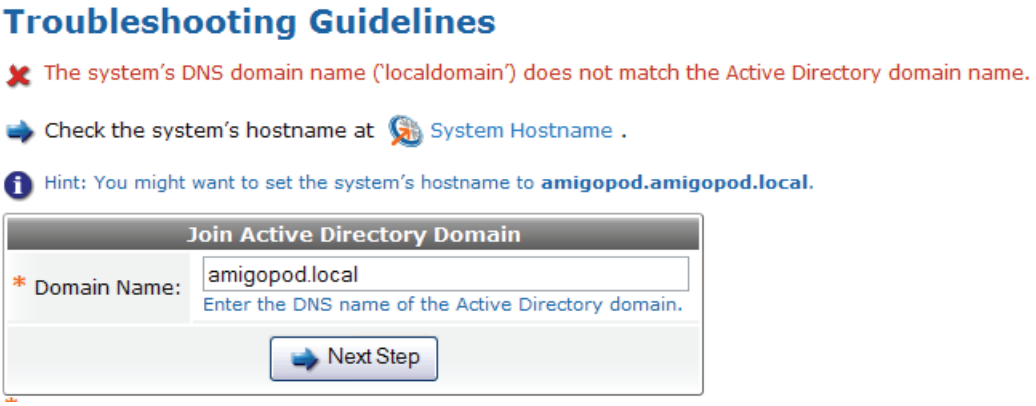


Joining an Active Directory Domain

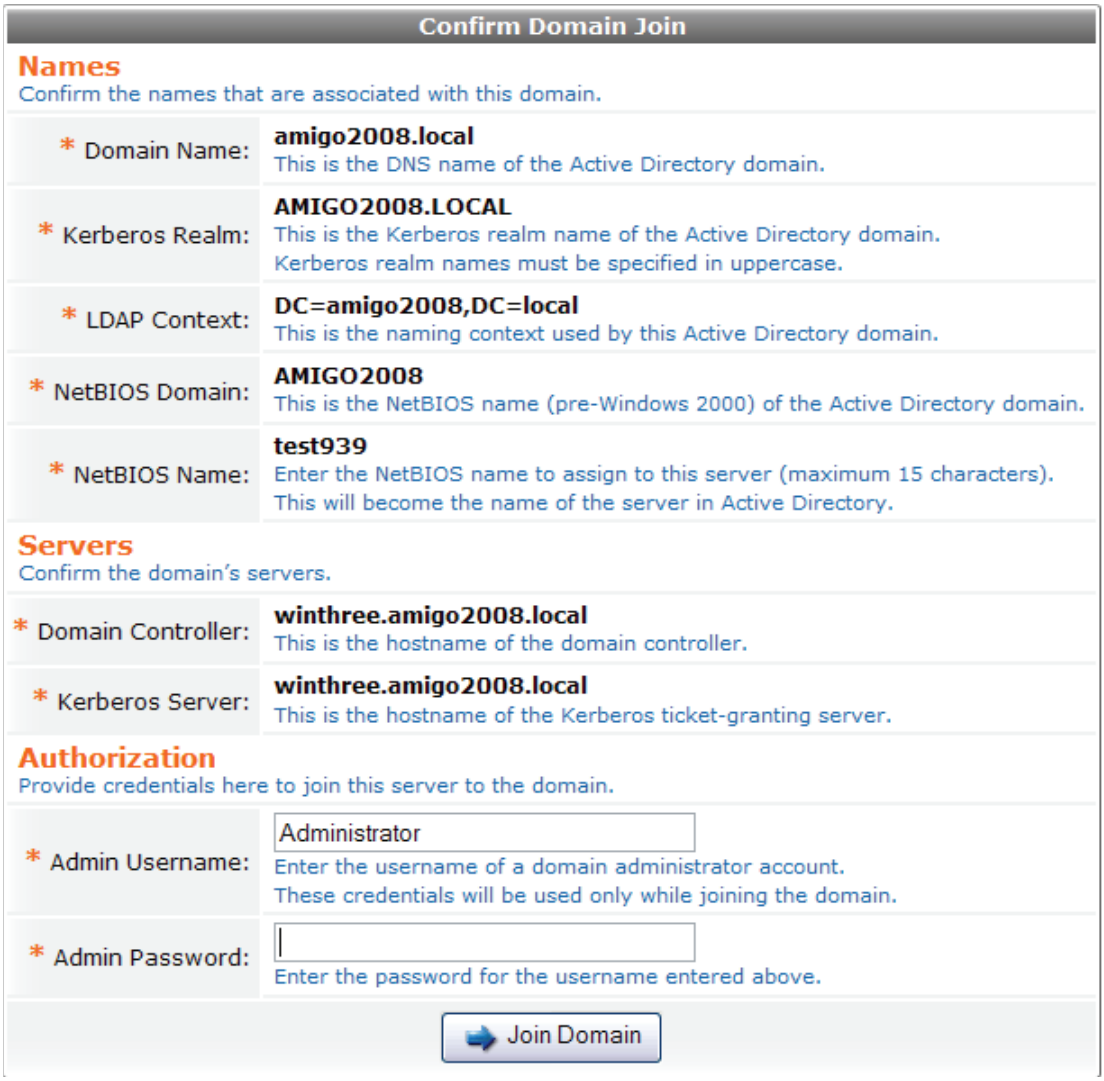
To start the two-step process to join the domain, click the **Join Domain** command link on the **RADIUS > Authentication > Active Directory Services** page.



The **Join Active Directory Domain** form is displayed, and includes troubleshooting tips.



When the server's DNS and network settings are correctly configured, all the necessary domain-related information is automatically detected.



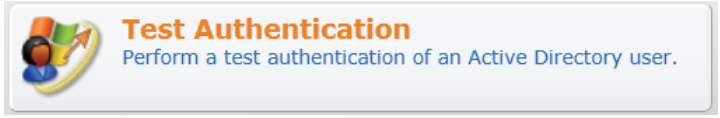
Use the **Edit Settings** link at the top of this page if any of the automatically detected settings need to be modified.

Joining the server to the Active Directory domain then requires entering the username and password for a domain administrator account. Click the **Join Domain** button to complete the process.

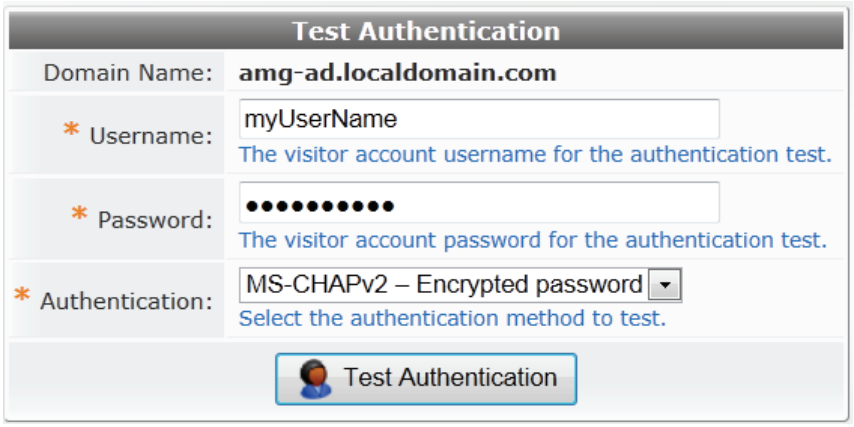
Once the domain has been joined, the status is available on the Active Directory Services page.

Testing Active Directory User Authentication

To verify that the domain has been joined successfully, click the **Test Authentication** command link on the **RADIUS > Authentication > Active Directory** page.



Provide a username and password for a user in the domain to verify that authentication is working.

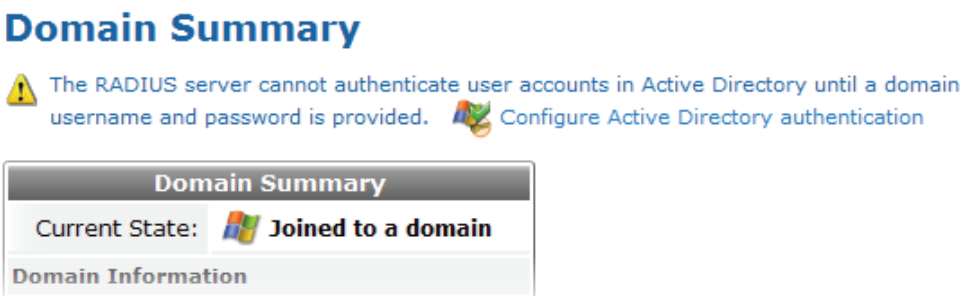


The following options are available in the Authentication drop-down list:

- **MS-CHAPv2 – Encrypted password** – Use this option to encrypt the user's password using the MS-CHAPv2 authentication method and verify it with the server. A successful authentication using this method can only be performed when the ClearPass Guest server has joined the domain.
- **Plain text password** – Use this option to perform a plain-text verification of the user's password.

Configuring Active Directory Domain Authentication

After joining the domain, an additional step is required in order to perform user authentication.



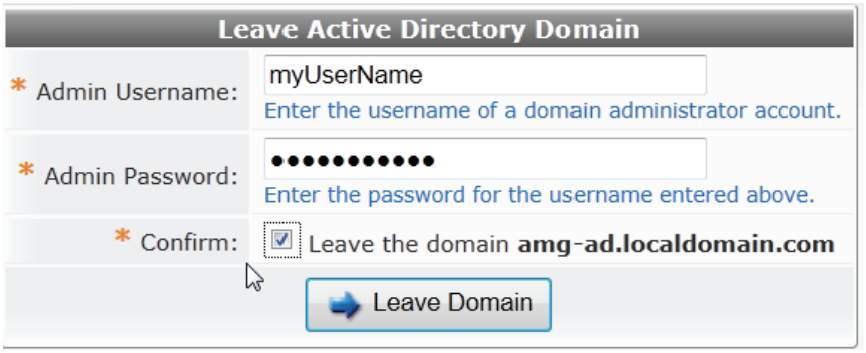
The username and password of a domain user is required to perform an LDAP bind to the Active Directory domain controller, so that LDAP search operations can be performed for other user accounts in the directory. The credentials provided do not need to be those of a domain administrator; a restricted user account may be provided here. Only user lookup operations are performed with this user account.

To provide the domain credentials that will be used when authenticating via LDAP, click the **Configure Active Directory authentication** link on the **RADIUS > Active Directory Services** page.

Leaving an Active Directory Domain

To remove the server from the domain, click the **Leave Domain** command link on the **RADIUS > Authentication > Active Directory** page.

As with joining the domain, the credentials for a domain administrator are required to perform this operation.



Provide these credentials in the **Leave Active Directory Domain** form and click the **Leave Domain** button.

External Authentication Servers (EAS)

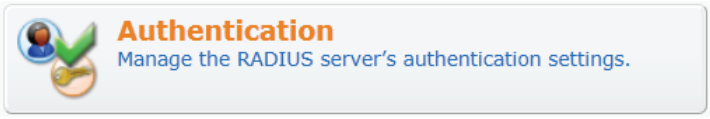
Many networks have more than one place where user credentials are stored. Networks that have different types of users, geographically separate systems, or networks created by integrating different types of systems are all situations where user account information can be spread across several places.

However, network access equipment is often shared between all of these users. This requires that different authentication sources be integrated for use by the network infrastructure.

ClearPass Guest's RADIUS server supports multiple **external authentication servers**, allowing user accounts from different places to be authenticated using a common industry-standard interface (RADIUS requests).

Use the **Authentication** command link on the **RADIUS** page to create and manage authentication servers, and to modify system settings related to user authentication.

To perform certain types of user authentication, such as using the MS-CHAPv2 protocol to verify a username and password, the RADIUS server must first be joined to an Active Directory domain. See Active Directory Domain Services for more information.



Types of External Authentication Server

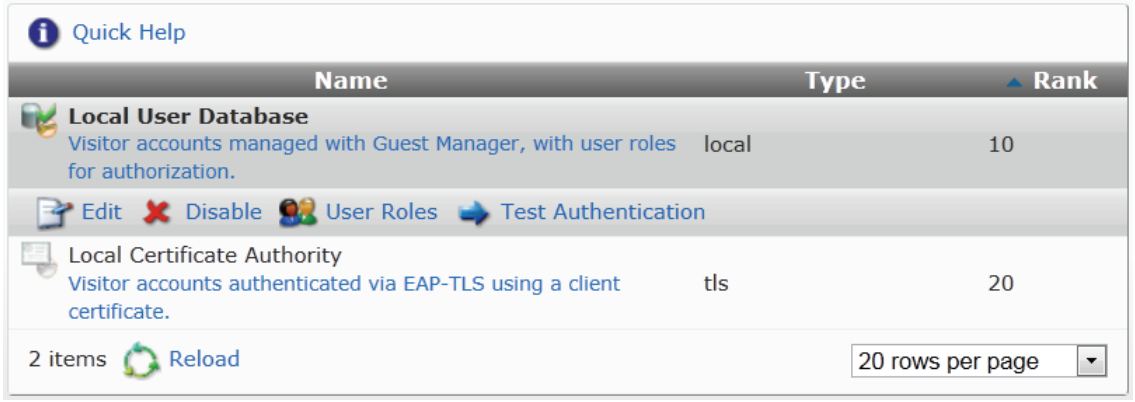
An authentication server may be one of five types:

- **Local user database** — User accounts defined in Guest Manager.
- **Microsoft Active Directory**—User accounts defined in a forest or domain and authenticated by the domain controller. Both user and machine accounts may be authenticated. Additionally, support is provided for authenticating users with a supplied username of either "DOMAIN\user" or "user".
- **LDAP server** (Lightweight Directory Access Protocol)—User accounts stored in a directory.
- **Proxy RADIUS server**—User accounts authenticated by another RADIUS server.
- **Local Certificate Authority**—The client provides their own local certificate authority to issue private certificates for users within its organization. Visitor accounts are authenticated through EAP-TLS, and the authorization method can be configured.

Managing External Authentication Servers

To view the list of external RADIUS authentication servers and create, edit, enable or disable, delete, test, view user roles or configure EAP for them, go to **RADIUS > Authentication > Authentication Servers**.

The RADIUS Authentication Servers page lists all available sources that may be used for authentication.



Changing the properties of an authentication server requires restarting the RADIUS server. When this is necessary, a link is displayed at the top of the page.

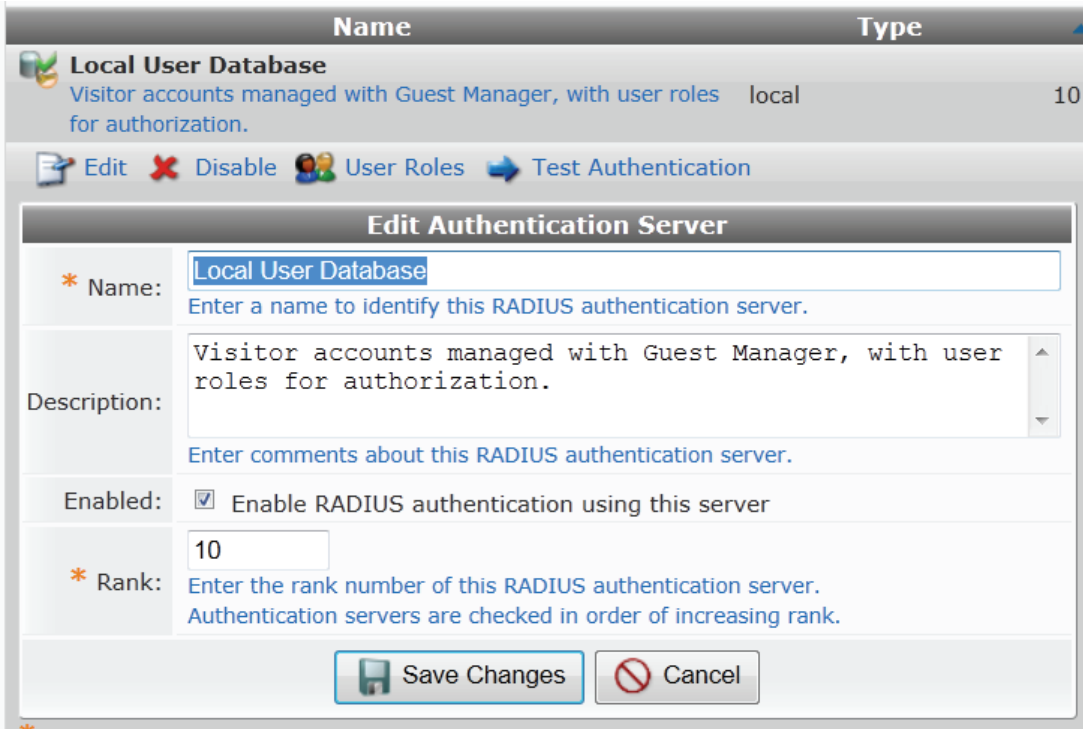
The Test Authentication option for a server may be used to check the connection to an authentication server, or verify the authorization rules that have been configured. For Local Certificate Authority external authentication servers, additional testing options are included to simulate EAP-TLS authentication with a client certificate.

For information on editing an external authentication server, see "Configuring Properties for External Authentication Servers."

For information on testing an external authentication server, see "Testing External Authentication Servers."

Configuring Properties for External Authentication Servers

To configure the settings for an external authentication server, click the server's **Edit** link on the RADIUS Authentication Servers page. The server's row expands to include the Edit Authentication Server form.



The top part of the form contains basic properties for the external authentication server.

The middle part of the form differs depending on the type of authentication being performed:

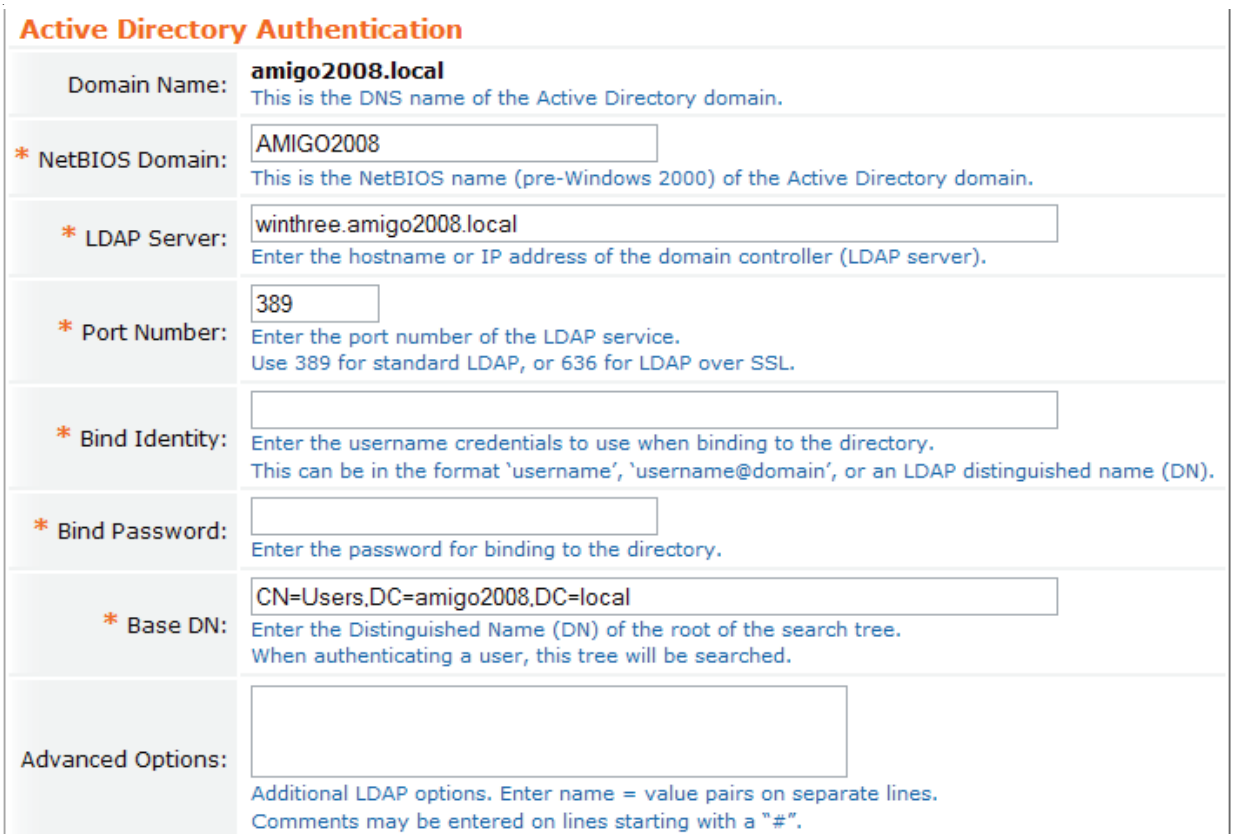
- **Active Directory Authentication Server**— See "Configuring an Active Directory EAS"
- **LDAP Authentication Server—** See "Configuring an LDAP EAS"
- **Proxy RADIUS Authentication Server**— See "Configuring a Proxy RADIUS EAS"
- **Local Certificate Authority Authentication Server**— See "Configuring a Local Certificate Authority EAS"

The bottom part of the form controls the authorization settings for this server. See "Configuring Authorization for External Authentication Servers" in this chapter for details.

Configuring an Active Directory EAS

Microsoft Active Directory user accounts are defined in a forest or domain and authenticated by the domain controller. Both user and machine accounts may be authenticated. Additionally, support is provided for authenticating users with a supplied username of either "DOMAIN\user" or "user". For more information on managing Active Directory domains, see Active Directory Domain Services.

For Active Directory external authentication servers, the following fields are displayed in the Edit Authentication Server form. Most of the settings for the authentication server are automatically detected when joining the domain; however, a Bind Identity (username) and Bind Password are required in order to authenticate users against the directory.

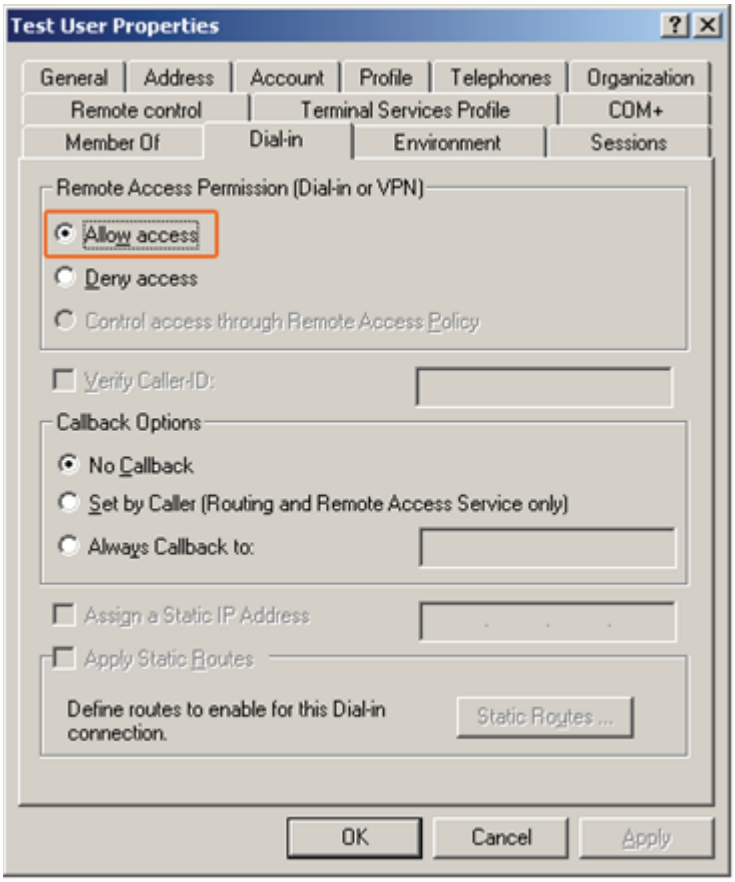


- **NetBIOS Domain** – automatically detected when joining the domain.
- **LDAP Server** and **Port Number** – the hostname or IP address of the domain controller, with the corresponding port number of the LDAP service.
- **Bind Identity** and **Bind Password** – credentials used to bind to the directory.
- **Base DN** – the LDAP distinguished name of the root of the search tree. This is typically the Users container within the directory, but may be set to the root of the directory (for example, `DC=example,DC=com`) in order to authenticate both user and machine accounts.
- **Advanced Options** – additional options controlling authentication against the directory.

The following advanced options may be required in several common situations and are documented below:

- **access_attr_used_for_allow** = yes: Determines if the access_attr LDAP attribute is used to allow access or to deny access to a user.
- **access_attr** = msNPAllowDialin: The LDAP attribute name to be used for authorization checks.

The default value for this attribute corresponds to the Active Directory “Remote Access Permission” setting.



NOTE

The default settings for the “access_attr” and “access_attr_used_for_allow” settings mean that only users with the Remote Access Permission selected above will be authorized.

To authorize all users in Active Directory, regardless of the individual user account settings for remote access permission, use the following settings:

```
access_attr = nonexistentAttribute
access_attr_used_for_allow = no
```

Additional details about the precise operation of these parameters are as follows:

If access_attr_used_for_allow is “yes”, then the access_attr attribute is checked for existence in the user object.

- If the attribute exists and is not set to FALSE, the user is permitted access.
- If the attribute exists and is set to FALSE, the user is denied access.
- If the attribute does not exist, the user is denied access.

  If access_attr_used_for_allow is “no”, then the access_attr attribute is checked for existence in the user object.

- If the attribute exists, the user is denied access.
- If the attribute does not exist, the user is permitted access.

ldap_connections_number = 5

The number of concurrent connections to make to the LDAP server.

timeout = 4

The number of seconds to wait for the LDAP query to finish.

timelimit = 3

The number of seconds the LDAP server has to process the query (server-side time limit).

net_timeout = 1

The number of seconds to wait for a response from the LDAP server (network failures).

use_mppe = yes

If this option is set to 'yes', MS-CHAP authentication will return the RADIUS attribute MS-CHAP-MPPE-Keys for MS-CHAPv1, and MS-MPPE-Recv-Key/MS-MPPE-Send-Key for MS-CHAPv2.

require_encryption = yes

If 'use_mppe' is enabled, 'require_encryption' makes encryption moderate.

require_strong = yes

'require_strong' always requires 128 bit encryption.

with_ntdomain_hack = yes

Windows sends the RADIUS server a username in the form of DOMAIN\user, but sends the challenge response based on only the user portion. Enable this option to handle this behavior correctly.

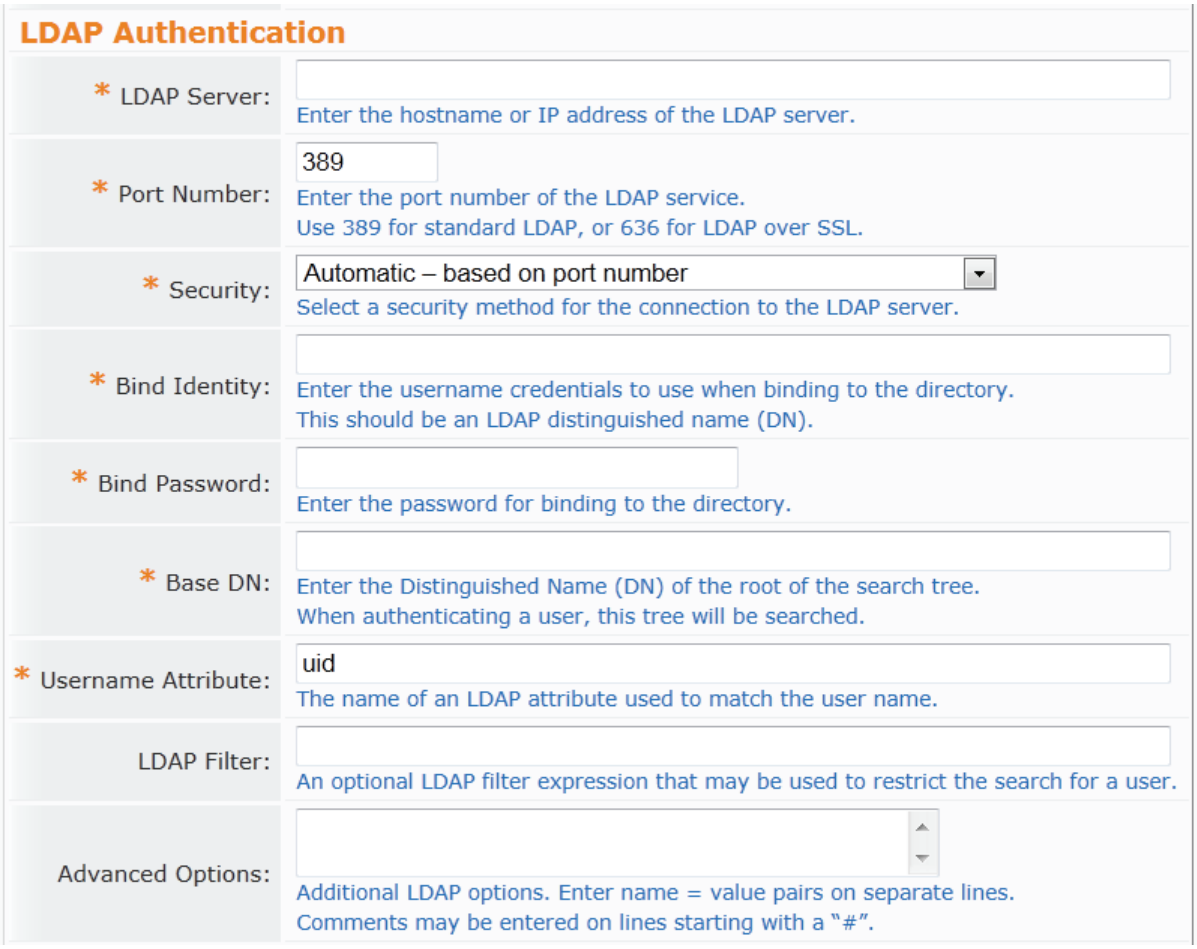
ntlm_auth_domain = *domain name*

Domain name to provide when performing an NTLM authentication; this is only required in certain circumstances—for example, authentication of users in a network using multiple domains and RADIUS servers.

For additional settings, See "LDAP Module Configuration" in the Reference chapter. The LDAP module options that are described here. Note that to set an advanced option for an Active Directory external authentication server, specify the LDAP module option name **without** the "ldap." prefix.

Configuring an LDAP EAS

For **LDAP** external authentication servers, the following fields are displayed in the Edit Authentication Server form.



- **LDAP Server** and **Port Number** – the hostname or IP address of the LDAP server, with the corresponding port number of the LDAP service.
- **Security** – select from one of these options:
  - **Automatic – based on port number** – LDAP connections to port 636 are encrypted using TLS, while all other port numbers use an unencrypted LDAP connection.
  - **Use Start TLS operation to upgrade to a secure connection** – this option, when it is supported by the LDAP server, allows a standard LDAP connection on port 389 to be upgraded to a connection supporting TLS.
  - **Use TLS to connect securely** – enforce a TLS connection regardless of the port number, and never perform unencrypted LDAP.
- **Certificate Check** – displayed when one of the TLS security options is selected. See "Managing Certificates for External Authentication Servers" in this chapter for information about installing digital certificates for external authentication servers. The certificate verification options that may be selected are:
  - **Do not request or verify the server's certificate** – perform no verification of the server's identity.
  - **Request the server's certificate but do not verify it** – check the server's identity, but do not fail authentications if the server's identity cannot be verified.
  - **Require a valid server certificate (recommended)** – check the server's identity, and fail authentications if the server's identity cannot be verified.
- **Bind Identity and Bind Password** – credentials used to bind to the directory.

- **Base DN** – the LDAP distinguished name of the root of the search tree. This is typically a user's container within the directory, but may be different depending on the directory's schema.
- **Username Attribute** – the LDAP attribute that corresponds to the username. A filter expression is built that matches the value of the RADIUS Access-Request's User-Name attribute with this attribute value in the directory.
- **LDAP Filter** – an optional LDAP filter expression that may be used to restrict the matching, over and above the standard filtering applied by usernames. For example, specifying the expression `(objectClass=user)` will ensure that only LDAP objects with the specified type will be matched.
- **Advanced Options** – additional options controlling authentication against the directory. For information about additional LDAP configuration options, including enabling Novell eDirectory support, see "LDAP Module Configuration" in the Reference chapter.

The following advanced options may be required in several common situations and are documented below:

ldap_opt_referrals = yes

If set to "yes", the directory may provide an LDAP referral from the directory to answer the request. This option must be set to "no" if you are contacting an Active Directory LDAP server.

access_attr_used_for_allow = yes

access_attr = *empty*

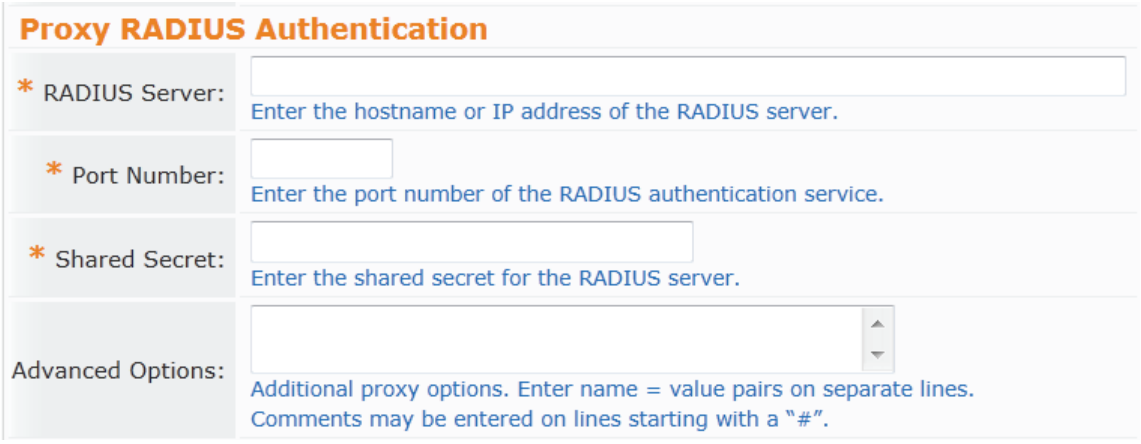
To configure the authorization method for an LDAP external authentication server, see "Configuring Authorization for External Authentication Servers."

See "Configuring Properties for External Authentication Servers" for a description of properties in this chapter.

For additional settings, refer to the LDAP module options. See "LDAP Module Configuration" in the Reference chapter. Note that to set an advanced option for an LDAP external authentication server, specify the LDAP module option name **without** the "ldap." prefix.

Configuring a Proxy RADIUS EAS

For Proxy RADIUS external authentication servers, the following fields are displayed in the Edit Authentication Server form.

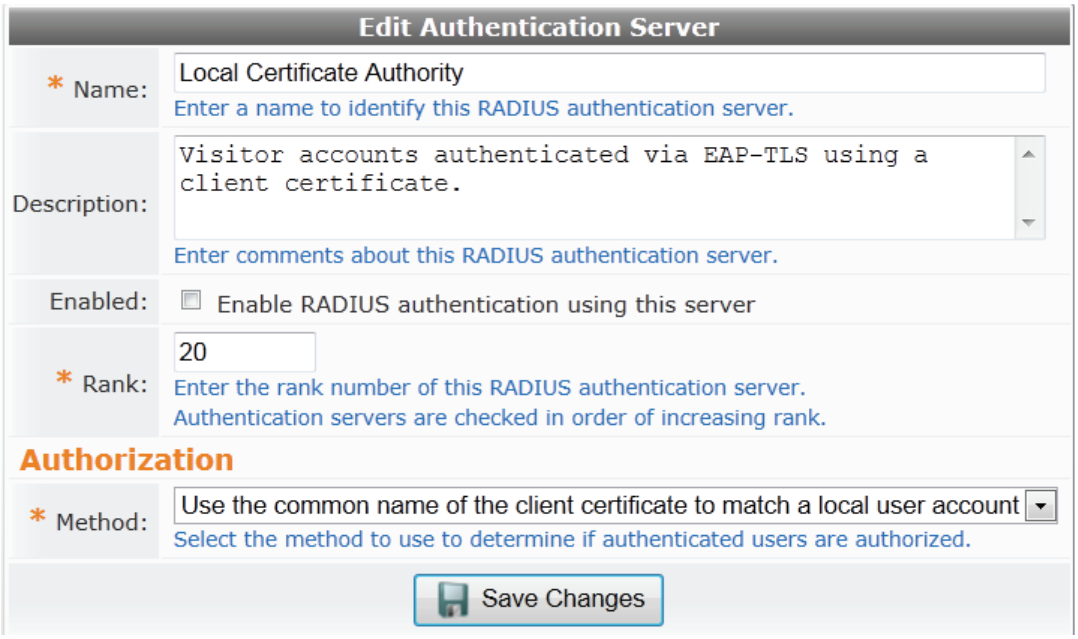


- **RADIUS Server** and **Port Number** – the hostname or IP address of the RADIUS server, with the corresponding port number of the RADIUS authentication service (typically 1812, but can also be 1645).
- **Shared Secret** – the shared secret used by ClearPass Guest as a client of the proxy RADIUS server.
- **Advanced Options** – additional options controlling authentication against the proxy server. No advanced options are currently defined.

To configure the authorization method for a Proxy RADIUS external authentication server, see "Configuring Authorization for External Authentication Servers."

Configuring a Local Certificate Authority EAS

For Local Certificate Authority authentication servers, the following fields are displayed in the Edit Authentication Server form.



1. In the **Name** field, enter a name to uniquely identify this server.
2. (Optional) You can use the **Description** field to include additional information.
3. (Optional) To enable RADIUS authentication for this server, mark the check box in the **Enabled** row.
4. In the **Rank** row, enter a number to specify the ranking order for this server. Authentication servers are checked in order of increasing rank.
5. Under the Authorization heading, choose an authorization method from the **Method** drop-down list. Method options available for Local Certificate Authority servers are:
   - No authorization - Authenticate only
   - Use the common name of the certificate to match a local user account
   - Assign a fixed user role (Contractor, Employee, or Guest)
   - Use PHP code to assign a user role

   For information about these authorization methods, see "Configuring Authorization for External Authentication Servers."

The Test Authentication form for Local Certificate Authority servers includes EAP-TLS settings. For information on testing a Local Certificate Authority authentication server, see "Testing External Authentication Servers."

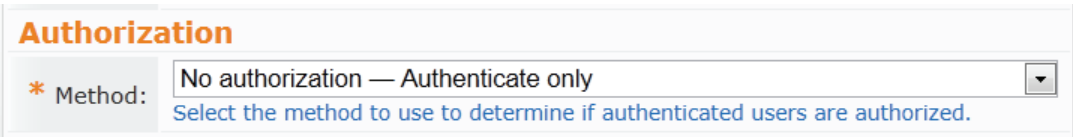
For Local Certificate Authority authentication servers, the RADIUS Authentication Server form also includes a link to the Extensible Authentication Protocol Configuration page, where you can manage EAP configuration settings and view certificate information for the server. See "EAP and 802.1X Authentication and Certificate Management" in this chapter.

Configuring Authorization for External Authentication Servers

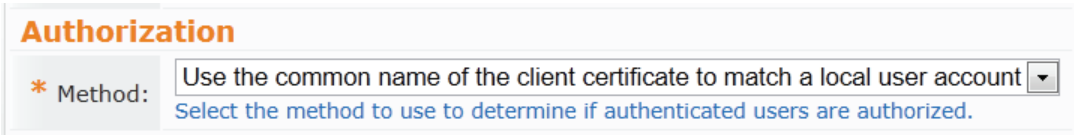
The level of authorized access an authenticated user can have is controlled by the external authentication server's authorization method. To configure a server's authorization method, use the options under the Authorization heading of the RADIUS server's Edit Authentication form.

For more information about authorization methods, including examples, see "About Authorization Methods in External Authentication Servers" in this chapter.

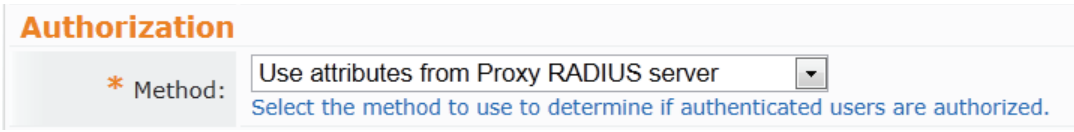
- **No authorization—Authenticate only** may be used to remove all RADIUS attributes not related to authentication.



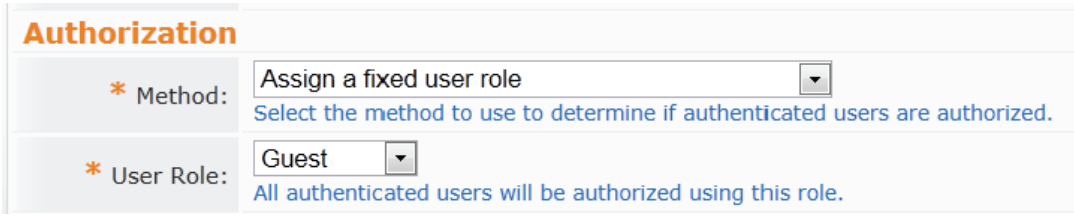
  - The RADIUS server will return an Access-Accept or Access-Reject message indicating the result of the authentication attempt.
- **Use the common name of the client certificate to match a local user account** may be specified for users authenticated via EAP-TLS on a client's local certificate server.



  - The RADIUS server will return an Access-Accept or Access-Reject message indicating the result of the authentication attempt.
- **Use attributes from Proxy RADIUS server** may be used with a Proxy RADIUS external authentication server.

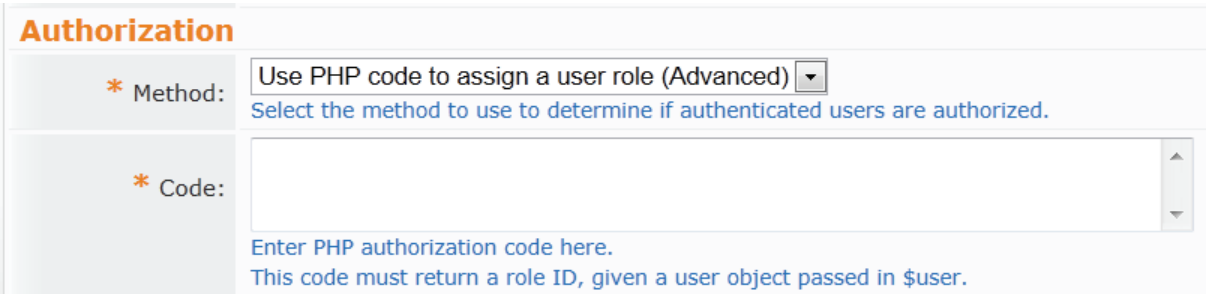


  - The RADIUS server passes through the Access-Accept or Access-Reject message from the proxy server, as well as all RADIUS attributes returned by the proxy server.
  - Use this option when authorization is performed entirely by the proxy RADIUS server.
- **Assign a fixed user role** may be used to map all users authenticated by an external authentication server into a single RADIUS user role.



  - The RADIUS server will return an Access-Reject message if the user authentication fails.
  - If the authentication is successful, the user is authorized using the specified role. The RADIUS server will return an Access-Reject message if the authorization fails.
  - The RADIUS server will return an Access-Accept message that includes the corresponding attributes from the user role if the authentication and authorization steps are both successful.

- **Use PHP code to assign a user role (Advanced)** may be used to control the mapping between the user account returned by an external authentication server and the RADIUS user role.



  - The RADIUS server will return an Access-Reject message if the user authentication fails.
  - If the authentication is successful, the authorization code is evaluated. The user object returned from the external authentication server is available as the variable **$user**.
  - The PHP code should return one of the following values:
    - The ID of a user role (that is, an integer value) to assign that role to the external user.
    - NULL to indicate no role (that is, authentication only).
    - FALSE or a standard result type such as `array('error' => 1, 'message' => 'description of failure')` to indicate an authorization failure
  - Authorization of the user then continues using the specified role ID. The RADIUS server will return an Access-Reject message if the authorization fails.
  - The RADIUS server will return an Access-Accept message that includes the corresponding attributes from the user role if the authentication and authorization steps are both successful.

Click the **Save Changes** button to complete the creation or modification of the external authentication server.


NOTE

You will be prompted to restart the RADIUS server after making configuration changes affecting external authentication.

About Authorization Methods in External Authentication Servers

The level of authorized access an authenticated user can have is controlled by the external authentication server's authorization method.

There are two aspects to user authorization:

- Is the user allowed? Yes/no decisions can be made in the context of authorization. Examples: user account not enabled; user account expired; user account exceeded a traffic quota within a certain time window.
- What are the user's permitted limits? These are not yes/no decisions, but might involve a calculation based on previous usage (for example, via the accounting-based authorization functions), or based on properties of a user account (for example, maximum session lifetime is based on the expiration time for the account).

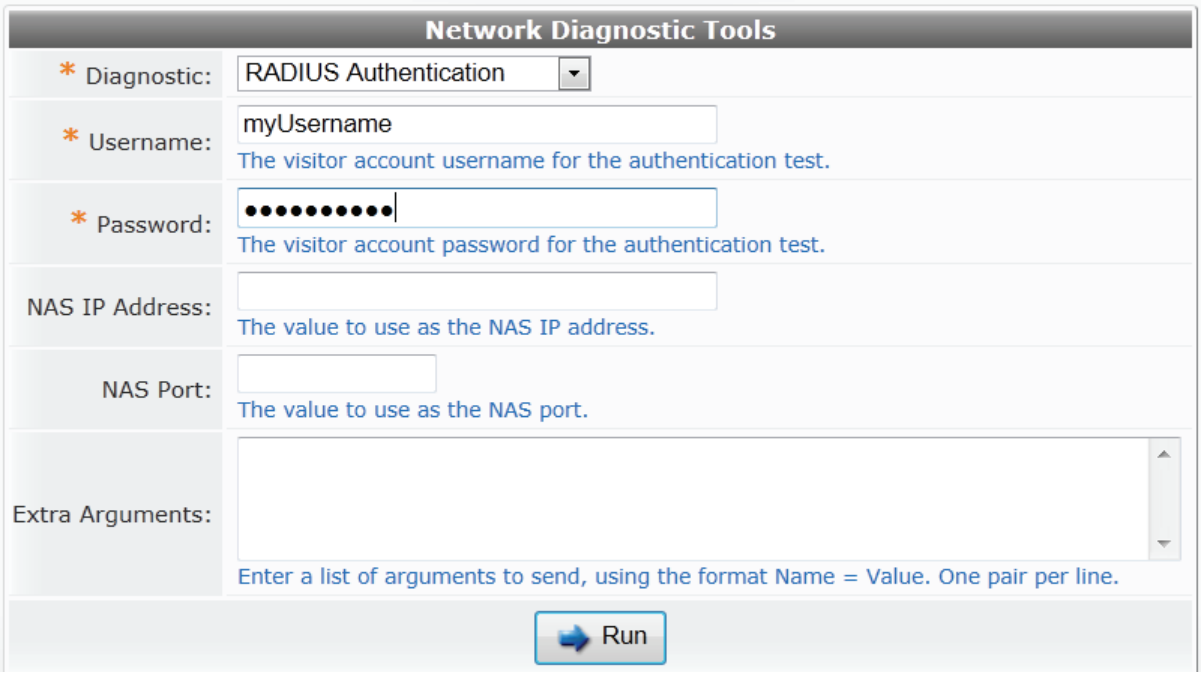
Each server's authorization method can be configured. The authorization methods available vary according to the type of authentication server:

- **No authorization — Authenticate only** may be used to provide a basic user authentication service. The RADIUS server will respond with an Access-Accept or Access-Reject for the authentication attempt. Only RADIUS attributes directly related to user authentication will be returned; all other attributes will be ignored.

- **Use role assigned to local user** is the only authorization method available for the local user database. If the user's authentication attempt is successful, the RADIUS server will respond with an Access-Accept message that includes the RADIUS attributes defined for the user's role.
- **Use the common name of the client certificate to match a local user account** may be specified for users authenticated via EAP-TLS on a client's local certificate server.
- **Use attributes from Proxy RADIUS server** is an authorization method available only for Proxy RADIUS servers. The RADIUS attributes returned by the external RADIUS server are returned unmodified.
- **Assign a fixed user role** may be used to assign all authenticated users to a particular user role. If the user's authentication attempt is successful, the RADIUS server will respond with an Access-Accept message that includes the RADIUS attributes defined for the fixed role that has been selected for this authentication server.
- **Use PHP code to assign a user role (Advanced)** may be selected to return a role ID for users authenticated via EAP-TLS on a client's local certificate server. The PHP authorization code is entered on the Edit Authentication Server form.

The RADIUS Authentication diagnostic can be used to demonstrate the difference between the various authorization methods.

To use the diagnostic, navigate to **RADIUS Services > Server Control** and click the **Test RADIUS Authentication** command link. Enter the username and password for a user that is externally authenticated.



Click the **Run** button to perform RADIUS authentication and display the results:

- With authorization method **No authorization – Authenticate only**:

```
Sending Access-Request of id 165 to 127.0.0.1 port 1812
User-Name = "demouser"
User-Password = "XXXXXXXX"
rad_recv: Access-Accept packet from host 127.0.0.1:1812, id=165, length=20
```

Note that in this case, no RADIUS attributes are returned. The Access-Accept or Access-Reject result indicates whether the user was successfully authenticated.

- With authorization method **Assign a fixed user role**:

```
Sending Access-Request of id 122 to 127.0.0.1 port 1812
User-Name = "demouser"
User-Password = "XXXXXXXX"
rad_recv: Access-Accept packet from host 127.0.0.1:1812, id=122, length=27
Reply-Message = "Guest"
```

Note that in this case, the RADIUS attribute returned (Reply-Message) corresponds to the user role selected.

- With authorization method **Use PHP code to assign a user role (Advanced)** – more complex authorization rules can be implemented to specify which role to assign to an authenticated user. Authorization can use any of the available properties of the user account, as well as taking into account other factors such as the time of day, previous usage, and more.

Advanced Authorization — Example 1

This example covers the case where a domain contains several organizational units (OUs), and the users in each OU are to be mapped to a specific RADIUS role ID.

To determine the appropriate role ID, navigate to **RADIUS Services > User Roles** and check the ID column for the appropriate role.

For example, to implement the following configuration:

- OU **East** should be mapped to RADIUS role ID 4
- OU **Central** should be mapped to RADIUS role ID 5
- OU **West** should be mapped to RADIUS role ID 6

Make sure the following configuration is set:

1. First, ensure that the Base DN for the authentication server is set to the root of the domain – for example: **DC=server,DC=local** – rather than the “users” container. This is necessary as the organizational units are located below the top level of the directory and cannot be searched from the **CN=Users** container.
2. Select the authorization method **Use PHP code to assign a user role (Advanced)** and use the following code:

```
if (stripos($user['distinguishedname'],'OU=East')!== false) return 4;
if (stripos($user['distinguishedname'],'OU=Central')!== false) return 5;
if (stripos($user['distinguishedname'],'OU=West')!== false) return 6;
return false;
```

Explanation: During user authorization, the distinguished name of the user (which will contain the user’s OU) is checked against the defined rules, and an appropriate role ID is returned. If no match is found, false is returned, which means that authorization fails and the user’s Access-Request will be rejected. Information on the stripos function for case-insensitive substring matching can be found at stripos().

Advanced Authorization — Example 2

This example covers the case where users are assigned group memberships, and users in a particular group are to be mapped to a specific RADIUS role ID.

To determine the appropriate role ID, navigate to **RADIUS Services > User Roles** and check the ID column for the appropriate role.

For example, to implement the following configuration:

- Members of the **Domain Admins** group should be mapped to RADIUS role ID 4
- Members of the **Users** group should be mapped to RADIUS role ID 5
- All other users should be rejected

Select the authorization method **Use PHP code to assign a user role (Advanced)** and use the following code:

```
if (in_array('CN=Domain Admins,CN=Users,DC=server,DC=local', $user['memberof']))
return 4;
if (in_array('CN=Users,CN=Builtin,DC=server,DC=local', $user['memberof'])) return 5;
return false;
```

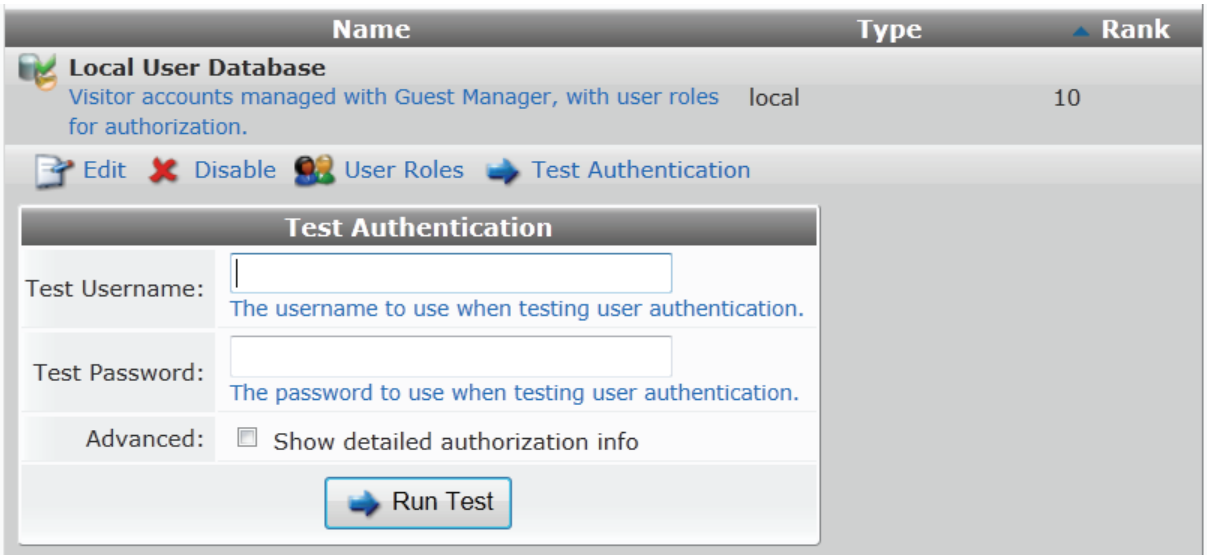
Explanation: During user authorization, the 'memberOf' attribute of the user (which will contain a list of the groups to which the user belongs) is checked against the defined rules, and an appropriate role ID is returned. If no match is found, false is returned, which means that authorization fails and the user's Access-Request will be rejected.

The in_array() comparison is done in a case-sensitive manner. Be sure to use the correct case as returned by the LDAP query for the group name. Also note that the complete distinguished name (DN) for the group must be specified, as this is the value checked for in the array of values returned for the 'memberOf' attribute.

The primary group of a user assigned in Active Directory cannot be checked in this way, as Active Directory does not return the primary group in the values of the 'memberOf' attribute. You can build logic that uses the $user['primarygroupid'] property instead to work around this issue.

Testing External Authentication Servers

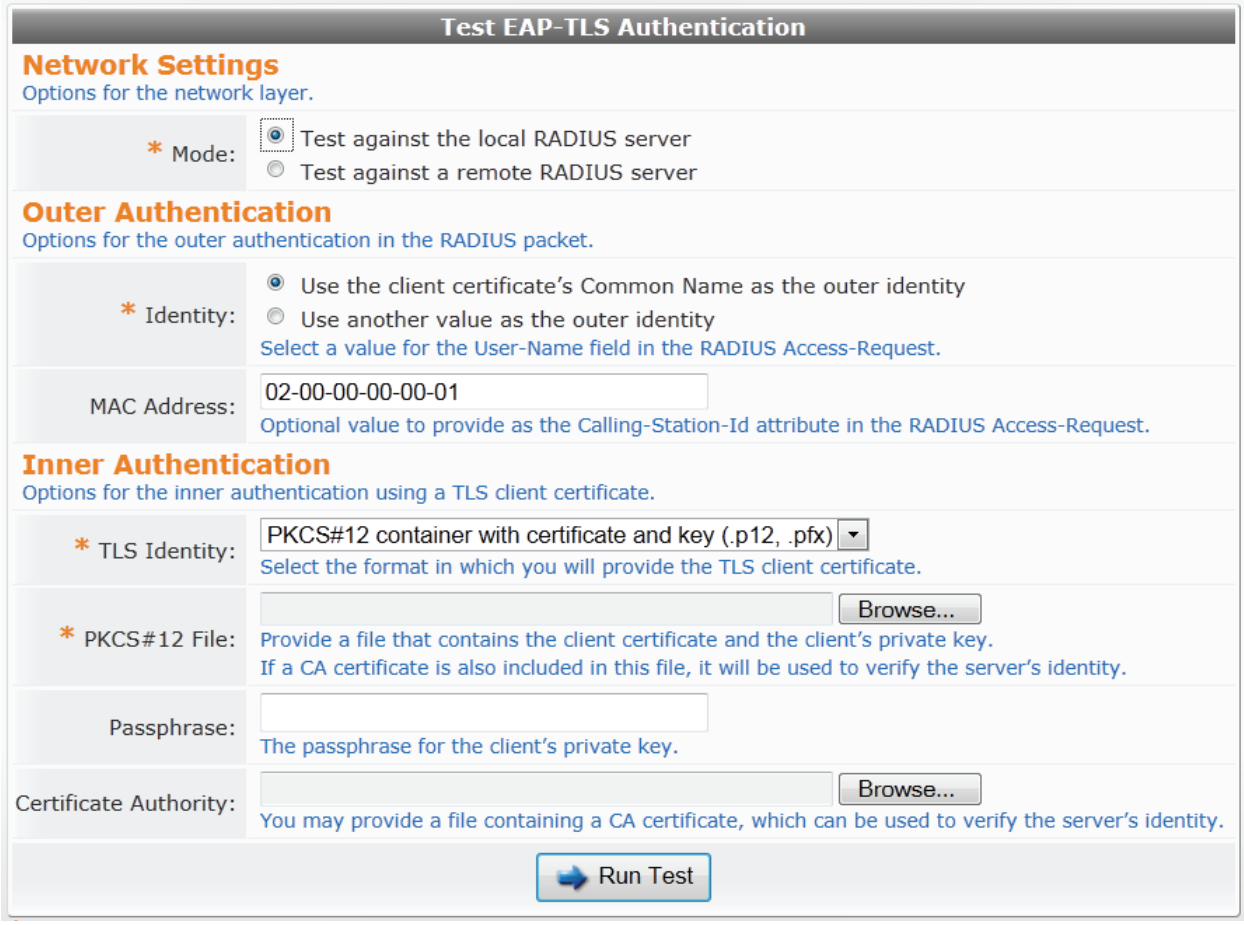
The Test Authentication option for a server may be used to check the connection to an authentication server, or verify the authorization rules that have been configured. To test an authentication server, click its **Test Authentication** link on the Edit Authentication Server form. The server's row expands to include the Test Authentication form.



1. In the **Test Username** and **Test Password** fields, enter the information for a user's credentials stored on the server.
2. (Optional) To view additional details—for example, authentication rules, or account status or permitted limits—mark the **Show detailed authorization info** check box in the **Advanced** row.
3. Click the **Run Test** button. A progress bar is shown during the test, and results are displayed below the Test Authentication form.

Testing a Local Certificate Authority EAS

For Local Certificate Authority external authentication servers, additional testing options are included to simulate EAP-TLS authentication with a client certificate.



1. To specify the network layer to test against, mark the radio button in the **Mode** row for either the local RADIUS server or a remote RADIUS server.
2. To indicate the value for the User-Name field for outer authentication in the RADIUS access request, mark one of the radio buttons in the **Identity** row. You can use either the client's local certificate's common name or another value.
3. (Optional) You may enter a value in the **MAC Address** field for the Calling-Station-Id attribute.
4. In the **TLS Identity** drop-down list, choose the format of the TLS client certificate. The rest of the options available in the Inner Authentication area of the form depend on the TLS Identity selected. To provide details for the selected TLS identity, do one of the following:

If you selected *PKCS#12 container with certificate and key (.p12, .pfx)* for the TLS identity:

1. In the **PKCS#12** row, browse to the file in your system that contains both the client certificate and the client's private key. When this file is uploaded, if a CA certificate is also included, it is used to verify the server's identity.
2. (Optional) In the **Passphrase** row, you may enter the passphrase for the client's private key.
3. (Optional) To provide a file containing a CA certificate for verifying the server's identity, you can use the **Certificate Authority** row to browse to the file.

If you selected *Separate certificate and key files (.pem, .cer, .crt)* for the TLS identity:

1. In the **PKCS#12** row, browse to the file in your system that contains both the client certificate and the client's private key. When this file is uploaded, if a CA certificate is also included, it is used to verify the server's identity.
2. In the **Client Certificate** row, browse to the file containing the client certificate. This must be a base-64 encoded (PEM) or binary encoded (DER) certificate.
3. In the **Client Private Key** row, browse to the file containing the client's private key. This must be a base-64 encoded (PEM) or binary encoded (DER) private key file.
4. (Optional) In the **Passphrase** row, you may enter the passphrase for the client's private key.
5. (Optional) To provide a file containing a CA certificate for verifying the server's identity, you can use the **Certificate Authority** row to browse to the file.

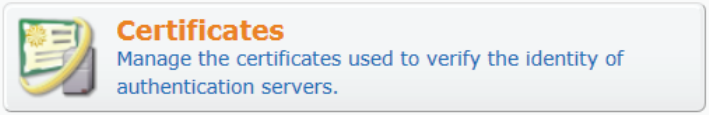
If you selected *Copy and paste as text* for the TLS identity:

1. In the **PKCS#12** row, browse to the file in your system that contains both the client certificate and the client's private key. When this file is uploaded, if a CA certificate is also included, it is used to verify the server's identity.
2. In the **Client Certificate** row, copy and paste the client certificate. This block of encoded text must include the lines "BEGIN CERTIFICATE" and "END CERTIFICATE".
3. In the **Client Private Key** row, copy and paste the client's private key. This block of encoded text must include the lines "BEGIN RSA PRIVATE KEY" and "END RSA PRIVATE KEY".
4. (Optional) In the **Passphrase** row, you may enter the passphrase for the client's private key.
5. (Optional) To provide a file containing a CA certificate for verifying the server's identity, you can use the **Certificate Authority** row to browse to the file.

When you have completed the fields for the network settings, outer authentication, and inner authentication, click the **Run Test** button.

Managing Certificates for External Authentication Servers

Use the **Certificates** command link on the **RADIUS > Authentication** page to manage the list of trusted certificates used to identify external authentication servers.



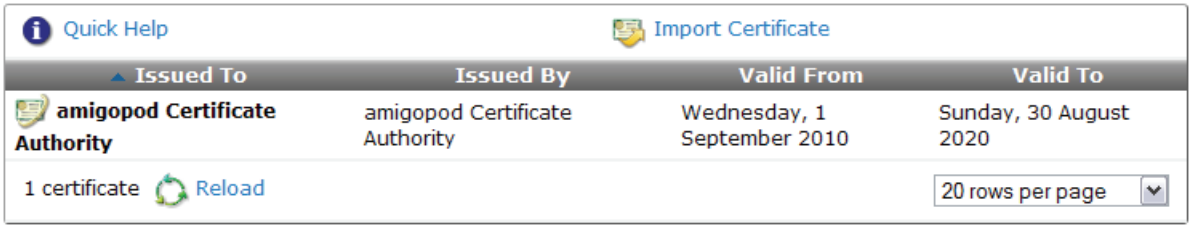
External authentication servers may be configured to use a TLS (Transport Layer Security) connection. For example, LDAP connections on port 636 use TLS (SSL) to provide a secure connection.

TLS connections offer two kinds of security guarantees: **privacy** (meaning that the content of communications cannot be intercepted or modified), and **authentication** (meaning that the identity of the server can be verified).

The public key infrastructure (PKI) required to provide these guarantees is based on the X.509 standard for digital certificates.

To verify the identity of an authentication server, use the RADIUS Certificates list view to install one or more digital certificates for a certificate authority (CA). These certificates will be trusted for the purposes of identifying a remote server.

When a TLS connection to an authentication server is established, the authentication server must identify itself with a certificate issued by one of the trusted certificate authorities. If the authentication server's identity cannot be established, the connection will fail.



The list displays the certificates that have been installed. By default, the list is empty.

After selecting a certificate in the list, the following actions are available:

- **Show Details** – display information about the certificate, including its unique "fingerprint" identifier and technical information about the certificate.
- **Export Certificate** – download the certificate in one of several different formats (PKCS#7, base-64 encoded, binary X.509, or plain text).
- **Delete** – remove the certificate so that it will no longer be used for trust purposes.

To import a new certificate, click the **Import Certificate** tab. Use the **Import Certificate** form to specify a certificate file to upload.

The supported formats for digital certificates are:

- **Binary X.509 certificate** – also known as ASN.1 or DER format. Certificates in this format typically have the file extension **.cer** or **.crt**.
- **Base-64 encoded** – also known as PEM format. Certificates in this format typically have the file extension **.cer**, **.cert** or **.pem**.
- **PKCS#7 container** – multiple certificates may be included in these containers. Certificates in this format typically have the file extension **.p7b**.

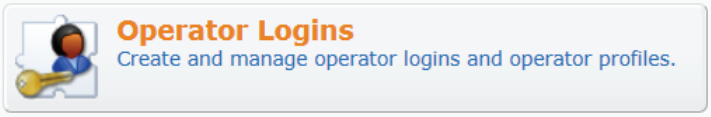
An operator is a company's staff member who is able to log in to ClearPass Guest. Different operators may have different roles that can be specified with an operator profile. These profiles might be to administer the ClearPass Guest network, manage guests, or run reports.

Operators may be defined locally in ClearPass Guest, or externally in an LDAP directory server.

Accessing Operator Logins

The Operator Logins management is located in the Administrator section of the application.

Use the Operator Logins command link on the **Administrator** start page to access the Operator Logins features.



Alternatively, use the Administrator navigation menu to jump directly to any of the features within 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.

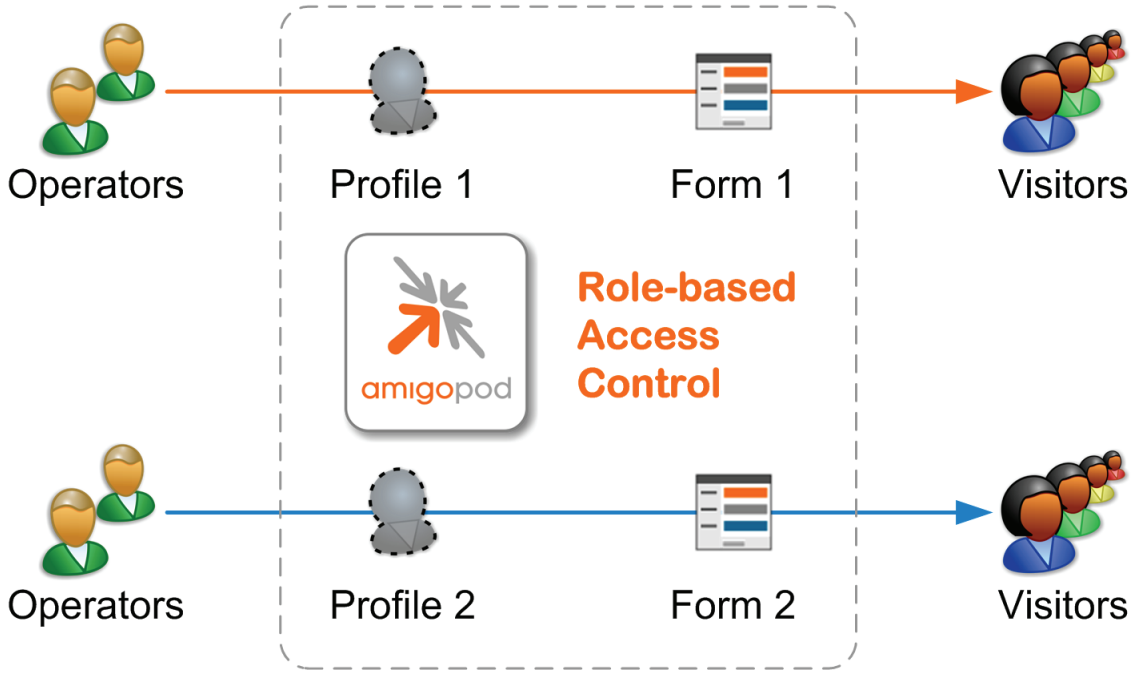
Two types of operator logins are supported: local operators and operators who are defined externally in your company's directory server. Both types of operators use the same login screen.

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 table.

Figure 23 *Operator profiles and visitor access control*



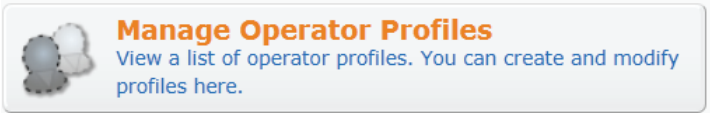
See "About Operator Logins" in this chapter for details on configuring different forms and views for operator profiles.

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.

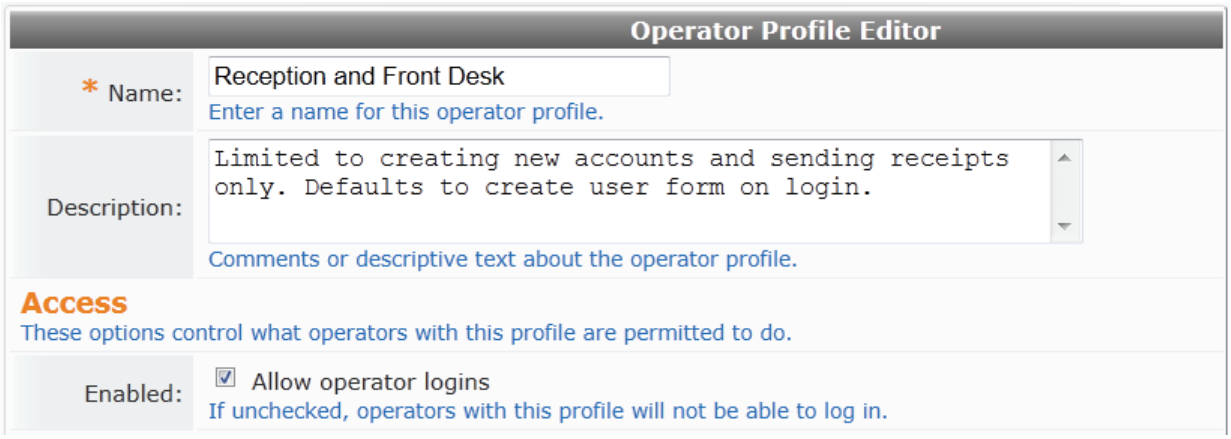
Click the **Manage Operator Profiles** command link on the **Administrator > Operator Logins** page to define new operator profiles, and to make changes to existing operator profiles.



Creating an Operator Profile

Click the **Create Operator Profile** link to create a new operator profile.

The **Operator Profile Editor** form is displayed. This form has several sections, which are described in more detail below.



The fields in the first area of the form identify the operator profile and capture any optional information:

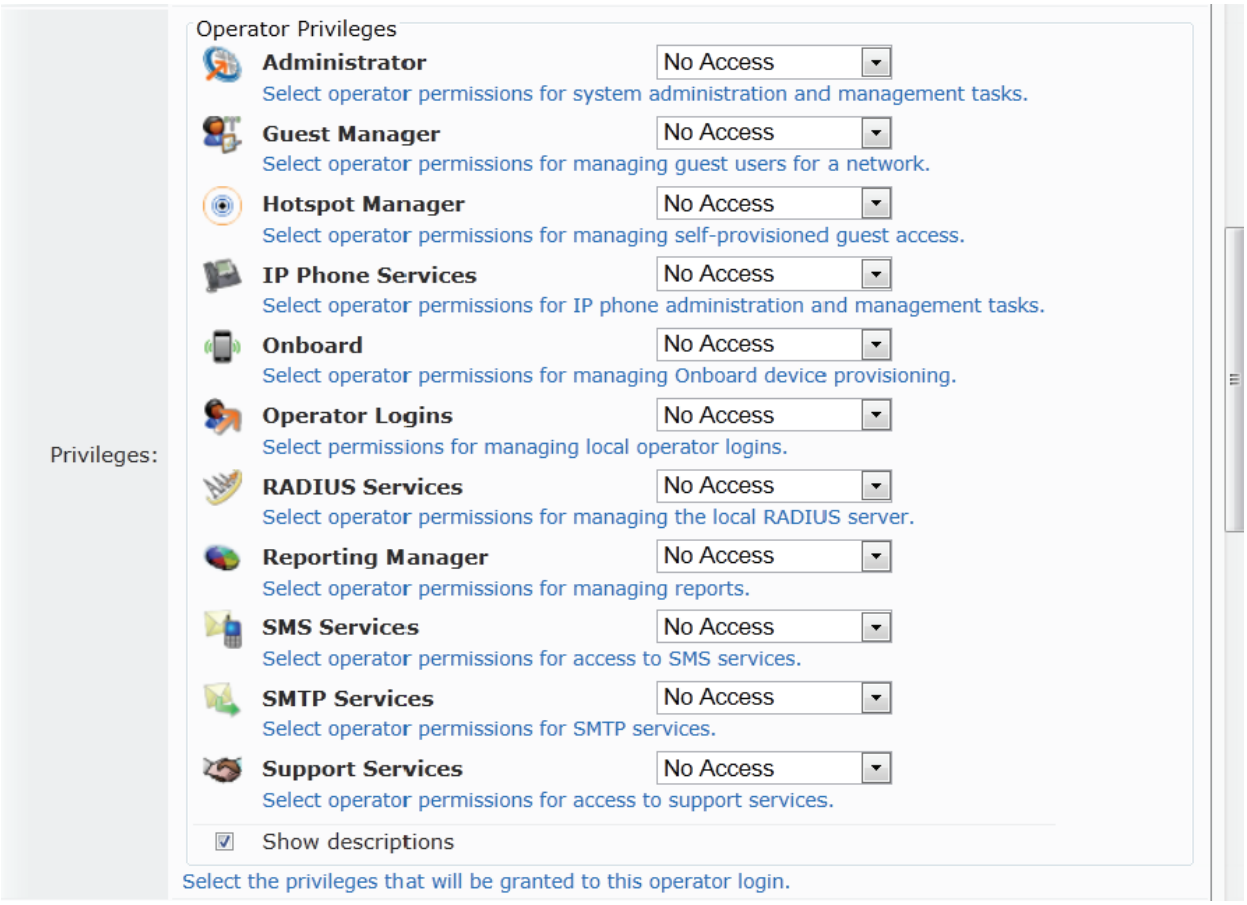
1. You must enter a name for this profile in the **Name** field.
2. (Optional) You may enter additional information about the profile in the **Description** field.

The fields in the second area of the form define permissions for the operator profile:

1. To disable a profile, unmark the **Allow Operator Logins** check box in the **Enabled** row. If a profile is disabled, any operators with that profile will be unable to log in to the system. This may be useful when performing system maintenance tasks.
2. In the **Password Options** row, you may keep the default setting or choose an option from the drop-down list.

   Password options are as follows:

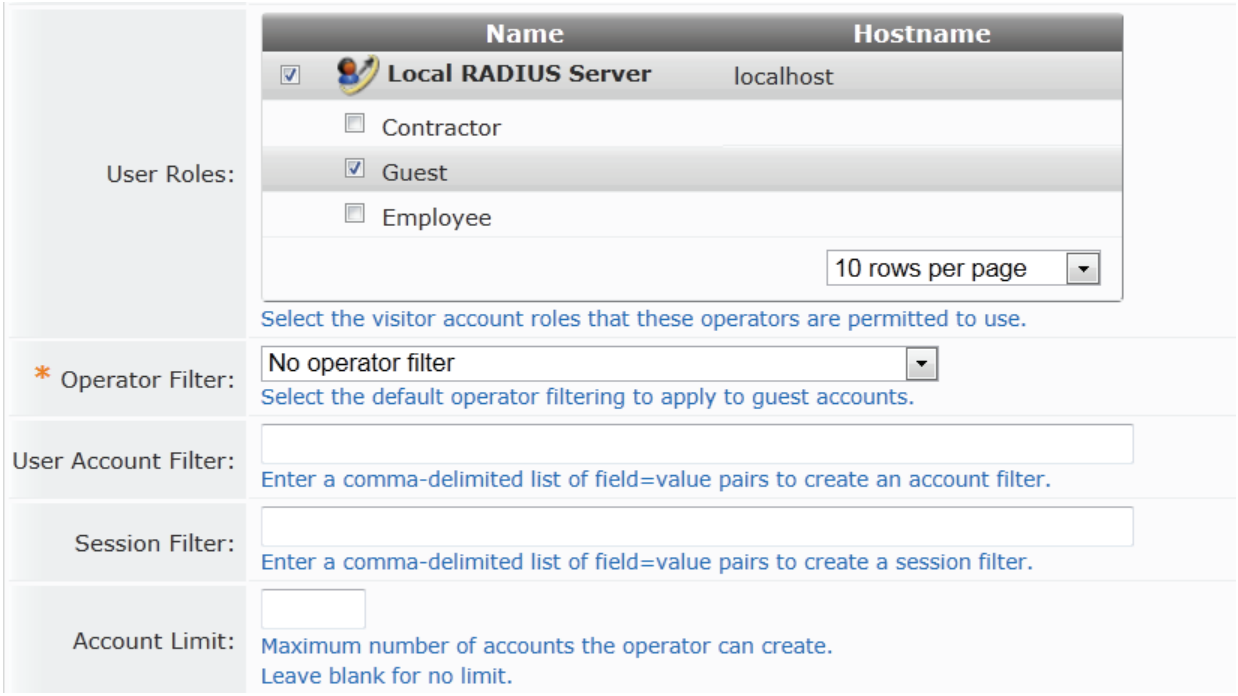
   - **Allow operators to change their password** – Enables the Change Password link in the navigation, which allows an operator to change their password. This is the default setting.
   - **Prevent operators from changing their password** – The password cannot be changed by the operator. Use this option if a single operator login will be shared by several people.
   - **Force a password change on their next login** – The operator will be prompted to change their password the next time they log in to the application.
   - **Force a password change on their first login** – The operator will be prompted to change their password the first time they log in to the application.
3. In the **Privileges** area, use the drop-down lists to select the appropriate permissions for this operator profile.



For each permission, you may grant No Access, Read Only Access, Full Access, or Custom access. The default in all cases is No Access. This means that you must select the appropriate privileges in order for the profile to work. See "Operator Profile Privileges" in this chapter for details about the available access levels for each privilege.

If you choose the **Custom** setting for an item, the form expands to include additional privileges specific to that item.

4. The **User Roles** list allows you to specify which user databases and roles the operator will be able to access.



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.

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.

5. The **Operator Filter** may be set to limit the types of accounts that can be viewed by operators. Options include: default, no operator filter, only show accounts created by the operator, and only show accounts created by operators within their profile.
6. The **User Account Filter** and **Session Filter** fields are optional, and allow you to create and configure these filtering options:
   - The **User Account Filter** field lets you create a persistent filter applied to the user account list. For example, this feature is 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.
   - The **Session Filter** field lets you create a filter for only that session. To create a session filter, enter a comma-delimited list of field-value pairs. Supported operators are described below.

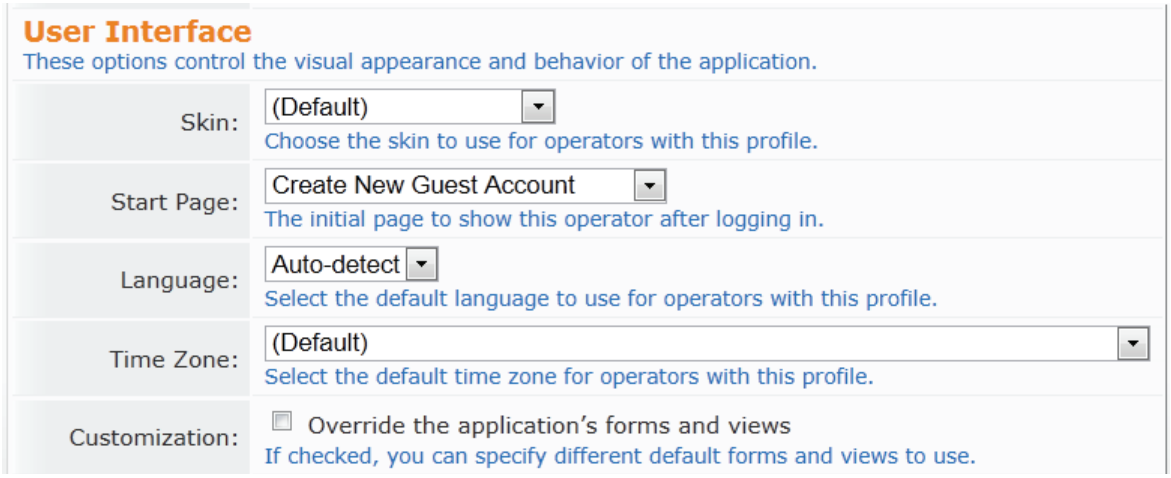
The user can enter a simple substring to match a portion of the username or any other fields that are configured for search, and may include the following operators:

Table 19 *Operators supported in filters*

Operator	Meaning	Additional Information
=	is equal to	You may search for multiple values when using the equality (=) or inequality !=) operators. To specify multiple values, list them separated by the pipe character (|). 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".
!=	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	

7. In the **Account Limit** row, you can enter a number to specify the maximum number of accounts an operator can create. Note that disabled accounts are included in the account limit. To set no limit, leave the Account Limit field blank.

Configuring the User Interface



The fields in the third 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" in this chapter.

1. (Optional) In the **Skin** row, the **Default** setting indicates that the skin plugin currently marked as enabled in the Plugin Manager will be used. To have a different skin displayed for users with this operator profile, choose one of the available skins from the drop-down list. For more information on skins, see "Configuring the Aruba ClearPass Skin Plugin" in the Administrator Tasks chapter.
2. (Optional) In the **Start Page** row, the **Default** setting 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.

3. (Optional) In the **Language** row, the default setting is **Auto-detect**. This lets the application determine the operator's language preference from their local system settings. To specify a particular language to use in the application, choose the language from the drop-down list.
4. (Optional) In the **Time Zone** row, the **Default** setting indicates that the operator's time zone will default to the system's currently configured time zone. You can use the drop-down list to specify a particular time zone.

Customizing Forms and Views

1. (Optional) In the **Customization** row, to specify that an operator profile should use a different form when creating a new visitor account, select the **Override the application's forms and views** check box. 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.
2. Click the **Save Changes** button to complete the creation of an operator profile.

Operator Profile Privileges

The privilege selections available for an operator profile provide you with control over the functionality that is available to operators.

No Access means that 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 means that the operator can see the options available but is unable to make any changes to them.

Full Access means that all the options are available to be used by the operator.

Custom access allows you to choose individual permissions within each group. For example, Guest Manager allows you to control access to the following areas:

- 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

Refer to the description of each individual operator privilege to determine what the effects of granting that permission will be.

Managing Operator Profiles

Once a profile has been created you are able to view, to edit and to create new profiles. When you click an operator profile entry in the Operator Profiles list, a menu appears that allows you to perform any of the following operations:

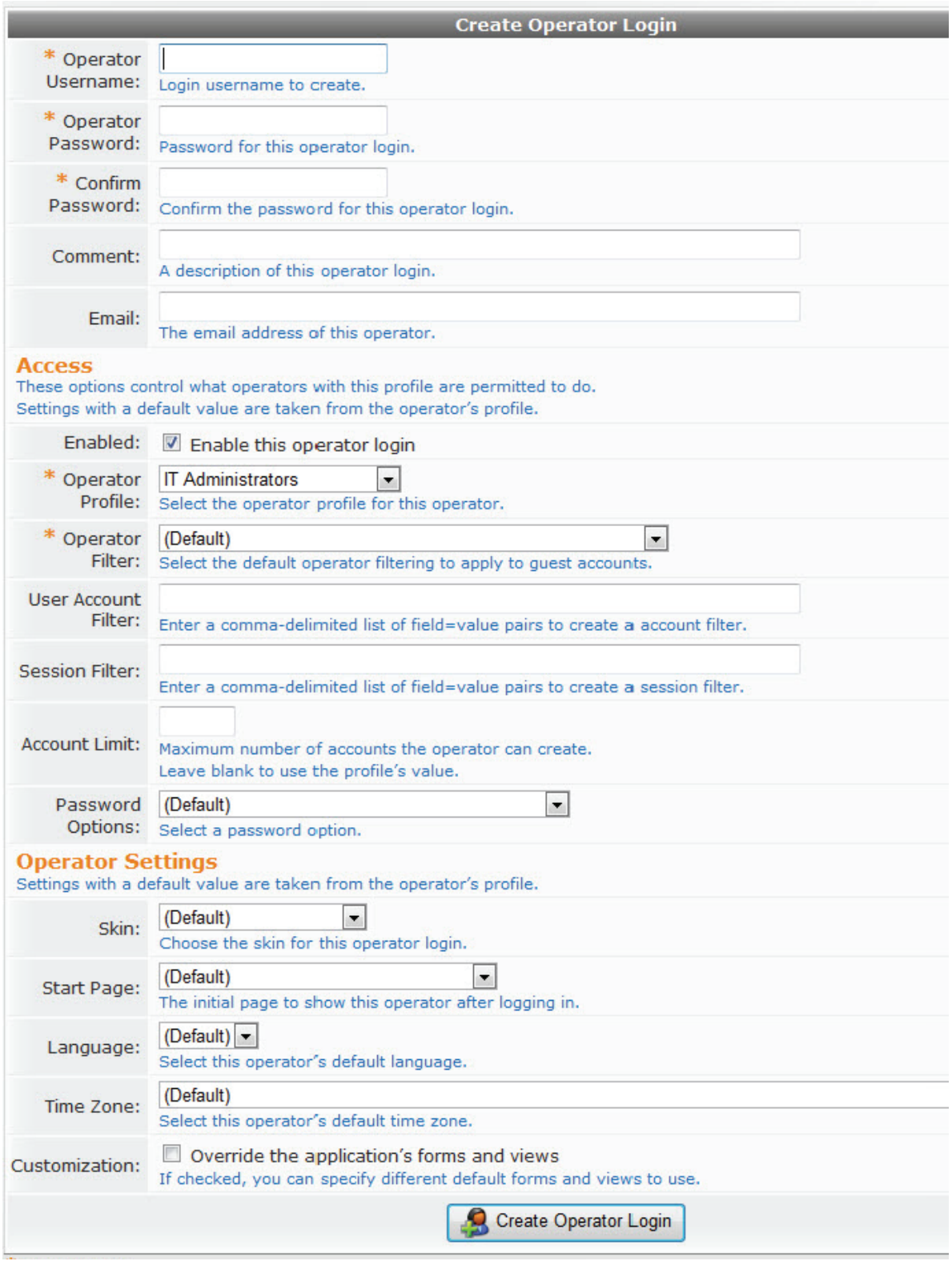
- **View/Hide Details** – displays or hides configuration details for the selected operator profile, including the profile name, description, operator login access, and the settings for the defined skin, start page, language and time zone.
- **Edit** – changes the properties of the specified operator profile
- **Delete** – removes the operator profile from the Operator Profiles list
- **Duplicate** – creates a copy of an operator profile
- **Create Operator** – opens the **Create Operator Login** form, allowing you to create a new operator login associated with the selected operator profile.
- **Show Operators** – shows a list of operator login names associated with that operator profile
- **Show Usage** – opens a window in the Operator Profiles list that shows if 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.

Local Operator Authentication

Local operators are those defined in ClearPass Guest.

Creating a New Operator

After you create a profile, you can create an operator to use that profile.



Any properties for the operator login that are set to (Default) are taken from the operator profile. The **Operator Filter** field lets you select from three other options besides Default:

- No operator filter—All guest accounts display.
- Only show accounts created by the operator—Only guest accounts created by the operator display.
- Only show accounts by operators created within their profile—Only guest accounts created by all operators within a profile display.

The **User Account Filter** and **Session Filter** fields are optional, and allow you to create and configure these filtering options:

- The **User Account Filter** lets you create a filter for the user account list that cannot be overridden by the operator. This filter is designated by role and is persistent. For example, this feature is useful in large deployments where an administrator wants the operators to only 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.
- The **Session Filter** field lets you create a filter that cannot be overridden by the operator for only that session. To create a session filter, enter a comma-delimited list of field-value pairs. Supported operators are described below.

  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 20 *Operators supported in filters*

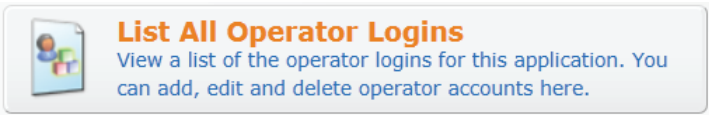
Operator	Meaning	Additional Information
=	is equal to	You may search for multiple values when using the equality (=) or inequality !=) operators. To specify multiple values, list them separated by the pipe character (|). For example, specifying the filter "role_id=2|3, custom_field=Value" restricts the user accounts displayed to those with role IDs 2 and 3 (Guest and Employee), and with the field named "custom_field" set to "Value".
!=	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	

The **Account Limit** field lets you set a limit for the number of accounts that an operator can create. Note that disabled accounts are included in the account limit. Leave the Account Limit field blank to use the Operator profile's account limit setting.

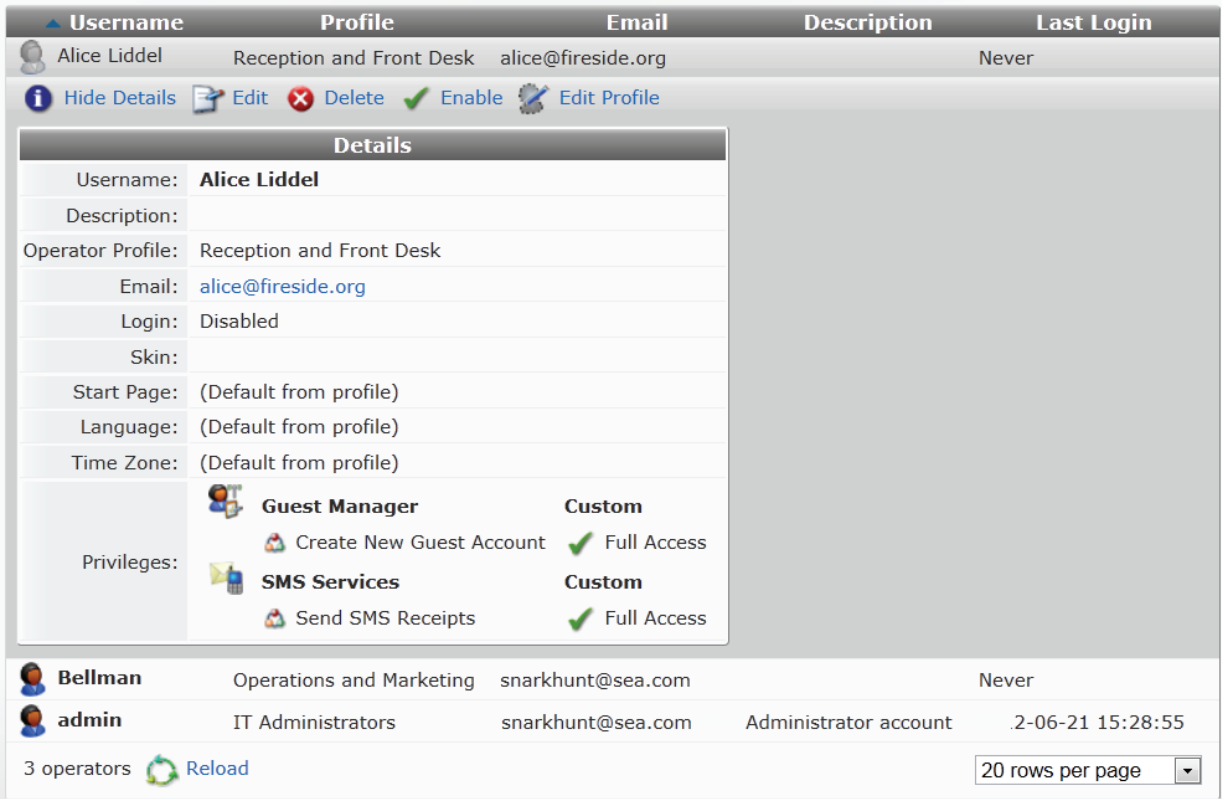
Once all the fields have been completed, click the ✔ **Create Operator Login** button to finalize the creation of this operator login.

Viewing All Operator Logins

To view a list of operators, go to **Administrator > Operator Logins** and click the **List All Operator Logins** command.



The Operator Logins list opens.



When you click an operator login entry in the Operator Logins list, the row expands to provide links that allow you to perform various operations. Depending on the operator entry, the operations available may include:

- **View/Hide Details**—displays or hides configuration details for the selected operator login
- **Edit**—opens the Edit Operator Login page for changing the properties of the specified operator login
- **Delete**—removes the operator login from the Operator Logins list
- **Disable**—temporarily disables an operator login while retaining its entry in the Operator Logins list
- **Enable**—reenables a disabled operator login
- **Duplicate**—makes a copy of the profile to use as a basis for a new profile
- **Edit Profile**—opens the operator profile editor, allowing you to edit the operator profile associated with the selected operator login name
- **Create Operator**—opens the Create Operator Login page
- **Show Operators**—adds a list of the operators that have the selected profile, and shows username, description, and actions for each
- **Show Usage**—adds a list of the number of logins and operator servers currently using the selected profile

Changing Operator Passwords

To change the password for an operator, edit the operator login and type a new password in the “Operator Password” and “Confirm Password” password fields. You may also want to select “Force a password change on their next login” under Password Options to allow the operator to select a new password.

Operators can change their own passwords by navigating to **Home > Change Password**, entering a new password into the **Change Password** form, then clicking the **Set Password** button to save your new password.

LDAP 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.

The **Manage LDAP Server** and the **LDAP Translation Rules** commands allow you to set up operator logins integrated with a Microsoft Active Directory domain or another LDAP server.

NOTE

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.

Manage LDAP 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, POSIX-compliant directory servers, and RADIUS servers.

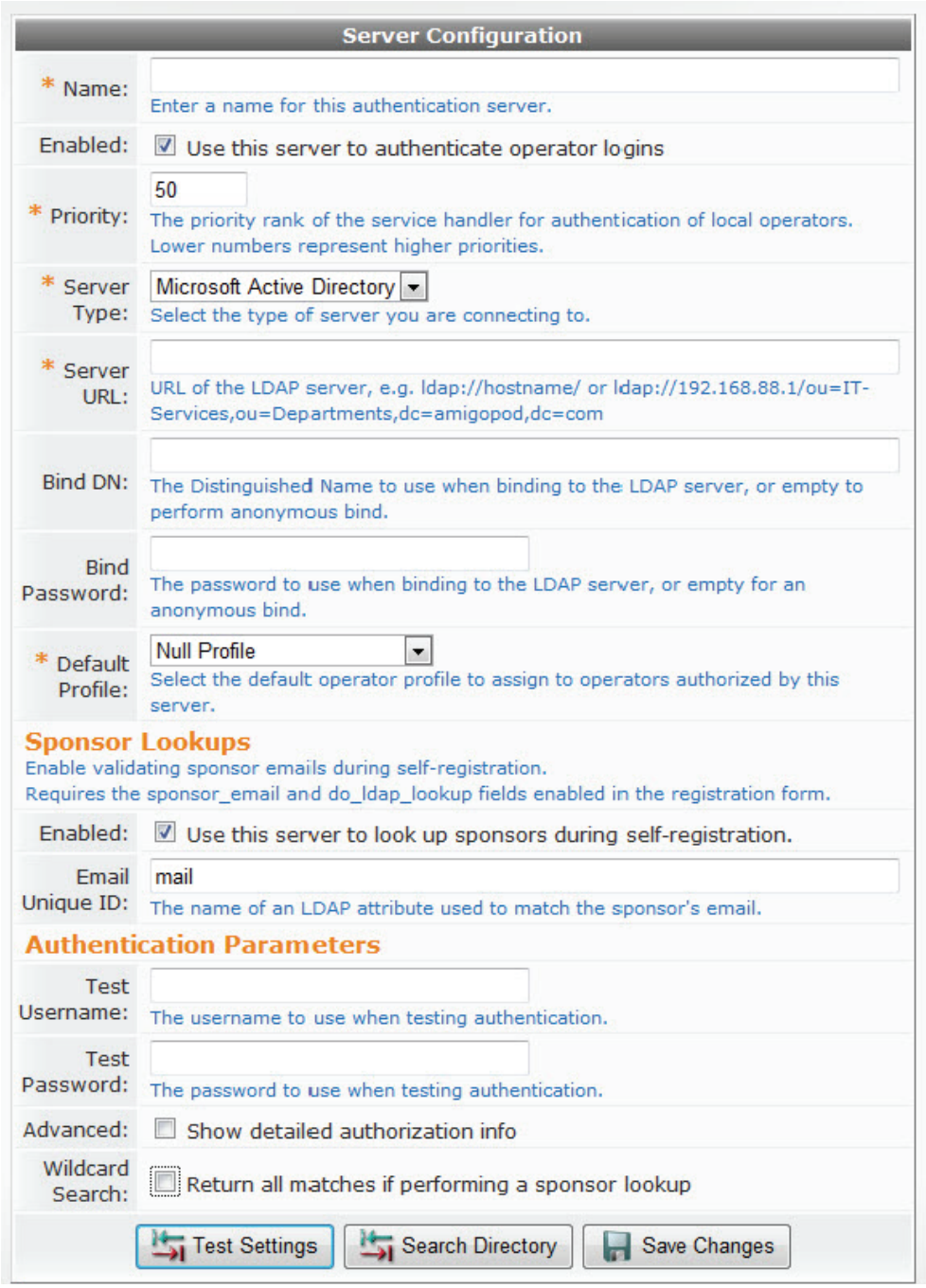
When an operator attempts to log in, each LDAP server that is enabled for authentication is checked, in order of priority from lowest to highest.

Once 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.

Creating an LDAP Server

To create an LDAP server, go to **Administrator > Operator Logins > Servers** , then click the **Create new LDAP server** link below the server list. The Edit Authentication Server form opens.



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" in this chapter for more details about the types of LDAP URL you may specify.

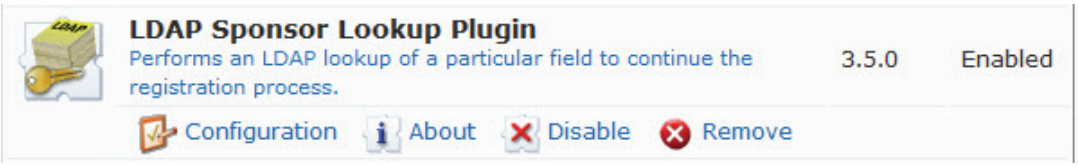
Select the **Enabled** option if you want this server to authenticate operator logins.

This form allows you to specify the type of LDAP server your system will use. Click the **Server Type** drop-down list and select one of the following options:

Table 21 *Server Type Parameters*

Server Type	Required Configuration Parameters
Microsoft Active Directory	• **Server URL**: The URL of the LDAP server • **Bind DN**: The password to use when binding to the LDAP server, or empty for an anonymous bind. • **Bind Password**: If your LDAP server does not use anonymous bind, you must supply the required credentials to bind to the directory. (Leave this field blank to use an anonymous bind.) • **Default Profile**: The default operator profile to assign to operators authorized by this LDAP server.
POSIX Compliant:	• **Server URL**: The URL of the LDAP server • **Bind DN**: The password to use when binding to the LDAP server, or empty for an anonymous bind. • **Bind Password**: The password to use when binding to the LDAP server. Leave this field blank to use an anonymous bind. • **Base DN**: The Distinguished Name to use for the LDAP search. • **Default Profile**: The default operator profile to assign to operators authorized by this LDAP server.
Custom	• **Server URL**: The URL of the LDAP server • **Bind DN**: The password to use when binding to the LDAP server, or empty for an anonymous bind. • **Bind Password**: The password to use when binding to the LDAP server. Leave this field blank to use an anonymous bind. • **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 retreive. Or leave bland to retrieve all attributes (default). • **Default Profile**: The default operator profile to assign to operators authorized by this LDAP server.
RADIUS	• **RADIUS Server**: The hostname or IP address of the RADIUS server. • **Port Number**: The port number of the RADIUS authentication service. • **Shared Secret**: The shared secret for the RADIUS server. • **Authentication Method**: The authentication method that supplies the credentials. • **Default Profile**: The default operator profile to assign to operators authorized by this server.

Select the **Enabled** check box under **Sponsor Lookups** if you want to enable the validation of sponsor emails during self-registration. This option causes this server to 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. This feature requires the LDAP Sponsor Lookup plugin. Use the Plugin Manager to verify that this plugin is available.



Once you have completed the form, check your settings by clicking the **Test Settings** button. Use the **Test Username** and **Test Password** fields to supply a username and password for the authentication check. If the authentication is successful, the operator profile assigned to the username will be displayed. If the authentication fails, an error message will be displayed. See "LDAP Operator Server Troubleshooting" in this chapter for information about common error messages and troubleshooting steps to diagnose the problem.

Click the **Save Changes** button to save 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

For Microsoft Active Directory, 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://192.168.88.1/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 **ldap3s://** if you are using LDAP v3 over SSL/TLS.

When Microsoft Active Directory is selected as the Server Type, LDAP v3 is automatically used.

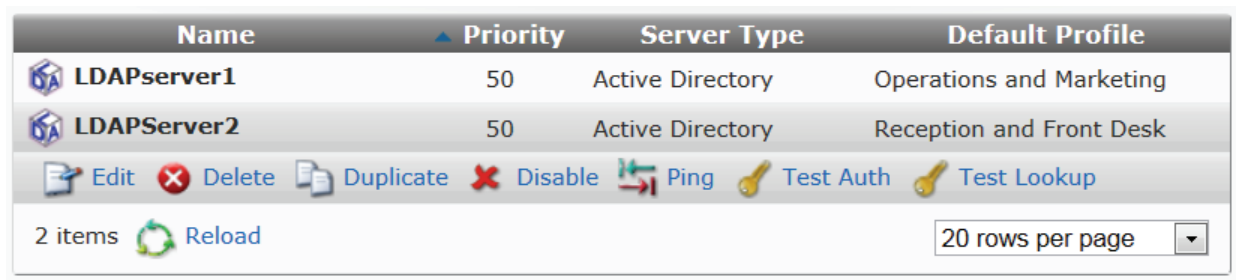
An LDAP v3 URL has the format **ldap://host:port/dn?attributes?scope?filter?extensions**.

- **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.

Viewing the LDAP Server List

Once you have defined one or more LDAP servers, those servers will appear in the LDAP server list on the **Administrator > Operator Logins > Servers** page.



Select any of the LDAP servers in the list to display options to perform the following actions on the selected server:

- **Edit**—Changes the properties of an LDAP server.
- **Delete**—Removes the server from the LDAP server list.
- **Duplicate**—Creates a copy of an LDAP server.
- **Disable**—Temporarily disables a server while retaining its entry the server list.
- **Enable**—Reenables 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.
- **Test Auth**—Adds a **Test Operator Login** area in the LDAP servers form that allows you to test authentication of operator login values.
- **Test Lookup**—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.

LDAP Operator Server Troubleshooting

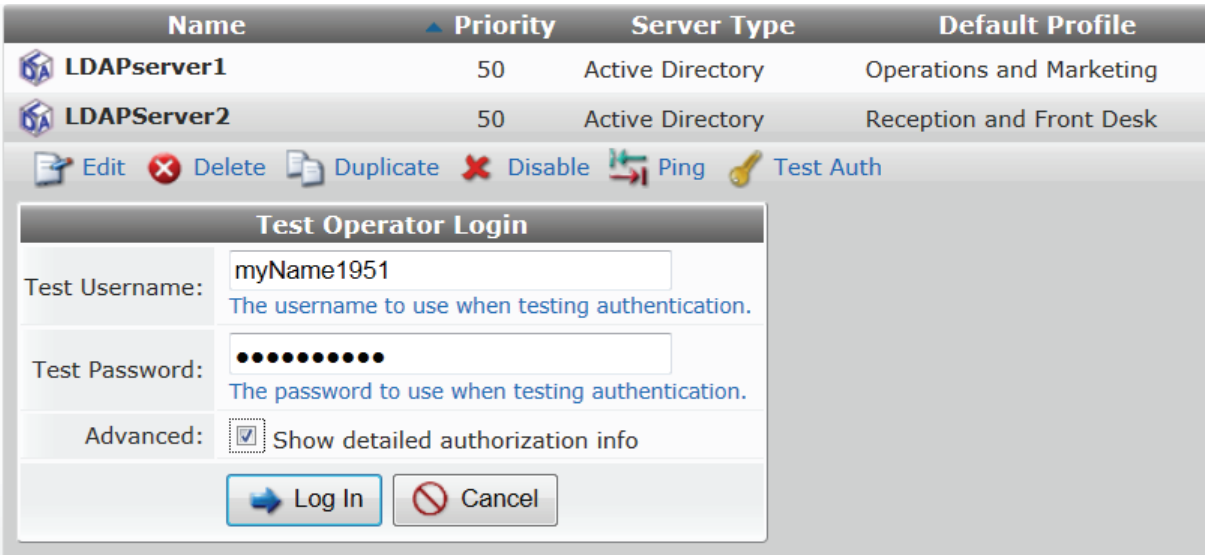
You can use the LDAP Operator Servers list to troubleshoot network connectivity, operator authentication, and to look up operator usernames.

Testing Connectivity

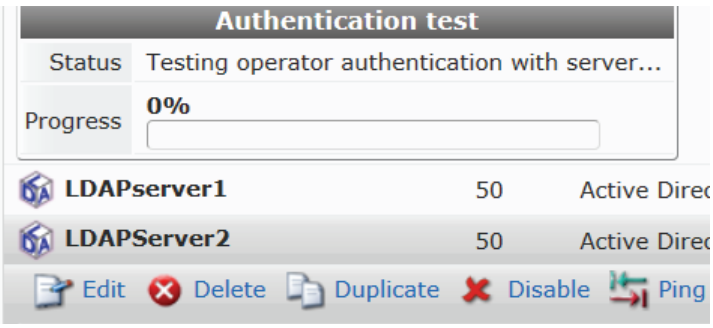
To test network connectivity between an LDAP server and the ClearPass Guest server, click the **Ping** link in the server's row. The results of the test appear below the server entry in the LDAP server table.

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 Test Operator Login area is added to the page.



2. Enter an operator username and password for the LDAP Server.
3. (Optional) Click the **Advanced** check box to display detailed authorization information for the specified operator.
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.



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" in this chapter 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) Click the **Advanced** check box to display detailed authorization information for the specified sponsor.
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 such as: "LDAP Bind failed: Invalid credentials (80090308: LdapErr: DSID-0C090334, comment: AcceptSecurityContext error, data **525**, vece), bind DN was: …"

Table 22 *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
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 DNs 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

LDAP translation rules specify how to determine operator profiles based on LDAP attributes for an authenticated operator.

Translation rules may be created by navigating to **Administrator > Operator Logins > Translation Rules** then clicking the **Create new translation rule** link.

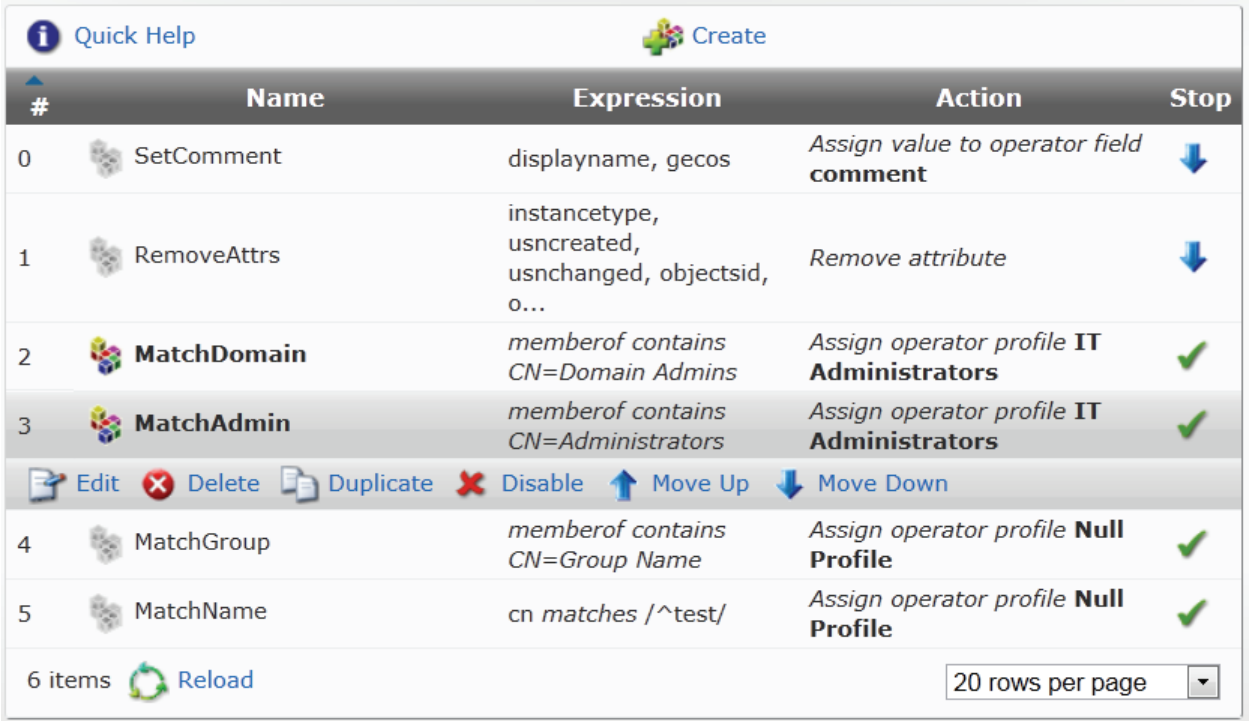
To create a new LDAP translation rule:

1. In the **Name** field, enter a self-explanatory name for the translation rule. In the example above the translation rule is to check that the user is an Administrator, hence the name **MatchAdmin**.
2. Select the **Enabled** check box to enable this rule once you have created 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.
3. Click the **Matching rule** drop-down list and select a rule. The Matching Rule field can be one of:
   - (blank) – always matches
   - **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” in the Reference chapter 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

4. Select a Value. The **Value** field states what is to be matched, in this case **CN=Administrators** to look for a specific group of which the user is a member.
5. Click the **On Match** drop-down list and select the action the system should take when there is a match. Your options here are to:
   - **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.
   - **Assign custom value to operator field** – uses a template to assign a value to a specific operator field.
   - **Apply custom processing** – evaluates a template that may perform custom processing on the LDAP operator.
   - **Remove attribute from operator** – removes the selected LDAP attribute from the operator.
6. Click the **Operator Profile** drop-down list and select the profile to be assigned if there is a rule match. In the example shown above, if the Administrator group is matched, the **Administrator** profile is to be assigned.
7. Select the **Fallthrough** check box if you want to use multiple translation rules. 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.
8. Click **Save Changes** to save your rule settings.

The **Administrator > Operator Logins > Translation Rules** window shows a list of all configured translation rules.



Translation rules are processed in order, until a matching rule is found that does not have the Fallthrough field set.

To edit the matching rule list, select an entry in the table to display a menu that lets you perform the following actions:

- **Edit** – changes the configuration of matching rule
- **Delete** – removes matching rule from the list
- **Duplicate** – creates a duplicate copy of an existing rule
- **Disable** – temporarily disables the rule without deleting it from the rule list
- **Enable** – reenables a disabled operator login
- **Move Up** – moves the rule up to a higher priority on the rule list
- **Move Down** – moves the rule down to a lower priority on the rule list

Custom LDAP Translation Processing

When matching an LDAP translation rule, custom processing may be performed using a template.

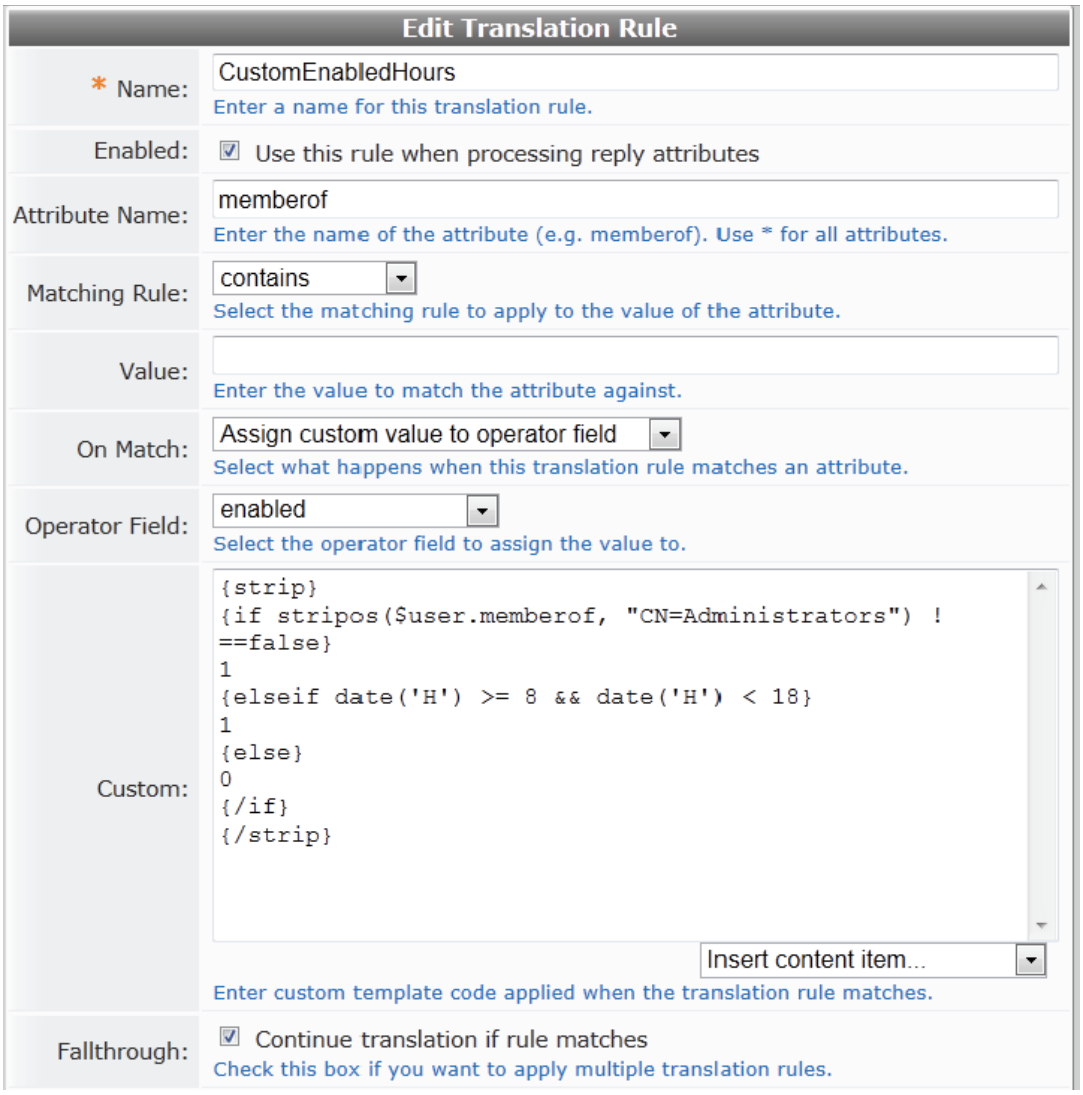
The template variables available are listed in the table below.

Table 23 *Template Variables*

Variable	Description
$attr	The name of the LDAP attribute that was matched.
$user	Contains settings for the operator, including all LDAP attributes returned from the server.

For a Smarty template syntax description, See "Smarty Template Syntax" in the Reference chapter. 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:



The Custom rule is:

```
{strip}
{if stripos($user.memberof, "CN=Administrators")!==false}
1
{elseif date('H') >= 8 && date('H') < 18}
1
{else}
0
{/if}
{/strip}
```

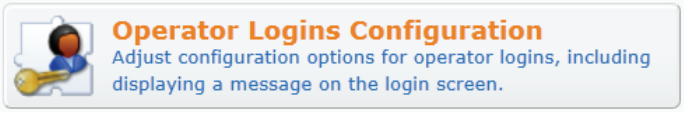
Explanation: The rule will always match on the “memberof” attribute that contains the user’s list of groups. The operator field “enabled” will determine if the user is permitted to log in or not. The custom template uses the {strip} block function to remove any whitespace, which makes the contents of the template easier to understand. The {if} statement first checks for membership of the Administrators group using the PHP stripos() 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.

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.

Options related to operator passwords may also be specified, including the complexity requirements to enforce for operator passwords.

Navigate to **Administrator > Operator Logins** and click the **Operator Logins Configuration** command link to modify these configuration parameters.



Custom Login Message

If you are deploying ClearPass Guest in a multi-lingual environment, you can specify different login messages depending on the currently selected language.

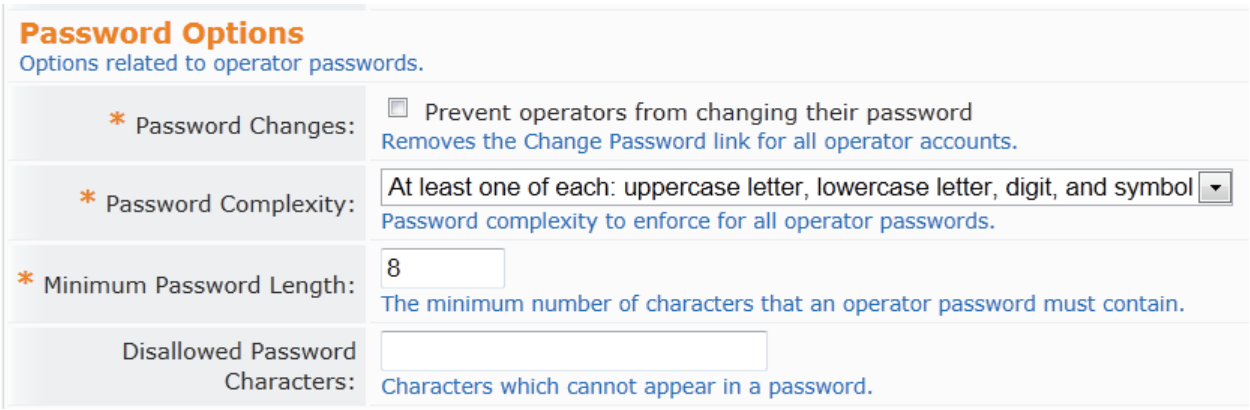
The following example from the demonstration site uses Danish (da), Spanish (es) and the default language English, as highlighted in bold:

```
{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">
```

In the **Login Footer** field, enter any HTML information that you want displayed in the Operator Login form. Select the login skin from the **Login Skin** drop-down menu. Options include the default skin or a customized skin.

Operator Password Options

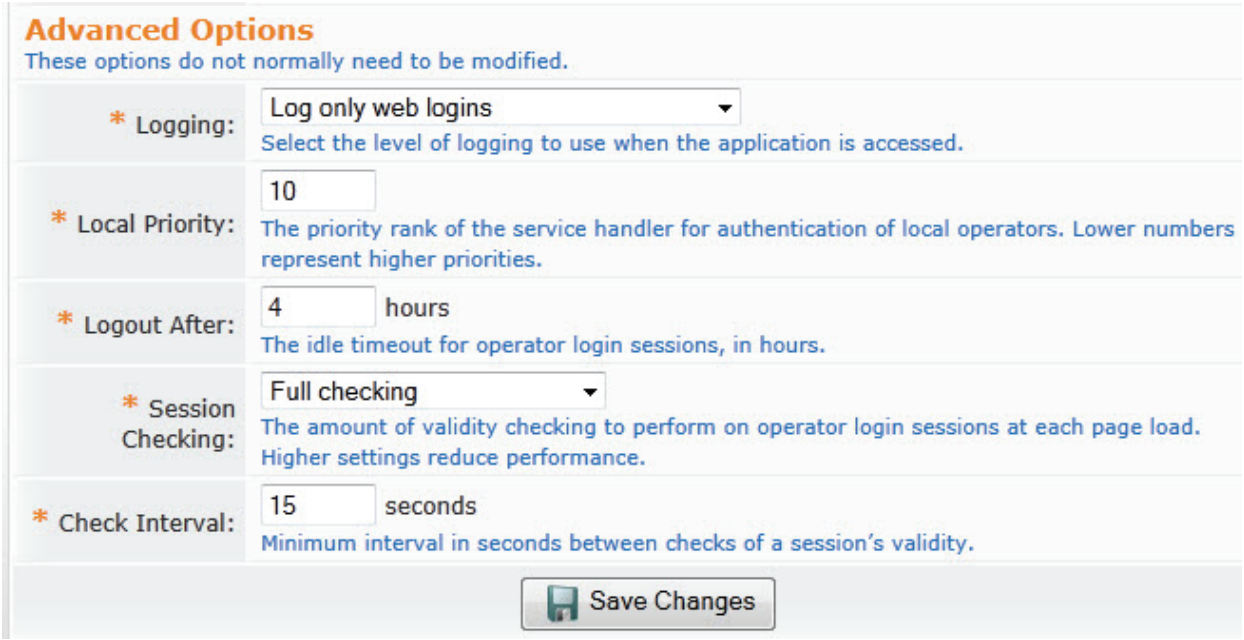


The password complexity for operators may be specified here. The following options are available:

- **No password complexity requirement** – a password policy is not defined by the system.
- **At least one uppercase and one lowercase letter**
- **At least one digit**
- **At least one symbol**
- **At least one of each: uppercase letter, lowercase letter, digit, and symbol** – the most secure form of password; this is the default and recommended setting.

A minimum password length of at least **8 characters** is recommended.

Advanced Operator Login Options



The following options are available in the Logging drop-down list:

- No logging
- Log only failed operator login attempts
- Log only Web logins
- Log only XMLRPC access
- Log all access

Log messages for operator logins, whether successful or unsuccessful, are shown in the application log.

Automatic Logout

The Logout After option in the Advanced Options section lets you configure an amount of idle time after which an operator's session will be ended.

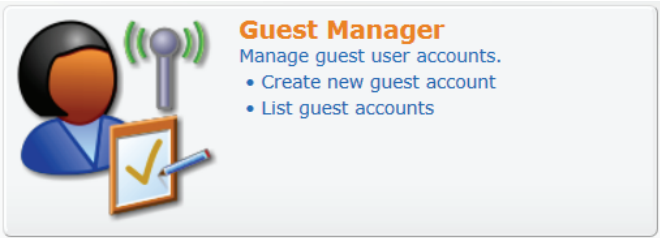
The value for Logout After should be specified in hours. You can use fractional numbers for values less than an hour; for example, use 0.25 to specify a 15 minute idle timeout.

The ability to easily create and manage guest accounts is the primary function of ClearPass Guest.

Guest Manager provides complete control over the user account creation process. Using the built-in customization editor you can customize fields, forms and views as well as the forms for guest self-registration.

Accessing Guest Manager

Use the Guest Manager command on the home page to access the guest management features.



Alternatively, use the Guest Manager navigation menu to jump directly to any of the features within Guest Manager.

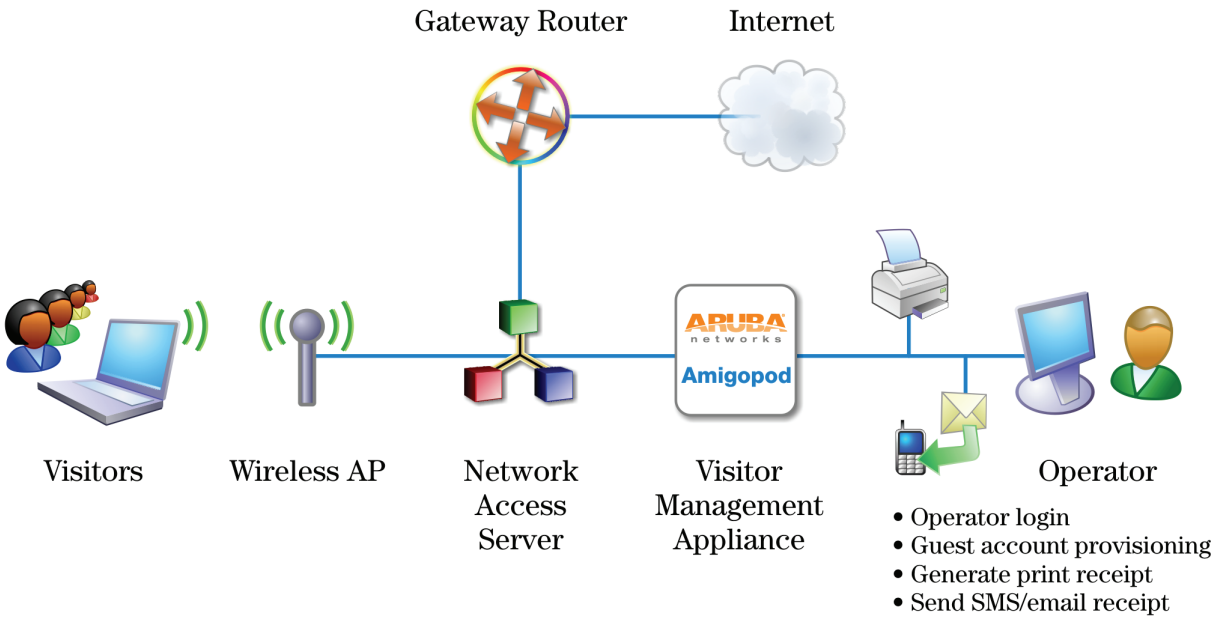
About Guest Management Processes

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 the next sections.

Sponsored Guest Access

The following figure shows the process of sponsored guest access. **See Figure 24**.

Figure 24 Sponsored guest access with guest created by operator



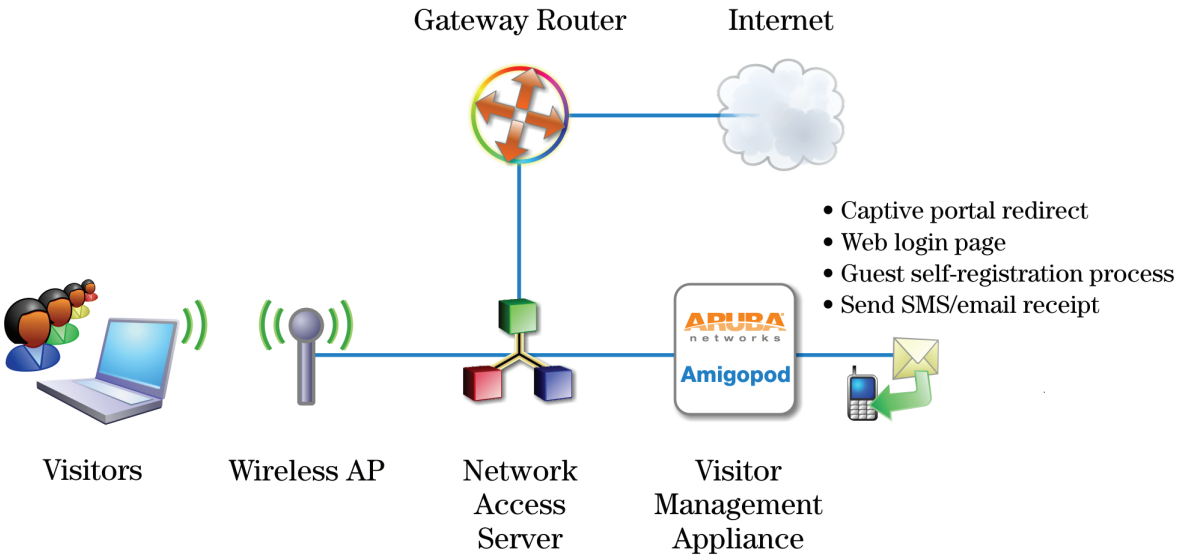
The operator creates the guest accounts and generates a receipt for the account.

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. Once authorized, 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. See Figure 25.

Figure 25 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 sent to her by SMS or email.

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

See "Customizing Self Provisioned Access" in this chapter for details on creating and managing self-registration pages.

Standard Guest Management Features

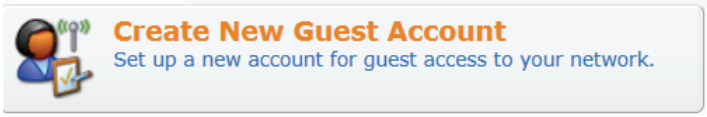
Guest Manager provides a complete set of features for managing guest accounts, including:

- Creating single guest accounts
- Creating multiple guest accounts
- Listing guest accounts and editing individual accounts
- Editing multiple accounts
- Viewing and managing active sessions
- Importing new accounts from a text file
- Exporting a list of accounts
- Viewing MAC devices
- Creating new MAC devices
- Customizing Guest Manager settings, forms, and views
- Customizing guest self-registration
- Creating and editing print templates

Creating a Guest Account

The **New Visitor Account** form is used to create a new visitor account.

This form (create_user) may be customized by adding new fields, or modifying or removing the existing fields. **See "Customizing Self Provisioned Access"** in this chapter for details about the customization process. The default settings for this form are described below.



To complete the form, first enter the visitor's details into the **Sponsor's Name**, **Visitor Name**, **Company Name** and **Email Address** fields. The visitor's email address will become their username to log into the network.

You can specify the account activation and expiration times. The visitor account cannot be used before the activation time, or after the expiration time.

The Account Role specifies what type of account the visitor should have.

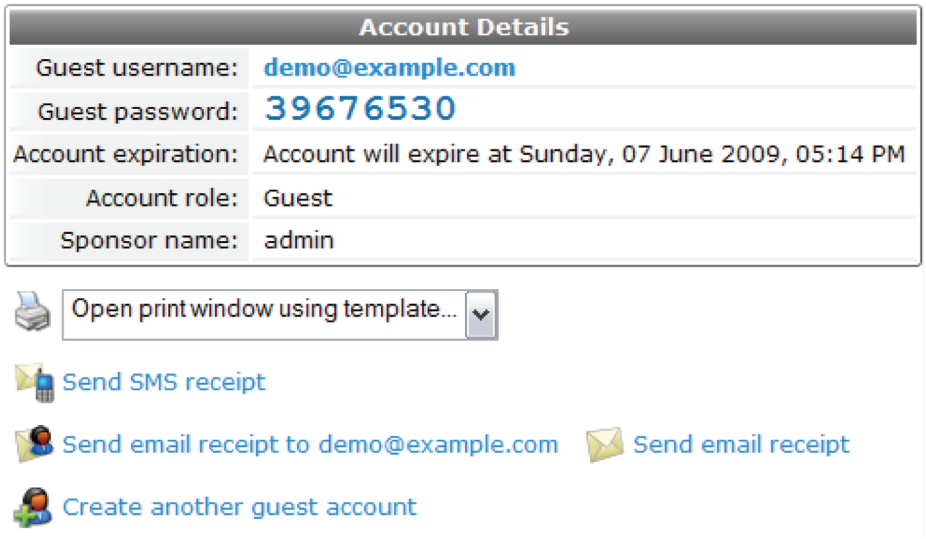
A random password is created for each visitor account. This is displayed on this form, but will also be available on the guest account receipt.

You must mark the Terms of Use check box in order to create the visitor account.

Click the **Create Account** button after completing the form.

Creating a Guest Account Receipt

Once a guest account has been created, the details for that account are displayed.



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

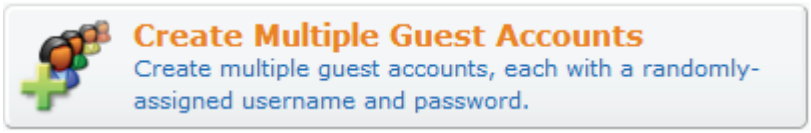
Click the **Send SMS receipt** link to send a guest account receipt via text message. Use the **SMS Receipt** form to enter the mobile telephone number to which the receipt should be sent.

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 **New Visitor 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 **New Visitor 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 Multiple Guest Accounts

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



NOTE

This form (create_multi) may be customized by adding new fields, or modifying or removing the existing fields. See "Customizing Self Provisioned Access" in this chapter for details about the customization process. The default settings for this form are described below.

To complete the form, you must enter the number of visitor accounts you want to create.

A random password will be created for each visitor account. This is not displayed on this form, but will be available on the guest account receipt.

You can specify the account activation and expiration times. The visitor accounts cannot be used before the activation time, or after the expiration time.

To create temporary “scratch c ard” accounts, you may specify a value for the Account Lifetime. This creates a visitor account with a timer that starts counting down once the visitor logs in for the first time. When the timer runs out, the account will expire.

If more than one account expiration time is set (for example, an account lifetime and a fixed expiration time), then the account will expire at the earliest of the expiration times.

The Account Role specifies what type of accounts to create.

Click the **Create Accounts** button after completing the form.

Creating Multiple Guest Account Receipts

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

To print the receipts, select an appropriate template from the **Open print window using template…** list. A new Web browser window will open and the Print dialog box will be displayed.

To download a copy of the receipt information in CSV format, click the **Save list for scratch cards (CSV file)** link. The fields available in the CSV file are:

- **Number** – the sequential number of the visitor account, starting at one
- **Username** – the username for the visitor account
- **Password** – the password for the visitor account
- **Role** – the visitor account’s role
- **Activation Time** – the date and time at which the account will be activated, or N/A if there is no activation time
- **Expiration Time** – the date and time at which the account will expire, or N/A if there is no activation time

- **Lifetime** – the 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

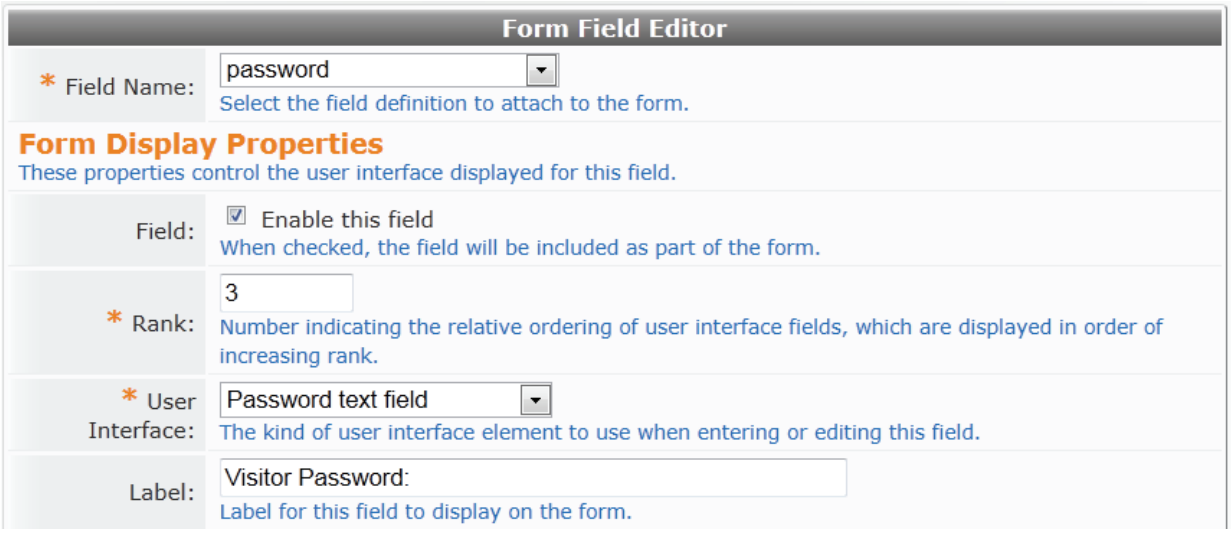
Creating a Single Password for Multiple Accounts

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 **Customization > 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.



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 **IsNonEmpty**.
7. Click **Save Changes**. The Customize Form Fields view opens again, and the password field is now included and can be edited.

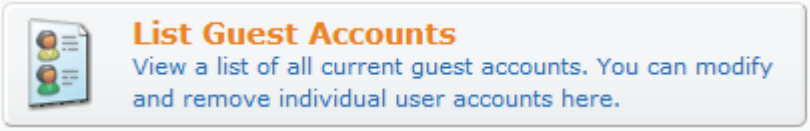
To create multiple accounts that all use the same password:

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

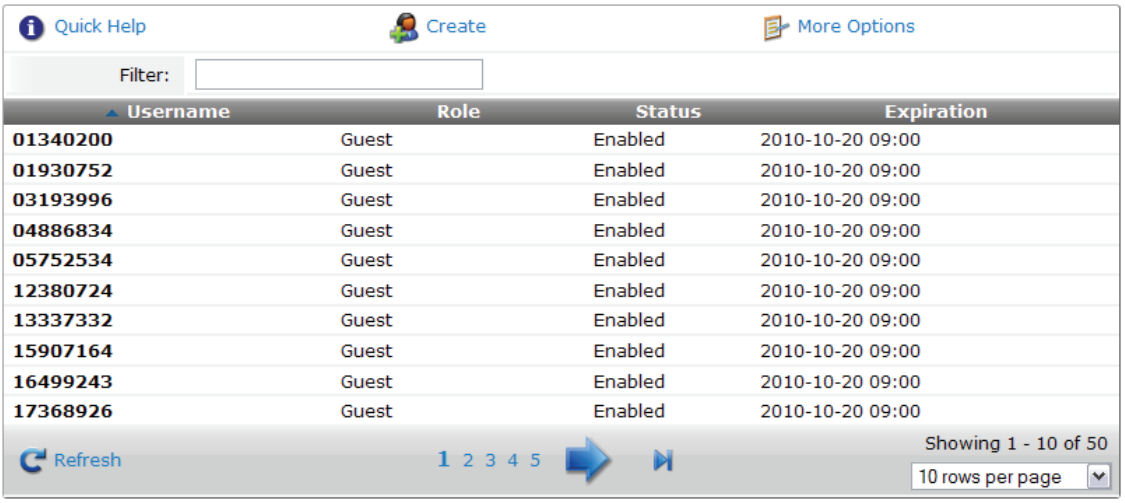
2. In the **Number of Accounts** field, enter the number of accounts you wish to create.
3. In the **Visitor Password** field, enter the password that is to be used by all the accounts.
4. Complete the other fields with the appropriate information, then click **Create Accounts**. The Finished Creating Guest Accounts view opens. The password and other account details are displayed for each account.

Managing Guest Accounts

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



This view (guest_users) may be customized by adding new fields or modifying or removing the existing fields. See "Customization of Fields" in this chapter for details about this customization process. The default settings for this view are described below.



The Username, Role, Status, 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.

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 24 *Operators supported in filters*

Operator	Meaning	Additional Information
=	is equal to	You may search for multiple values when using the equality (=) or inequality !=) operators. To specify multiple values, list them separated by the pipe character (|). 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".
!=	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.

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.

NOTE

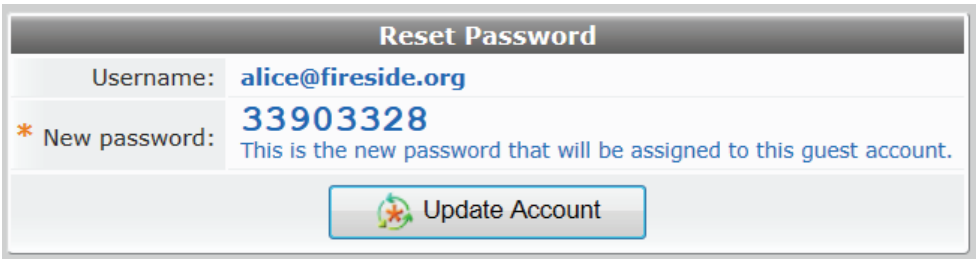
When the list contains many thousands of user accounts, consider using the Filter field to speed up finding a specific user account.

Use the **Create** tab to create new visitor accounts using the **New Visitor Account** form. See "Creating a Guest Account" 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.

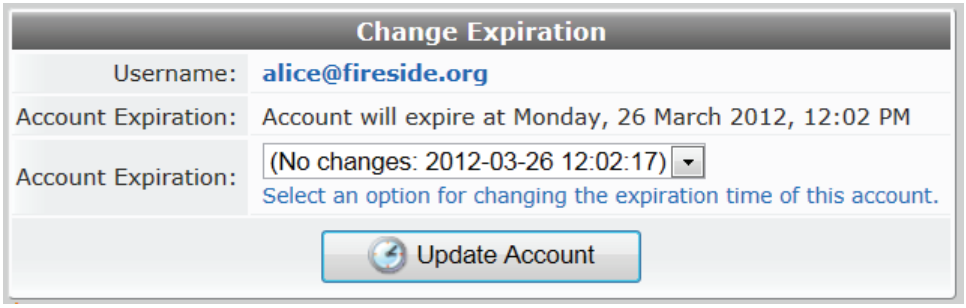
Click a user account's row to select it. You can then select from one of these actions:

- **Reset password** – Changes the password for a guest account. A new randomly generated password is displayed on the **Reset Password** form.



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

- **Change expiration** – Changes the expiration time for a guest account.



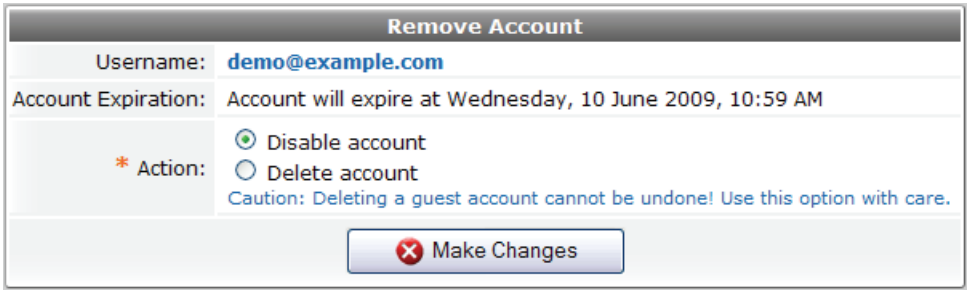
NOTE

This form (change_expiration) may be customized by adding new fields, or modifying or removing the existing fields. Refer to the section of this chapter for details about this customization process

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

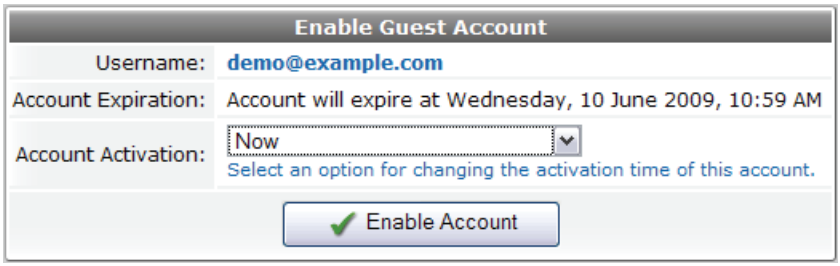
Click the **Update Account** button to set the new expiration time for the guest account. A new account receipt is then displayed, which allows you to print a receipt showing the updated account details.

- **Remove** – Disables or d eletes a guest account.



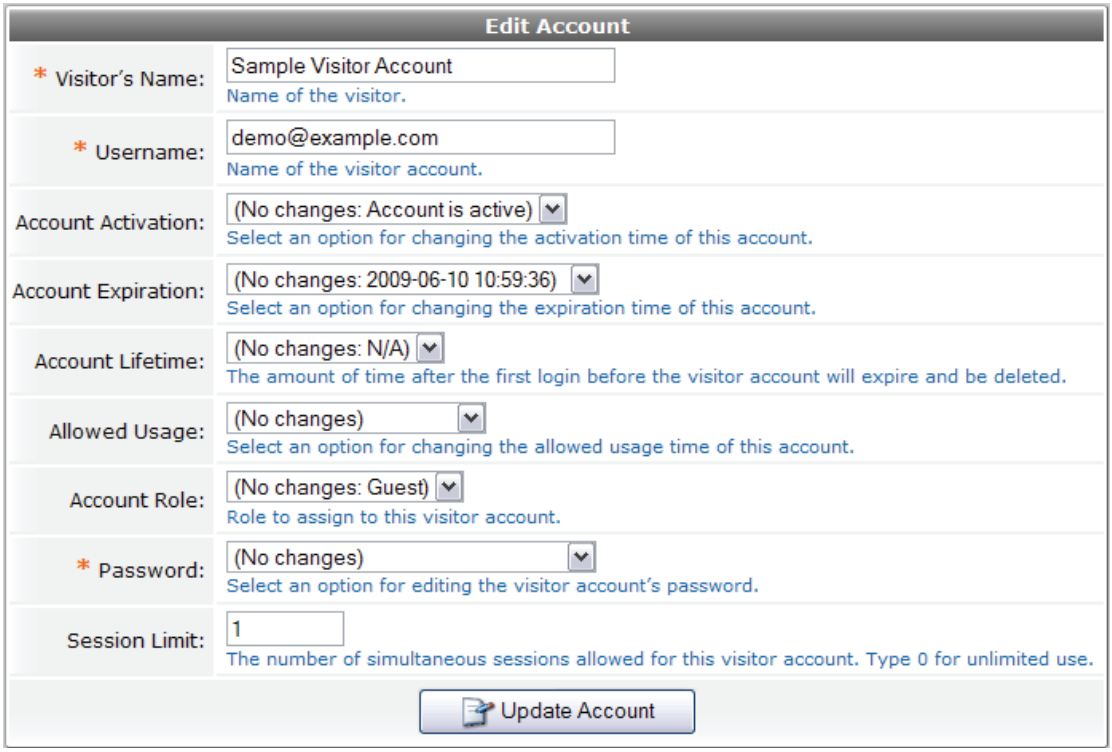
Select the appropriate Action radio button, and click the **Make Changes** button to disable or delete the account.

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



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

- **Edit** – Changes the properties of a guest account.



NOTE

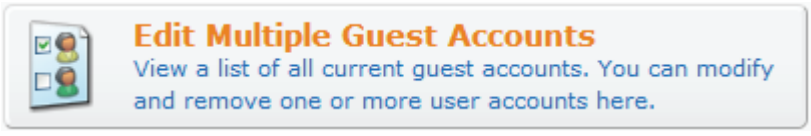
This form may be customized by adding new fields, or modifying or removing the existing fields. Refer to the section of this chapter for details about this customization process. This is the guest_edit form.

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

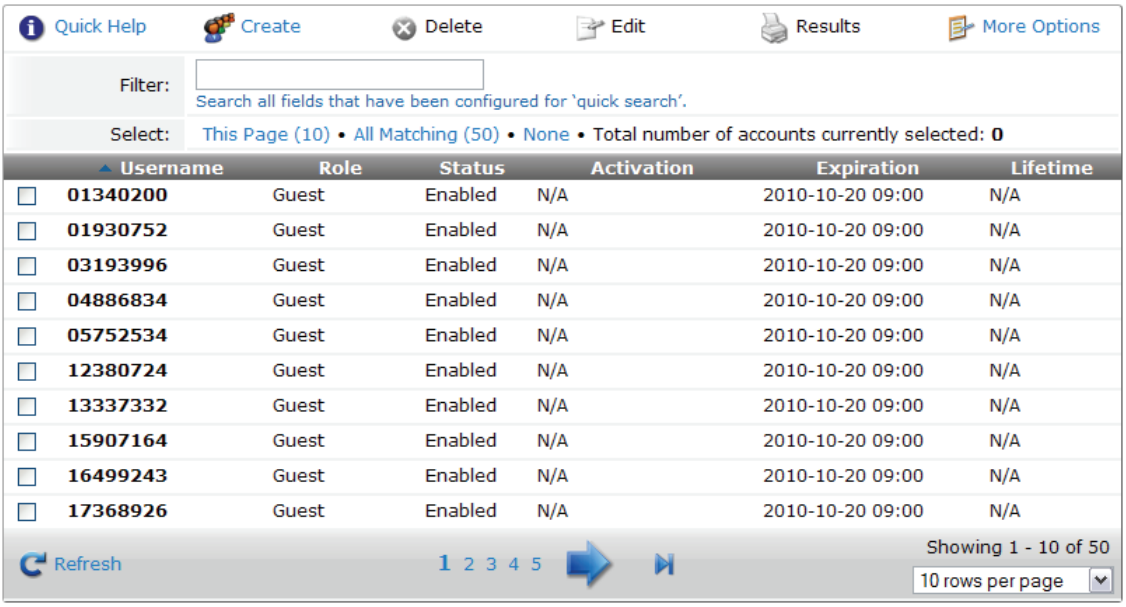
- **Sessions** – Displays the active sessions for a guest account. See "Active Sessions Management" in this chapter for details about managing active sessions.
- **Print** – Displays the guest account's receipt and the delivery options for the receipt. For security reasons, the guest's password is not displayed on this receipt. To recover a forgotten or lost guest account password, use the **Reset password** link.

Managing Multiple Guest Accounts

Use the **Edit Accounts** list view to work with multiple guest accounts. This view may be accessed by clicking the **Edit Multiple Guest Accounts** command link.



This view (guest_multi) may be customized by adding new fields or by modifying or removing the existing fields. **See "Customizing Self Provisioned Access"** in this chapter for details about this customization process. The default settings for this view are described below.



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 25 *Operators supported in filters*

Operator	Meaning	Additional Information
=	is equal to	You may search for multiple values when using the equality (=) or inequality !=) operators. To specify multiple values, list them separated by the pipe character (|). 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".
!=	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.

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.

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 unselect 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 Guest Accounts** form. See "Managing Multiple Guest Accounts" 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 available if there are no visitor accounts selected.

Use the **Edit** tab to make changes to multiple visitor accounts at once. This option is not available if there are no visitor accounts selected.

This form may be customized by adding new fields, or modifying or removing the existing fields. See "Customizing Self Provisioned Access" in this chapter for details about this customization process. This is the guest_multi_form form.

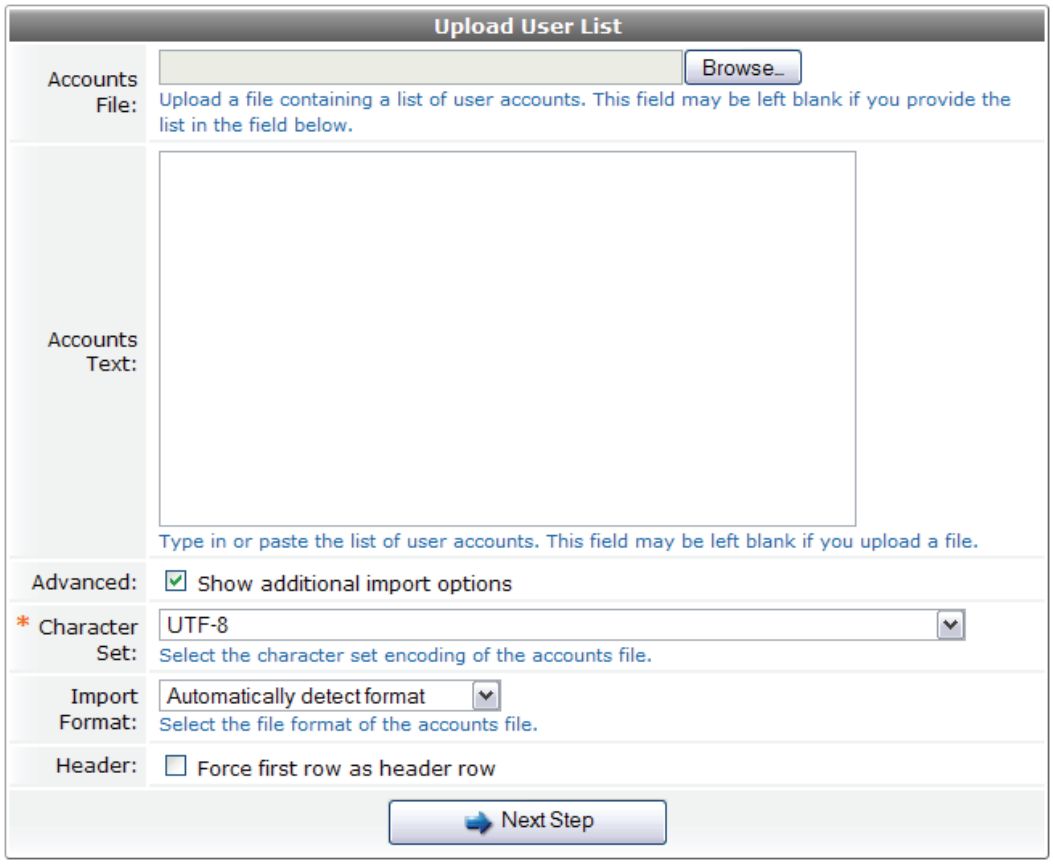
The **Results** tab will be automatically selected after you have made changes to one or more guest accounts. You can create new guest account receipts or download the updated guest account information. See "Creating Multiple Guest Account Receipts" in this chapter for more information.

The **More Options** tab includes **the Choose Columns** command link, which may be used to customize the view.

Importing Guest Accounts

Guest accounts may be created from an existing list by uploading the list to ClearPass Guest. Use the **Import Guest Accounts** command to start the process.

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 to the Accounts Text area.

Select the **Show additional import options** check box to display the following advanced import options:

- **Character Set**: 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 may 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**: The format of the accounts file is automatically detected. You may specify one of the following encoding types if the automatic detection is not suitable for your data.
  - XML
  - Comma separated values
  - Tab separated values
  - Pipe (|) separated values
  - Colon (:) separated values
  - Semicolon (;) separated values
- Select the **Force first row as header row** check box if your data contains a header row that specifies the field names. This option is only required if the header row is not automatically detected.

Click **Next Step** to upload the account data.

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

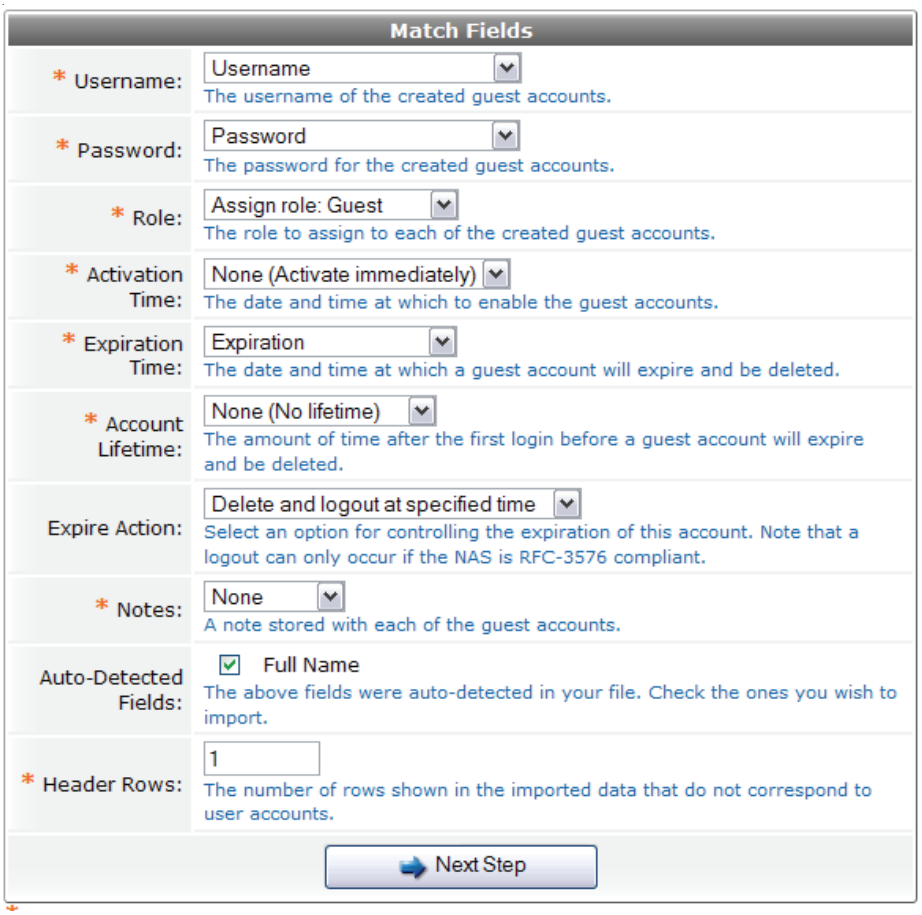
In this example, the following data was used:

```
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
```

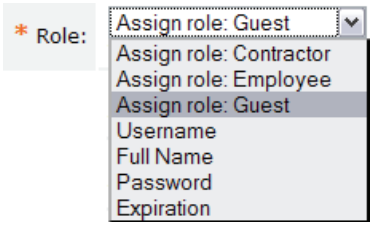
Because this data includes a header row that contains field names, the corresponding fields have been automatically detected in the data:

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

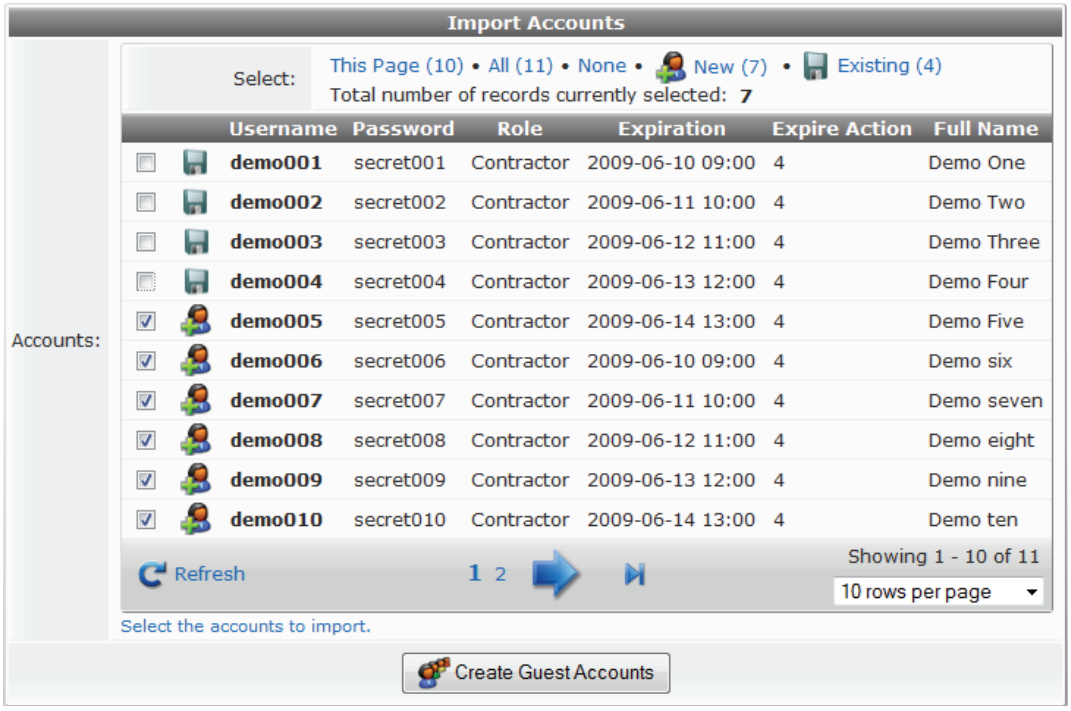


To complete the **Match Fields** form, make a selection from each of the drop-down lists. Choose a column name to use the values from that column when importing guest accounts, or select one of the other available options to use a fixed value for each imported guest account.



Click the **Next Step** button to preview the final result.

Step 3 of 3 displays a preview of the import operation. The values of each guest account field are determined, and any conflicts with existing user accounts are displayed.



The icon displayed for each user account indicates if 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.

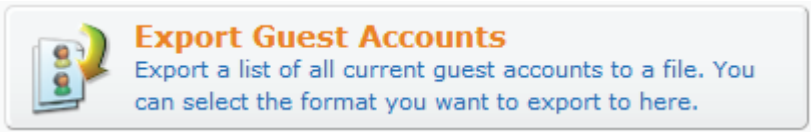
Click the check box by the account entries you want to create, or click one of the following options to select the desired accounts:

- Click the **This Page** link to select all entries on the current page.
- Click the **All** link to select all entries on all pages
- Click the **None** link to deselect all entries
- Click the **New** link to select all new entries
- Click the **Existing** link to select all existing user accounts in the list.

Click the **Create Accounts** 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" in this chapter for more information.

Exporting Guest Account Information

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



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.

This view (guest_export) may be customized by adding new fields, modifying or removing the existing fields. See "Customizing Self Provisioned Access" in this chapter for details about this customization process.

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)

The default XML format consists of a **<userlist>** element containing a **<user>** element for each exported guest account. The numeric ID of the guest account is provided as the "id" attribute of the **<user>** element.

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="yes" ?>
<userlist>
  <user id="43">
    <username>demo@example.com</username>
    <role_name id="2">Guest</role_name>
    <schedule_time>N/A</schedule_time>
    <expire_time>2009-06-10 10:59</expire_time>
    <expire_postlogin>0</expire_postlogin>
    <do_expire>4</do_expire>
  </user>
</userlist>
```

Guest Manager Customization

Guest Manager allows the entire guest account provisioning process to be customized. This is useful in many different situations, such as:

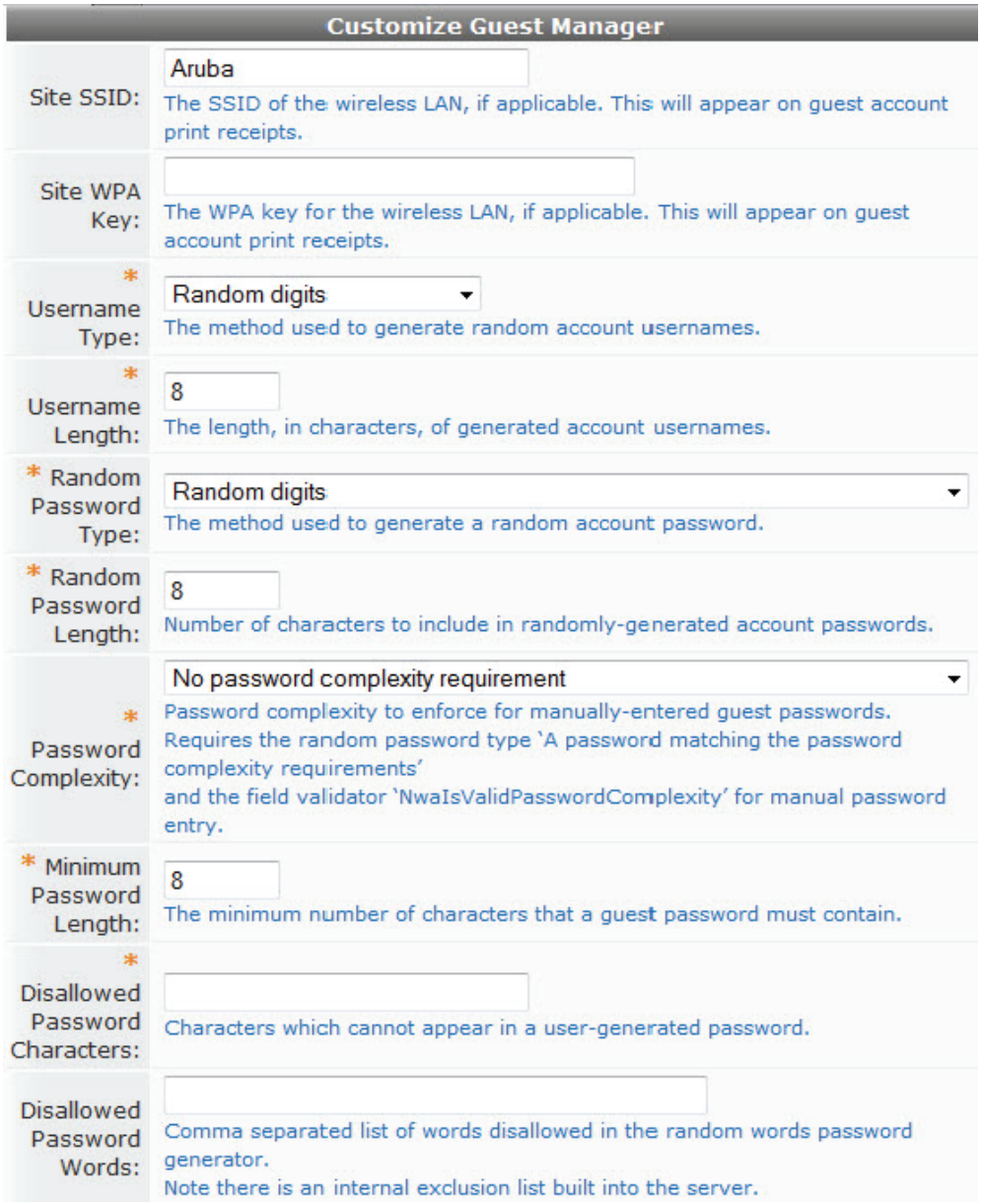
- **Self-registration** – Allow your guests to self-register and create their own temporary visitor accounts.
- **Visitor surveys** – Define custom fields to store data of interest to you, and collect this information from guests using customized forms.
- **Branded print receipts** – Add your own branding 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 Guest Manager plugin configuration holds the default settings for account creation. These settings can be modified by navigating to Customize Guest Manager within the Guest Manager Customization screen.

Figure 26 *Customize Guest Manager page (part 1)*

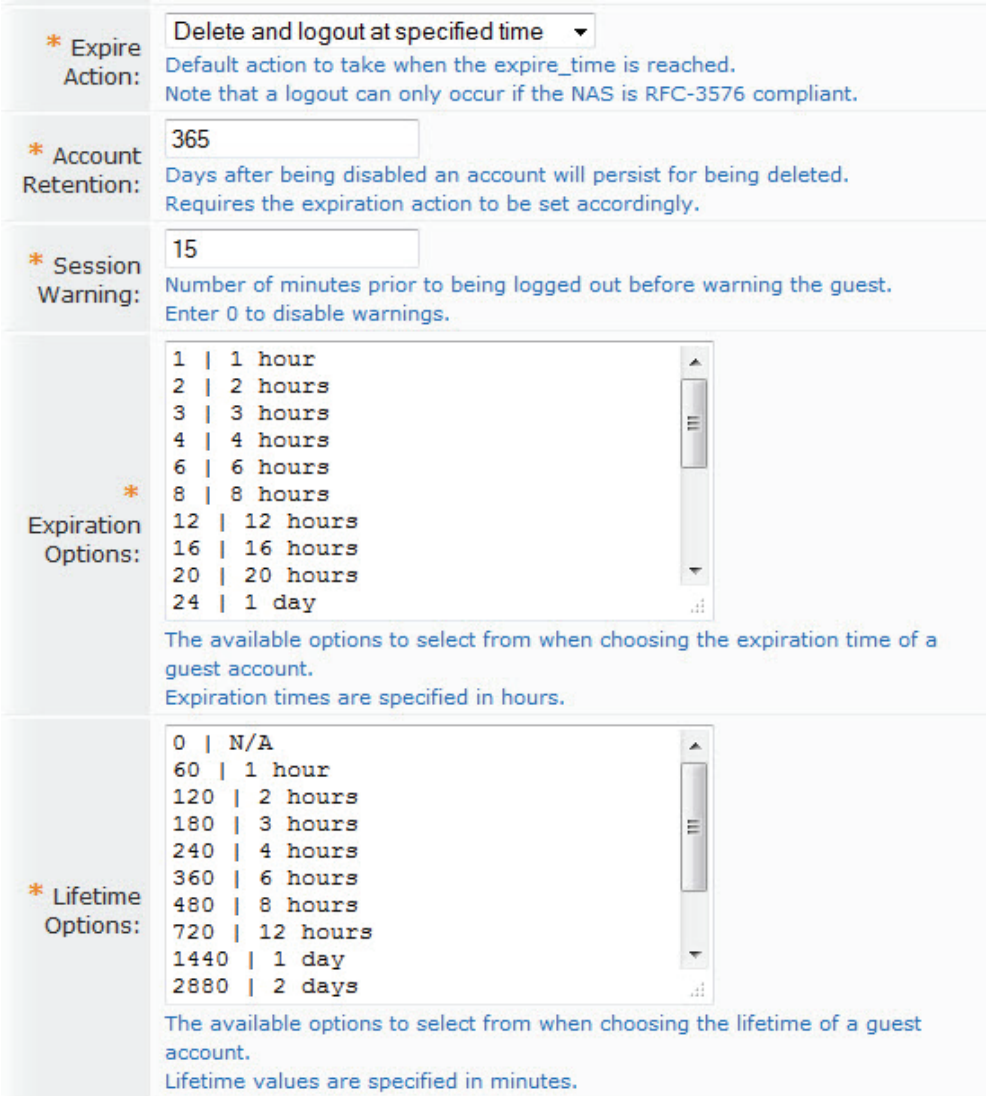


- **Username Type** – The default method used to generate random account usernames (when creating groups of accounts). This may be overridden by using the **random_username_method** field.

- **Username Length** –This field is displayed if the **Username Type** is set to “Random digits”, “Random letters”, “Random letters and digits” or “Sequential numbering”. The default length of random account usernames (when creating groups of accounts). This may be overridden by using the **random_username_length** field.
- **Username Format** – This field is displayed if the **Username Type** is set to “Format picture”. It sets the format of the username to be created. See “Format Picture String Symbols” in the Reference chapter 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.

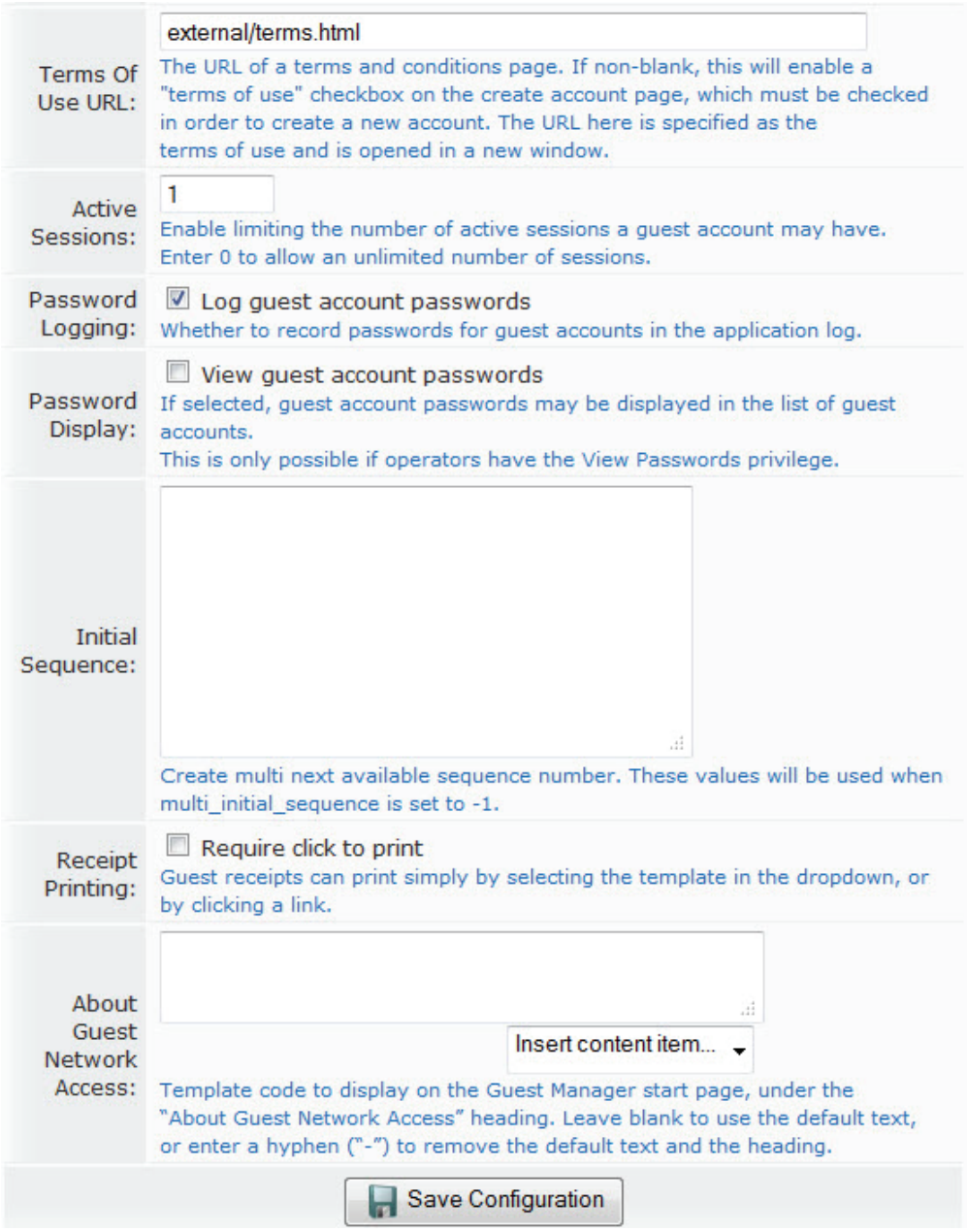
- **Random Password Type** –The default method used to generate random account passwords (when creating groups of accounts). This may be overridden by using the **random_password_method** field.
  - **Random Password Length** -- The default length of random account passwords (when creating groups of accounts). This may be overridden by using the **random_password_length** field
  - **Password Format** – This field is displayed if the **Password Type** field is set to “Format picture”. It sets the format of the password to be created. See “Format Picture String Symbols” in the Reference chapter for a list of the special characters that may be used in the format string. This may be overridden by using the **random_password_picture** field.
- **Password Complexity** – The 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 (`!#$%&()*+,-./:;<=>?@[\\]^_{|}~`,). The available options for this setting are:
  - 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** – The minimum acceptable password length for guests changing their account passwords.
- **Disallowed Password Characters** – Special characters that should not be allowed in a guest password. Spaces are not allowed by default.
- **Disallowed Password Words** – Enter a comma- separated list of words that are disallowed and will not be created by the random words password generator.

Figure 27 *Customize Guest Manager page (part 2)—continued*



- **Expire Action** – Default action to take when the expiration time is reached. There are four options. A logout can only occur if the NAS is RFC-3576 compliant.
- **Account Retention** – Deleted user accounts are available for reporting purposes. The default value is 1 year after the user account is deleted. If you do not want to retain any data, set the value to 0. If you want to view deleted accounts in a list view or report, add the delete_time field to the output and deleted users will automatically be included in the results.
- **Session Warning**– Number of minutes prior to being logged out before warning the guest. Enter 0 to disable warnings.
- **Expiration Options** – Default values for relative account expiration times. These options are displayed as the values of the “Expires After” field when creating a user account.

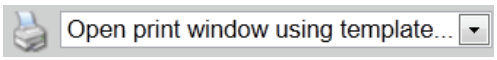
Figure 28 *Customize Guest Manager page (part 3)—continued*



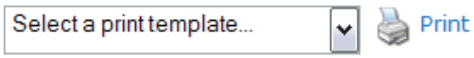
- **Lifetime Options** – Default values for account lifetimes. These options are displayed as the values of the “Account Lifetime” field when creating a user account.
- **Terms of Use URL** – URL of a terms and conditions page provided to sponsors. You may upload an HTML file describing the terms and conditions of use using the Content Manager (**See** **“Content Manager”** in the Administrator Tasks chapter). If this file is called **terms.html** then the Terms of Use URL should be **public/terms.html**.
- **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.
- **Password Logging** – By default, the 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 unselecting this check box.

- **Password Display** – Select the “View guest account passwords” to enable 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.
- **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.
- **Receipt Printing** – Select the “Require click to print” option to change the behavior of the receipt page.

  When this option is not selected, the default behavior is to provide a drop-down list of print templates and to open a new window when one is selected:

  When “Require click to print” is 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:

- **About Guest Network Access** – Allows the text displayed to operators on the Guest Manager start page to be customized, or removed (if a single hyphen “-” is entered).

About Fields, Forms, and Views

A field is a named item of information.

A form is a group of fields that is used to collect information from an operator, whereas 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.

Verification Properties

- **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

- **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:
  - "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.
- **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.

Visitor Account Activation Properties

- **enabled**: This field determines if the account is enabled or disabled; if not specified, the default is 1 (account is enabled).
- **do_schedule**, **modify_schedule_time**, **schedule_after** and **schedule_time**: These fields are used to determine the time at which the visitor account will be activated.
  - 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.
  - 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.

Visitor Account Expiration Properties

- **do_expire**, **modify_expire_time**, **expire_after** and **expire_time**: These fields are used to determine the time at which the visitor account will expire.
  - 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.
  - 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, then add that time in hours to the current time and use it as the expiration time (set **do_expire** to 4 if it has not otherwise been set).
  - Otherwise, if **expire_after** is zero, negative or unset, and **expire_time** has been specified, use that expiration time (and set **do_expire** to 4 if it has not otherwise been set). If the **expire_time** specified is in the past, set **do_expire** to 0 and ignore the specified expiration time.
  - Otherwise, if **expire_time** is not specified, then the **expire_time** is not set and **do_expire** will always be set to zero.
- **expire_postlogin**: 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).
- **expire_usage**: 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).

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)

Account Expiration Types

The **do_expire** field is used to specify what should happen to the guest account when the account expiration time is reached.

Table 26 *Account Expiration Types*

Value of “do_expire”	Meaning
0	Account will not expire
1	Disable
2	Disable and logout
3	Delete
4	Delete and logout

“Disable” indicates that the enabled field will be set to 0, which will prevent further authorizations using this account.

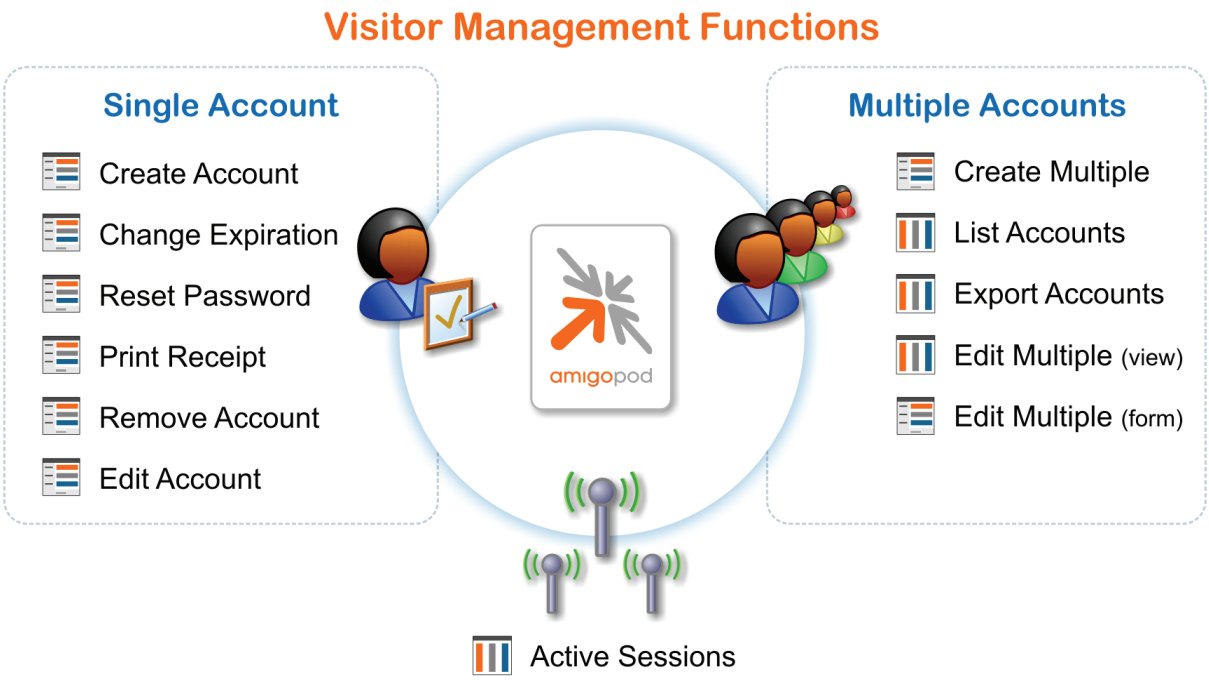
"Logout" indicates that a RADIUS Disconnect-Request will be used for all active sessions that have a username matching the account username. This option requires the NAS to support RFC 3576 dynamic authorization. See "RFC 3576 Dynamic Authorization" in this chapter for more information.

Standard Fields

See "Field, Form and View Reference" in the Reference chapter 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.



The table below lists all the forms and views used for visitor management.

Table 27 *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

Table 27 *Visitor Management Forms and Views (Continued)*

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

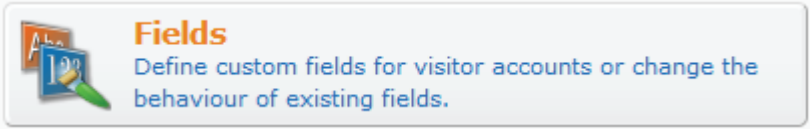
These standard views are defined in Guest Manager:

- **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" in this chapter.)
- **guest_users** view – displays a list of guest accounts optimized for working with individual accounts

Customization of 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.



NOTE

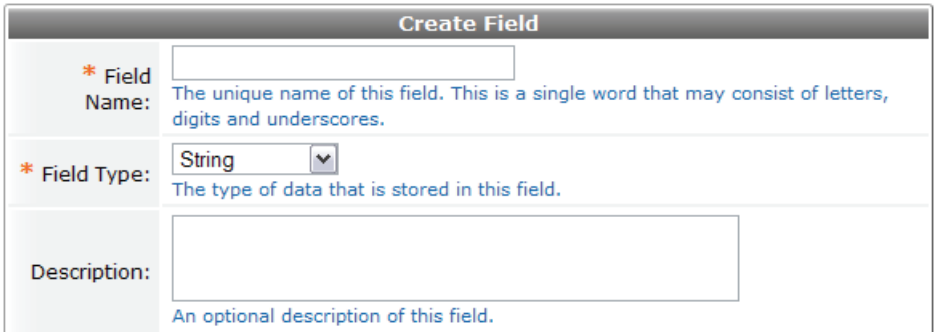
Fields that have a lock symbol cannot be deleted.

A complete list of fields is displayed when you click the **Fields** command link on the **Customize Guest Manager** page.

To display only the fields that you 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.

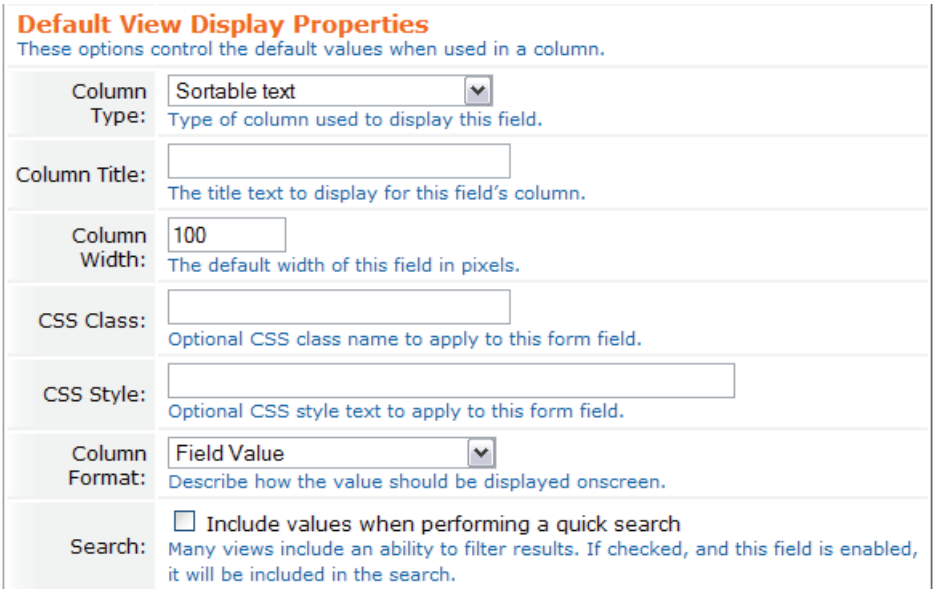
Creating a Custom Field

To create a custom field click the **Create** tab at the top of the window or the **Create a new field** link at the bottom of the window. The Create Field form is displayed.



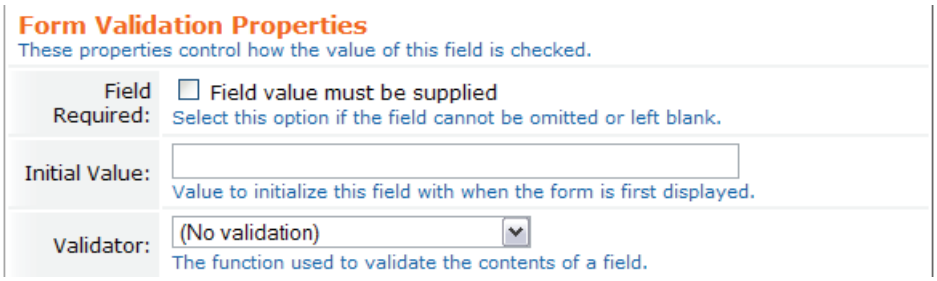
The Field Name is not permitted to have spaces but you can use underscores. Enter a description in the Description field. You can enter multiple-line descriptions which result in separate lines displayed on the form.

The Field Type can be one of String, Integer, Boolean or No data type. The No data type field would be used as a label, or a submit button.

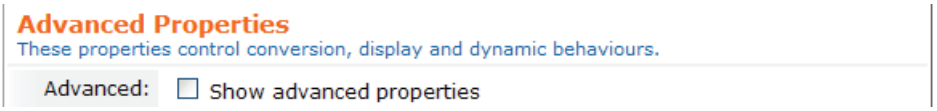


You can specify the default properties to use when adding this field to a view. **See "View Field Editor"** in this chapter for a description of the view display fields, including the Column Type and Column Format fields.

You can specify the default properties to use when adding the field to a form. **See "View Field Editor"** in this chapter for a list of the available user interface types.



You can specify the default validation rules that should be applied to this field when it is added to a form. **See "Form Validation Properties"** in this chapter for further information about form validation properties.



Select the **Show advanced properties** check box to reveal additional properties related to conversion, display and dynamic form behavior. **See "View Field Editor"** in this chapter for more information about advanced properties.

Click the **Save Changes** button to complete the creation of a new field. The new field is added at the top of the field list. You can re-sort the list to change the position of this new field. Alternatively you can reload the page.

Duplicating a Field

To duplicate a field, click the field to be duplicated, then click the **Duplicate** link. The field is copied and 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**.

Editing a Field

You are able to alter the properties of the field by making changes to the Field Name, Field Type or Description when you click the **Edit** link. This link is available when you click a field in the list view.

Click the **Save Changes** button to have the changes made permanent.

Deleting a Field

Fields that do not have a lock symbol can be deleted by clicking on the **Delete** link. You will be asked to confirm the deletion. If you want the deletion to take place you are informed when the deletion has been completed. A field that is currently in use on a form or view may not be deleted.

Displaying Forms that Use a Field

Click the **Show Forms** link to see a list of forms that use the selected field.

The list displays the forms that use the selected field. It also allows you to edit the form's fields by clicking on the **Edit Fields** link. Clicking on the **Use** link opens the form using that field.

If the field is used on multiple forms, you are able to select which form you would like to view.

Displaying Views that Use a Field

You are able to click the **Show Views** link to see a list of views that use the selected field.

The list displays the views that use the selected field. It also allows you to edit the view's fields by clicking on the **Edit Fields** link. Clicking on the **Use** link displays the view.

If the field is used on multiple views, you are able to select which view you would like to see.

Customization of Forms and Views

You are able to view a list of 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.

To view or customize forms and views, go to **Customization > Forms & Views**. The Customize Forms and Views page opens.

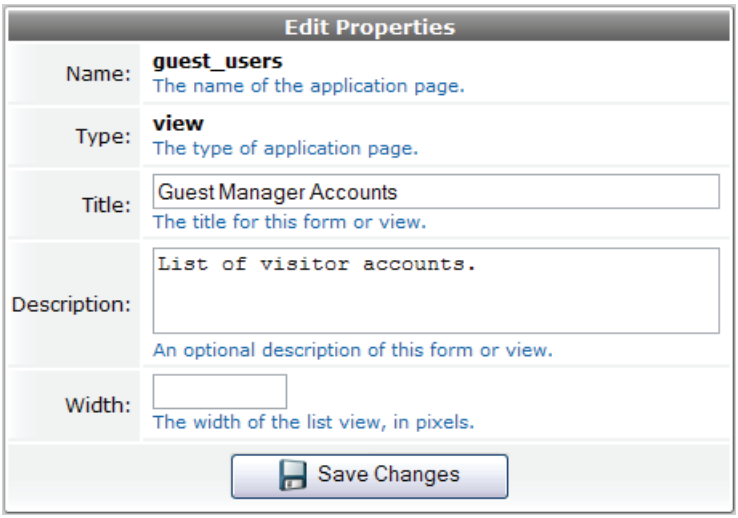
Editing Forms and Views

Clicking on the **Use** link opens the form or view for use in your Web browser.

An asterisk (*) shown next to a form or view indicates that the form or view has been modified from the defaults. Click the **Reset to Defaults** link to remove your modifications and restore the original form.

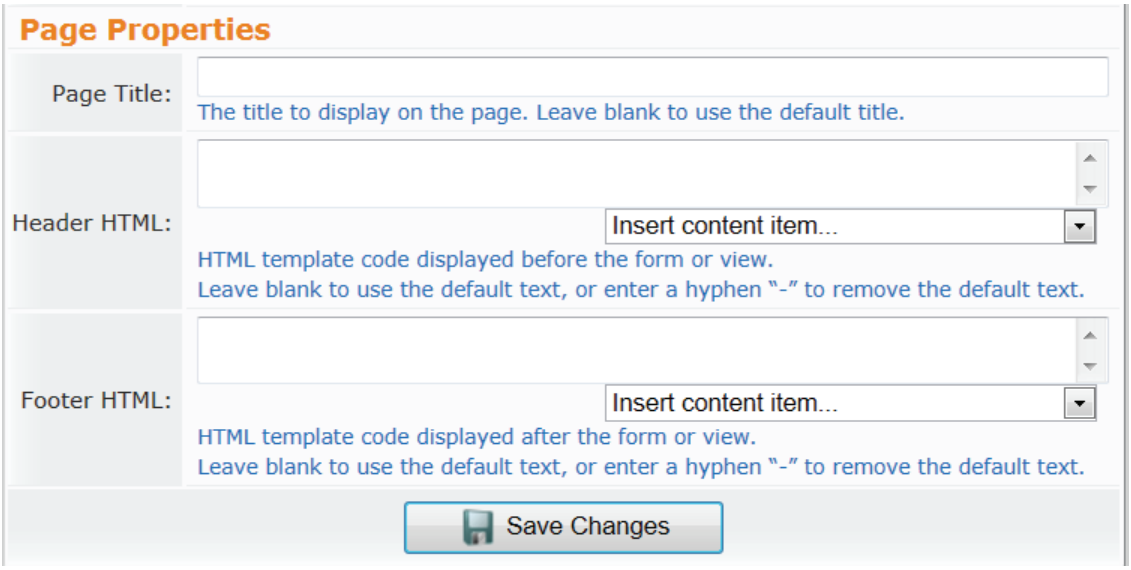
Resetting a form or view is a destructive operation and cannot be undone. You will be prompted to confirm the form or view reset before it proceeds.

The **Edit** icon link allows you to change the general properties of a form or view such as its title and description.



The Width field is only displayed for views. It specifies the total width of the list view in pixels. If blank, a default value is used.

You can customize the page title, header HTML, and footer HTML for many forms and views (for example, Create Guest Account, Edit Guest Accounts, and others). When these options are available, the Page Properties area is included on the Edit Properties form.



Duplicating Forms and Views

Click the **Duplicate** link to make a copy of a form or view.

Use the Duplicate link to provide different forms and views to different operator profiles. See "Role-Based Access Control for Multiple Operator Profiles" in the Operator Logins chapter 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 duplicated form or view has a name derived from the original, which cannot be changed. Use the Title and Description properties of the duplicated item to describe the intended purpose for the form or view.

Click the **Show Usage** link for a duplicated form or view to see the operator profiles that are referencing it.

Click the **Delete** link for a duplicated form or view to remove the copy. A duplicated item cannot be removed if it is referenced by an operator login account or an operator profile.

Editing Forms

To add a new field to a form, reorder the fields, or make changes to an existing field, go to **Customization > Forms & Views**, click the form's row in the Customize Forms & Views list, and then click the **Edit Fields** link. This opens the **Customize Form Fields** editor.

Quick Help Preview Form

Rank	Field	Type	Label	Description
10	**sponsor_name**	text	Sponsor's Name:	Name of the person sponsoring this guest account.
20	**visitor_name**	text	Visitor's Name:	Name of the visitor.
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	schedule_time	datetime	Activation Time:	Optional date and time at which to enable the visitor account. If blank, the visitor account will be enabled immediately.
60	**expire_after**	dropdown	Account Expiry:	Amount of time before this visitor account will expire.
65	**expire_time**	datetime	Expiration Time:	Optional date and time at which this account will expire. If blank, the expiration time will not be set.
70	**role_id**	dropdown	Account Role:	Role to assign to this visitor account.
75	enabled	checkbox	Account State:	
80	**password**	static	Visitor Password:	
90	**creator_accept_terms**	checkbox	Terms of Use:	
100	**submit**	submit	Create Account	

Form fields have a rank number, which specifies the relative ordering of the fields when displaying the form. The Customize Form Fields editor always shows the fields in order by rank.

The type of each form field is displayed. This controls what kind of user interface element is used to interact with the user. The label and description displayed on the form is also shown in the list view.

Click a form field in the list view to select it.

Use the **Edit** link to make changes to an existing field using the form field editor. Any changes made to the field using this editor will apply only to this field on this form.

Use the **Edit Base Field** link to make changes to an existing field 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).

The **Insert Before** and **Insert After** links can be used to add a new field to the form. Clicking one of these links will open a blank form field editor and automatically set the rank number of the new field.

Use the **Preview Form** tab at the top of the list view to see what the form 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.

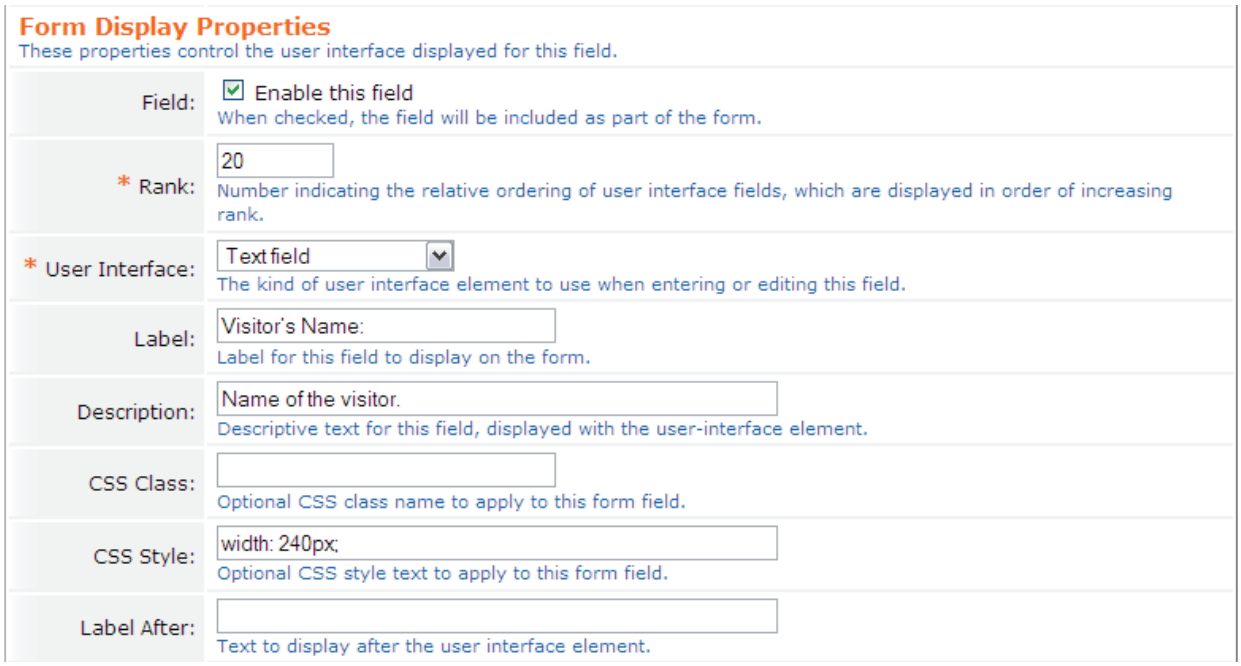
Each field can only appear once on a form. The Field Name selects which underlying field is being represented on the form.

The remainder of the form field editor is split into three sections:

- Form Display Properties
- Form Validation Properties
- Advanced Properties

Each of these sections is described in more detail below.

Form Display Properties

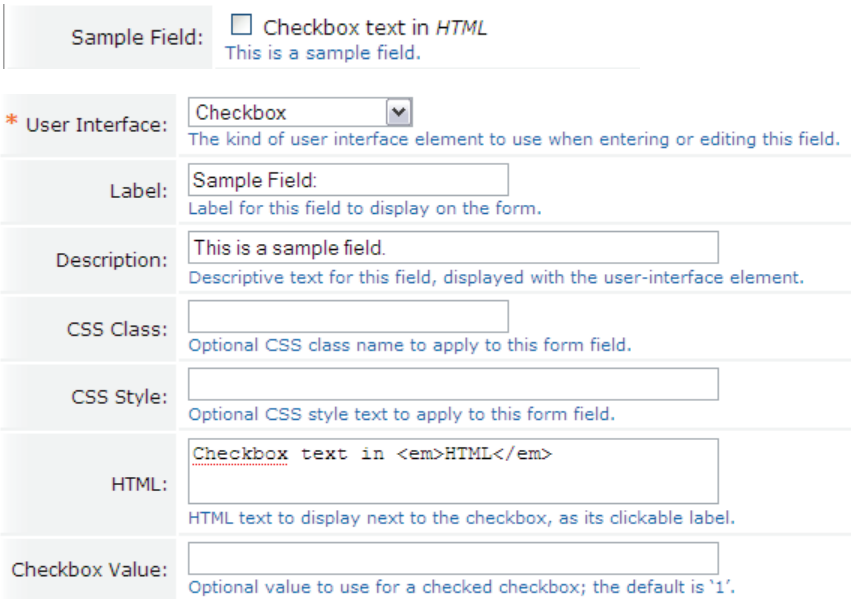


The form display properties control the user interface that this field will have. Different options are available in this section, depending on the selection you make in the User Interface drop-down list.

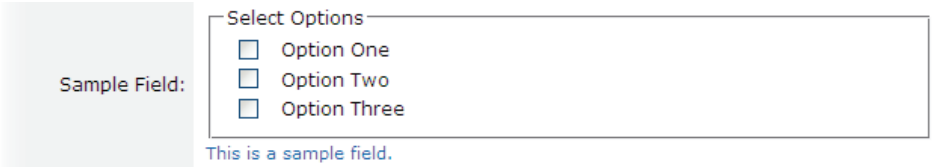
The available user interface elements are listed below, together with an example of each.

- **(Use default)** – The default user interface type defined for the field will be used.
- **No user interface** – 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** – A distorted image of several characters is shown. The image may be regenerated, or played as an audio sample for visually impaired users. When using the recommended validator for this field (NwaCaptchaIsValid), the security code must be matched or the form submit will fail with an error.

- **Check box** – A check box is displayed for the 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.



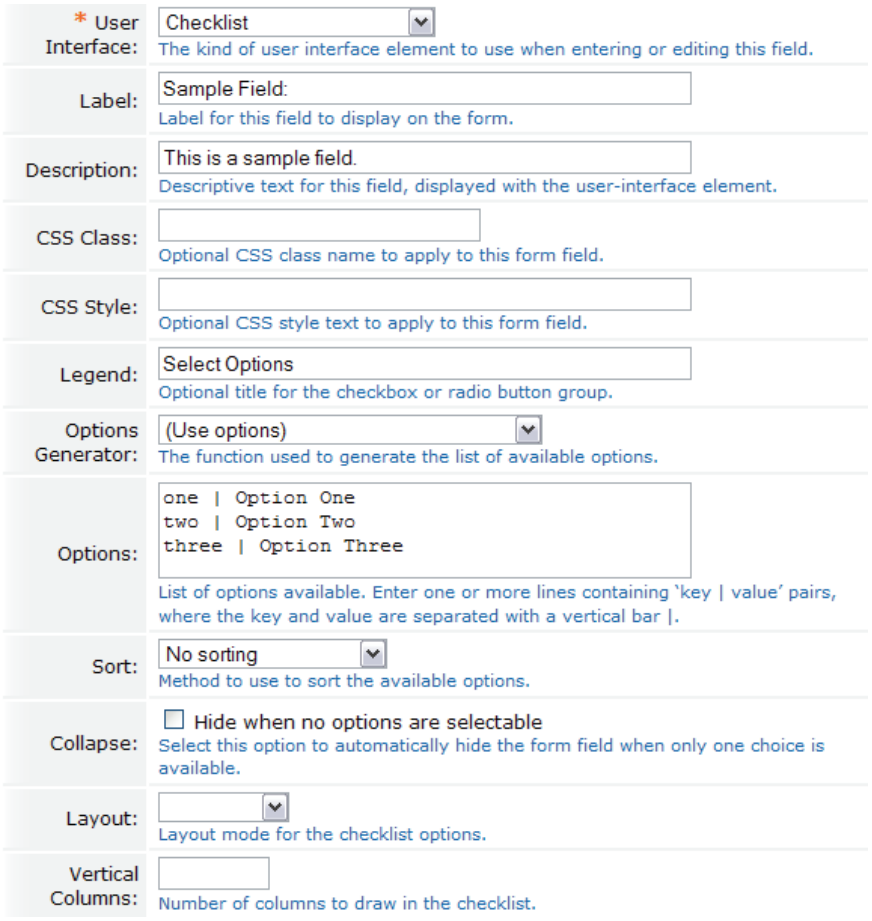
- **Checklist** – A list of check boxes is displayed. The text displayed for each check box is the value from the options list. Zero or more check boxes may be selected. This user interface type submits an array of values containing the option key values of each selected check box.

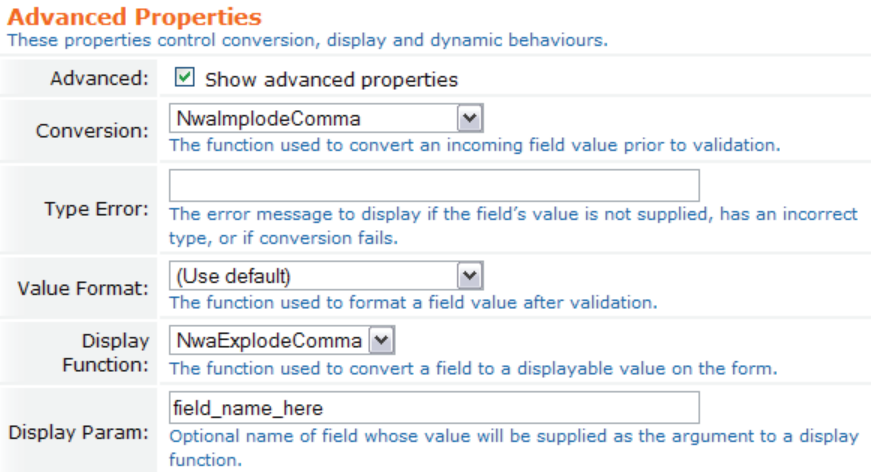


Because an array value may not be stored directly in a custom field, you should use the conversion and value formatting facilities to convert the array value to and from a string when using this user interface type.

To store a comma-separated list of the selected values, enable the Advanced options, select "NwaImplodeComma" for **Conversion**, select "NwaExplodeComma" for **Display Function** and enter the field's name for **Display Param**.

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.



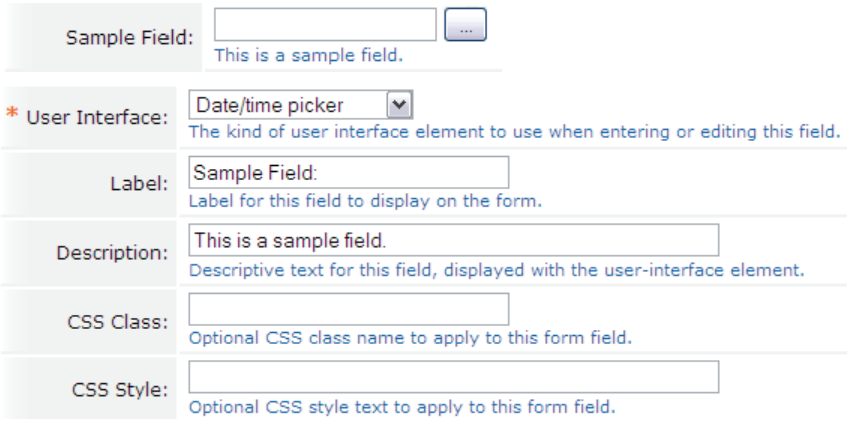


How this works: Suppose the first two check boxes are selected (in this example, with keys “one” and “two”). The incoming value for the field will be an array containing 2 elements, which can be written as `array("one", "two")`. The NwaImplodeComma conversion is applied, which converts the array value 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** – 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.

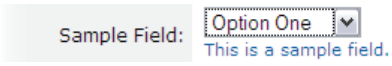
  The text value typed is submitted with the form. If using a date/time picker, you should validate the field value to ensure it is a date.

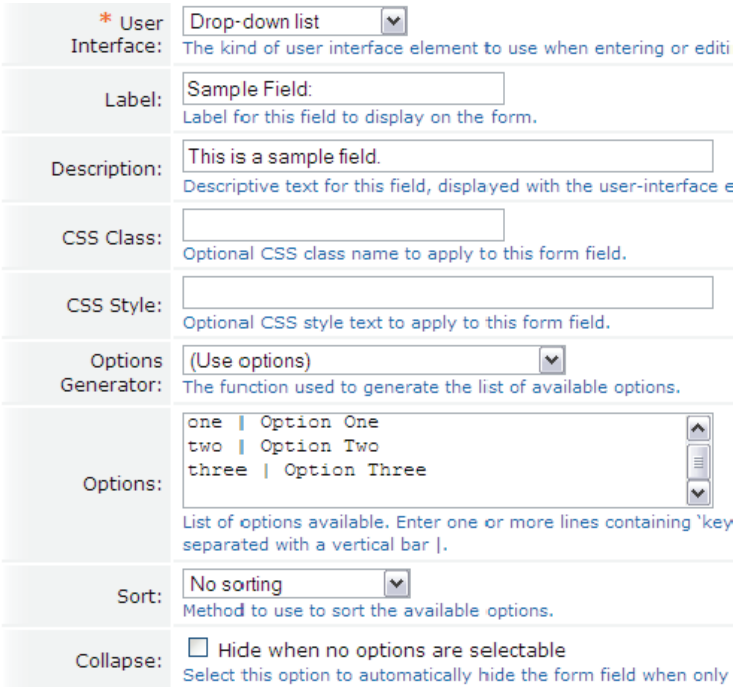
  Certain guest account fields, such as **expire_time** and **schedule_time**, require a date/time value to be provided as a UNIX time value. In this case, the conversion and display formatting options should be used to convert a human-readable date and time to the equivalent UNIX time and vice versa.



- **Drop-down list** – The field is displayed allowing a single choice from a drop-down list. 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.



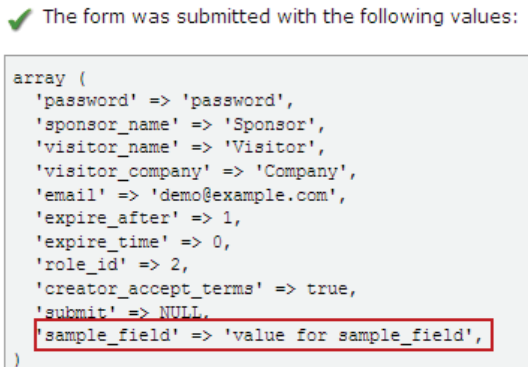


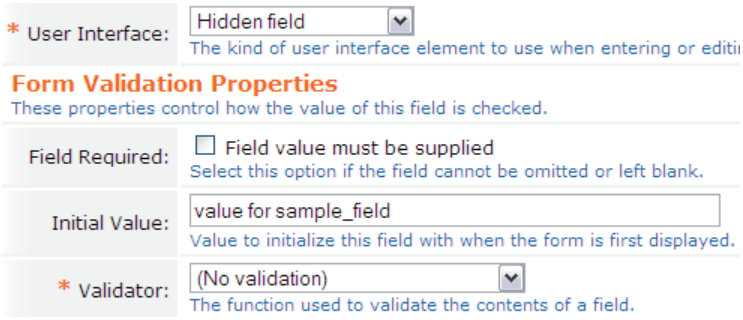
- **File upload** – Displays a file selection text field and dialog box (the exact appearance differs from browser to browser).

  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.

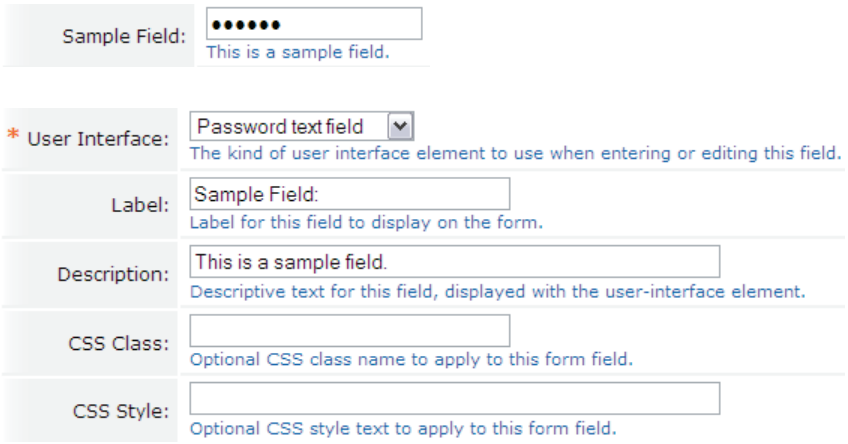
- **Hidden field** – If Hidden Field is selected in the User Interface drop-down list, the field is not displayed to the user, but is submitted with the form. This option is often used to force a specific value such as a user's role or an expiration date. However, it is possible for someone to use browser tools to modify the intial 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".

  To set the value to submit for this field, use the Initial Value option in the form field editor.

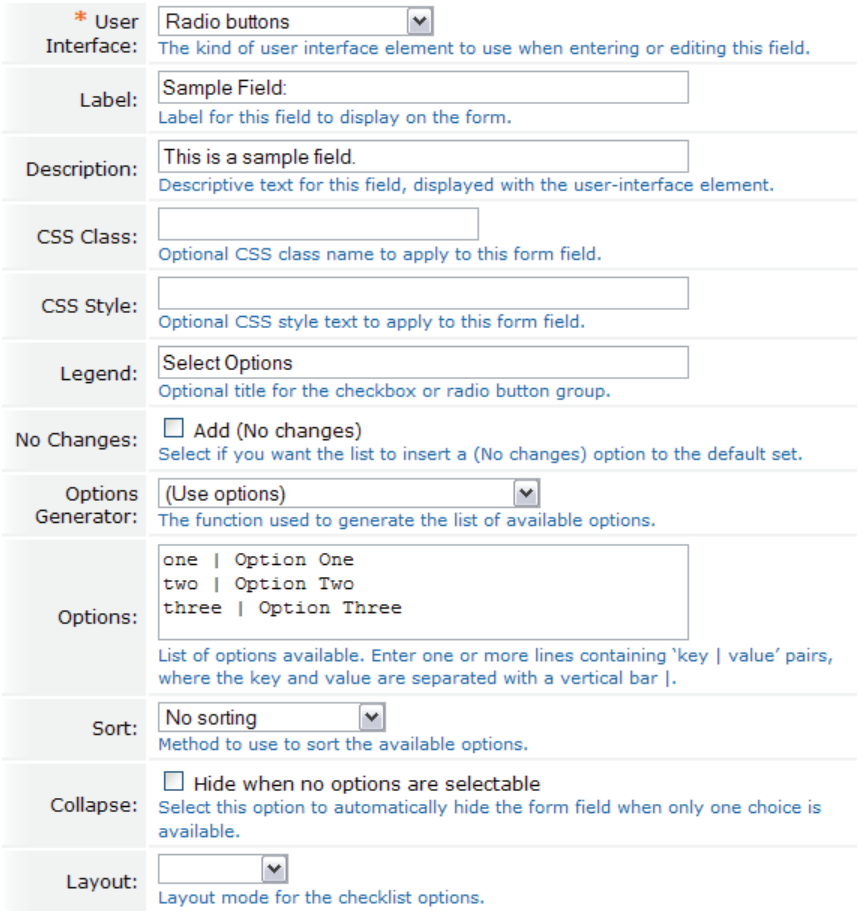




- **Password text field** – The field is displayed as a text field, with input from the user obscured. The text typed in this field is submitted as the value for the field.



- **Radio buttons** – The field is displayed as a group of radio buttons, allowing one to be selected. 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.

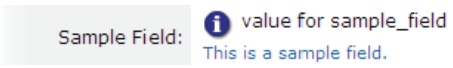


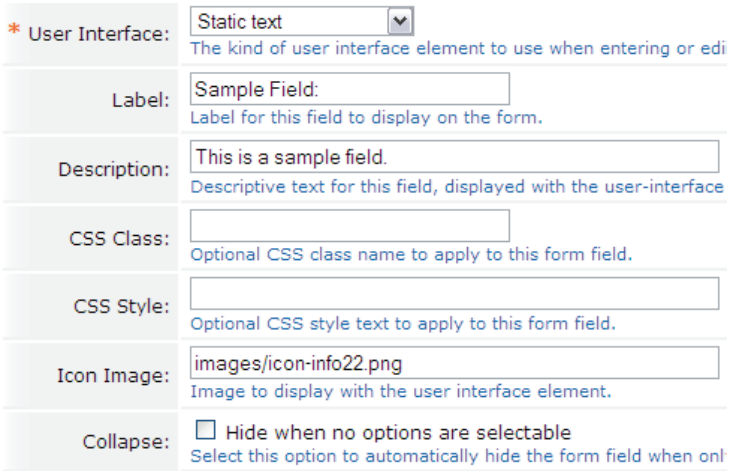
The "Vertical" and "Horizontal" layout styles control whether the radio buttons are organized in top-to-bottom or left-to-right order. The default is "Vertical" if not specified.

- **Static text** – 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.

  To set the value of this field, use the **Initial Value** option in the form field editor.

  If the **Hide when no options are selectable** check box is selected, the field will be hidden if its value is blank.



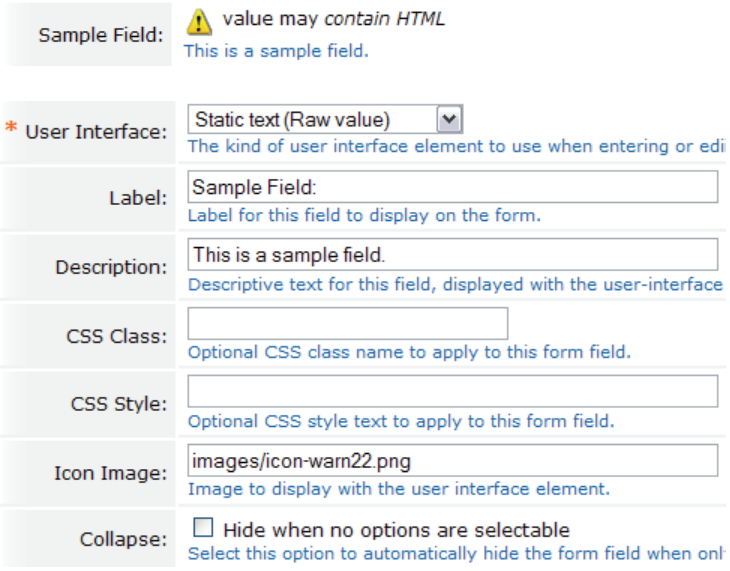


- **Static text (Raw value)** – The field's value is displayed as a non-editable text string. HTML characters in the value are not escaped, which allows you to display HTML markup such as images, links and font formatting.

  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.

  To set the value of this field, use **the Initial Value** option in the form field editor.

  If the "Hide when no options are selectable" option is selected, the field will be hidden if its value is blank.

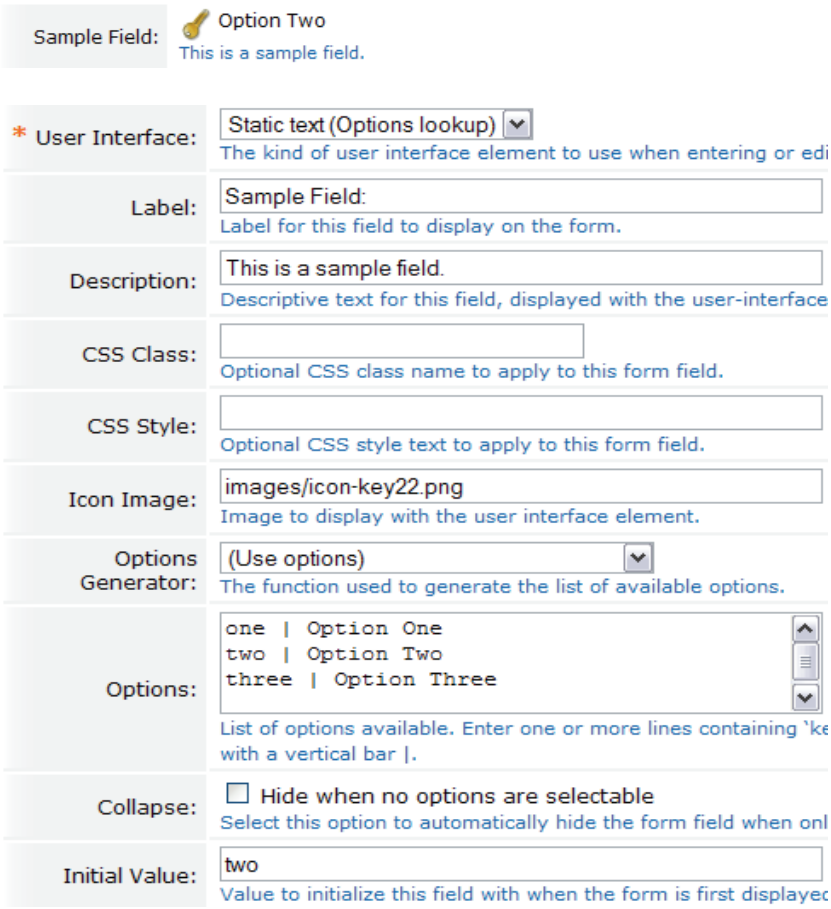


- **Static text (Options lookup)** – The value of the field is assumed to be one of the keys from the field's option list. The value displayed is the corresponding value for the key, as a non-editable text string.

  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.

  To set the value of this field, use the **Initial Value** option in the form field editor.

  If the **Hide when no options are selectable** check box is selected, the field will be hidden if its value is blank.

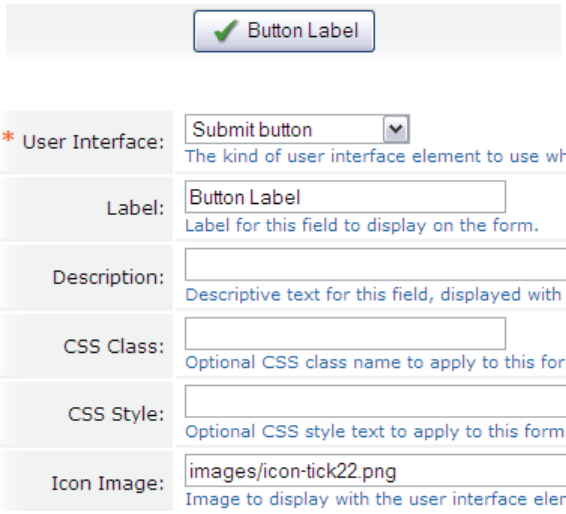


- **Static group heading** – The label and description of the field is used to display a group heading on the form. The field's value is not used, and the field is not submitted with the form.

  When using this user interface element, it is recommended that you use the "nwaImportant" CSS class to visually distinguish the group heading's title.

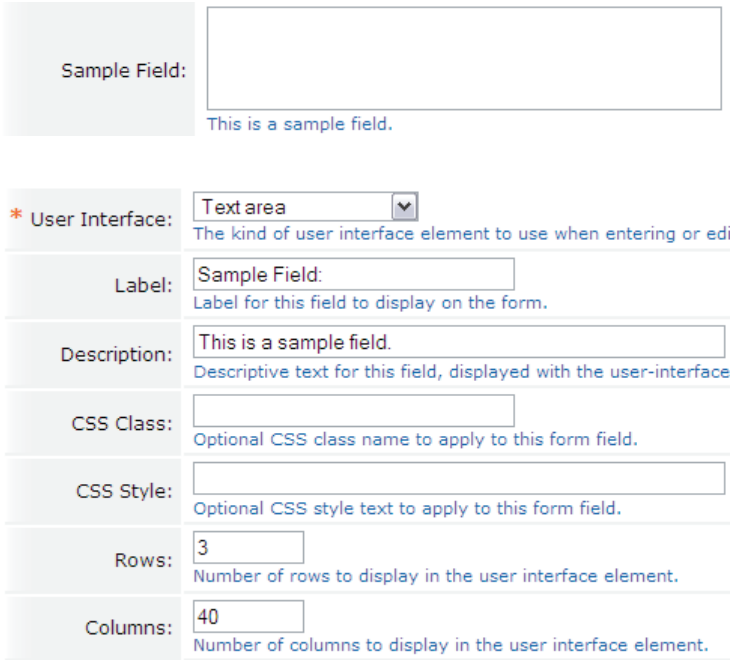
- **Submit button** – The field is displayed as a clickable form submit button, with the label of the field the label of the button. The description is not used. The field's value is ignored, and will be set to NULL when the form is submitted. To place an image on the button, an icon may be specified.

  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.



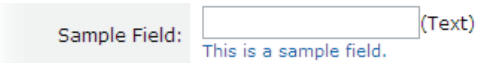
- **Text area** – The field is displayed as a multiple-line text box. The text typed in this box is submitted as the value for the field.

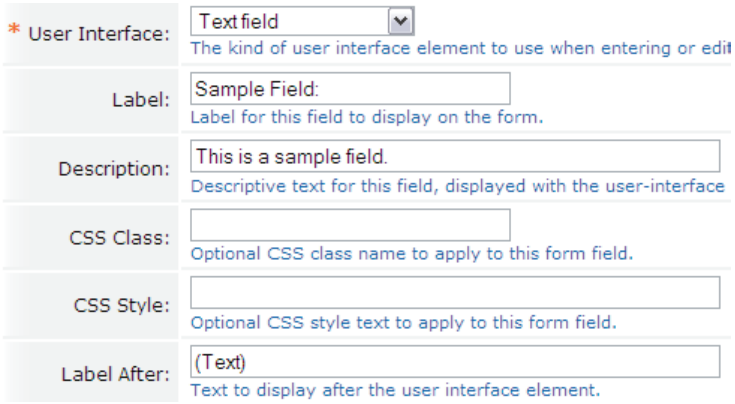
  It is recommended that you specify the desired minimum dimensions of the text area, either with the Rows and Columns options, or by specifying a width in the CSS Style (for example, "width: 460px; height: 100px;" specifies a 460 x 100 pixel minimum area).



- **Text field** – The field is displayed as a single-line text box. The text typed in this box is submitted as the value for the field.

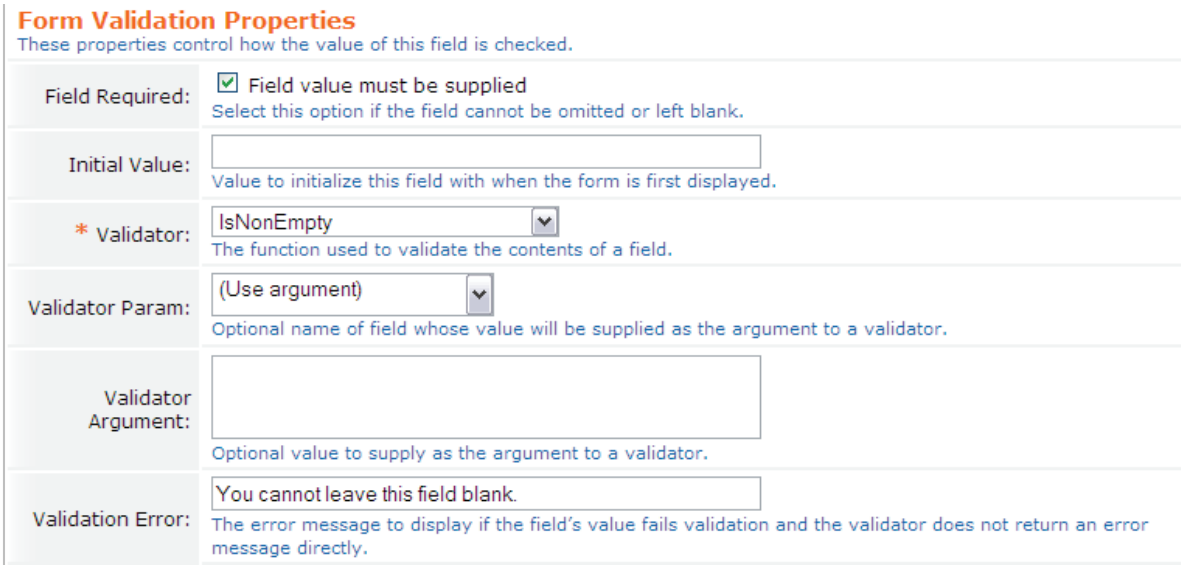
  A short text label may be placed after the text box using the Label After option.





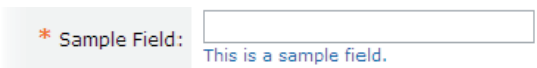
Form Validation Properties

The form va lidation 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.



The initial value for a form field may be specified. 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.

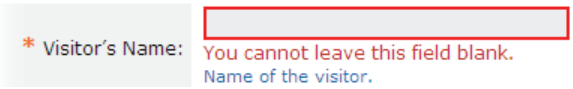
Select the **Field value must be supplied** check box to mark the field as a required field. Required fields are marked with an asterisk:



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.

All values supplied for a required field are always validated, including blank values.

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:



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.

To validate a specific field, choose a validator from the drop-down list. See "Form Field Validation Functions" in the Reference chapter for a description of the built-in validators.

The Validator Param is the name of a 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.

Set the Validator Param to its default value, "(Use argument)", to provide a fixed value as the argument to the validator.

The Validator Argument is used to provide 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.

Examples of Form field Validation

Example 1 – 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:

NOTE

The form field will contain an integer value, so you should set the field's type to Integer when creating it.

Use the PHP syntax **array(1, 100)** to specify the minimum and maximum values for the **IsInRange** validator. After saving changes on the form, this value will be internally converted to the equivalent code:

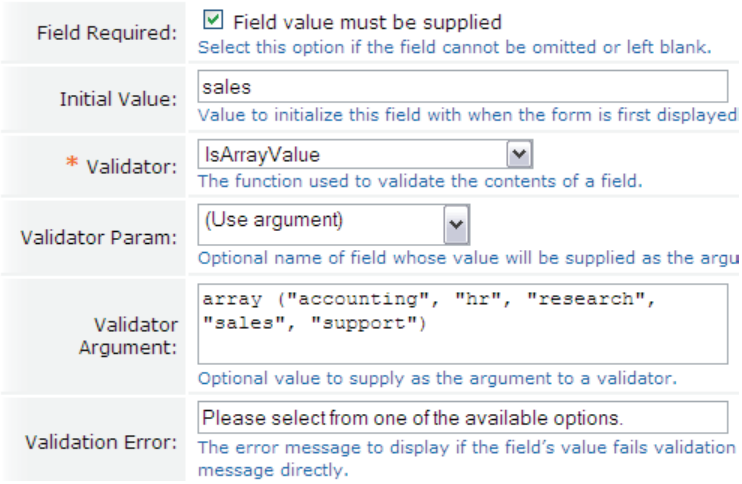
```
array (
  0 => 1,
  1 => 100,
)
```

With these validator settings, users that enter an invalid value will now receive a validation error message:

Furthermore, note that blank values, or non-numeric values, will result in a different error message:

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 under the Advanced Properties.

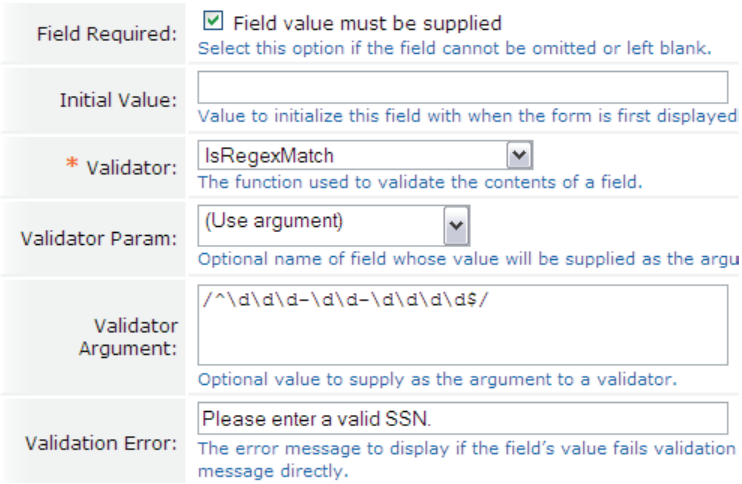
Example 2 – To create a form field that accepts one of a small number of string values, use the following settings in the form field editor:



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.

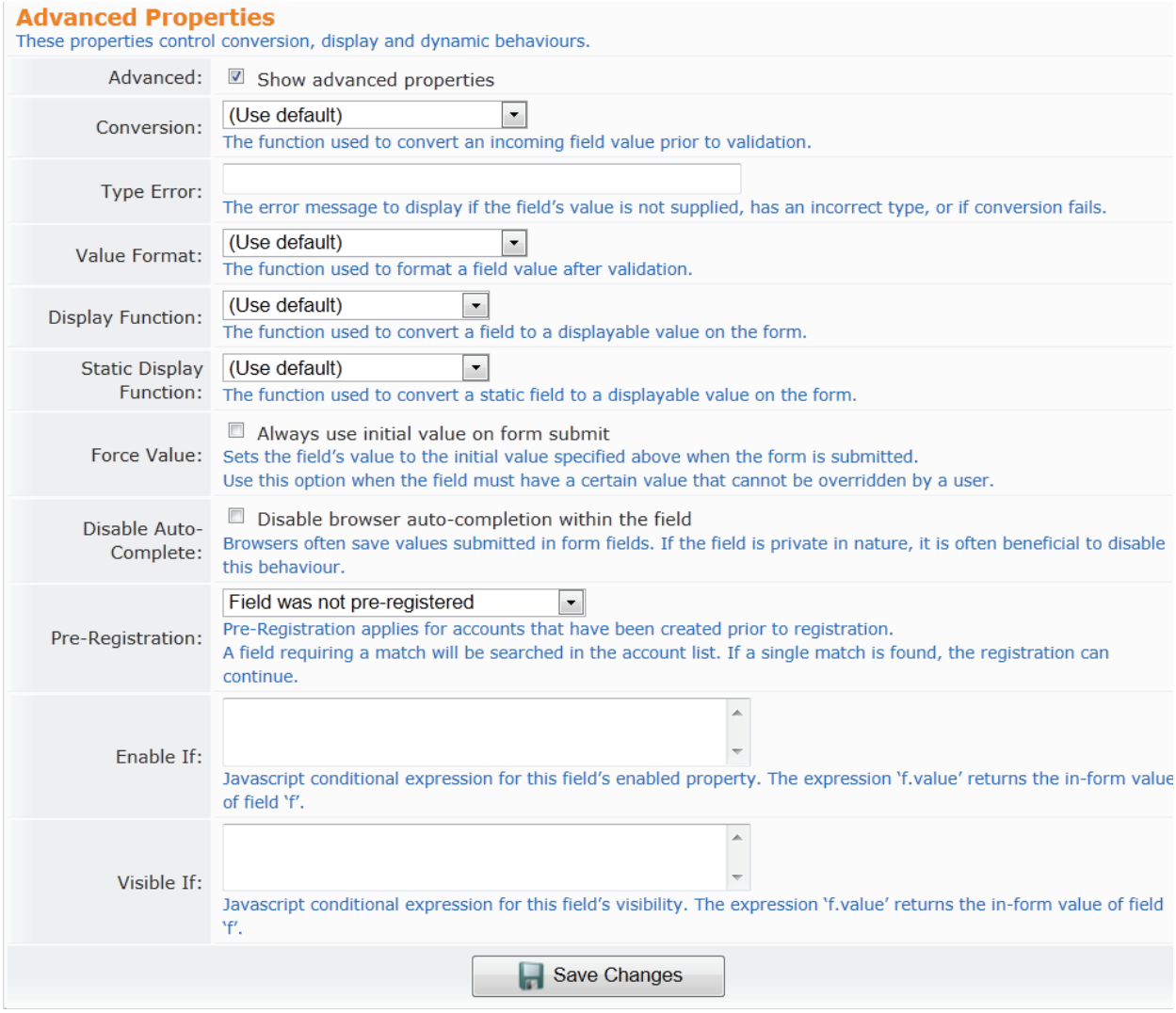
To match against a list of options used for a drop-down list or set of radio buttons, you can use the IsInOptionsList validator.

Example 3 – To create a form field that validates U.S. social security numbers using a regular expression, use the following settings in the form field editor:



Note 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" in the Reference chapter for more information about regular expressions.

Advanced Form Field Properties



The Advanced Properties control certain optional form processing behaviors. You can also specify JavaScript expressions to build dynamic forms similar to those found elsewhere in the application.

On the Customize Form Fields page, select the **Show advanced properties** check box to display the advanced properties in the form field editor.

The **Conversion**, **Value Format**, and **Display Function** options can be used to enable certain form processing behavior. See "Form Field Conversion Functions" and **"Form Field Display Formatting Functions"**.

In the **Force Value** row, use the **Always use initial value on form submit** check box to prevent attempts to override the value set for a 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.

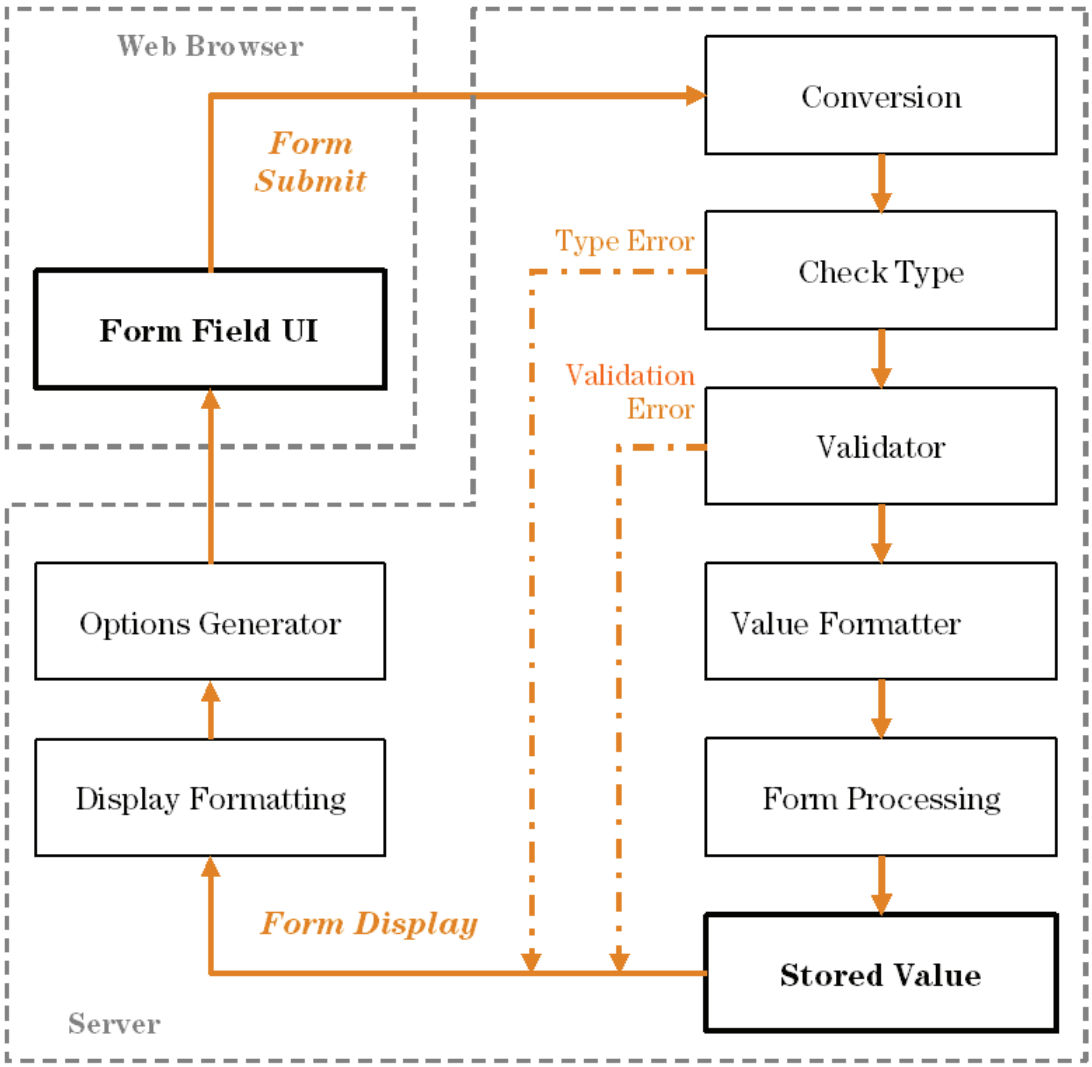
For pre-registered guest accounts, some fields may be completed during pre-registration and some fields may be left for the guest to complete at registration. You can use the **Pre-Registration** field to specify whether the guest's entry must match the preliminary value provided for a field during pre-registration.

- If a value was not provided for a field when the account was created, choose **Field was not pre-registered** from the drop-down list.
- If a preliminary value was provided for the field but the guest's entered value does not need to match case or all characters, choose **Guest must supply field** from the drop-down list. For example, a bulk account creation might use random usernames, and each visitor's entry in that field would not need to match exactly.
- If a preliminary value was provided for the field and the guest's entered value must match case or all characters, choose **Guest must supply field (match case)** from the drop-down list. 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.

Form Field Validation Processing Sequence

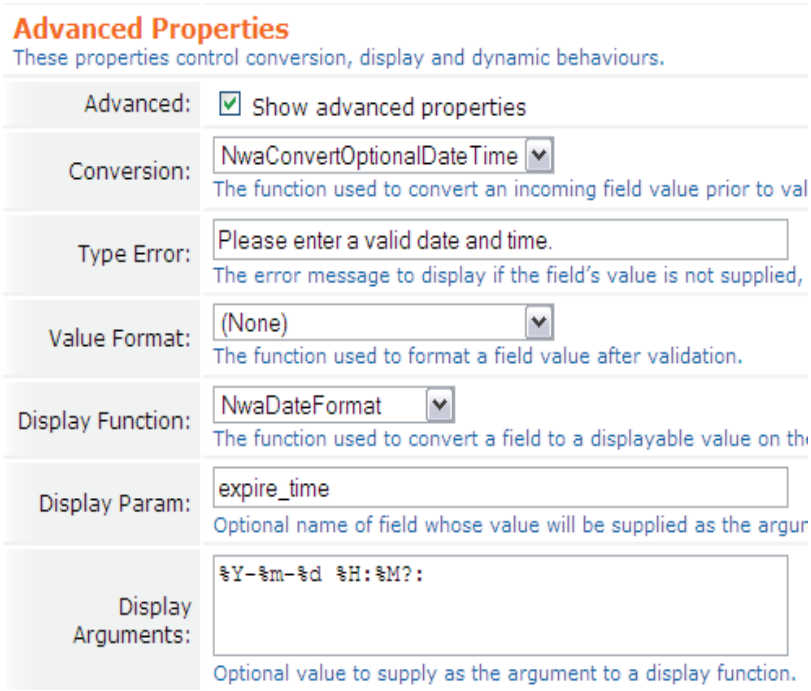
The following figure shows the interaction between the user interface displayed on the form and the various conversion and display options. **See Figure 29.**

Figure 29 *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).

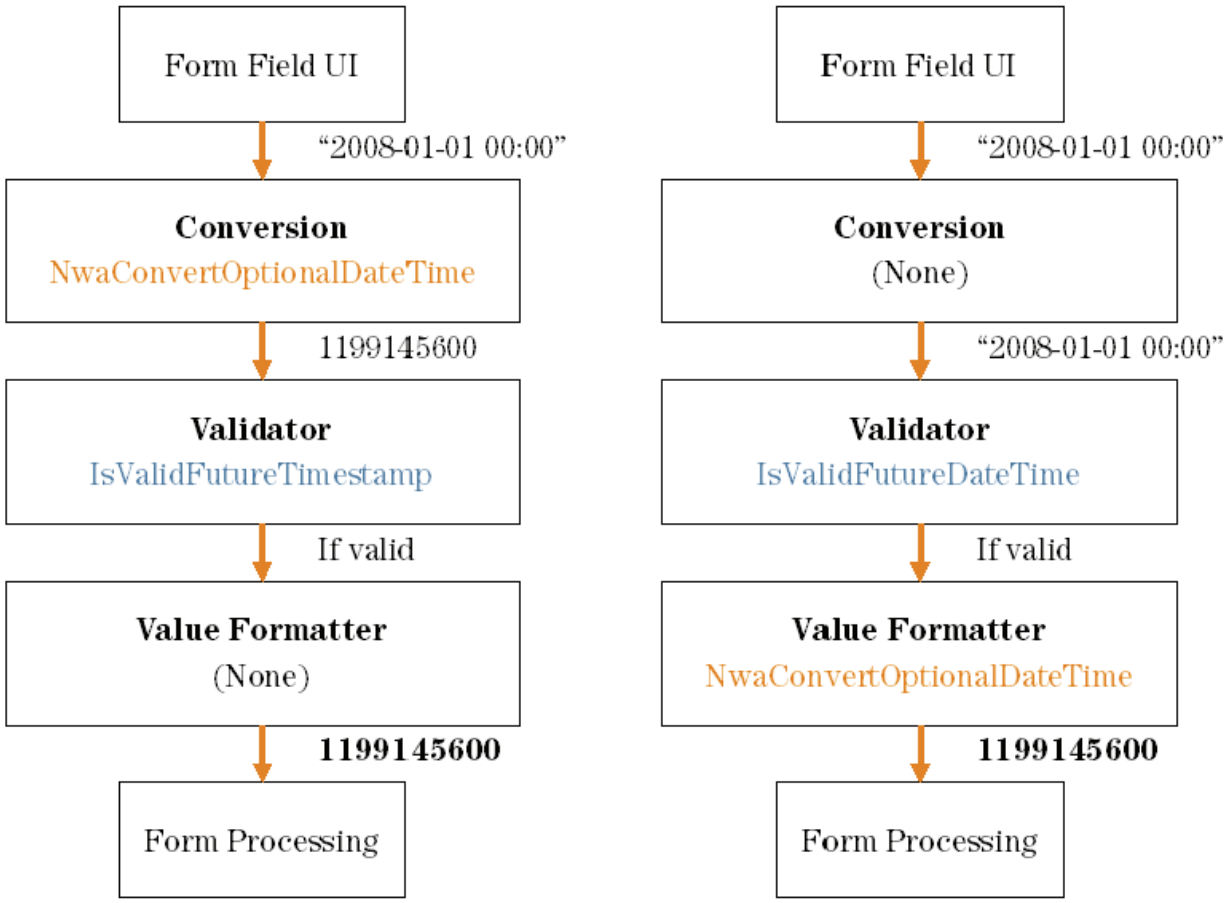


In this case, the Conversion function is set to NwaConvertOptionalDateTime to convert the string time representation from the form field (for example, "2008-01-01") to UNIX time (for example, 1199145600).

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:



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" in the Reference chapter 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" in the Reference chapter 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.

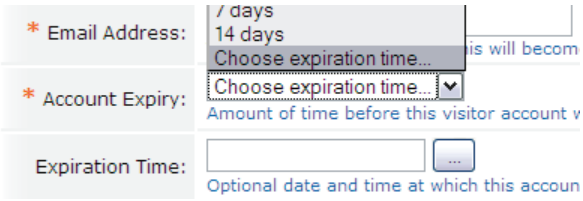
The expression must be a Boolean expression in the JavaScript language; statements and other code should not be included as this will cause a syntax error when the form is displayed in a Web browser.

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 Expiry** drop-down list. One of the values in this list is special: the **-1** option displays the value **Choose expiration time...**



When this option is selected, the **Expiration Time** field is then displayed, 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.

Additional examples of the **Visible If** conditional expressions can be found in the **guest_edit** form.

Editing Views

A view 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, select the view in the **Customize Forms & Views** list and click the **Edit Fields** link. This opens the Customize View Fields editor.

Quick Help Add Field

Rank	Field	Type	Title	Width
10	**username**	*sort*	*Username*	*160px*
20	visitor_company	*text*	*Company*	*100px*
30	visitor_phone	*sort*	*Phone*	*120px*
40	creator_name	*sort*	*Creator*	*100px*
50	sponsor_name	*text*	*Sponsor*	*100px*
60	**role_name**	*sort*	*Role*	*120px*
70	**enabled**	*sort*	*Status*	*75px*
80	**expire_time**	*sort*	*Expiration*	*180px*

View fields have a rank number, which specifies the relative ordering of the columns when displaying the view. The Customize View Fields editor always shows the columns in order by rank.

The type of each field is displayed. This controls what kind of user interface element is used to display the column, and whether the column is to be sortable or not. The title of the column and the width of the

column are also shown in the list view. Values displayed in *italics* are default values defined for the field being displayed.

Click a view field in the list view to select it.

Use the **Edit** link to make changes to an existing column using the view field editor. Any changes made to the field using this editor will apply only to this field on this view.

Use the **Edit Base Field** link to make changes to an existing field definition. 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).

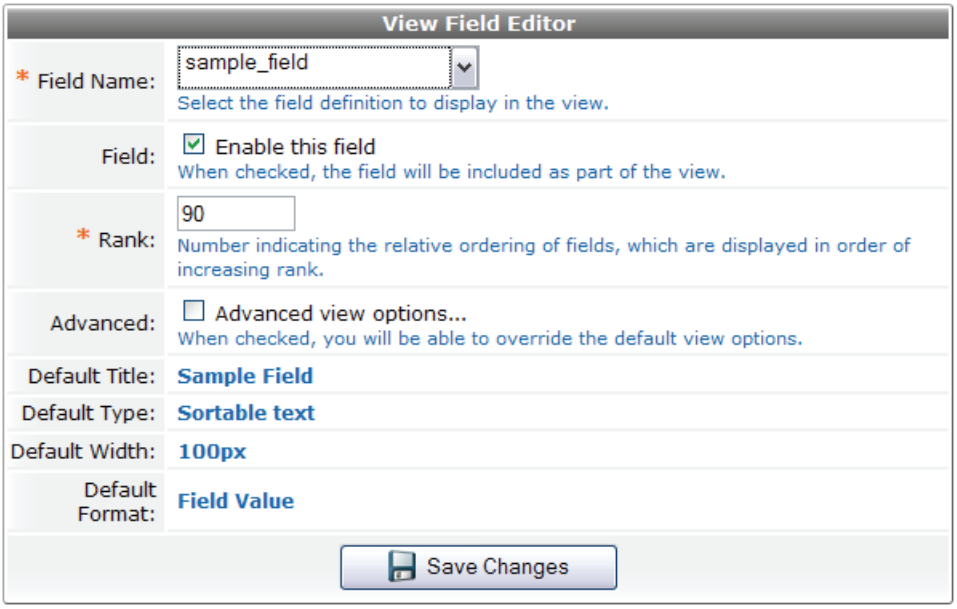
The **Insert Before** and **Insert After** links can be used to add a new column to the view. Clicking one of these links will open a blank view field editor and automatically set the rank number of the new column.

Use the **Enable Field** and **Disable Field** links to quickly turn the display of a column on or off.

Click the **Add Field** tab to add a new column to the view.

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 use the default view display properties for a field, you only need to select the field to display in the column and then click the **Save Changes** button.

To customize the view display properties, click the **Advanced view options...** check box.

The column type must be one of the following:

- **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.

The Column Format may be used to specify how the field's value should be displayed. You may choose from one of the following:

- **Field Value** – The value of the field is displayed as plain text.
- **Field Value (Un-Escaped)** – The value of the field is displayed as HTML.
- **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" in the Reference chapter for technical information about this display expression and a list of the functions that are available to format the value.

The Display Expression is a JavaScript expression that is used to generate the contents of the column. Generally, this is a simple expression that returns an appropriate piece of data for display, but more complex expressions can be used to perform arbitrary data processing and formatting tasks.

Customizing Self Provisioned Access

Guest self-registration allows an administrator to customize the process for guests to create their own visitor accounts.

The registration process consists of a data collection step (the 'register page') and a confirmation step (the 'receipt page').

You can define what information is collected from visitors on the registration page. 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 also includes a form, although typically this form will only contain static information about the guest account. Several different actions can be included on the receipt page, 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.

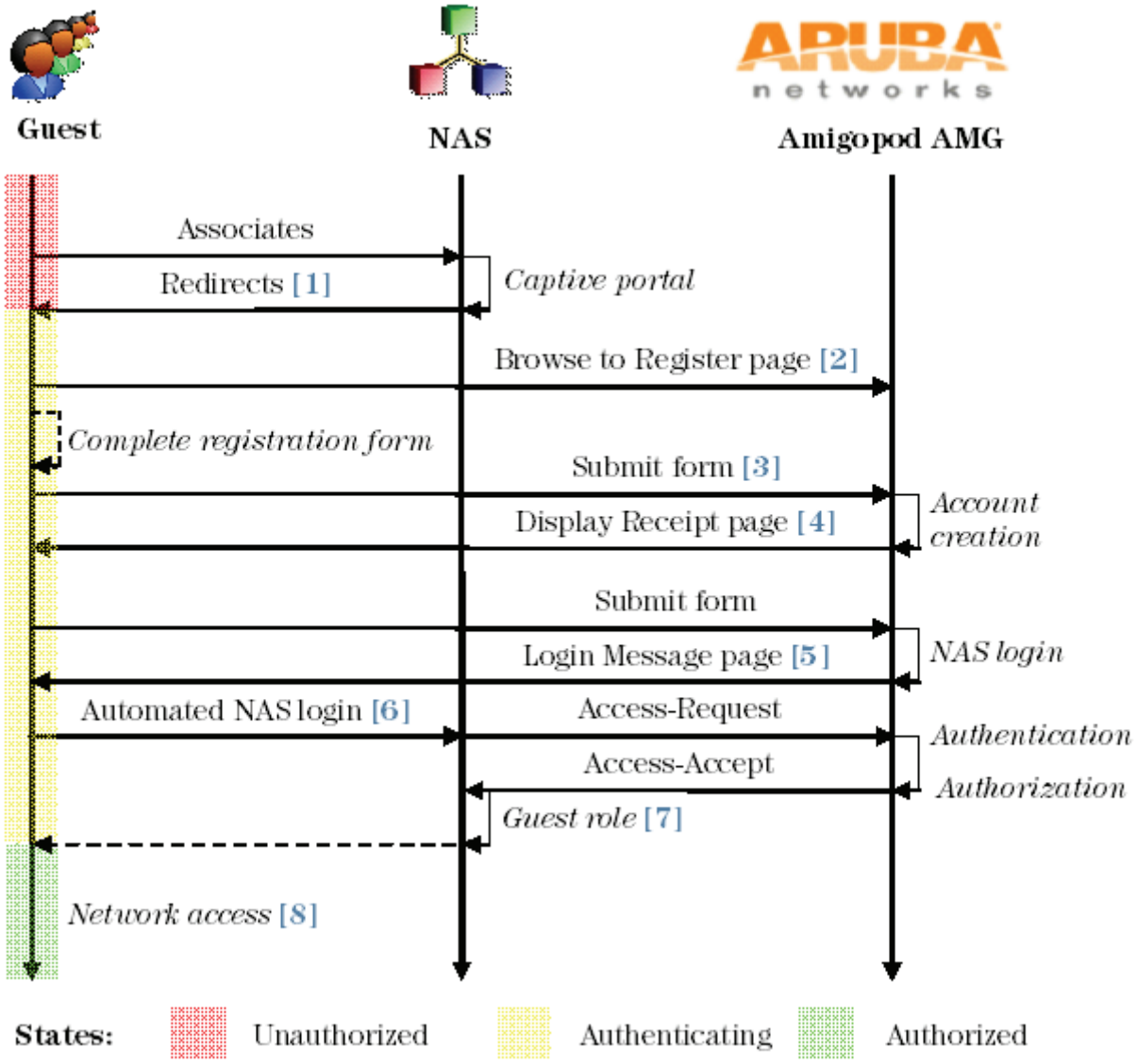
Detailed user interface customization can be performed for all parts of the self-registration process. You can define page titles, template code for the page header and footer, and choose a skin that controls the overall look and feel of self-registration. The default user interface customization can be disabled.

Self-Registration Sequence Diagram

To set up a captive portal with guest self-registration, configure your Network Access Servers to redirect guests to the URL of the 'Go To' link. To complete the portal, 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 as follows. **See Figure 30.**

Figure 30 *Sequence diagram for guest self-registration*



The captive portal redirects unauthorized users [1] to the register 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, 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].

Creating a Self-Registration Page

Click the **Create new self-registration page** link. The **Customize Guest Registration** form is displayed.

The Register Page is the name of a page that does not already exist. 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**.

Click the **Save Changes** button to save the self registration page. A diagram of the self registration process is displayed.

Click the **Save and Continue** button to proceed to the next step of the setup.

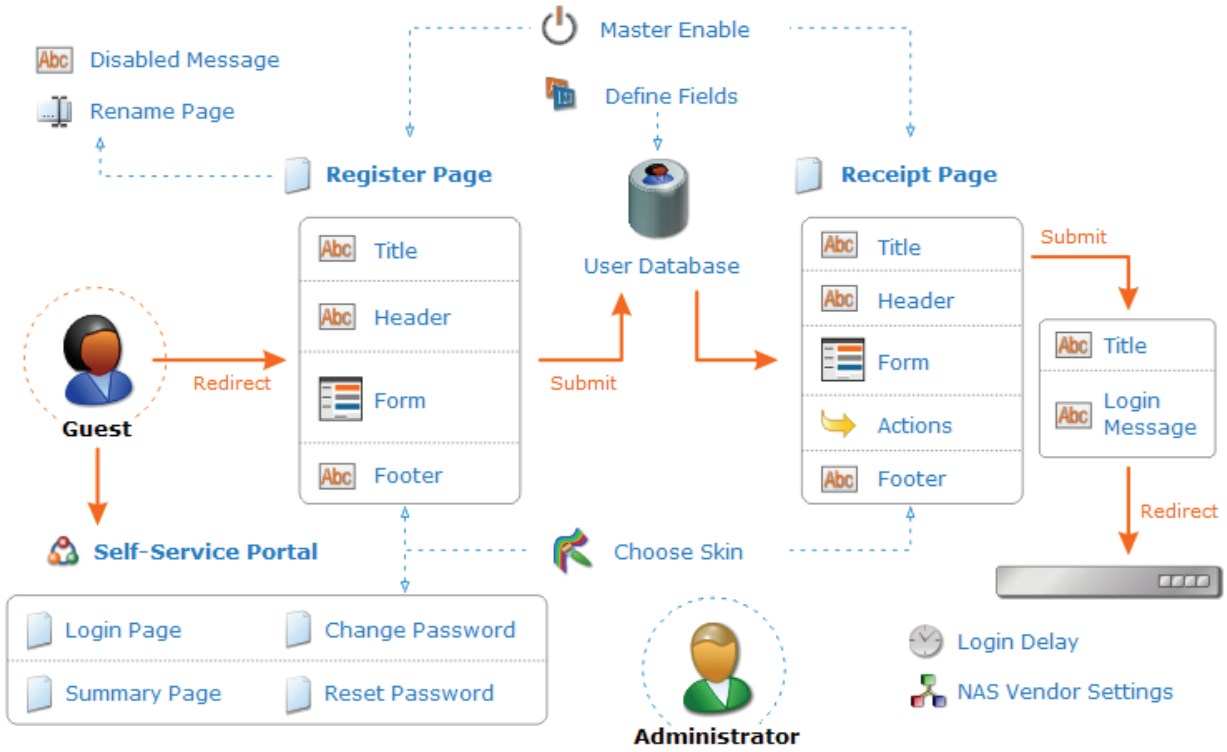
Once a self registration page has been created you are able to edit, delete, duplicate or go to it, providing self-registration has been enabled.

Editing Self-Registration Pages

The guest self-registration process is displayed in graphical form, shown below in **See Figure 31**. The workflow for the guest is shown using solid orange arrows, while the administrator workflow is shown with dotted blue arrows. To access this page in the WebUI:

1. Navigate to **Customization > Guest Self-Registration**
2. Select an entry in the **Guest Self-Registration** list, then click **Edit**.
3. The **Customize Guest Registration** workflow page appears, as shown below

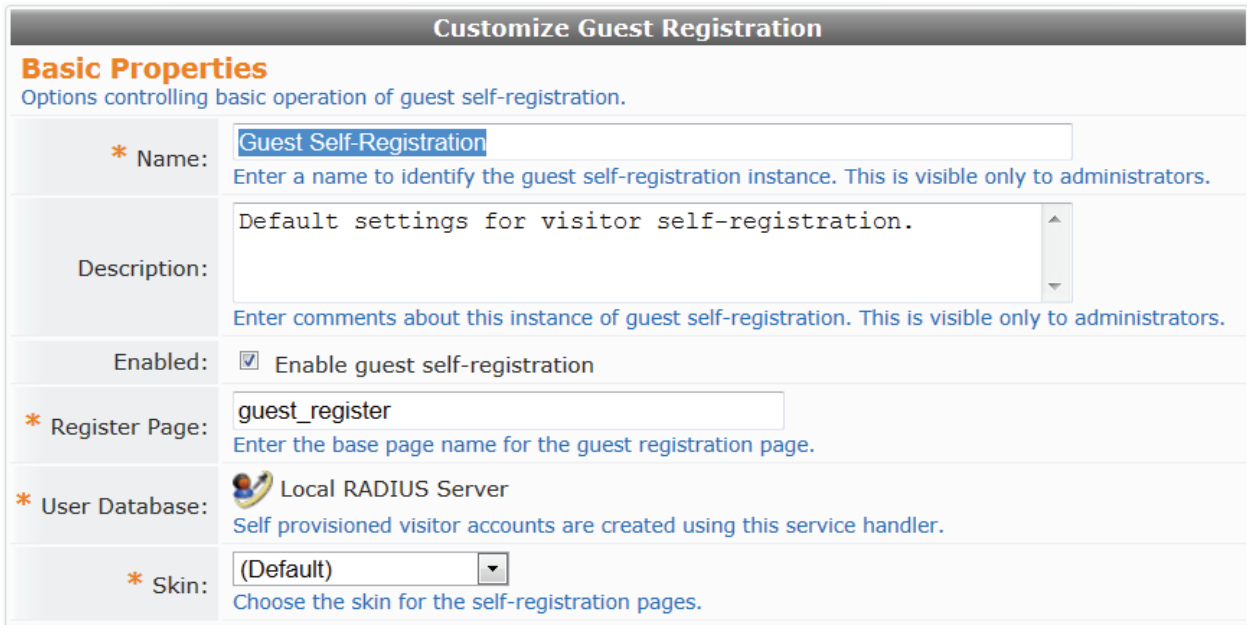
Figure 31 Guest self-registration process



A guest self-registration page consists of many different settings, which are divided into groups across several pages. Click an icon or label in the diagram to jump directly to the editor for that item.

Configuring Basic Properties for Self-Registration

Click the **Master Enable**, **User Database**, **Choose Skin**, or **Rename Page** links to edit the basic settings for guest self-registration.



The Basic Properties window has configurable settings such as Name, Description, enabling guest-self registration, Register Page, Parent, and Authentication.

Using a Parent Page

To use the settings from a previously configured self-registration page, select an existing page name from the **Parent** drop-down menu. This is useful if you need to configure multiple registrations. You can always override parent page vaules 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.

Paying for Access

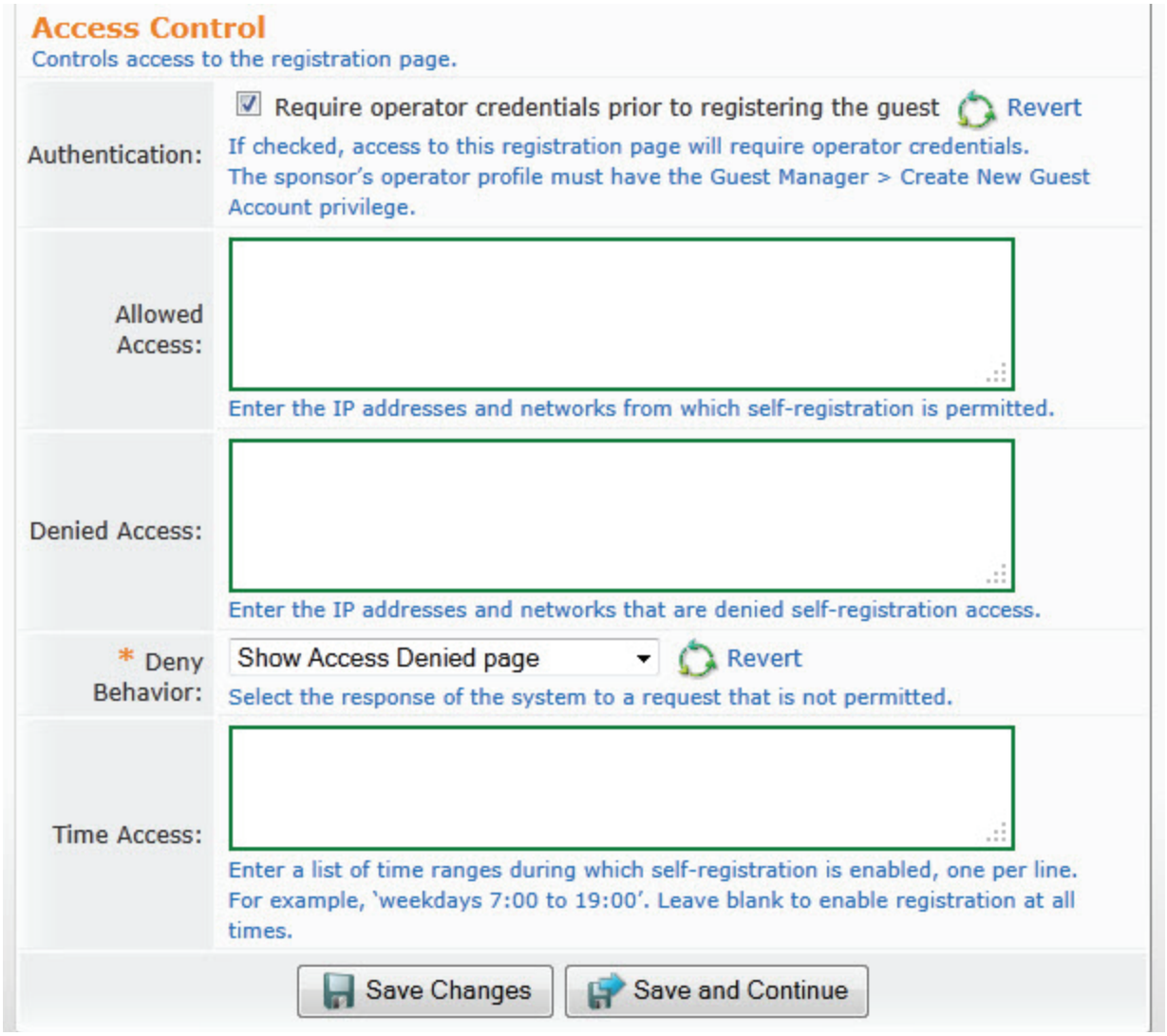
If you select a standalone self -registration, **(No parent- standalone)** option you can also configure the Hotspot option. You can configure this setting so that registrants have to pay for access.

Requiring Operator Credentials

If you want 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. The sponsor's operator profile must have the **Guest Manager > Create New Guest Account privilege** already configured.

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.

You can specify access restrictions for the self-registration page in the **Access Control** section of this form.



The **Allowed Access** and **Denied Access** fields are access control lists that determine if 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:

- **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

Use the **Deny Behavior** drop-down list to specify the action to take when access is denied. 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:

- 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

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 **0.0.0.0/0**.

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.

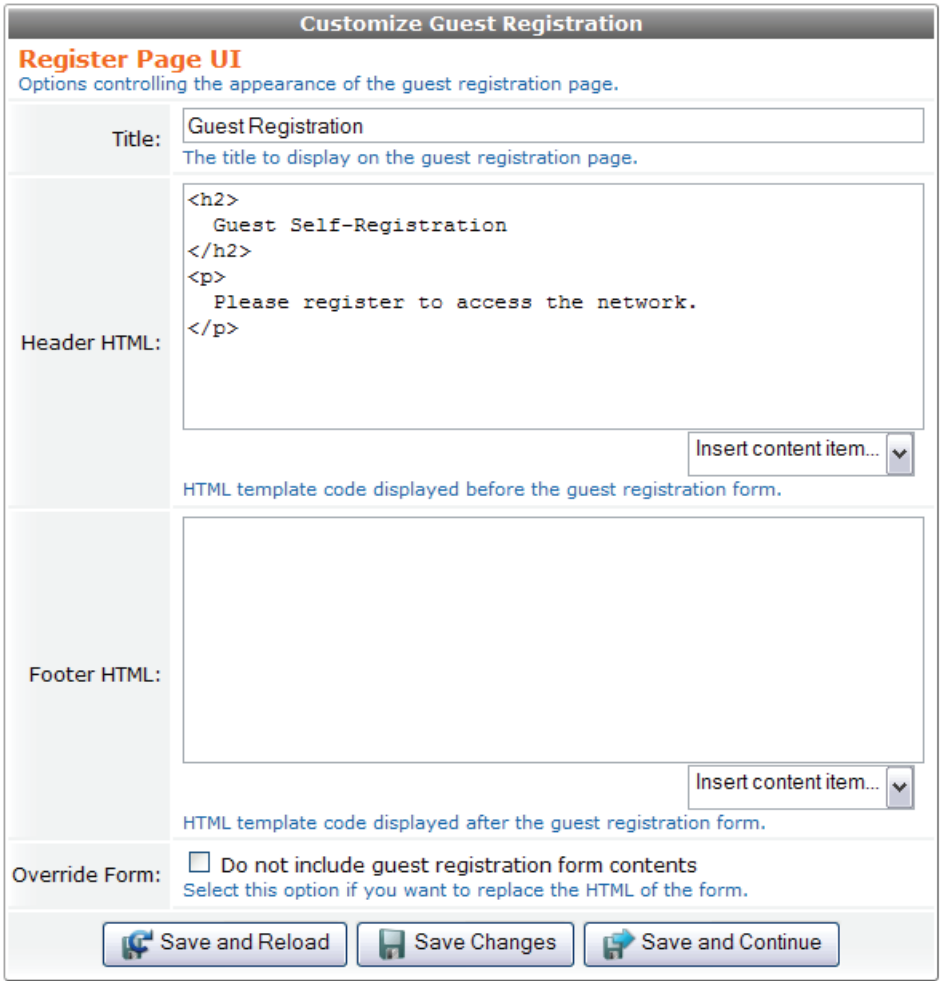
If the **Allowed Access** field is empty, all access will be allowed, except to clients with an IP address that matches any of the entries in the **Denied Access** field. This behavior is equivalent to adding the entry **0.0.0.0/0** to the **Allowed Access** field.

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 **0.0.0.0/0** to the Denied Access list.

Editing Registration Page Properties

To edit the properties of the registration page:

1. Navigate to **Customization > Guest Self-Registration**
2. Select an entry in the **Guest Self-Registration** list and click its **Edit** link. The **Customize Guest Registration** workflow page appears, as shown in Figure 31 on page 257.
3. Click the **Register Page** link, or one of the **Title**, **Header,** or **Footer** fields for the Register Page.



Template code for the title, header, and footer may be specified. See "Smarty Template Syntax" in the Reference chapter for details on the template code that may be inserted.

Select the **Do not include guest registration form contents** check box to override the normal behavior of the registration page, which is to display the registration form between the header and footer templates.

Click the **Save and Reload** button to update the self-registration page and launch or refresh a second browser window to show the effects of the changes.

Click the **Save Changes** button to return to the process diagram for self-registration.

Click the **Save and Continue** button to update the self-registration page and continue to the next editor.

Editing the Default Self-Registration Form Settings

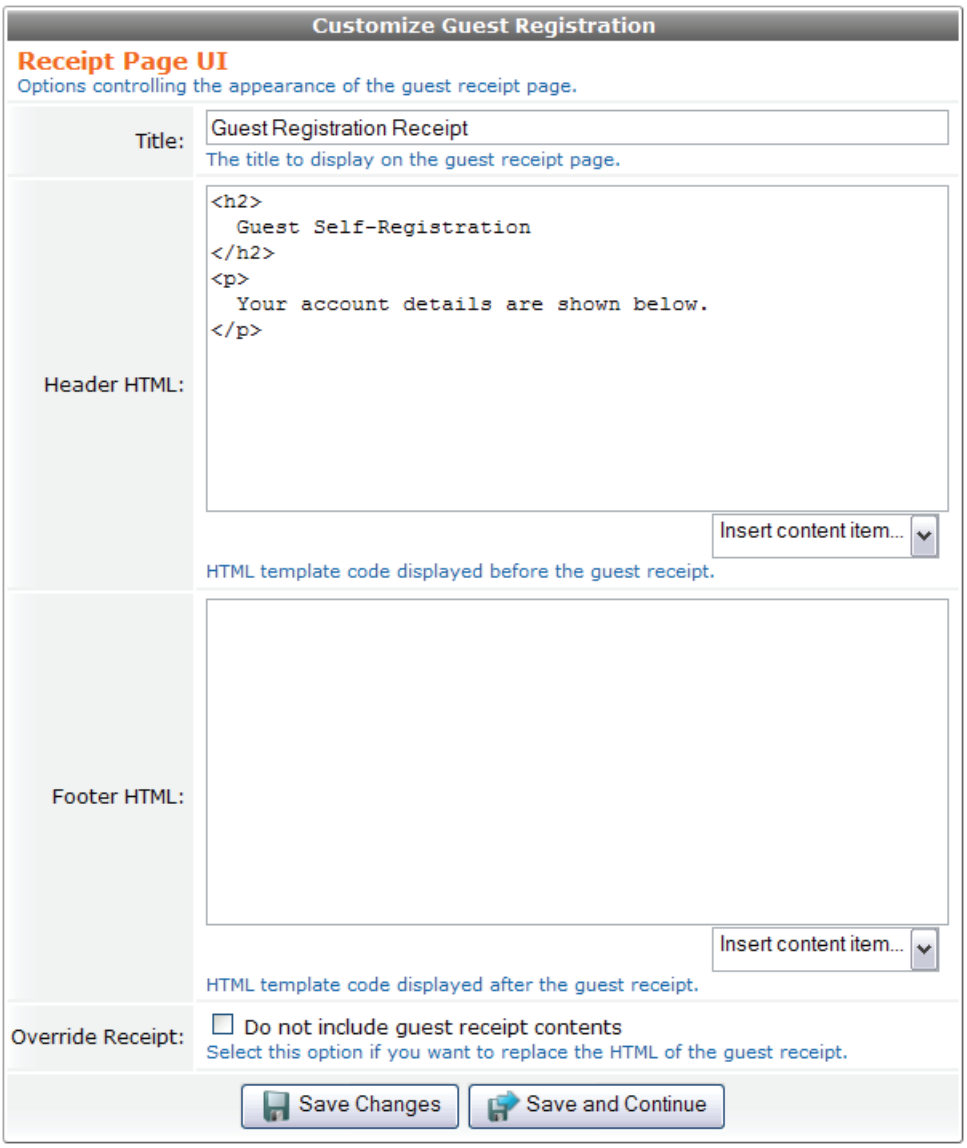
Click the **Form** link for the Register Page to edit the fields on the self-registration form.

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 hidden, and 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.
- The **role_id** field is hidden, and 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.
- 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.

Editing Guest Receipt Page Properties

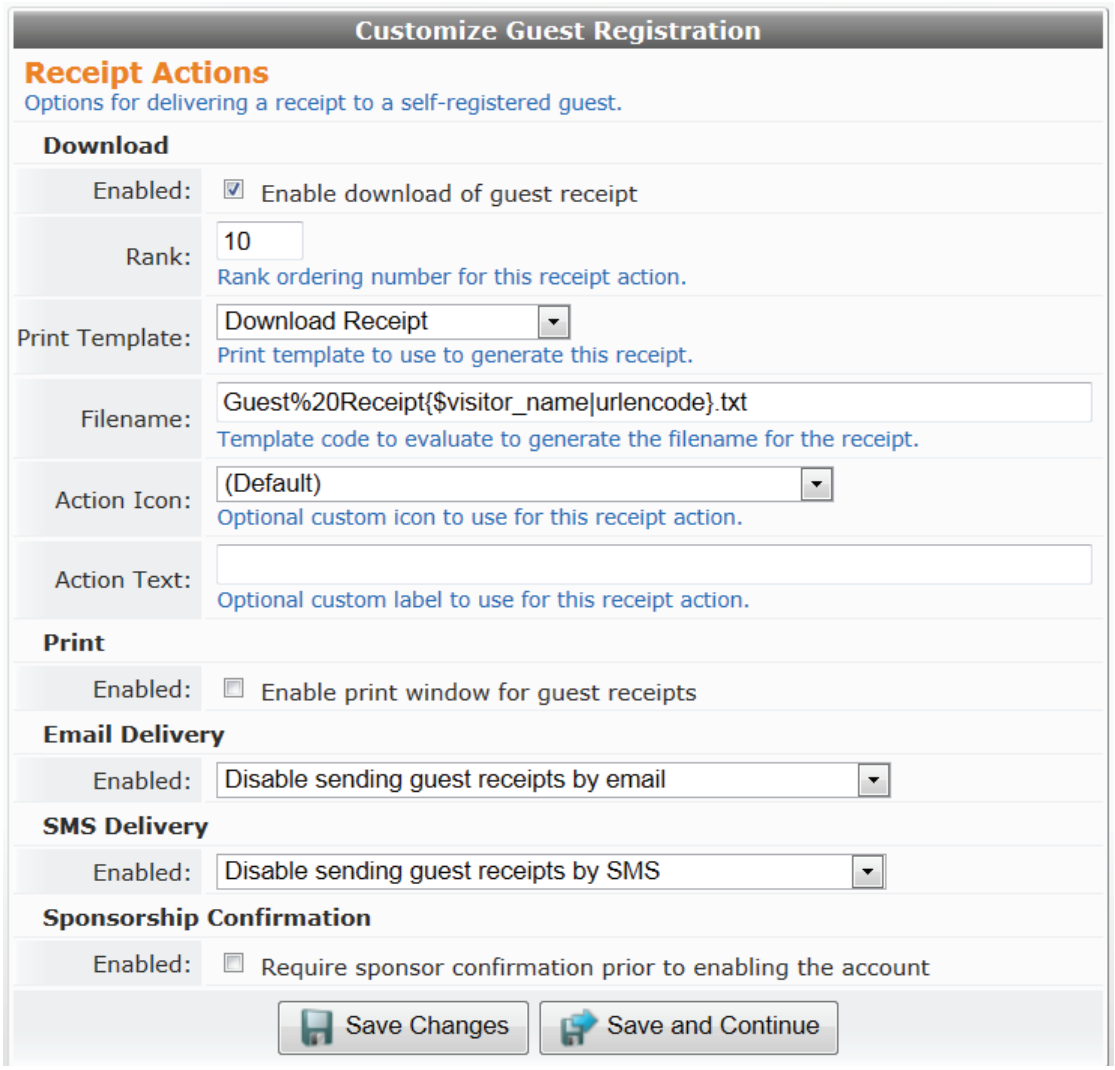
Click the **Receipt Page** link or one of the **Title**, **Header** or **Footer** fields for the Receipt Page to edit the properties of the receipt page. This page is shown to guests after their visitor account has been created.



Click the **Save Changes** button to return to the process diagram for self-registration.

Editing Receipt Actions

Click the **Actions** link to edit the actions that are available once a visitor account has been created.



Enabling Sponsor Confirmation for Role Selection

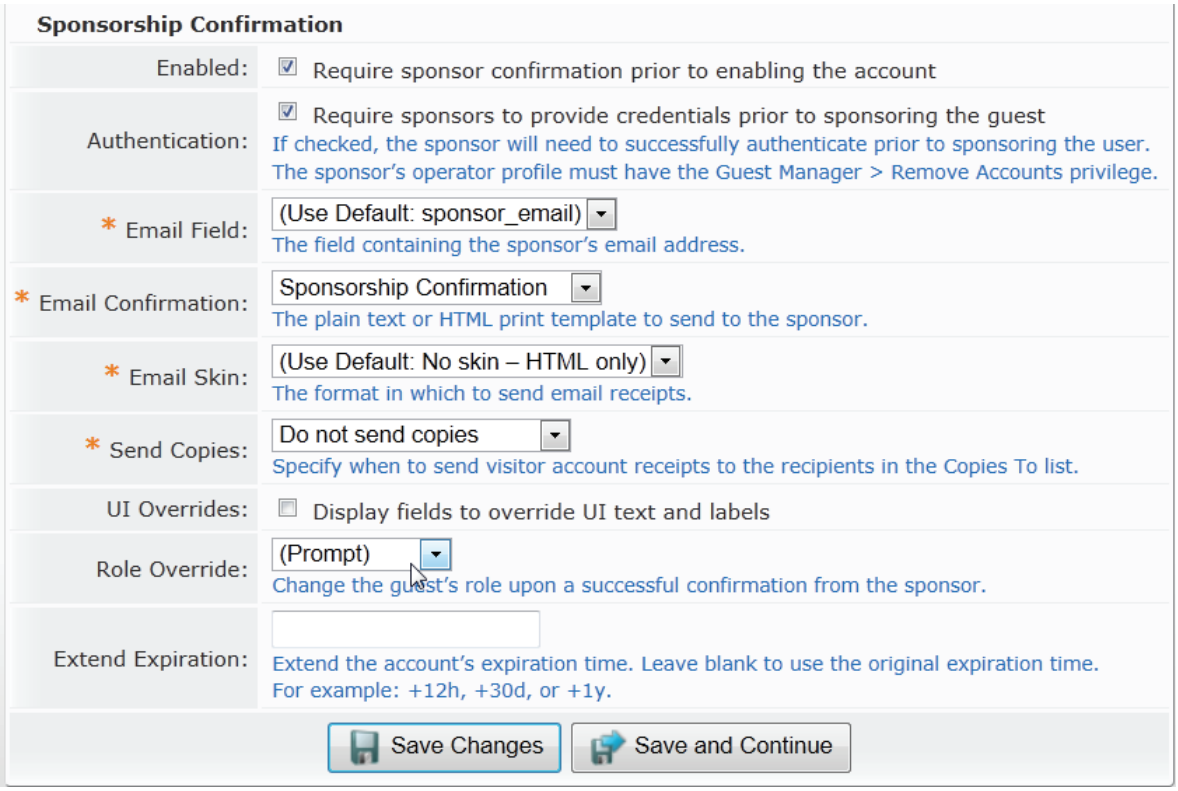
You can allow the sponsor to choose the role for the user account at the time the sponsor approves the self-registered account.

To enable role selection by the sponsor:

1. Go to **Customization > Guest Self-Registration**. Click the **Guest Self-Registration** row, then click its **Edit** link. The Customize Guest Registration diagram opens.
2. In the **Receipt Page** area of the diagram, click the **Actions** link.

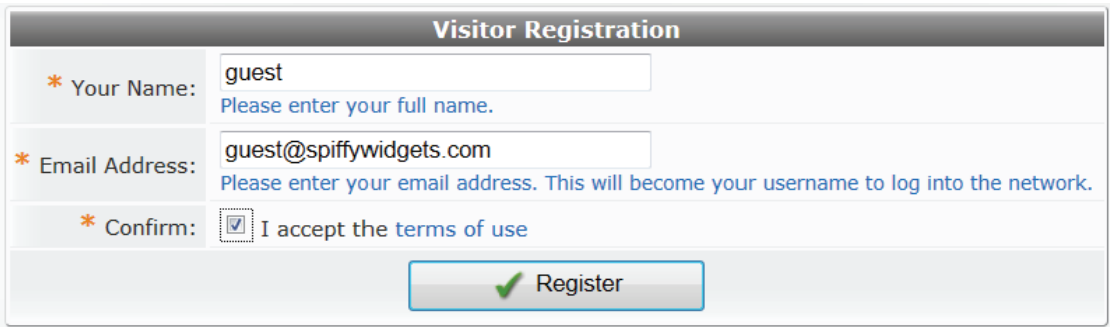
The Receipt Actions form opens.

3. In the **Sponsorship Confirmation** area at the bottom of the form, mark the **Enabled** check box for **Require sponsor confirmation prior to enabling the account**. The form expands to let you configure this option.



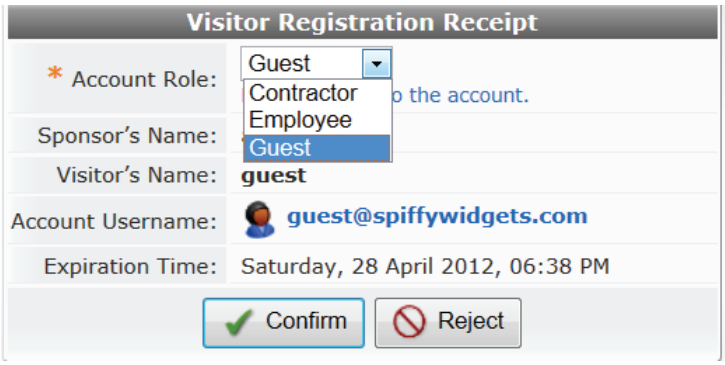
4. In the **Authentication** row, mark the check box for **Require sponsors to provide credentials prior to sponsoring the guest**.
5. In the **Role Override** row, choose **(Prompt)** from the drop-down list.
6. Complete the rest of the form with the appropriate information, then click **Save Changes**. The Customize Guest Registration diagram opens again.
7. Click the **Launch this guest registration page** link at the upper left to preview the Guest Registration login page.

The Guest Registration login page is displayed as the guest would see it.



When a guest completes the form and clicks the **Register** button, the sponsor receives an email notification.

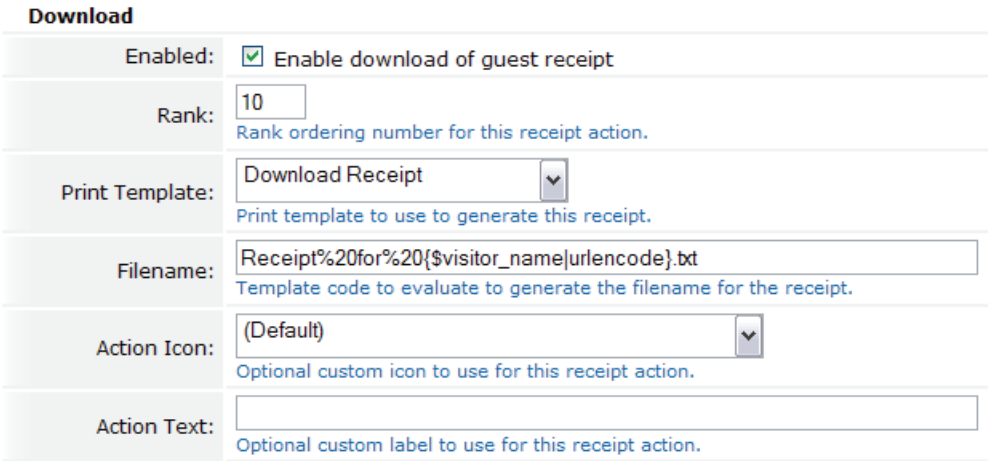
8. To confirm the guest's access, the sponsor clicks the **click here** link in the email, and is redirected to the Guest Registration Confirmation form.



9. In the **Account Role** drop-down list, the sponsor chooses the role for the guest, then clicks the **Confirm** button.

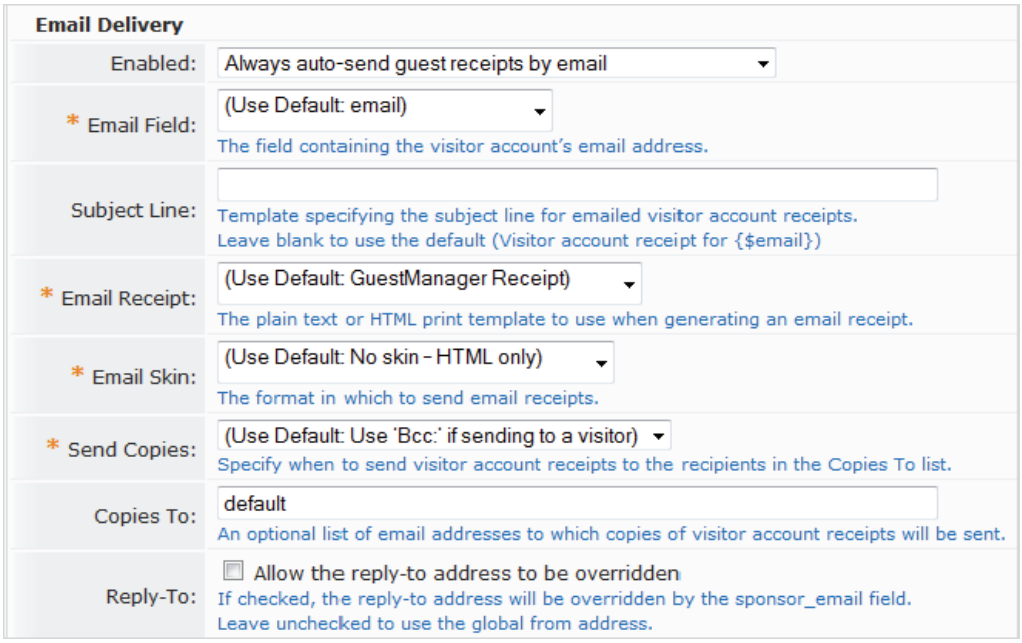
Editing Download and Print Actions for Guest Receipt Delivery

Select the **Download** or **Print** check box to enable the template and display options to deliver a receipt to the user as a downloadable file, or display the receipt in a printable window in the visitor's browser.



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.

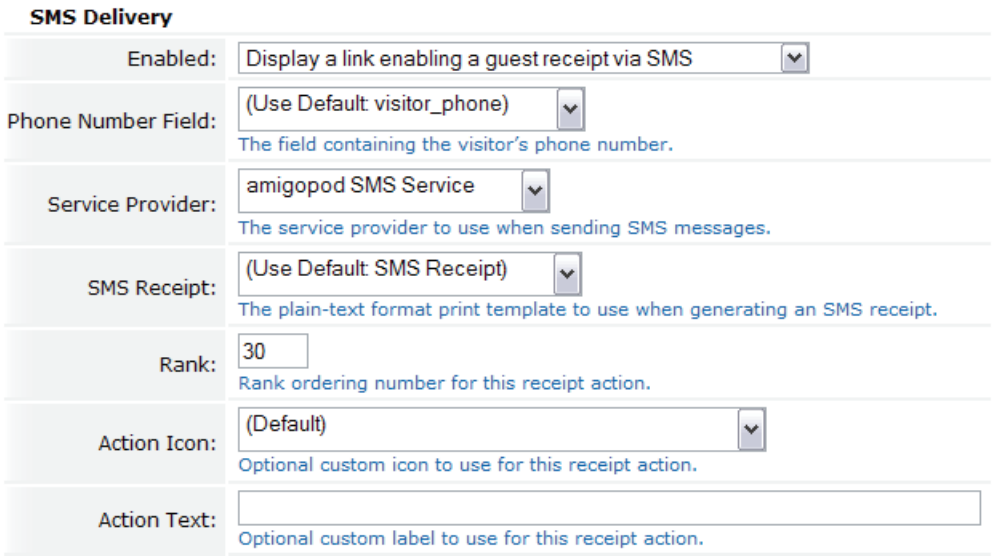


When email delivery is enabled, the following options are available to control email delivery:

- **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 "Copies To".

Editing SMS Delivery of Guest Receipts

The SMS Delivery options available for the receipt page actions allow you to specify the print template to use, the field containing the visitor's phone number, and the name of an auto-send field.

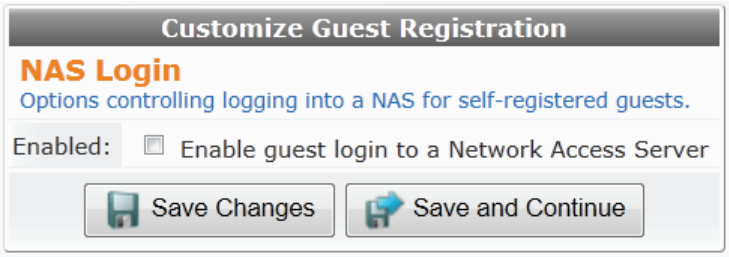


These options under Enabled are available to control delivery of SMS receipts:

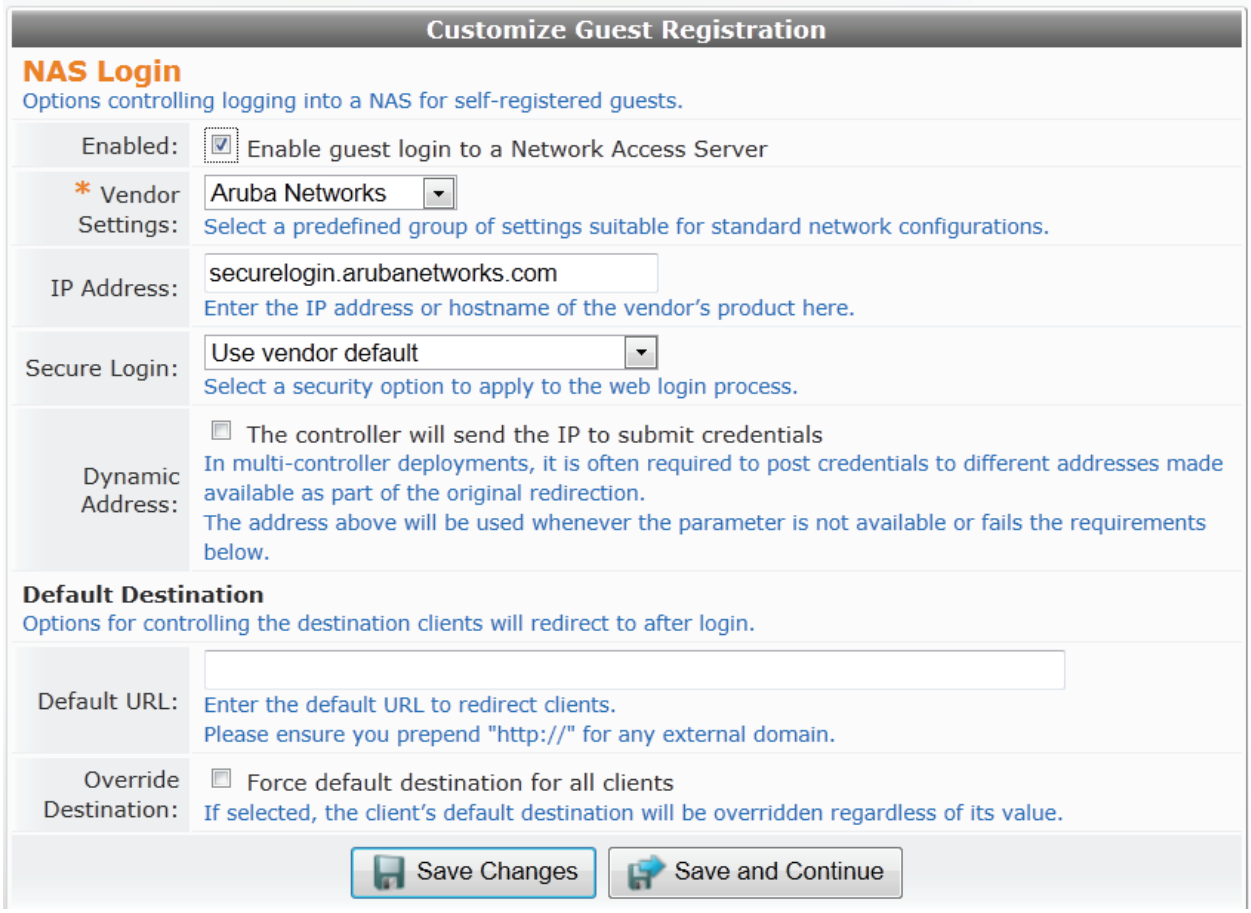
- **Disable sending guest receipts by SMS** – SMS receipts are never sent for a guest registration.
- **Always auto-send guest receipts by SMS** – An SMS receipt is always generated using the selected options, and will be sent to the visitor's phone number.
- **Auto-send guest receipts by SMS with a 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.

Enabling and Editing NAS Login Properties

To enable and edit the properties for automatic NAS login, click the **NAS** box or the **NAS Vendor Settings** link in the lower right corner of the **Customize Guest Registration**. The NAS Login form opens.



Mark the **Enabled** check box to expand the form.



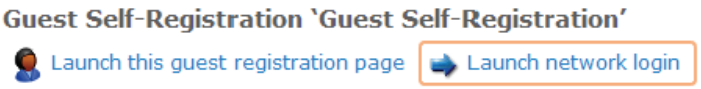
If automatic guest login is not enabled, the submit button on the receipt page will not be displayed, and automatic NAS login will not be performed.

Many of the properties on this page are the same as for a RADIUS Web Login page. For details about specifying NAS login settings, extra fields, or URL redirection parameters, See "Creating a Web Login Page" in the RADIUS Services chapter.

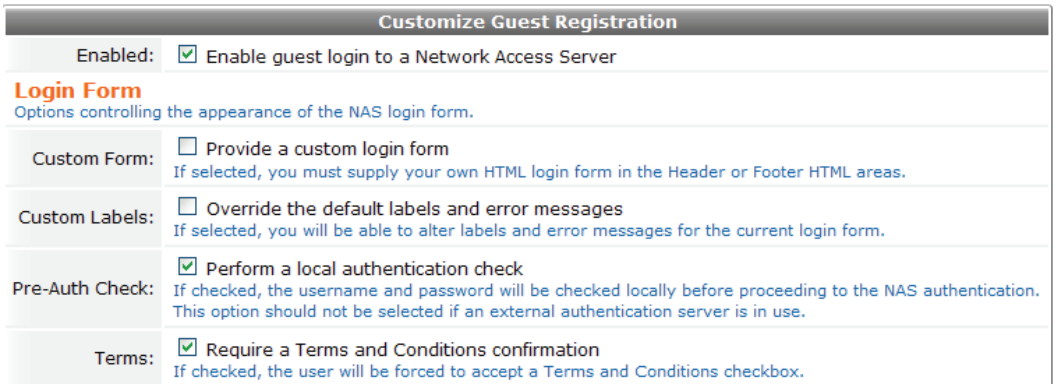
Editing Login Page Properties

Click the **Title** or **Login Message** fields for the login page to edit the properties of the login page. This page is displayed if automatic guest login is enabled and a guest clicks the submit button from the receipt page to log in.

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 use the **Launch network login** link from the self-registration process diagram, as shown below:

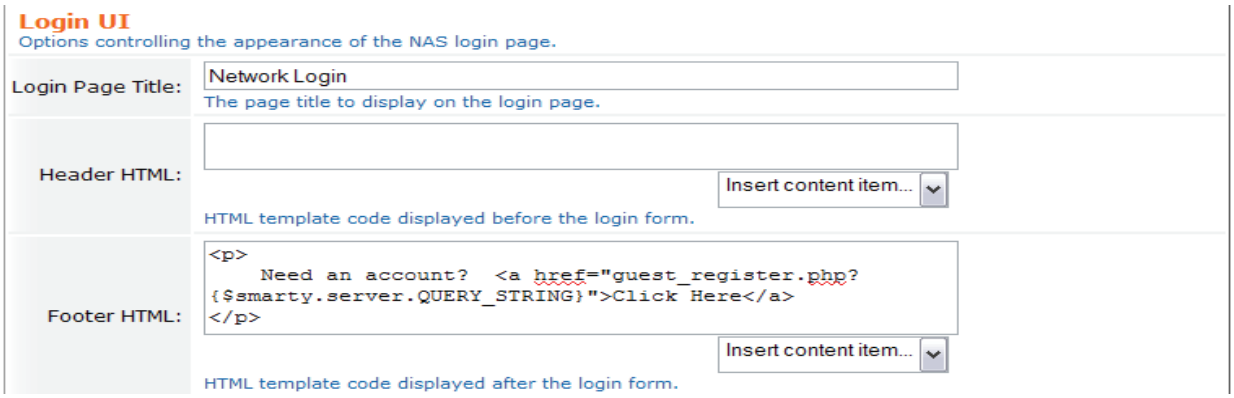


The options available under the **Login Form** heading may be used to customize the login page. These options are equivalent to the same RADIUS Web Login page. See "Creating a Web Login Page" in the RADIUS Services chapter for a description.

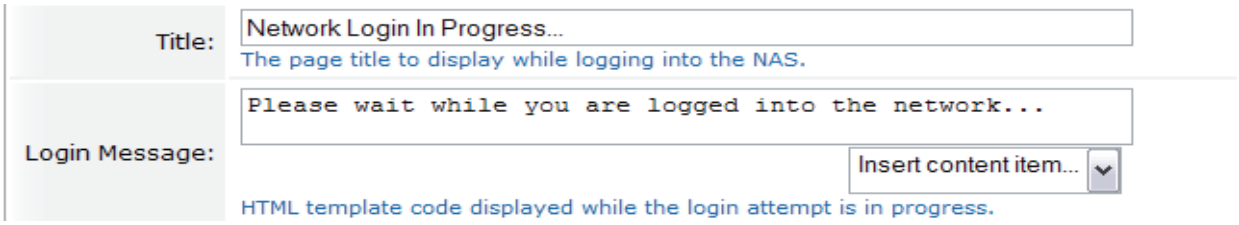


The login page consists of two separate parts: the login form page, and a login message page.

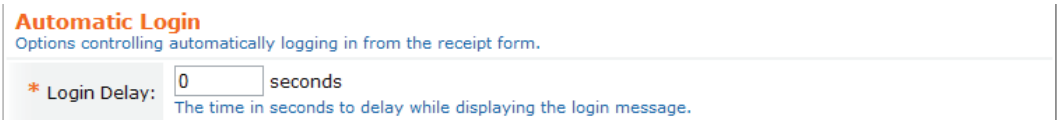
The login form page contains a form prompting for the guest's username and password. The title, header and footer of this page can be customized. If the **Provide a custom login form** option is selected, then the form must also be provided in either the Header HTML or Footer HTML sections.



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.



The login delay can be set; this is the time period, in seconds, for which the login message page is displayed.



Click the **Save Changes** button to return to the process diagram for self-registration.

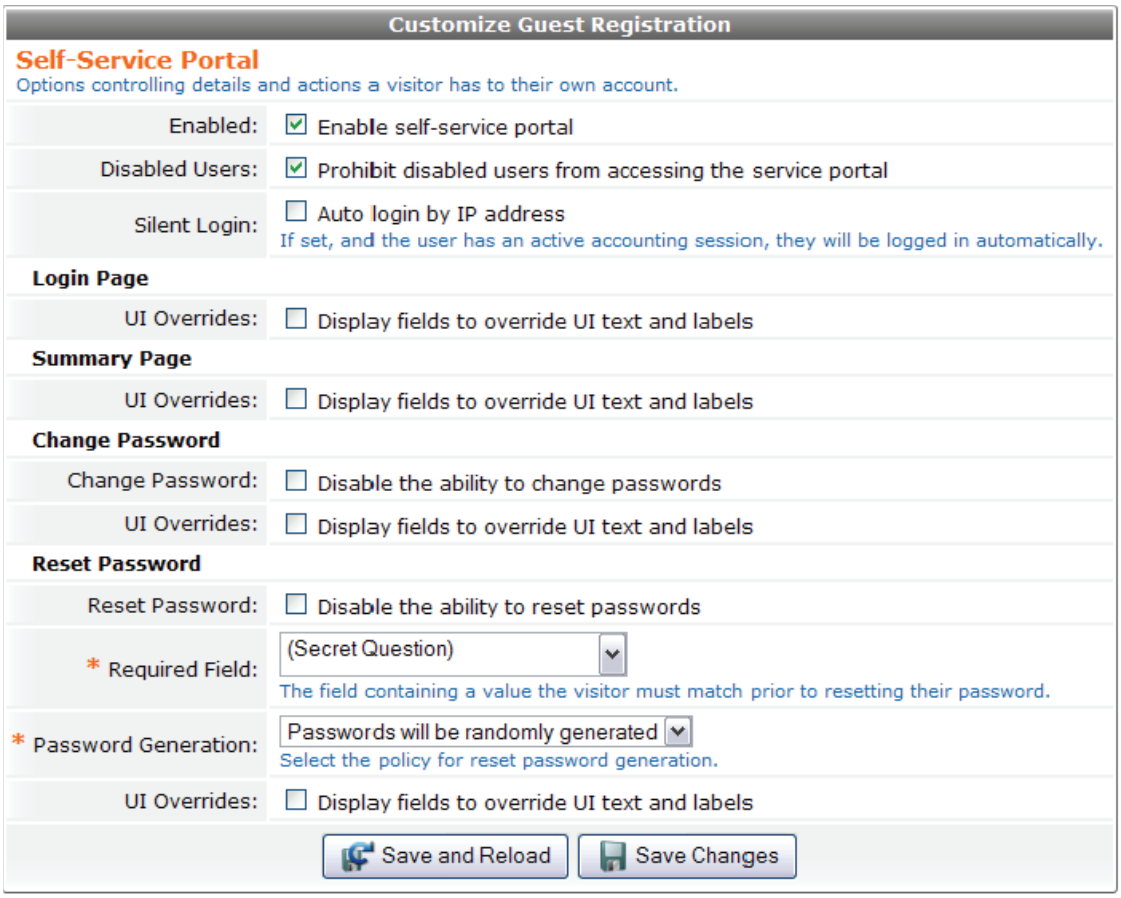
Self-Service Portal Properties

Click the **Self-Service Portal** link or one of the **Login Page**, **Summary Page**, **Change Password** or **Reset Password** links for the Self-Service Portal to edit the properties of 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".

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 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 allowing guests to recover a forgotten account password.



To adjust the user interface, use the override check boxes to display additional fields on the form. These fields allow you to customize all text and HTML displayed to users of the self-service portal.

The behavioral properties of the self-service portal are described below:

- The "Enable self-service portal" check box must be selected for guests to be able to access the portal. Access to the portal when it is disabled results in a disabled message being displayed; this message may be customized using the "Disabled Message" field.
- The "Disabled Users" check box controls whether a user account that has been disabled is allowed to log in to the portal.
- The "Change Password" check box controls whether guests are permitted to change their account password using the portal.
- The "Reset Password" check box controls whether guests are permitted to reset a forgotten account password using the portal. If this check box is enabled, the "Required Field" may be used to select a field value that the guest must match in order to confirm the password reset request.

If the "Auto login by IP address" option is selected, a guest accessing the self-service portal will be automatically logged in 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).

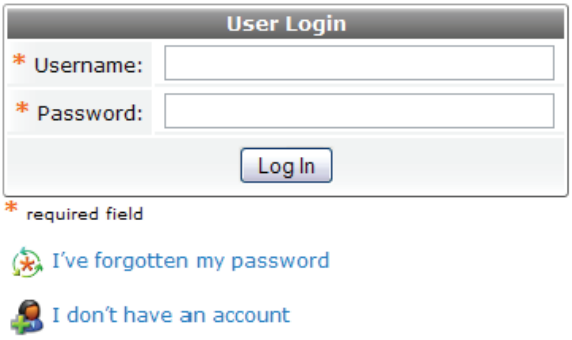
The Password Generation drop-down list controls what kind of password reset method is used in the portal. The default option is "Passwords will be randomly generated", but the alternative option "Manually enter passwords" may be selected to enable guests to select their own password through the portal.

Click the **Save Changes** button to return to the process diagram for self-registration.

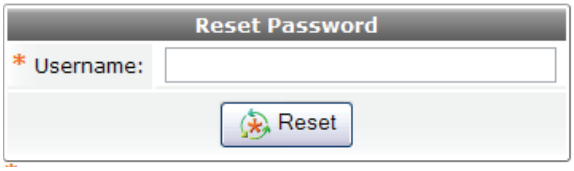
Resetting Passwords with the Self-Service Portal

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:



Clicking the **I've forgotten my password** link displays a form where the user password may be reset:



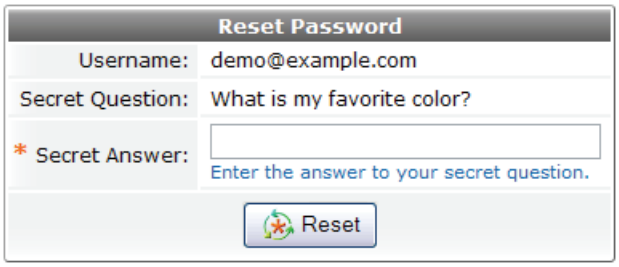
Entering a valid username will reset the password for that user account, and will then display the receipt page showing the new password and a login option (if NAS login has been enabled).

This feature allows the password to be reset for any guest account on the system, which may 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.

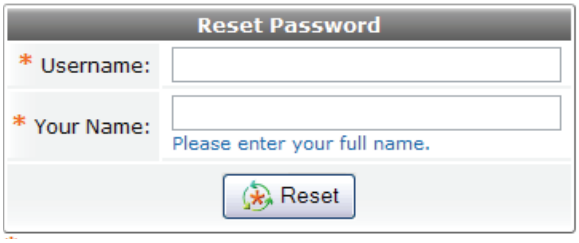
To enable a more secure password reset operation, first enable the **secret_question** and **secret_answer** fields to the registration form. The default appearance of these fields is shown below:

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:



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:



Customizing Print Templates

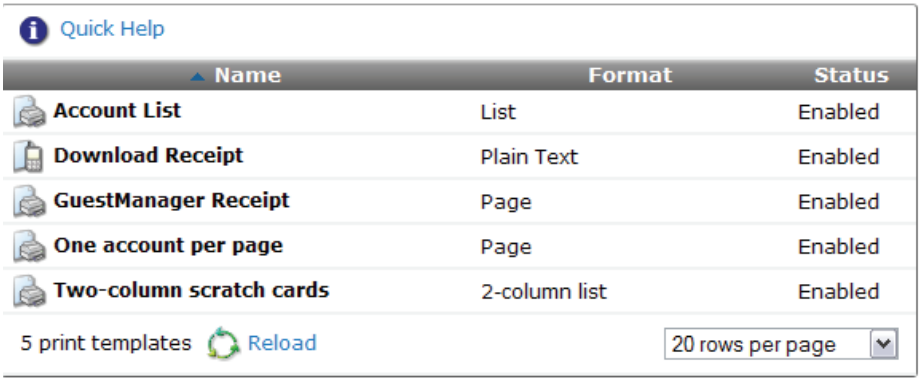
Print templates are used to define the format and appearance of a guest account receipt.

The Print Templates menu item is now located under the **Customization > Print Templates** navigation menu.

Click a print template's row in the table to select it. You can then choose to edit, duplicate, delete or preview the template.

The **Edit code** action is displayed for a print template when it has been created using the wizard, but subsequently modified. **See "Modifying Wizard-Generated Templates"** in this chapter for further information.

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" in this chapter.



Plain text print templates may be used with SMS services to send guest account receipts; See "About SMS Guest Account Receipts" in this chapter for details. Because SMS has a 160 character limit, the number of character 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

Print templates can be defined using the **Crea te new print template** link. This opens a window with four parts. The first part lists the variables that can be used in the template together with their meaning and an example of each.

Variable	Description	Example
{$u.username}	User account name	12345678
{$u.password}	User account password	87654321
{$u.enabled}	Non-zero if the user account is enabled	1
{$u.role_name}	Role assigned to user account	Guest
{$u.schedule_time}	Time at which the user account will become active	1155772123
{$u.expire_time}	Time at which the user account will expire	1155858523
{$u.expire_postlogin}	Lifetime of the user account login in minutes after login	120
{$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 user account	0
{$result.message}	Message related to the account creation	
{$timestamp}	Time at which the receipt was generated	1155752000
{$site_ssid}	SSID of the wireless LAN	amigopod
{$site_wpa_key}	WPA key for the wireless LAN	

This section is followed by three other sections: the body, the header and the footer. Each section must be written in HTML. There is provision in each section for the insertion of multiple content items such as logos.

You are able to 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" in the Reference chapter for further information on Smarty template syntax.

You are able to use an **{if}** statement to define a single print template that caters for 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 $action == "delete"}
{/if}
<table {$table_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}
```

If this code is placed in the User Account HTML section it will cater for the create, edit and delete options.

Print Template Wizard

The **Create new print template using wizard** link provides a simplified way to create print templates by selecting a basic style and providing a logo image, title and content text, and selecting the guest account fields to include.

A real-time preview allows changes made to the design to be viewed immediately.

To use the Print Template Wizard, first select a style of print template from the Style list. Small thumbnail images are shown to indicate the basic layout of each style. There are four built-in styles:

- **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** – 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.

Click the **Preview at right** or **Preview at bottom** link at the top of the page to move the real-time preview of the print template.

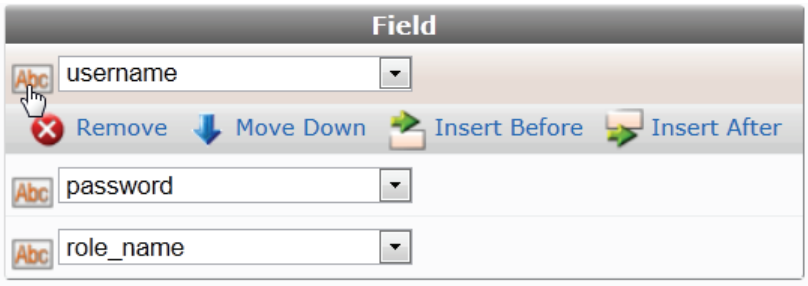
Each of the basic styles provides support for a logo image, title area, subtitle area, notes area, and footer text. These items can be customized by typing in an appropriate value in the Print Template Wizard.

NOTE

As the print template is a HTML template, it is possible to use HTML syntax as well as Smarty template code in these areas. **See "Reference"** chapter for reference material about HTML and Smarty template code.

The print template may also contain visitor account fields. The value of each field is displayed in the print template. By default, the wizard sets up the template with the **username**, **password** and **role_name** fields, but these may be customized.

Options in the **Fields** row let you add, remove, or change the order of fields. Use the drop-down list to choose the field name, then click the icon at the left of the drop-down list. The field's row expands to include the option links.



Use the **Remove**, **Move Up**, **Move Down**, **Insert Before**, and **Insert After** links to adjust the fields that are to be included on the print template.

Click the **Create Template** button to save your newly created print template and return to the list.

Modifying Wizard-Generated Templates

Once you have created a print template using the print template wizard, you can return to the wizard to modify it.

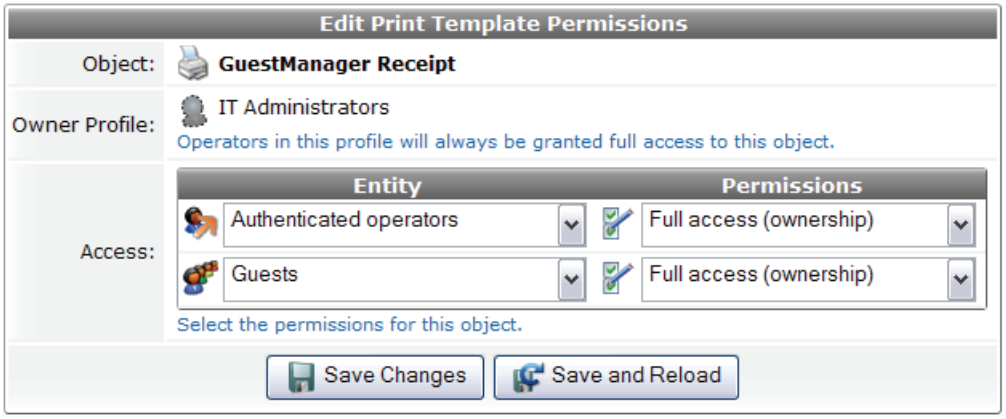
Click the **Edit print template code (Advanced)** link to use the standard print template editor. See "Creating New Print Templates" in this chapter for a description.

NOTE

If you use the wizard to edit a print template after changes have been made to it outside the wizard, those 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

The **Permissions** link can be used to control access to an individual print template, at the level of an operator profile. The Permissions link is only displayed if the current operator has the Object Permissions privilege. This privilege is located in the Administrator group of privileges.



The permissions defined on this screen apply to the print template identified in the "Object" line.

The owner profile always has full access to the print template.

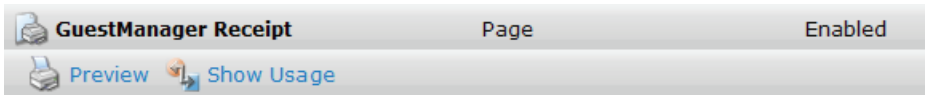
To control access to this print template by other entities, add or modify the entries in the "Access" list. To add an entry to the list, or remove an entry from the list, click one of the icons in the row. A **Delete** icon and an **Add** icon will then be displayed for that row.

Select one of the following entities in the Entity drop-down list:

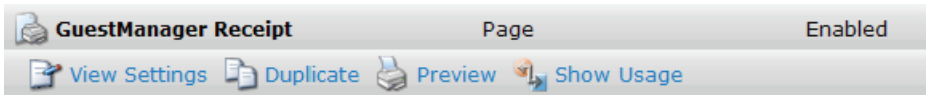
- **Operator Profiles** – a specific operator profile may be selected. The corresponding permissions will apply to all operators with that operator profile.
- Other Entities
  - **Authenticated operators** – the permissions for all operators (other than the owner profile) may be set using this item. Permissions for an individual operator profile will take precedence over this item.
  - **Guests** – the permissions for guests may be set using this item.

The permissions for the selected entity can be set using the Permissions drop-down list:

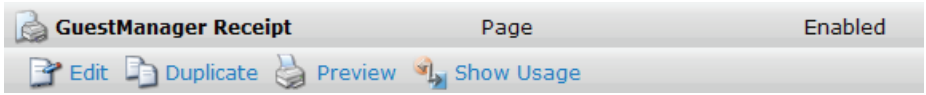
- **No access** – the print template is not visible in the list, and cannot be used, edited, duplicated, or deleted.
- **Visible-only access** – the print template is visible in the list, but cannot be edited, duplicated, or deleted.



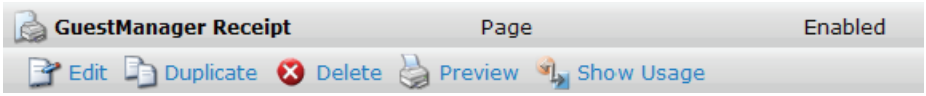
- **Read-only access** – the print template is visible in the list, and the settings for it may be viewed. The print template cannot be edited or deleted.



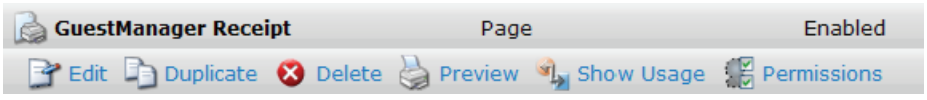
- **Update access** – the print template is visible in the list, and may be edited. The print template cannot be deleted and the permissions for the print template cannot be modified.



- **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.



- **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.



Configuring Access Code Logins

This section explains how to configure the Guest Manager to create multiple accounts that have the ability to log in in with only the username. We will refer to this as an **Access Code**. Access Code logins requires the following plugin versions: RADIUS Services 3.0.4 or later, and GuestManager Plugin 3.0.3. To verify you have the correct plugin versions installed, navigate **to Administrator > Plugin Manager > Manage Plugins** and check the version number in the list.

Customize Random Username and Passwords

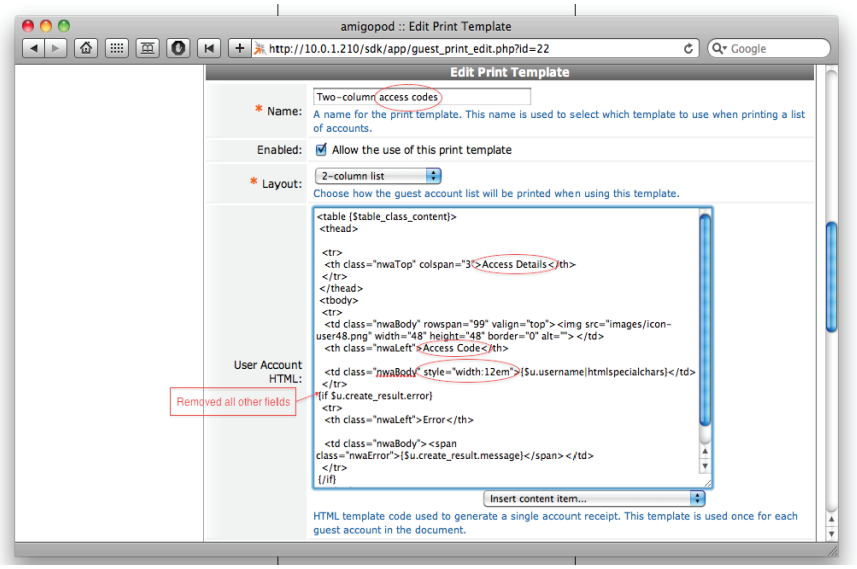
In this example we will set the random usernames and passwords to be a mix of letters and digits.

1. Navigate to **Customization > Guest Manager**. The **Customize Guest Manager** field appears.
2. In the **Username Type** field, select **Random Letters and digits**. Note that the generator matching the complexity will also include a mix of upper and lower case letters.
3. In the Username **Length field**, select **8** characters.
4. Configure other settings. See "Default Settings for Account Creation" in this chapter for a description, then click **Save Configuration** to save your changes.

Create the Print Template

By default, the print templates include username, password, 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 templates.

1. Navigate to **Customization > Print Templates.**
2. Select **Two-column scratch cards** and click **Duplicate**.
3. Select the **Copy of Two-column scratch cards** template, then click **Edit**.
4. In the **Name** field, substitute **Access Code** for **Username** as shown below.

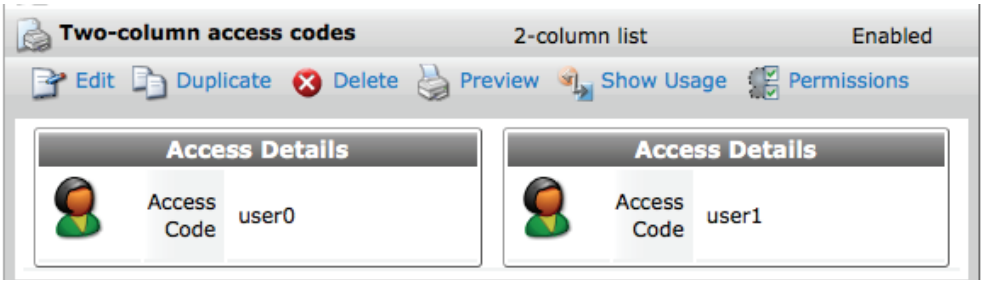


5. Remove extraneous data from the **User Account HTML** field. Example text is shown below.

```
<table {$table_class_content}>
 <thead>
<tr>
   <th class="nwaTop" colspan="3">Access Details</th>
  </tr>
 </thead>
 <tbody>
  <tr>
   <td class="nwaBody" rowspan="99" valign="top"><img src="images/icon-user48.png"
width="48" height="48" border="0" alt=""></td>
   <th class="nwaLeft">Access Code</th>
<td class="nwaBody" style="width:12em">{$u.username|htmlspecialchars}</td>
  </tr>
 {if $u.create_result.error}
  <tr>
```

```
   <th class="nwaLeft">Error</th>
<td class="nwaBody"><span class="nwaError">{$u.create_result.message}</span></td>
  </tr>
 {/if}
 </tbody>
</table>
```

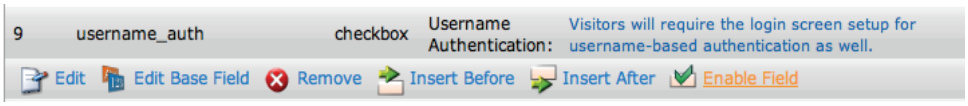
6. Click **Save Changes** to save your settings.
7. To preview the new template, select the template in the Guest Manager Print Templates list, then click Preview. The template created in this example appears as shown below.



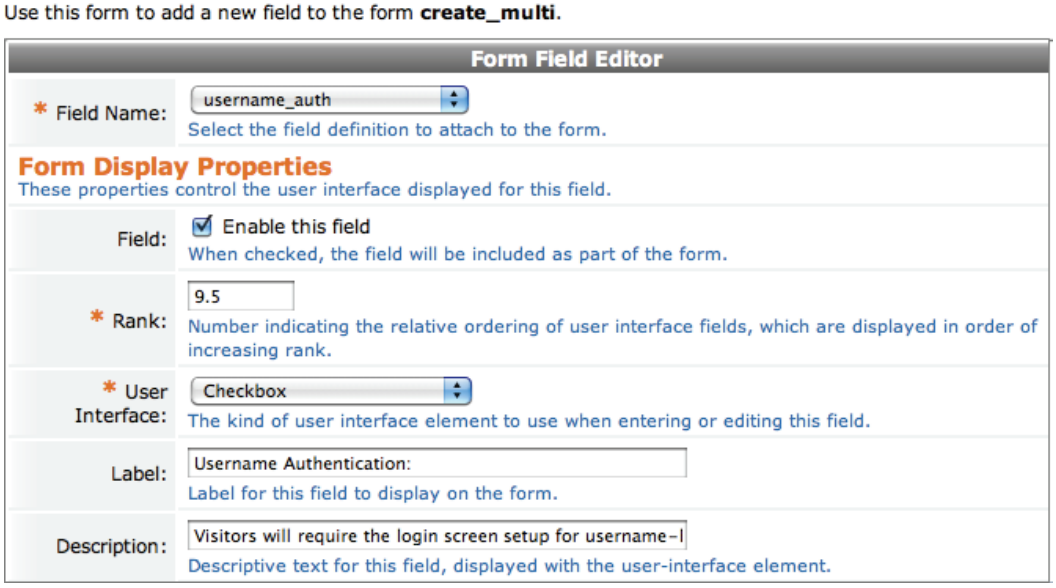
Customize the Guest Accounts Form

Next, modify the **Guest Accounts** form to add a flag that to allows access-code based authentication.

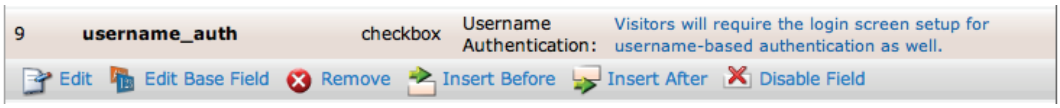
1. Navigate to **Customization > Forms & Views.**
2. In the **Customize Forms & Views** list, select **create_multi** and then click **Edit Fields**.
3. In the **Edit Fields** list, look for a field named username_auth. If the field exists, but is not bolded and enabled, select it and click **Enable Field**.



If the field does *not* exist, select any field in the list (for example, **num_accounts**) and 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. Once the field is enabled or inserted, you should see it bolded in the list of fields.



Create Access Code Guest Accounts

Once the account fields have been customized, you can create new accounts.

1. Navigate to **Guests > Create Multiple.**
2. Select the **Username Authentication** field added in the procedure above. (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 fours hours after the visitors first log in, whichever comes first.

3. Click **Create Accounts** to display the **Finished Creating Guest Accounts** page. If you create large number of accounts are created at one time they may not all be displayed at the same time. (This will not affect the printing action in the following step.)

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"** for a description of this procedure. A new window or tab will open with the cards.

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 **Administrator > Plugin Manager > List Available Plugins**. For information on plugin management, see "Plugin Manager" in the Administrator Tasks chapter.

MAC Address Formats

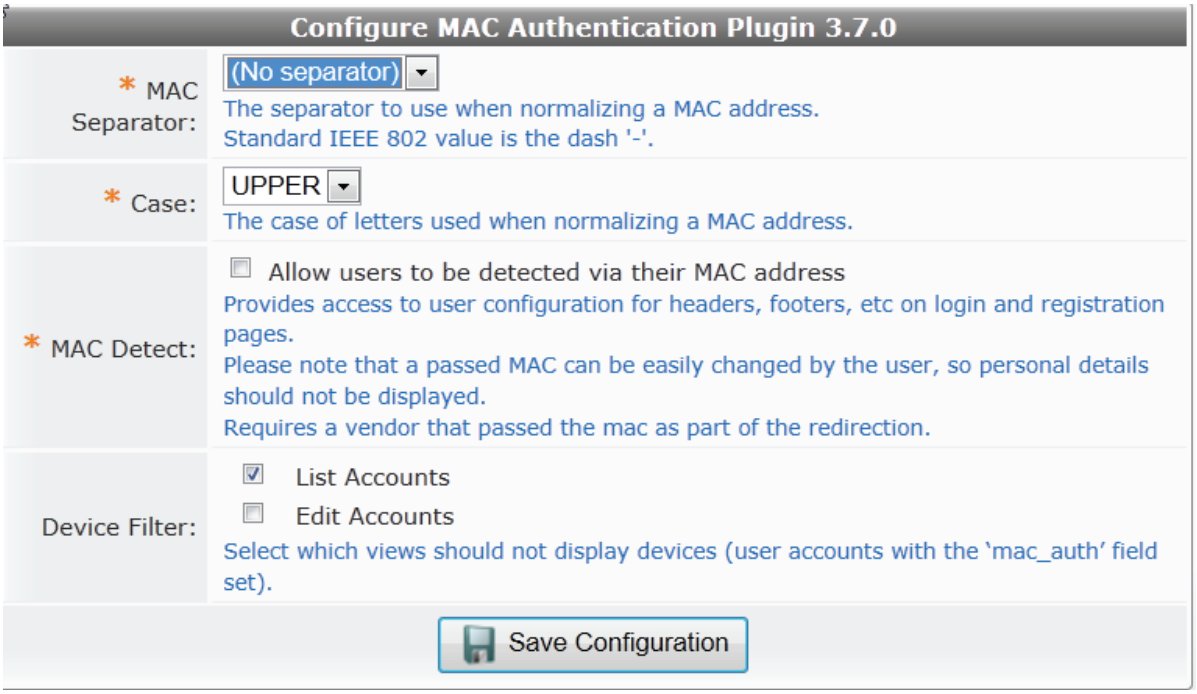
Different vendors format the client MAC address in different ways—for example:

- 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

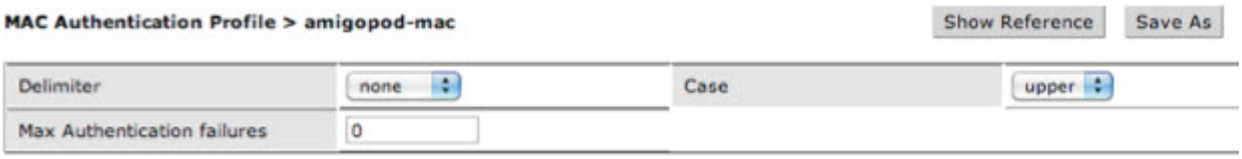
Administrator > Plugin Manager > Manage Plugins and click the **Configuration** link for the **MAC Authentication Plugin**. The MAC Authentication Plugin page opens.

Figure 32 *MAC Authentication Plugin—Configuration*



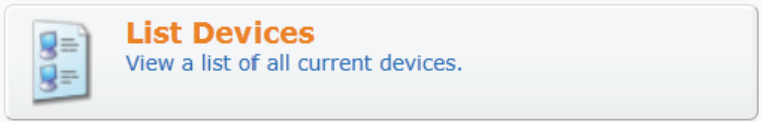
On the controller, the fields look as follows:

Figure 33 *MAC Authentication Profile*

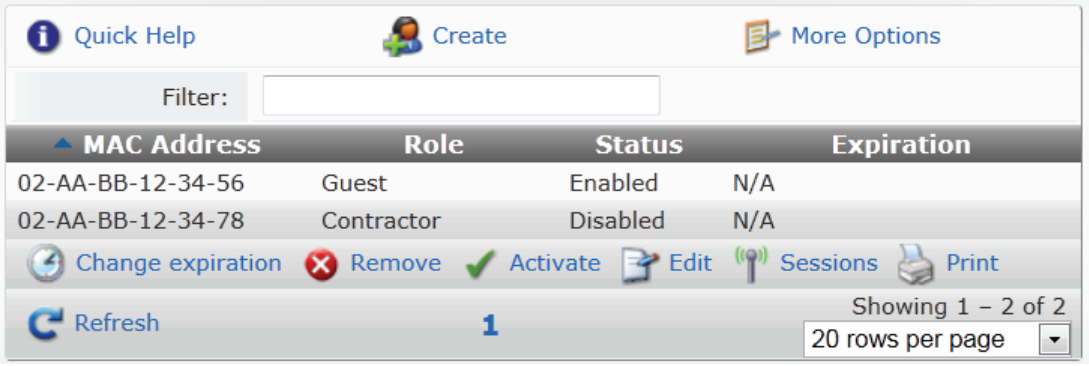


Managing Devices

To view the list of current MAC devices, go to **Guests > List Devices**.



The Guest Manager Devices page opens.



All devices created by one of methods described in the following section are listed. Options on the form let you change a device's account expiration date; remove, activate, or edit the device; view active sessions or details for the device; or print details, receipts, confirmations, or other information.

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 28 *Operators supported in filters*

Operator	Meaning	Additional Information
=	is equal to	You may search for multiple values when using the equality (=) or inequality !=) operators. To specify multiple values, list them separated by the pipe character (|). 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".
!=	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	

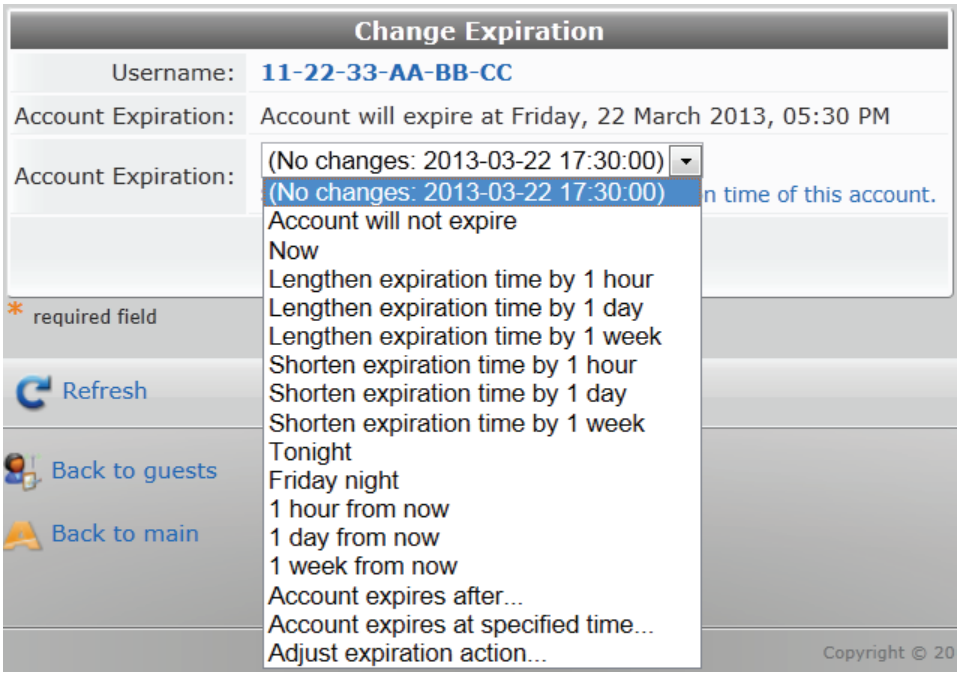
To restore the default view, click the **Clear Filter** link.

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.

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

Changing a Device's Expiration Date

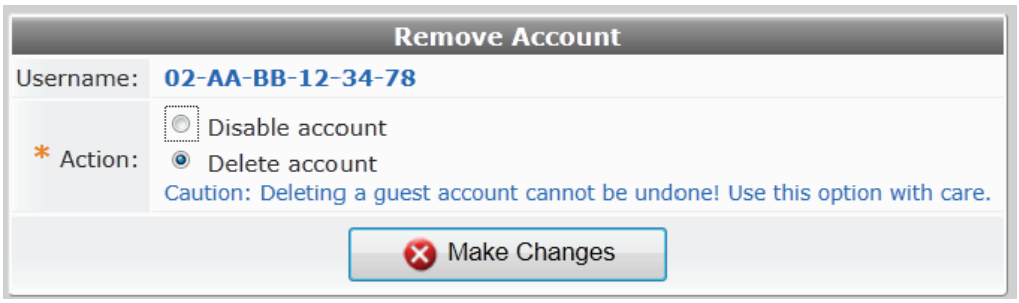
To change a device's expiration date, click the device's row in the Guest Manager Devices list, then click its **Change expiration** link. The row expands to include the Change Expiration form.



1. In the **Account Expiration** row, choose one of the options in the drop-down list to set an expiration date:
   - If you choose **Account expires after**, the **Expires After** row is added to the form. Choose an interval of hours, days, or weeks from the drop-down list.
   - If you choose **Account Expires at a specified time**, the **Expiration Time** 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.
2. If you choose any option other than "will not expire" or "now" in the Account Expiration field, the **Expire Action** row is added to the table. Use the drop-down list in this row to specify one of the following actions: delete, delete and log out, disable, or disable and log out.
3. Click **Update Account** to commit your changes.

Disabling and Deleting Devices

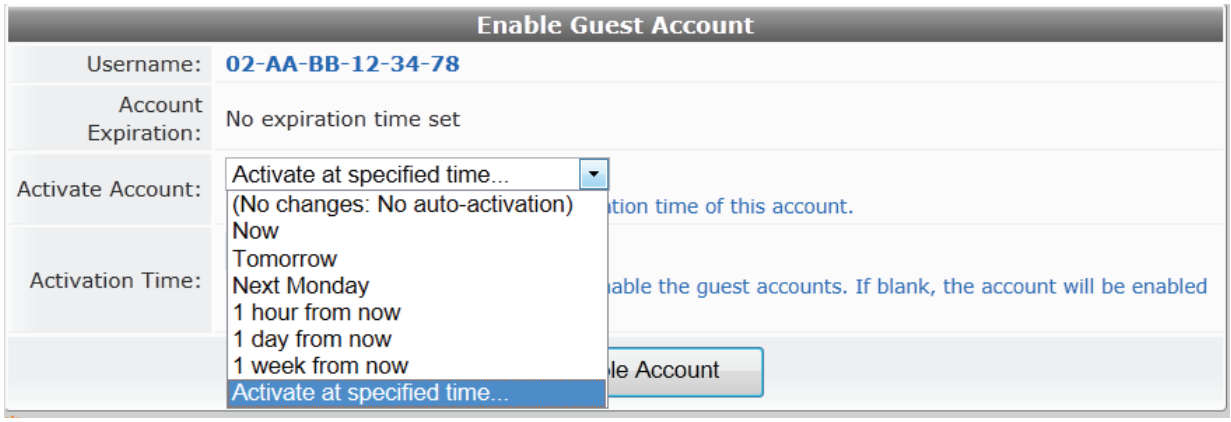
To remove a device's account by disabling or deleting it, click the device's row in the Guest Manager Devices list, then click its **Remove** link. The row expands to include the Remove Account form.



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

Activating a Device

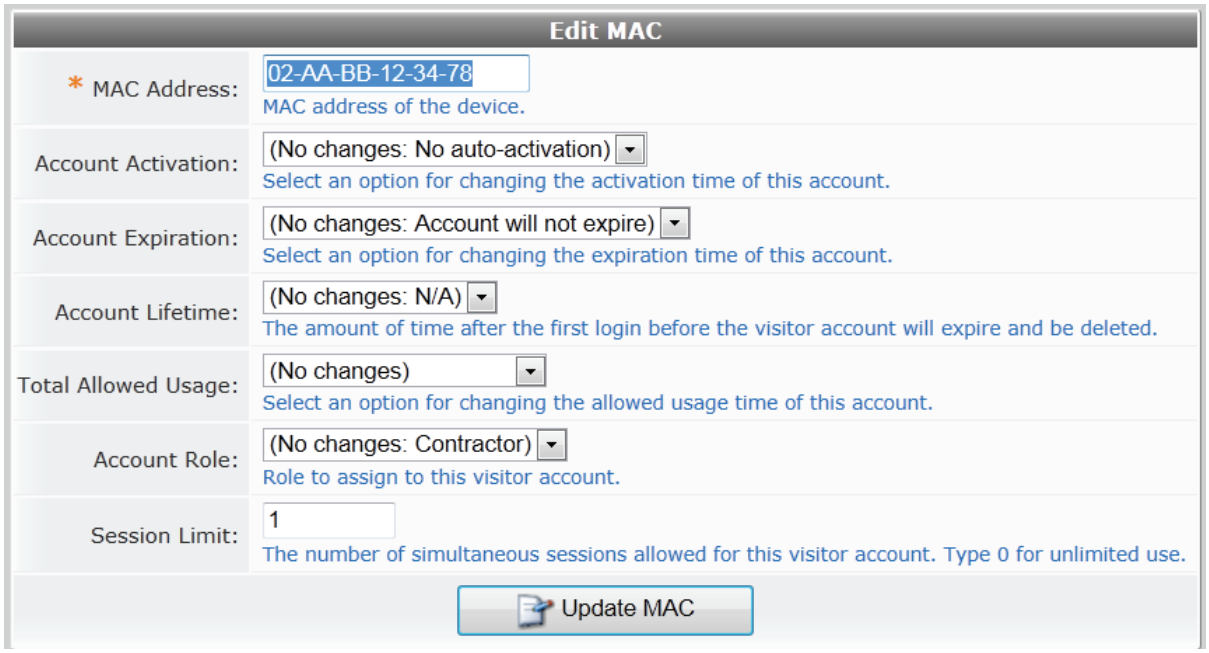
To activate a disabled device's account, click the device's row in the Guest Manager Devices list, then click its **Activate** link. The row expands to include the Enable Guest Account form.



1. In the **Activate Account** row, choose one of the options in the drop-down list to specify when to activate the account. You may choose an interval, or you may choose to specify a time.
2. If you choose **Activate at specified time**, the **Activation Time** 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.
3. Click **Enable Account** to commit your changes.

Editing a Device

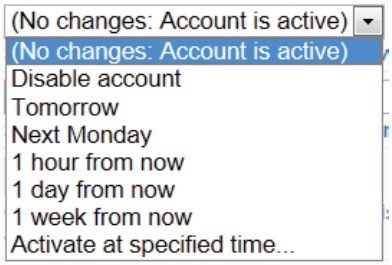
To edit a device's account, click the device's row in the Guest Manager Devices list, then click its **Edit** link. The row expands to include the Edit MAC form.



1. You can change the device's address in the **MAC Address** row.

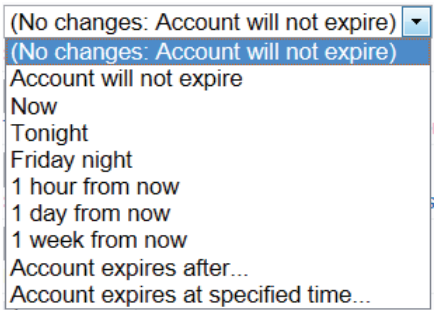
   If you need to modify the configuration for expected separator format or case, go to **Administrator > Plugin Manager > Manage Plugins** and click the **Configuration** link for the **MAC Authentication Plugin**.

2. If you need to change the activation time, choose one of the options in the **Account Activation** drop-down list. You may choose to activate the account immediately, at a preset interval of hours or days, or at a specified time.



   - If you choose **Activate at a specified time**, the **Activation Time** 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.

3. If you need to change the expiration time, choose one of the options in the **Account Expiration** drop-down list. You may terminate the account immediately, at a preset interval of hours or days, or at a specified time.



   - If you choose any time in the future, the **Expire Action** row is added to the form. Use this drop-down list to 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 **Expires After** row is added to the form. Choose an interval of hours, days, or weeks from the drop-down list. The maximum is two weeks.
   - If you choose **Account Expires at a specified time**, the **Expiration Time** 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.

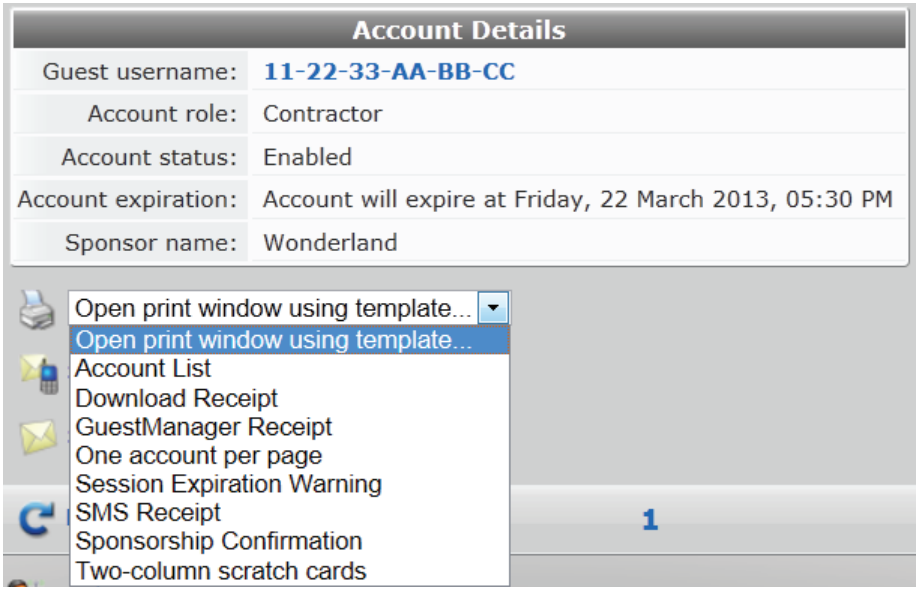
4. To change a visitor account's duration after first login, you may choose a preset interval of hours or days from the **Account Lifetime** drop-down list. The visitor's account expires and is deleted when this interval has passed after they first log in. The maximum is one week.
5. To change the maximum usage allowed for the account, choose an option from the **Total Allowed Usage** drop-down list. You may set the total usage to one or two hours, add one or two hours to the existing setting, or subtract one or two hours from the existing setting.
6. You can use the **Account Role** drop-down list to change the visitor's assigned role.
7. In the **Session Limit** row, you may enter the number of simultaneous sessions to allow for this account. To allow an unlimited number of simultaneous sessions, enter 0.
8. To commit your changes, click **Update MAC**.

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".

Viewing and 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 form and a drop-down list of information that can be printed for the device.



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.

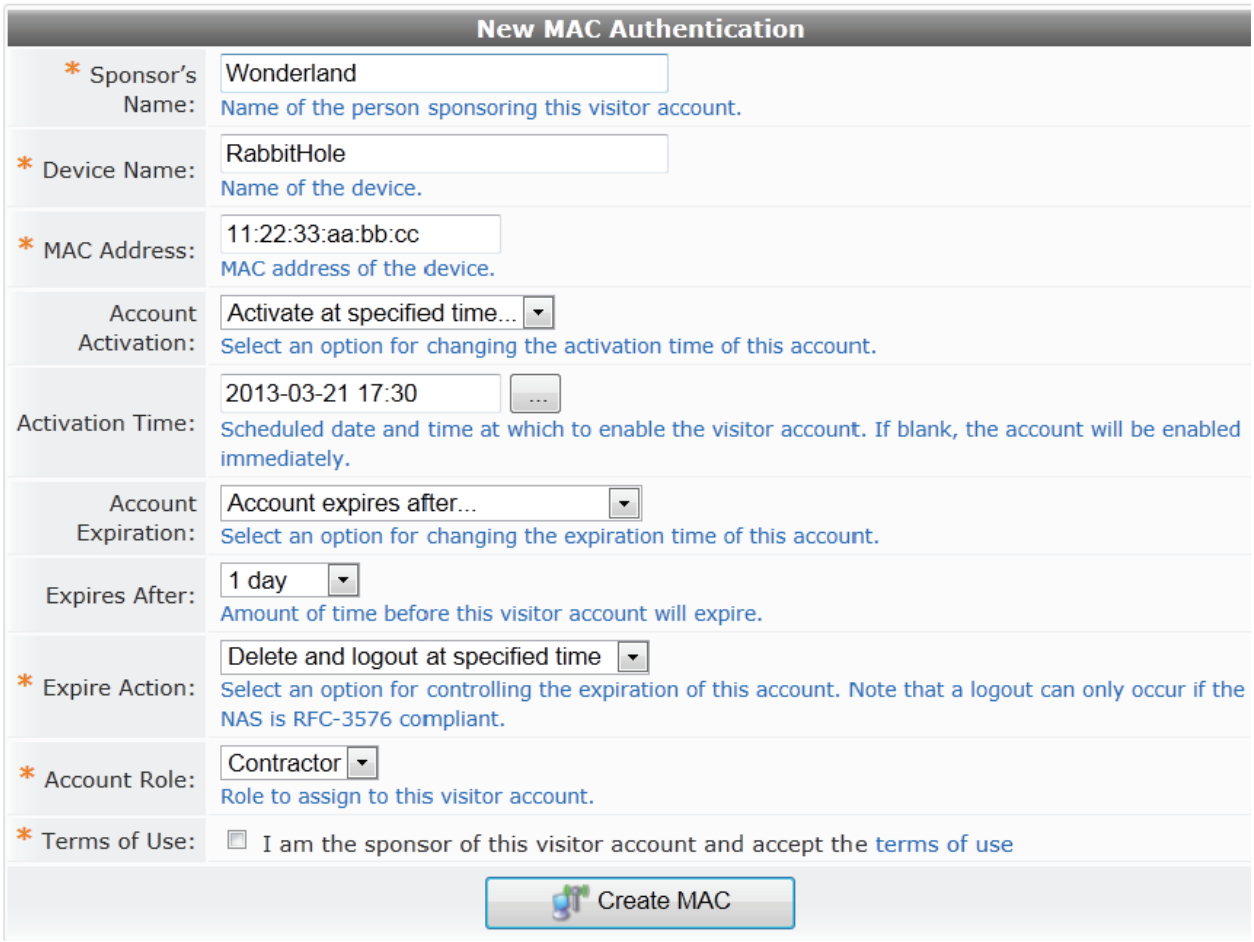
MAC Creation Modes

MAC device accounts may be created in three ways:

- Manually in ClearPass Guest using the Create 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 visitor account

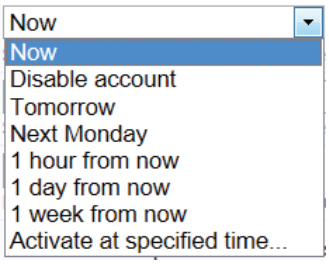
Creating Devices Manually in ClearPass Guest

If you have the MAC address, you can create a new device manually. Go to **Guests > List Devices** and click the **Create** link, or you can go to the Guests navigation page and click the **Create Device** command. The New MAC Authentication page opens.



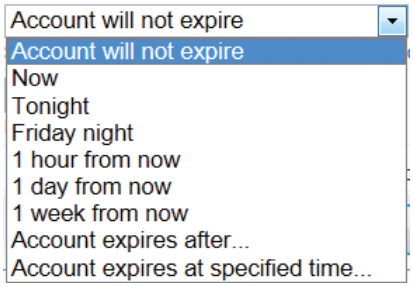
1. In the **Sponsor's Name** row, enter the name of the person sponsoring the visitor account.
2. Enter the name for the device in the **Device Name** row.
3. Enter the address in the **MAC Address** row.

   If you need to modify the configuration for expected separator format or case, go to **Administrator > Plugin Manager > Manage Plugins** and click the **Configuration** link for the **MAC Authentication Plugin**.
4. Choose one of the options in the **Account Activation** drop-down list. You may choose to activate the account immediately, at a preset interval of hours or days, at a specified time, or leave the account disabled.



   - If you choose **Activate at a specified time**, the **Activation Time** 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.

5. To set the account's expiration time, choose one of the options in the **Account Expiration** drop-down list. You may set the account to never expire, or to expire at a preset interval of hours or days, or at a specified time.



   - If you choose any time in the future, the **Expire Action** row is added to the form. Use this drop-down list to 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 **Expires After** row is added to the form. Choose an interval of hours, days, or weeks from the drop-down list. The maximum is two weeks.
   - If you choose **Account Expires at a specified time**, the **Expiration Time** 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.
6. Use the **Account Role** drop-down list to assign the visitor's role.
7. In the **Terms of Use** row, first click the **terms of use** link and read the agreement, then mark the check box to agree to the terms.
8. To commit your changes and create the device, click **Create MAC**. The Account Details and print options are displayed. For more information, see "Viewing and Printing Device Details".

Creating Devices During Guest Self-Registration - MAC Only

This section describes how to configure a guest self-registration so that it creates a MAC device account. Once 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 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, go to **Customization > Forms and Views**. In the **guest_register** row, click the **Edit Fields** link. The Customize Form Fields page opens. If you do not see mac or mac_auth in the list, click the **Customize fields** link above the list. Click the **Edit** link in the field's row. In the Define Custom Field form, edit the 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 34 *Modify fields*

Rank	Field	Type	Label	Description
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
45	**mac**	hidden	MAC Address:	MAC address of the client.
47	**mac_auth**	hidden		
50	schedule_time	datetime	Activation Time:	Optional date and time at which to enable the visitor account. If blank, the visitor account will be enabled immediately.
60	**expire_after**	hidden	Account Expiry:	Amount of time before this visitor account will expire.
65	expire_time	datetime	Expiration Time:	Optional date and time at which this account will expire. If blank, the expiration time will not be set.
70	**role_id**	hidden	Account Role:	Role to assign to this visitor account.
75	enabled	checkbox	Account State:	Select an option for changing the status of this visitor account.
90	**creator_accept_terms**	checkbox	Confirm:	
99	**auto_update_account**	hidden		
100	**submit**	submit	Register	

Edit the receipt form fields:

- Edit **username** to be a **Hidden field**
- Edit **password** to be a **Hidden field**

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 redirectd to the captive portal page.

Creating Devices During Guest 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, go to **Customization > Forms and Views**. In the **guest_register** row, click the **Edit Fields** link. The Customize Form Fields page opens. If you do not see mac or mac_auth_pair in the list, click the **Customize fields** link above the list. Click the **Edit** link in the field's row. In the Define Custom Field form, edit the 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. Note 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.

Accounting-Based MAC Authentication

Accounting-based MAC authentication is a way to cache the MAC used during an initial authentication so that the device does not need to authenticate again. The visitor authenticates with their regular credentials, using a regular Web login or some form of transparent login, and the application server registers the MAC for future use. The device may be configured to do this automatically, or you may enter the following PHP code.

Edit the role of your guests and add the following:

- Attribute: **Tmp-String-0**
- Value: *blank*
- Condition: **Enter condition expression...**

Expression:

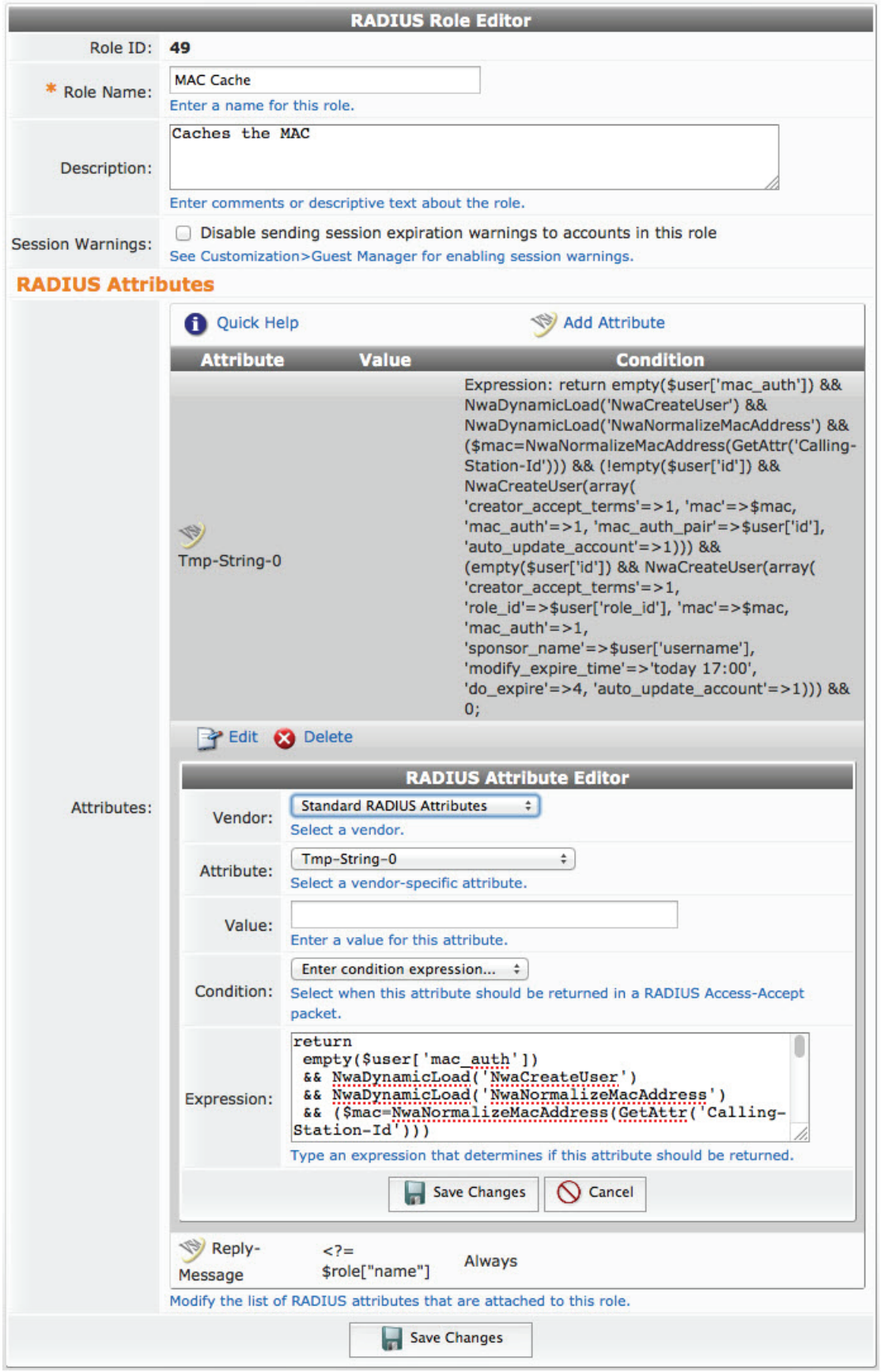
```
return
 empty($user['mac_auth'])
 && NwaDynamicLoad('NwaCreateUser')
 && NwaDynamicLoad('NwaNormalizeMacAddress')
 && ($mac=NwaNormalizeMacAddress(GetAttr('Calling-Station-Id')))
 && ((!empty($user['id']) && NwaCreateUser(array(
     'creator_accept_terms'=>1,
     'mac'=>$mac,
     'mac_auth'=>1,
     'mac_auth_pair'=>$user['id'],
     'create_time' => time(),
     'auto_update_account'=>1)))
    || (empty($user['id']) && NwaCreateUser(array(
     'creator_accept_terms'=>1,
     'role_id'=>$user['role_id'],
     'mac'=>$mac,
     'mac_auth'=>1,
     'sponsor_name'=>$user['username'],
     'modify_expire_time'=>'today 17:00',
     'do_expire'=>4,
     'create_time' => time(),
     'auto_update_account'=>1)))
    )
 && 0;
```

Annotated Expression: the following code is an annotated explanation of how the above code works.

```
return
 empty($user['mac_auth']) // Not already a MAC device...
 && NwaDynamicLoad('NwaCreateUser') // Required call
```

```
 && NwaDynamicLoad('NwaNormalizeMacAddress') // Required call
 && ($mac=NwaNormalizeMacAddress(GetAttr('Calling-Station-Id'))) // All MACs need to
be normalized
 && ((!empty($user['id']) && NwaCreateUser(array(// We are caching the MAC for a
local user account
     'creator_accept_terms'=>1,
     'mac_auth'=>1, // Flag as a MAC so it shows in List Devices
     'mac'=>$mac, // The normalized MAC
     'mac_auth_pair'=>$user['id'], // Formally pair the two accounts.  Cross links
and whatnot in the GUI.  A number of data items synched
     //'modify_expire_time'=>'Friday 17:00', // OPTIONAL.  Fixed caching time.
Default inherits paired account.
     'create_time' => time(), // initialize the creation time
     'auto_update_account'=>1)))
    || (empty($user['id']) && NwaCreateUser(array( // This is an external server
     'creator_accept_terms'=>1,
     'role_id'=>$user['role_id'], // Match the role to the current.
     'mac_auth'=>1, // Flag as a MAC Device
     'mac'=>$mac,
     'sponsor_name'=>$user['username'],// Set sponsor_name so we know who created it
and our sponsor filtering can kick in.
     'modify_expire_time'=>'Friday 18:00', // Fixed caching time.  Choose an
appropriate expression.
     //'do_expire'=>4, // This will default to the global and is not needed unless
overriding.
     'create_time' => time(), // initialize the creation time
     'auto_update_account'=>1)))
    )
 && 0;
```

Figure 35 *RADIUS Role Editor*



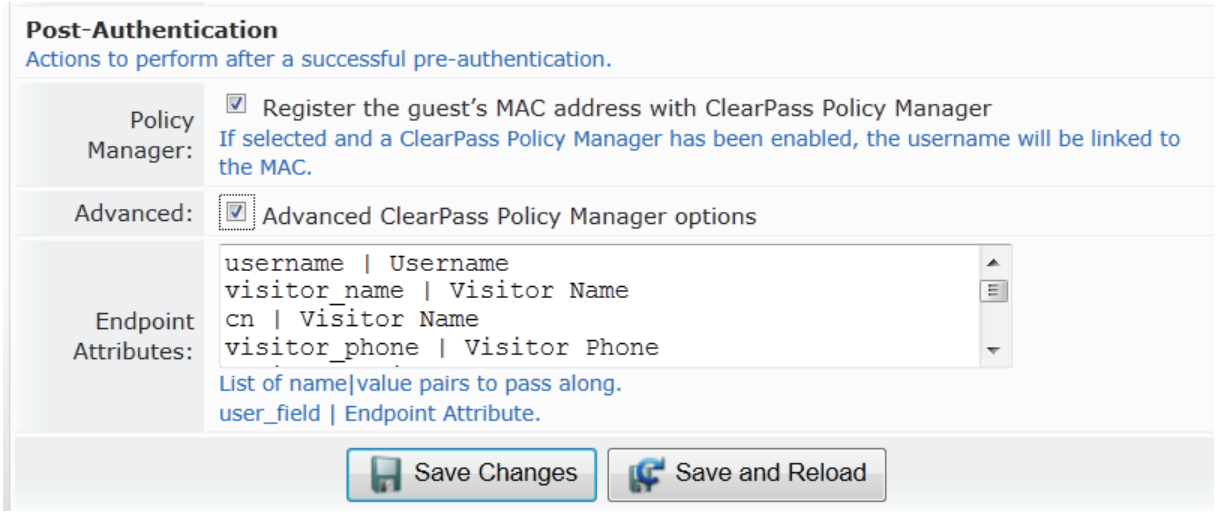
Note that **modify_expire_time** supports any valid syntax of strtotime.

Automatically Registering MAC Devices in ClearPass Policy Manager

If ClearPass Policy Manager is enabled, 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. Do one of the following:
   - To configure auto-registration through a Web login page, go to **Customization > Web Logins**, click the row of the page you wish to configure, then click its **Edit** link. The RADIUS Web Login Editor form opens.
   - To configure auto-registration for an address through the guest self-registration workflow, go to **Customization > Guest Self-Registration**, click the row of the page to be used, then click its **Edit** link. The Customize Guest Registration diagram opens. Click the **Advanced Editor** link at the lower left corner of the diagram. The Customize Guest Registration form opens with several property areas displayed.
2. Scroll down to the **Post-Authentication** area. On the Web Login Editor, this is at the bottom of the page. On the Customize Guest Registration form, it is within the **Login Form** area of the page.



3. In the **Policy Manager** row, mark the check box to register the guest's MAC address with ClearPass Policy Manager. The Advanced row is added to the form.
4. In the **Advanced** row, mark the check box to enable advanced options in ClearPass Policy Manager. The Endpoint Attributes row is added to the form.
5. In the **Endpoint Attributes** row, enter name|value pairs for the user fields and Endpoint Attributes to be passed.
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 **Guests > Import Guests** 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

2-Factor Authentication

2-factor authentication checks against both credentials and the MAC address on record.

Tying the MAC to the visitor account will depend on the requirements of your deployment. In practice you would probably add **mac** as a text field to the **create_user** form. When **mac** is enabled in a self-registration it will be included in the account as long as **mac** is passed in the URL. Relying on self-registration may defeat the purpose of two-factor authentication, however.

The 2-factors are performed as follows:

1. Regular RADIUS authentication using username and password
2. Role checks the user account mac against the passed Calling-Station-Id.

Edit the user role and the attribute for **Reply-Message** or **Aruba-User-Role**. Adjust the condition from **Always** to **Enter conditional expression**.

```
return !MacEqual(GetAttr('Calling-Station-Id'), $user['mac']) && AccessReject();
```

There is an alternative syntax where you keep the condition at **Always** and instead adjust the **Value**.

```
<?= MacEqual(GetAttr('Calling-Station-Id'), $user['mac']) ? $role["name"] :
AccessReject()
```

or

```
<?= MacEqual(GetAttr('Calling-Station-Id'), $user['mac']) ? 'Employee' : AccessReject()
```

MAC-Based Derivation of Role

Depending on whether the MAC address matches a registered value, you can also adjust which role is returned. The controller must be configured with the appropriate roles and the reply attributes mapping to them as expected.

Edit the **Value** of the attribute within the role returning the role to the controller.

If you are on the registered MAC, apply the **Employee** role, otherwise set them as **Guest**.

```
<?= MacEqual(GetAttr('Calling-Station-Id'), $user['mac']) ? 'Employee' : 'Guest'
```

This can be expanded if you create multiple MAC fields. Navigate to **Customize > Fields** and duplicate **mac**. Rename it as mac_byod and then add it to the 'create_user and guest_edit forms. In this example the account has a registered employee device under mac, and a registered BYOD device under mac_byod.

```
<?= MacEqual(GetAttr('Calling-Station-Id'), $user['mac_byod']) ? 'BYOD' :
(MacEqual(GetAttr('Calling-Station-Id'), $user['mac']) ? 'Employee' : 'Guest')
```

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.

Navigate to **Administrator > Plugin Manager > Manage Plugins: MAC Authentication: Configuration** and enable **MAC Detect**.

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>
```

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.

Disable MAC authentication on the controller.

Navigate to **Administrator > Plugin Manager > Manage Plugins: MAC Authentication: Configuration** and enable **MAC Detect**.

Create a **Web Login**

- Authentication: **Anonymous**
- Anonymous User: **_mac** *(_mac is a special secret value)*
- Pre-Auth Check: **Local**
- Terms: **Require a Terms and Conditions confirmation**

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.

You may 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>
```

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

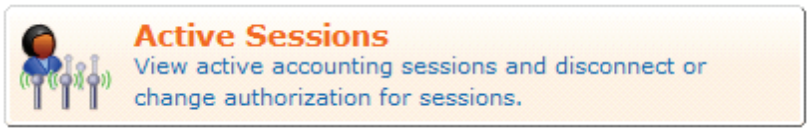
```
{if !$guest_receipt.u.username}<div style="display:none">{/if}
```

and the first line of the footer be:

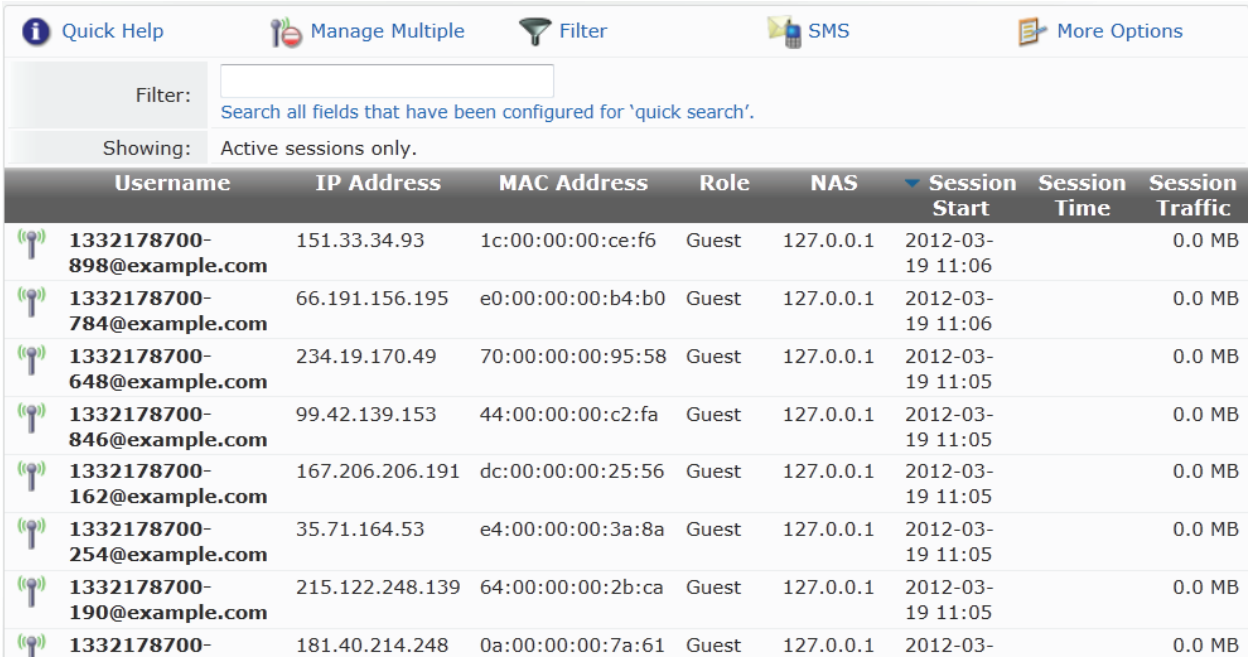
```
{if !$guest_receipt.u.username}</div>{/if}
```

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.



To view and manage active sessions for the RADIUS server, go to **Guests > Active Sessions**. The Active Sessions list opens. 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.



Username	IP Address	MAC Address	Role	NAS	Session Start	Session Time	Session Traffic
1332178700-898@example.com	151.33.34.93	1c:00:00:00:ce:f6	Guest	127.0.0.1	2012-03-19 11:06		0.0 MB
1332178700-784@example.com	66.191.156.195	e0:00:00:00:b4:b0	Guest	127.0.0.1	2012-03-19 11:06		0.0 MB
1332178700-648@example.com	234.19.170.49	70:00:00:00:95:58	Guest	127.0.0.1	2012-03-19 11:05		0.0 MB
1332178700-846@example.com	99.42.139.153	44:00:00:00:c2:fa	Guest	127.0.0.1	2012-03-19 11:05		0.0 MB
1332178700-162@example.com	167.206.206.191	dc:00:00:00:25:56	Guest	127.0.0.1	2012-03-19 11:05		0.0 MB
1332178700-254@example.com	35.71.164.53	e4:00:00:00:3a:8a	Guest	127.0.0.1	2012-03-19 11:05		0.0 MB
1332178700-190@example.com	215.122.248.139	64:00:00:00:2b:ca	Guest	127.0.0.1	2012-03-19 11:05		0.0 MB
1332178700-	181.40.214.248	0a:00:00:00:7a:61	Guest	127.0.0.1	2012-03-		0.0 MB

- On the Manage Multiple Sessions form, the start time of each session is used to select the sessions to work with. To find relevant sessions easily, sort the list view by the **Session Start** column before you begin session management tasks.
- 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.

- To display only sessions that meet certain criteria, click the **Filter** tab. For more information, see "Filtering the List of Active Sessions".
- To perform actions on multiple sessions, such as closing open or stale sessions or disconnecting or reauthorizing active sessions, click the **Manage Multiple** tab. For more information, see "Managing Multiple Active Sessions".
- To send SMS notifications to visitors, click the **SMS** tab. For more information, see "Sending Multiple SMS Alerts".
- To include additional fields in the Active Sessions list, or delete fields from it, click the **More Options** tab. The Customize View Fields page opens. For more information, see "Editing Forms".

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.

For information on configuring RADIUS server options, see "Server Configuration" in the RADIUS Services chapter. For details of the options that can be configured, including accounting update intervals and elapsed time before a session is considered stale, see "RADIUS Server Options" in the Reference chapter.

- **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 auth orization 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:

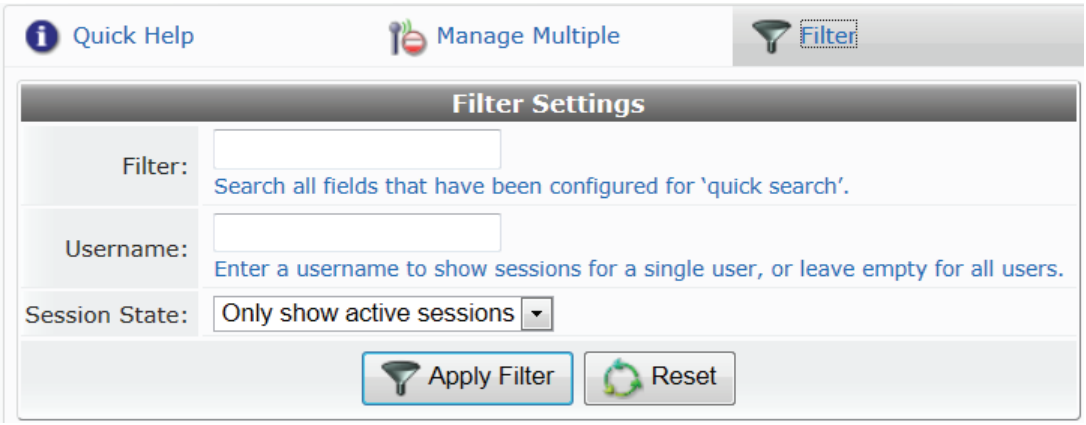
- **Disconnect** causes a Disconnect-Request message to be sent to the NAS for an active session, requesting that the NAS terminate the session immediately. The NAS should respond with a Disconnect-ACK message if the session was terminated or Disconnect-NAK if the session was not terminated.
- **Reauthorize**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

You can use the **Filter** tab to narrow the search parameters and quickly find all matching 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 29 *Operators supported in filters*

Operator	Meaning	Additional Information
=	is equal to	You may search for multiple values when using the equality (=) or inequality !=) operators. To specify multiple values, list them separated by the pipe character (|). 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".
!=	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.

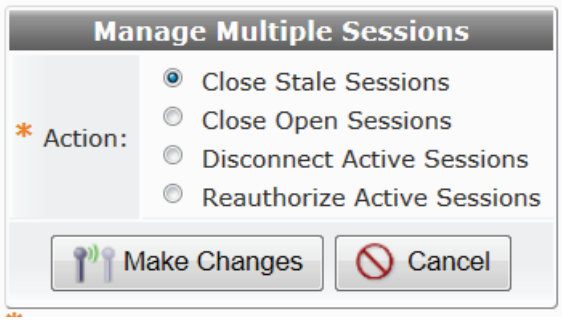
Click the **Apply Filter** button to save your changes and update the view, or click the **Reset** button to remove the filter and return to the default view.

Managing Multiple Active Sessions

To close multiple stale or open sessions, or disconnect or reauthorize multiple sessions, click the **Manage Multiple** tab. the Manage Multiple Sessions form opens.

Closing All Stale Sessions Immediately

By default, the Close Stale Sessions option is selected when the Manage Multiple Sessions form opens. This option allows you to quickly close all stale sessions with one click. Stale sessions should be closed to keep accounting statistics accurate.



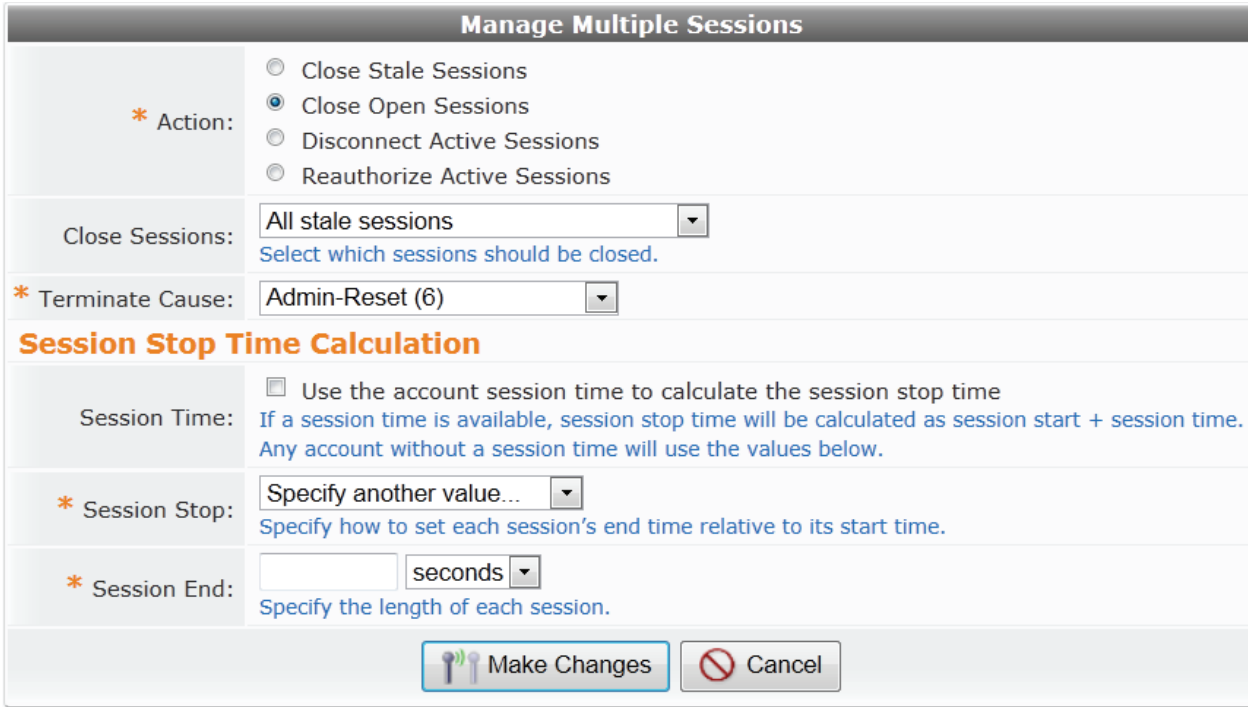
- To close all stale sessions, leave the **Close Stale Sessions** radio button marked and click **Make Changes**. All stale sessions are closed and are removed from the Active Sessions list.

A session is considered stale after 24 hours without an accounting update indicating session traffic. This is the default value, and can be configured for the RADIUS server.

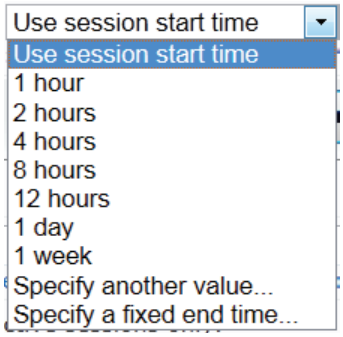
Closing All Stale Sessions and Specifying a Duration

You can choose to close all stale sessions at a specified time, and include the reason for closing them.

1. To close all stale sessions at a certain time, mark the **Close Open Sessions** radio button on the Manage Multiple Sessions form. The form expands to include rows for calculating the stop time.



2. In the **Close Sessions** drop-down list, leave the **All stale sessions** option selected.
3. In the **Terminate Cause** drop-down list, select the reason for closing the sessions.
4. (Optional) If you mark the **Session Time** check box, sessions with an elapsed session time available will be closed when you commit your changes on this form. The session's stop time will be calculated as the session start time plus the elapsed session time.
5. Use the **Session Stop** drop-down list to specify how the stop time will be calculated for each session.



- If you choose **Use session start time**, the session will be closed when you commit your changes on this form.
- To specify a range of time after a session's start time, choose one of the options for hours, day, or week. Sessions will be closed when that amount of time has elapsed after the start time. Since this setting is relative to start time, each session may be closed at a different time.
- To specify a range of time that is not included in the list, select the **Specify another value** option. This adds the Session End row to the form, where you can set a time interval.
  - In the **Session End** row, enter a number value in the text box, and choose the time interval from the drop-down list—either seconds, minutes, hours, days, or weeks.

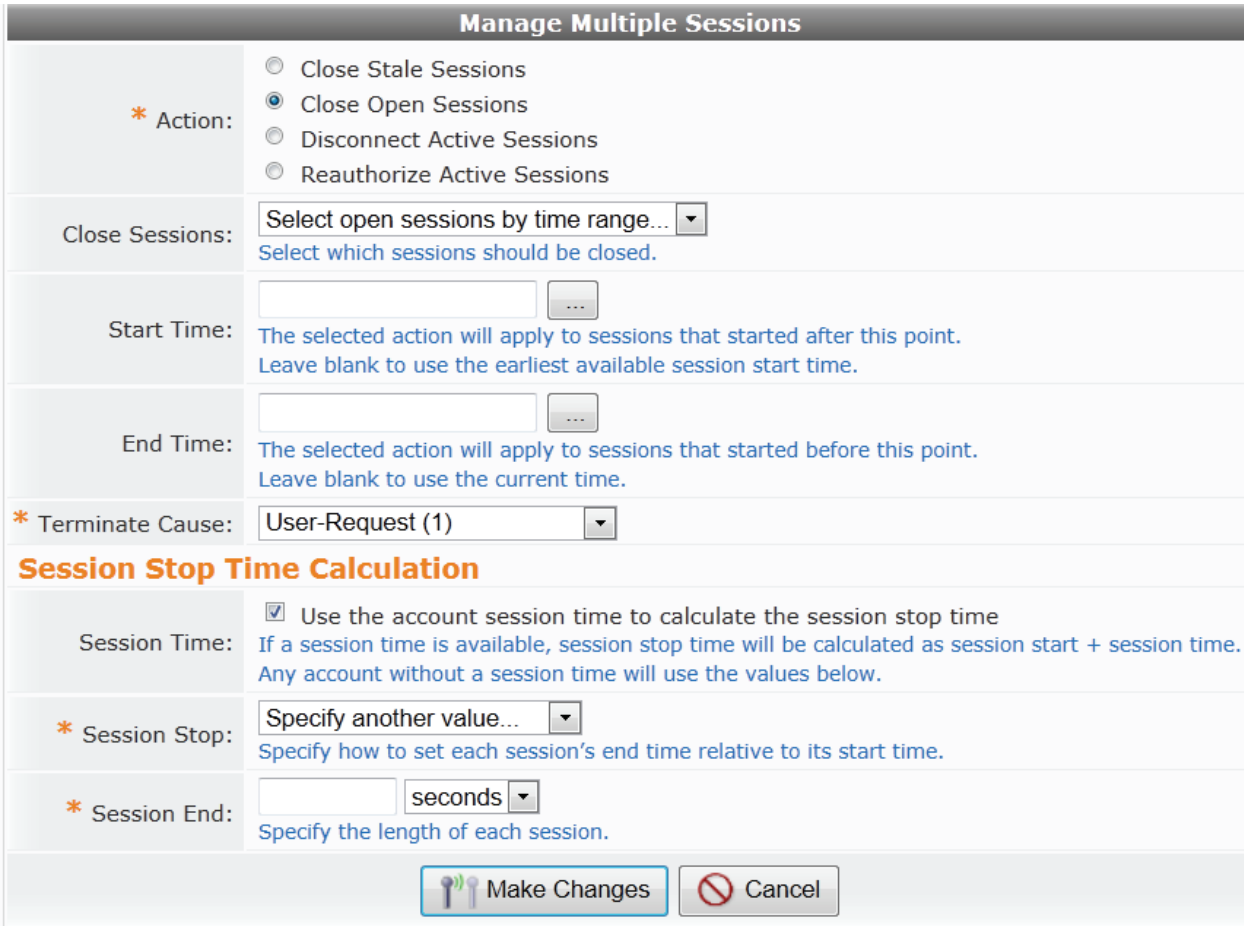
- To set a specific date and time, choose **Specify a fixed end time** from the drop-down list. This adds the Session End row to the form, with a calendar option.
  - In the **Session End** row, click the button to open the calendar picker. In the calendar, use the arrows to select the year and month, click the number s in the **Time** fields to increment the hours and minutes, then click a day to select the date.

6. When your entries on the form are complete, click **Make Changes.** The stale sessions are closed according to the criteria you specified.

Closing Specified Open Sessions

You can select open sessions within a time range to close, include the reason for closing them, and specify when to close them.

1. To close a selection of open sessions, mark the **Close Open Sessions** radio button on the Manage Multiple Sessions form. The form expands to include rows for calculating the stop time.
2. In the **Close Sessions** row, choose **Select open sessions by time range** from the drop-down list. The form expands to also include rows for selecting the range of open sessions.

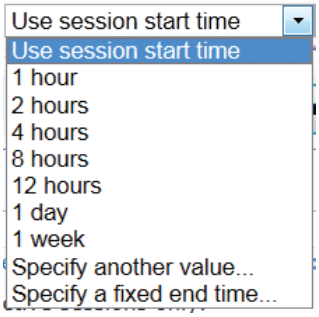


3. Use the **Start Time** row to indicate the beginning of the time range for selecting sessions. To specify a time for the beginning of the range, click the button to open the calendar picker. In the calendar, use the arrows to select the year and month, click the numbers in the **Time** fields to increment the hours and minutes, then click a day to select the date.
   - If this field is left empty, the earliest available session start time is used.
   - If you leave both the Start Time and End Time fields empty, all open sessions are selected.
4. Use the **End Time** row to indicate the end of the time range for selecting sessions. To use the current time, leave this field blank. To specify a time for the end of the range, 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 this End Time field is specified and the Start Time field is left empty, all sessions that started before the specified end time are selected.
- If this End Time field and the Start Time field are both specified, all sessions that started between the start time and end time are selected.

5. In the **Terminate Cause** drop-down list, select the reason for closing the sessions.
6. (Optional) If you mark the Session Time check box, sessions with an elapsed session time available will be closed when you commit your changes on this form. The session's stop time will be calculated as the session start time plus the elapsed session time.
7. Use the **Session Stop** drop-down list to specify how the stop time will be calculated for each session.



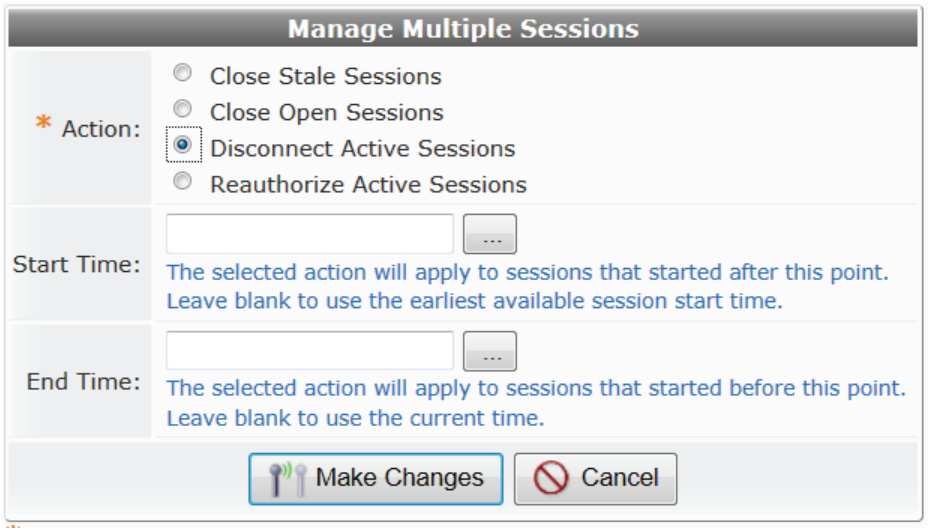
- If you choose **Use session start time**, the session will be closed when you commit your changes on this form.
- To specify a range of time after a session's start time, choose one of the options for hours, day, or week. Sessions will be closed when that amount of time has elapsed after the start time. Because this setting is relative to start time, each session may be closed at a different time.
- To specify a range of time that is not included in the list, select the **Specify another value** option. This adds the Session End row to the form, where you can set a time interval.
  - In the **Session End** row, enter a number value in the text box, and choose the time interval from the drop-down list—either seconds, minutes, hours, days, or weeks.
- To set a specific date and time for closing that will apply to all selected sessions, choose **Specify a fixed end time** from the drop-down list. This adds the Session End row to the form, with a calendar option.
  - In the **Session End** row, click the button to open the calendar picker. In the calendar, use the arrows to select the year and month, click the number s in the **Time** fields to increment the hours and minutes, then click a day to select the date.

8. When your entries on the form are complete, click **Make Changes.** The selected sessions are closed according to the criteria you specified.

Disconnecting or Reauthorizing Active Sessions

If the NAS equipment has RFC 3576 support, you can disconnect or dynamically reauthorize active sessions.

1. On the Manage Multiple Sessions form, to disconnect sessions, mark the **Disconnect Active Sessions** radio button. To reauthorize sessions, mark the **Rauthorize Active Sessions** radio button. The form expands to include rows for specifying the time range of sessions to select.

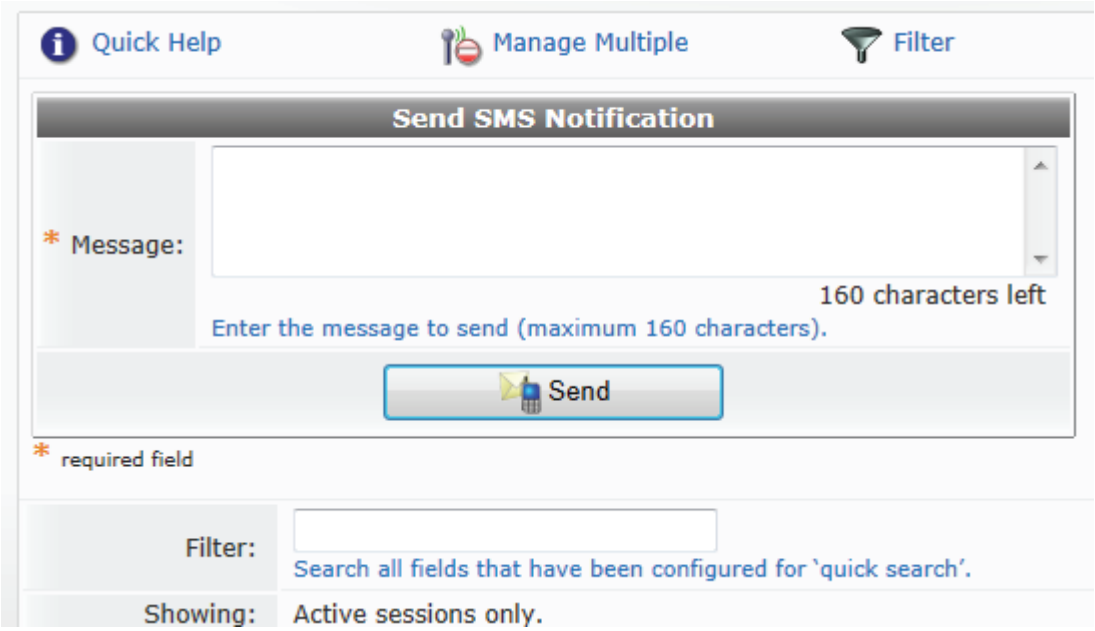


2. Use the **Start Time** row to indicate the beginning of the time range for selecting sessions. To specify a time for the beginning of the range, click the button to open the calendar picker. In the calendar, use the arrows to select the year and month, click the numbers in the **Time** fields to increment the hours and minutes, then click a day to select the date.
   - If this field is left empty, the earliest available session start time is used.
   - If you leave both the Start Time and End Time fields empty, all open sessions are selected.
3. Use the **End Time** row to indicate the end of the time range for selecting sessions. To use the current time, leave this field blank. To specify a time for the end of the range, 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 this End Time field is specified and the Start Time field is left empty, all sessions that started before the specified end time are selected.
   - If this End Time field and the Start Time field are both specified, all sessions that started between the start time and end time are selected.
4. When your entries on the form are complete, click **Make Changes.**
   - If you selected Disconnect Active Sessions as the action, the selected sessions are immediately terminated.
   - If you selected Reauthorize Active Sessions as the action, the selected active sessions are dynamically reauthorized and corresponding session properties are updated.

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.

1. To create an SMS message, click the **SMS** tab on the Active Sessions page. The Send SMS Notification form opens.



2. Use the filter to specify the group of addresses that should receive the message. See Filtering the List of Active Sessions. 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**.

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 are also able to use SMS Services to send an SMS from your Web browser.

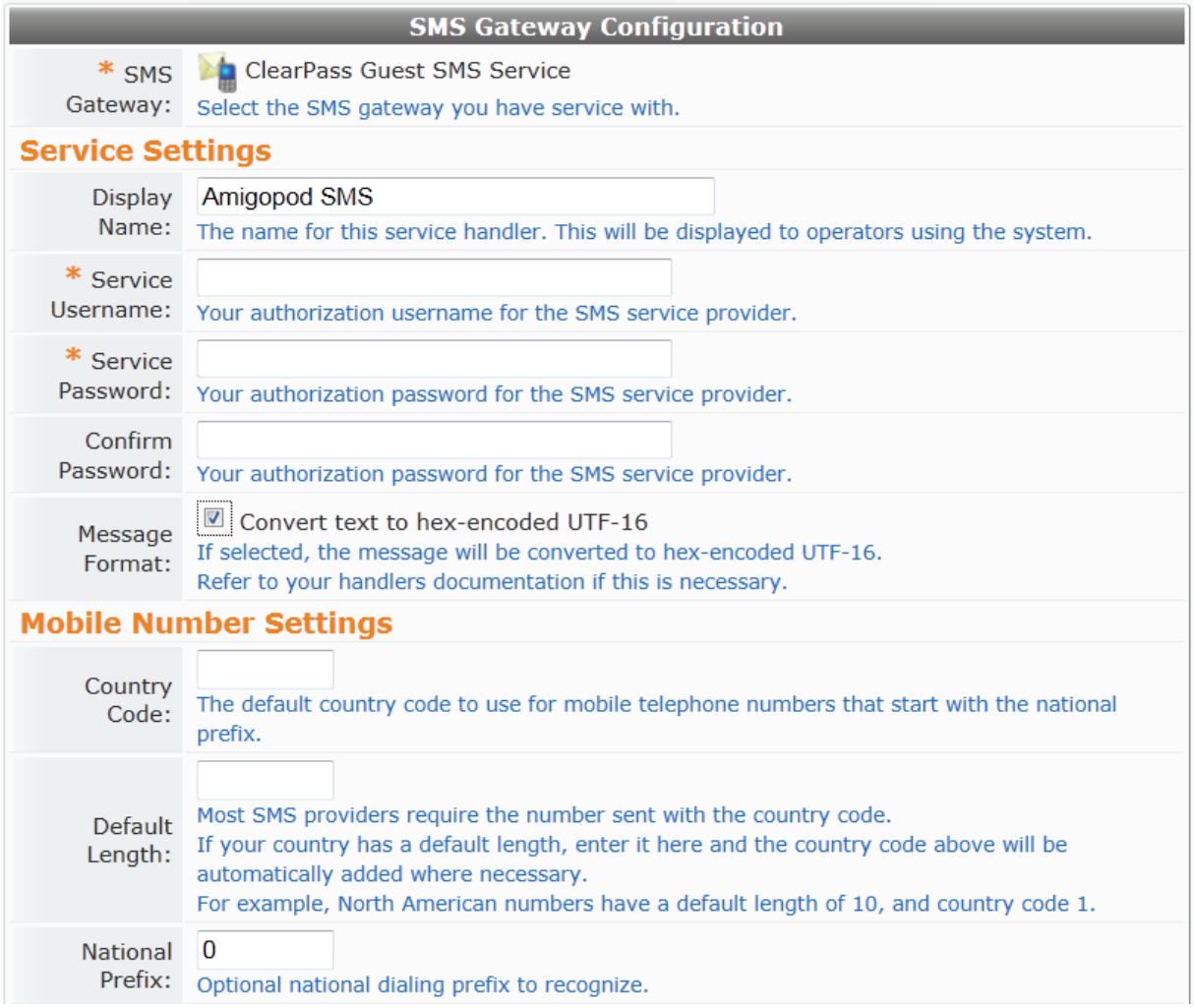
To use the SMS features, you must have the SMS Services plugin installed.

Configuring SMS Gateways

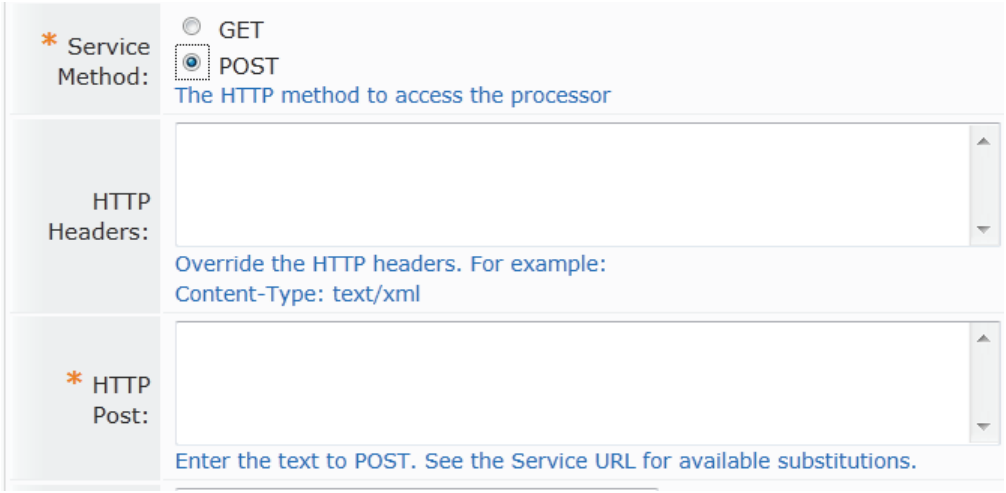
You can configure the application to send SMS messages using the **Manage SMS Gateways** link on the **Administrator > SMS Services** page.

The **SMS Gateways** window displays the name and available credits for any currently defined SMS gateways. To create a new SMS gateway, click the **Create new SMS gateway** link to display the **SMS Service Configuration** form.

The first part of the form includes the Service Settings and Mobile Number Settings areas.



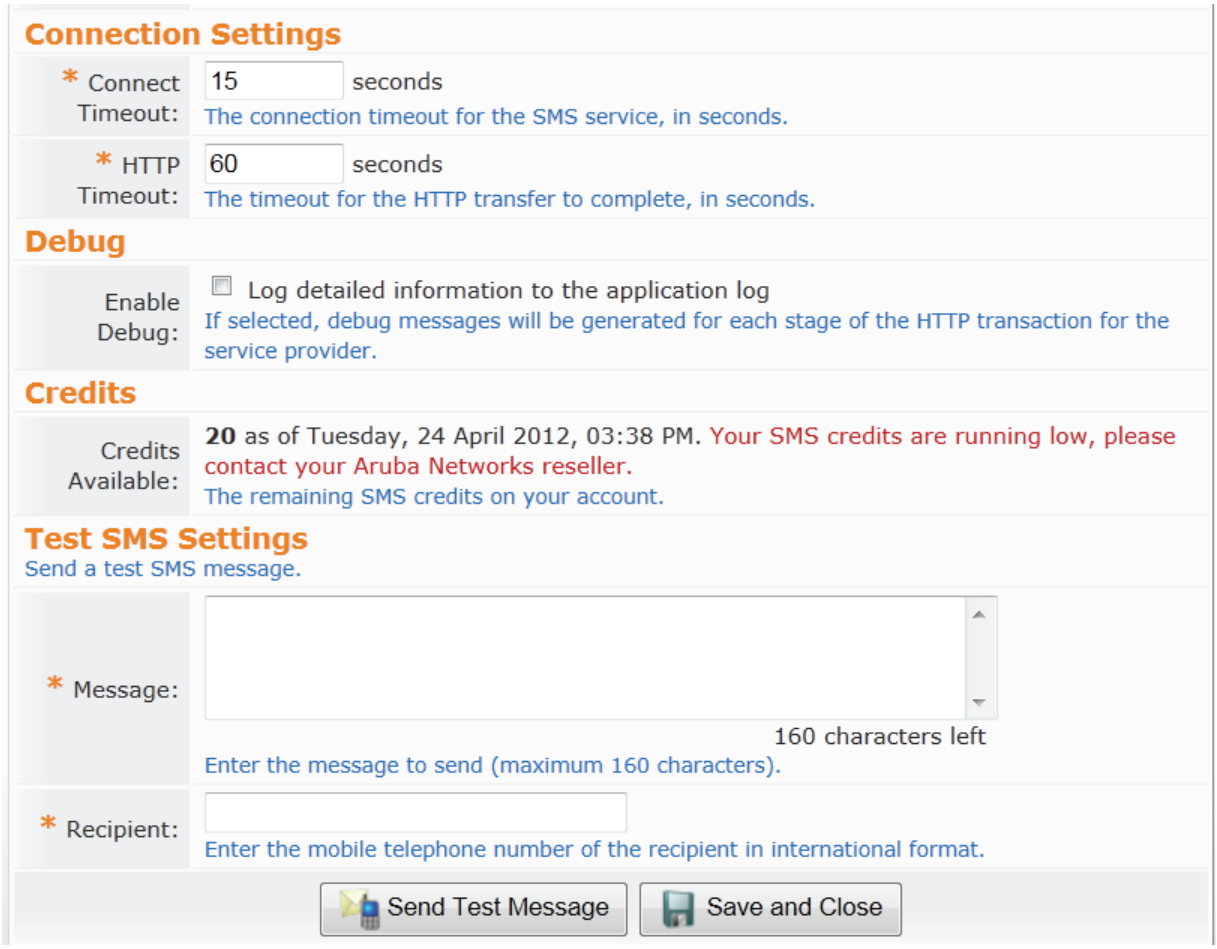
In the **SMS Gateway** field, if you choose **Custom HTTP Handler** from the drop-down list, you may specify the HTTP method to use. The form displays the configuration options for that gateway type, and the **Service Method** row includes the GET and POST options. When you select the **POST** option, the HTTP Headers and HTTP Post rows are added. You can use the text fields in these rows to override HTTP headers and enter the text to post.



If needed for custom SMS handlers, you can specify that the message format should be converted to hex-encoded UTF-16 (Unicode).

If your country uses a national dialing prefix such as “0”, you may enter this on the form. 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.

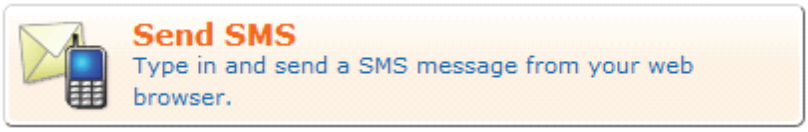
The second part of the form includes the Connection Settings, Debug, Credits, and Test SMS Settings areas.



Complete the fields with the appropriate information, then click either **Send Test Message** or **Save and Close**. The new configuration settings will take effect immediately.

Sending an SMS

You are able to send an SMS, if the system has been configured to allow this, by clicking the **Send SMS** command link on the **Administrator > SMS Services** page.



The **New SMS Message** form appears

Complete the form by typing in the SMS message and entering the mobile phone number that you are sending the SMS to. If multiple services are available, you may also choose the service to use when sending the message.

NOTE

The SMS is limited to a maximum length of 160 characters. The number of remaining characters is displayed on this form.

Click the **Send Message** button to send the SMS.

About SMS Credits

Each SMS message sent consumes one credit.

To determine the number of remaining SMS credits, navigate to the **Administrator > SMS Gateways** window. The **Credits Available** field indicates the number of remaining SMS credits for your account. This value is determined once the first message has been sent, and is updated after sending each message.

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 once the “Credits Available” value reaches the warning threshold (the default value is 50).
- A second low-credit warning is sent once the “Credits Available” value reaches half the warning threshold.
- A final message is sent once the “Credits Available” value reaches zero.

NOTE

To adjust the warning threshold, set the Credit Warning value in the configuration for the SMS Services Plugin.

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.

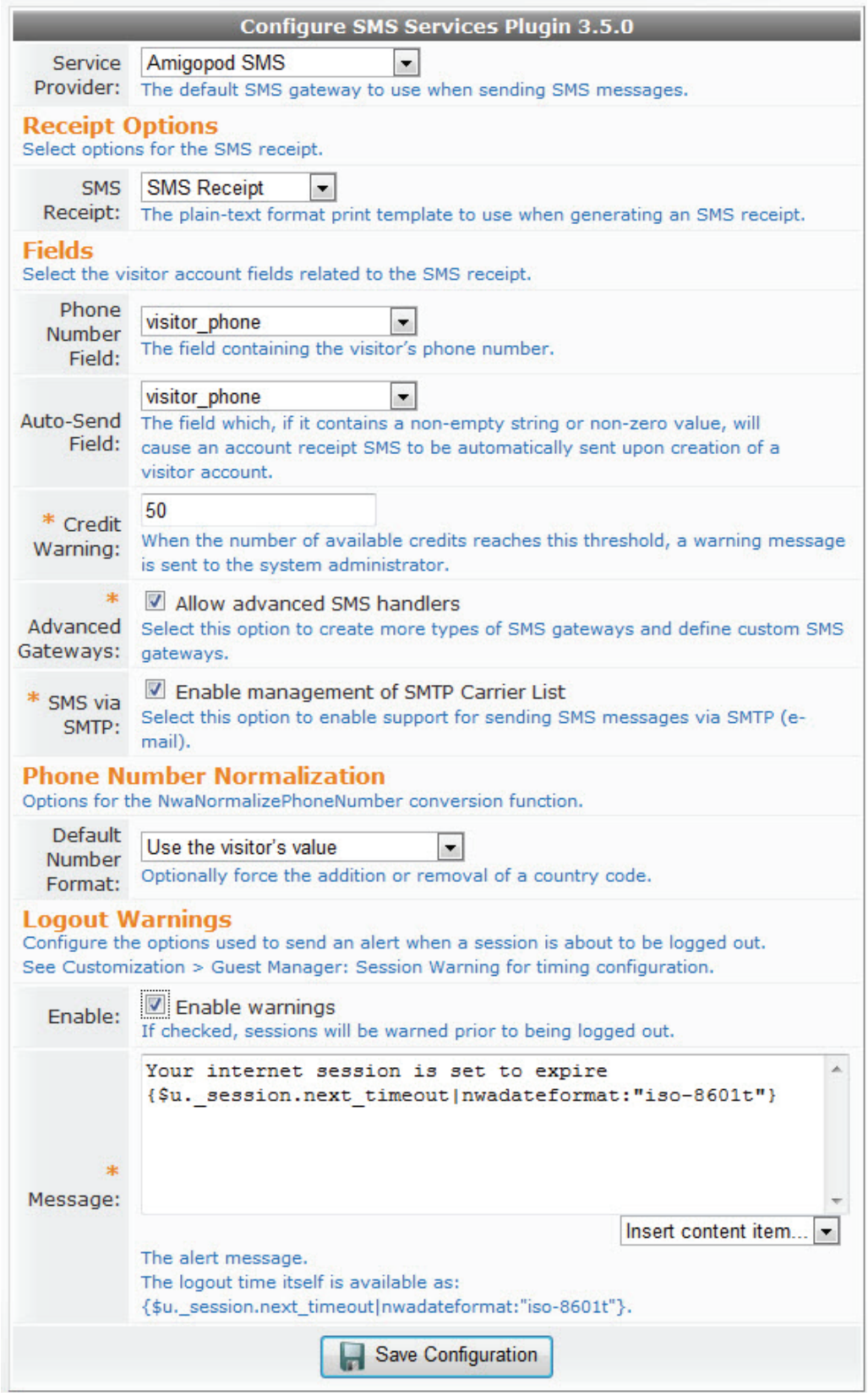
To manually send an SMS receipt, navigate to the **Guests > List Accounts** window, select the guest to which you want to send a receipt, then click the **Send SMS receipt** link displayed on the guest account receipt page.

When using guest self-registration, SMS Delivery options are available for the receipt page actions; **See** **"Editing SMS Delivery of Guest Receipts"** in this chapter for full details.

SMS Receipt Options

The SMS Services plugin configuration allows you to configure options related to SMS receipts. These settings can be viewed and modified using the Plugin Manager.

Figure 36 *Configure SMS Services Plugin*



SMS Receipt – Select the print template to be used when an SMS receipt is created. The print template used for the receipt must be in plain text format.

- **Phone Number Field** – Select which guest account field contains the guest's mobile telephone number. This field is used to determine the SMS recipient address.

- **Auto-Send Field** – Select a 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 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** – When SMS credits get below this threshold, the system will send a warning to the system administrator.
- **Advanced Gateways** – Select this option to configure SMS gateways from multiple SMS providers. ClearPass Guest SMS services support SMS USA, SMS Worldwide, AQL, Sirocco, Tempos 21 and Upside Wireless SMS gateways.
- **SMS via SMTP** – Select this option to allow visitor account receipt messages to be sent in an email using the defined SMTP server.
- **Phone Number Normalization** – The phone number normalization process translates phone strings that are entered in various formats into a single standard format. Click this drop-down list and select one of the following options:
  - **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 *0412345678* would normalize to *+61412345678* 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.
- **Logout Warnings** – Check **Enable warnings** if you to send an alert sent when the session is about to be logged out. Enter the exact text that you want to appear as the alert. You can set the time for warnings using the Guest Manager customization page.

Customize SMS Receipt

Navigate to **Customization > SMS Receipts** to configure SMS receipt options. These fields are described for the SMS plugin configuration page. Use the SMS receipt page for further customization.

Figure 37 *Customize SMS Receipt page*

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.

- **sms_warn_before_message** – This field overrides the logout warning message. If blank or unset, the default value from the Customize SMS Receipt page is used.

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.

SMTP Services

With SMTP Services, you can configure ClearPass Guest to send customized guest account receipts to visitors and sponsors by email.

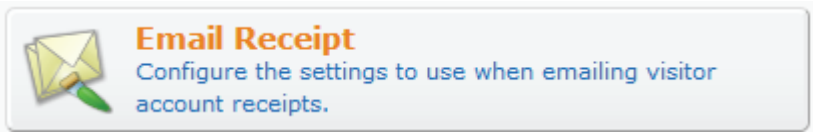
Email receipts may be sent in plain text or HTML format.

As of SMTP Services 2.1.0, 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.

Configuring SMTP Services

You can configure the default settings used when generating an email receipt by clicking the **Customize Email Receipt** command link, which is available on the Customize Guest Manager page.



See "Email Receipt Options" in this chapter for details about the email receipt options.

See "SMTP Configuration" in the Adminstrator Tasks chapter for details about configuring the SMTP server settings used to deliver outbound email messages.

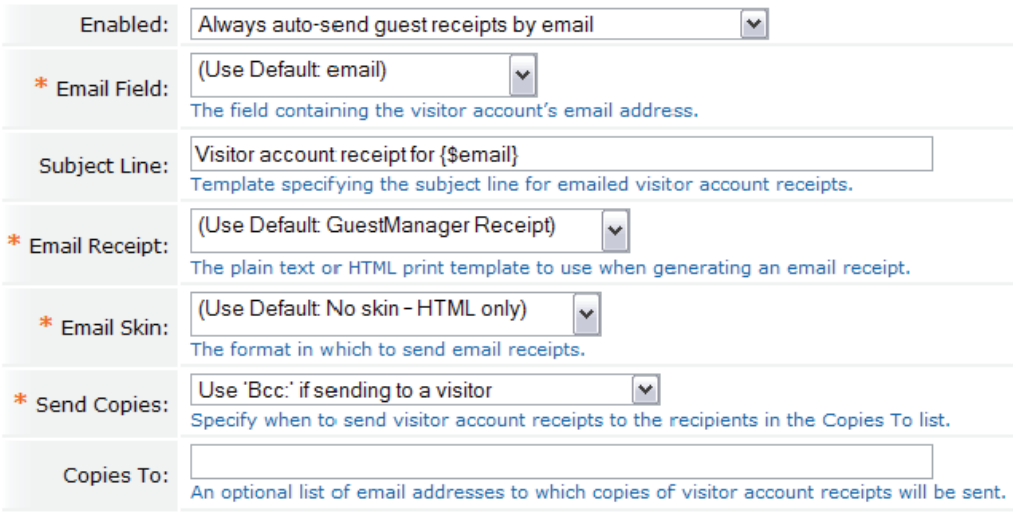
About Email Receipts

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 by clicking the **Send email receipt** link displayed on the guest account receipt page.

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.



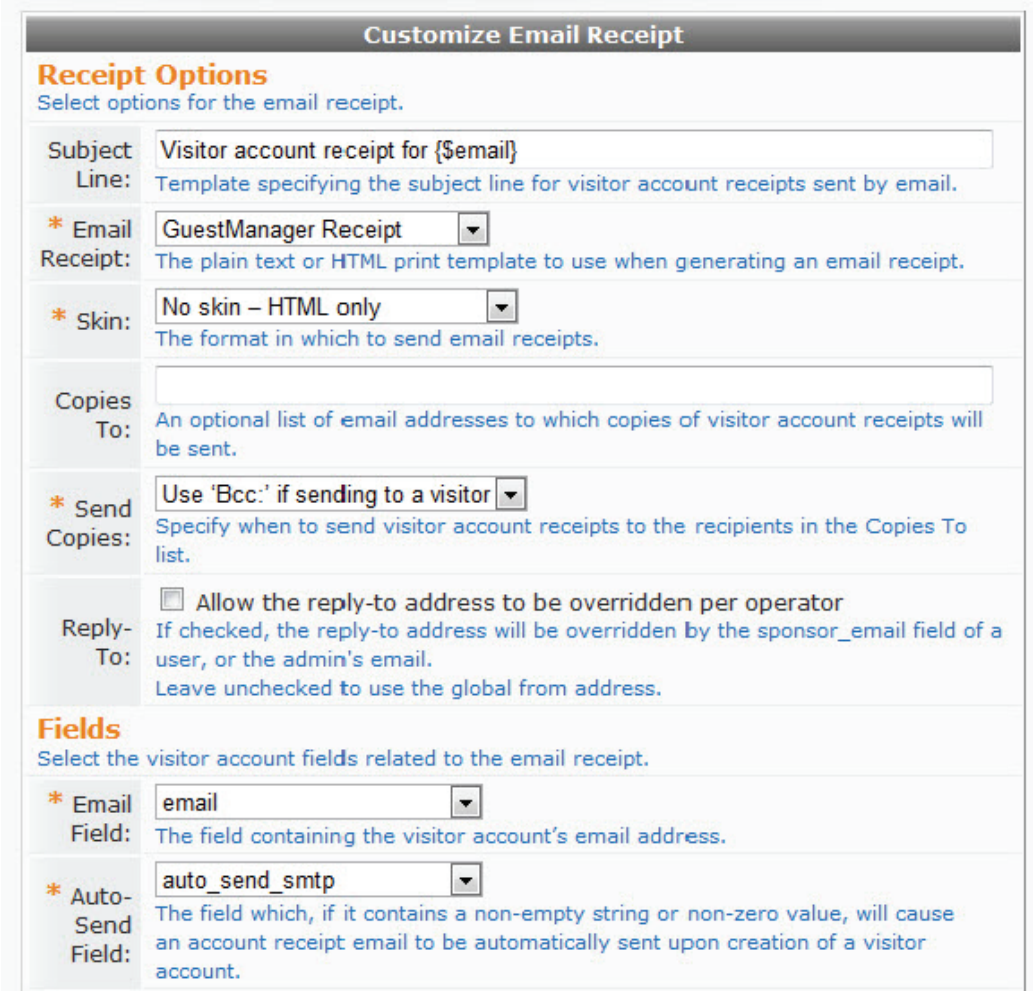
These options under Enabled are available to control email delivery:

- **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 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_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 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.

Email Receipt Options

The **Customize Email Receipt** form may be used to set default options for visitor account email receipts.

Figure 38 *Customize Email Receipt page*



The 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" in the Reference chapter for more information on template syntax.

The Skin drop-down list allows you to specify a skin to be used to provide the basic appearance of the email. You may select from one of the installed skins, or use one of these special options:

- **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.

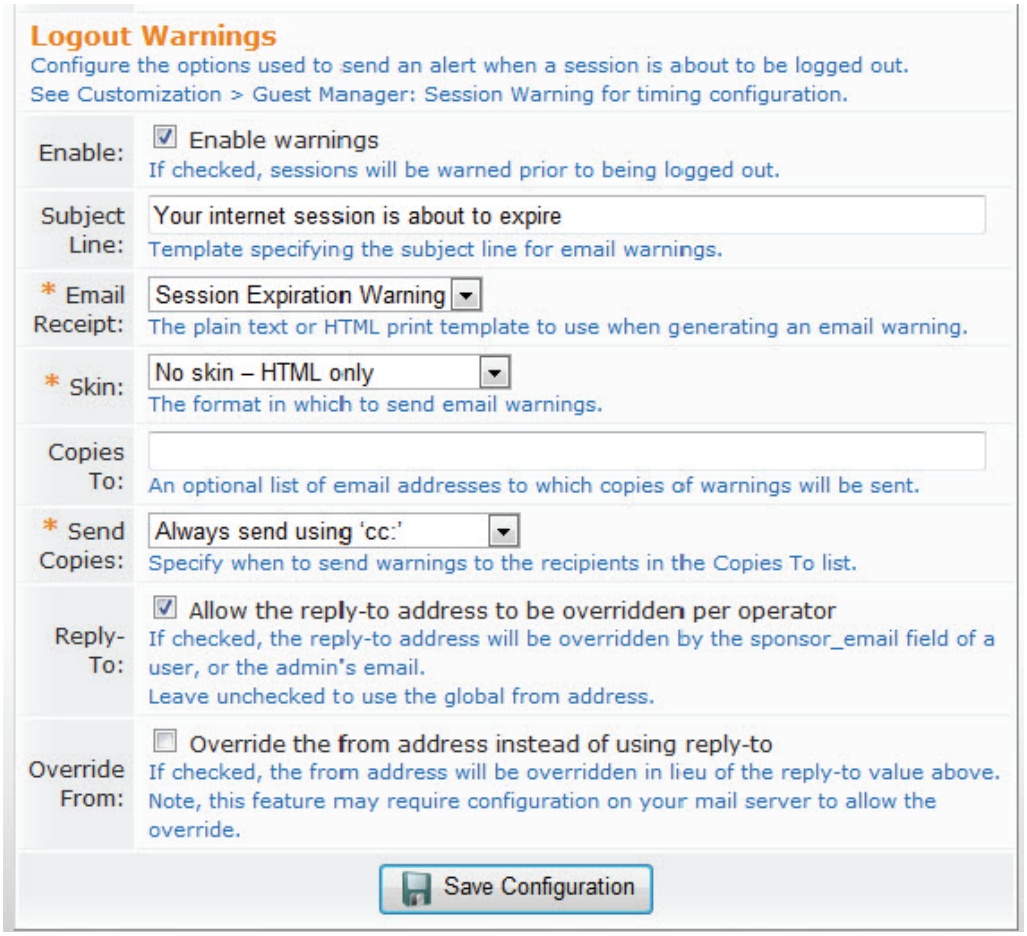
When sending an email message using HTML formatting, the images and other resources required to display the page will be included in the message.

Copies of the generated email receipts may be sent to one or more additional email addresses, which can be specified in the Copies To list. The Send Copies drop-down list specifies how these copies are sent:

- **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.

Figure 39 *Customize Email Receipt page—continued*



Check **Enable warnings** if you to send an alert sent when the session is about to be logged out. Enter the exact text that you want to appear as the alert in the **Subject Line** field. You can set the time for warnings using the Guest Manager customization page. See "Guest Manager Customization" .

Check **Allow the reply-to address to be overridden per operator** if you want the reply-to address to be overridden by the sponsor_email field of the user or the admin's email. If you check this field than the **Override the from address instead of using reply-to** check box displays. Check this if you want the from address to be overridden instead of the reply-to value. field may require configuration on your mail server to allow the override.

Click the **Save Changes** button when you have completed the form. The new configuration settings will take effect immediately.

SMTP Receipt Fields

The behavior of email receipt operations can be customized with certain guest account fields. You do this on a per user basis.

- **smtp_enabled** – 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_subject** – 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** – 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_receipt_format** – 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_email_field** – 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_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 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** – 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_cc_action** – This field 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.

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.
- **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.

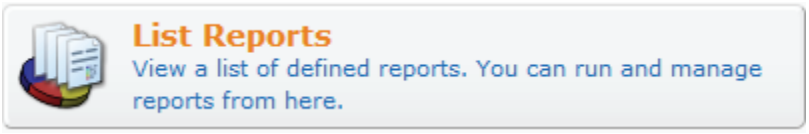
The Reporting Manager provides you with a set of tools to summarize the visitor accounts that have been created and analyze the accounting data collected by the RADIUS server. Through the predefined reports and the custom reports you can create using the report editor, you can get a complete picture of the network usage of your guests.

Accessing Reporting Manager

Use the **Reporting** command link on the home page to access the reporting features.

Viewing Reports

Use this list view to run reports, view reports that have already been generated, and manage the report definitions.



There are twelve predefined reports.

- **Average link utilization** – This report calculates the average link utilization for all accounting traffic in the selected period.
- **Average session time per day** – This report calculates the average elapsed time for each session in the selected period.
- **Average traffic volume per session** – This report calculates the average amount of data traffic for each session in the selected time period.
- **Average traffic volume per user** – This report calculates the average traffic volume from accounting traffic per unique user per day.
- **Daily link utilization** – This report calculates the average daily link utilization for accounting traffic in the selected period.
- **Number of concurrent sessions** – This report shows the total number of concurrent sessions throughout a time interval, sampling every 5 minutes.
- **Number of concurrent sessions by role** – This report shows the number of concurrent sessions according to the user's role across a time interval.

- **Number of sessions per NAS** – This report shows the total number of sessions per NAS in the selected period.
- **Number of sessions per day** – This report shows the total number of sessions per day.
- **Number of users per day** – This report shows the number of distinct users per day.
- **Top 10 users by total traffic** – This report summarizes the total data volume of all users, and displays the top 10 users by total data sent and received.
- **Total data traffic per day** – This report shows how the total amount of sent and received data traffic for all sessions varies on a daily basis.

You can create new report definitions with the report editor by clicking the **Create new report** link. **See** **"Resetting Report Definitions"** in this chapter for an overview of custom reports.

Click the **More Options** tab to access functions for importing and exporting report definitions.

Running and Managing Reports

Click the predefined report that you want to run. This displays an action row containing links to the following commands: **View HTML**, **History**, **Run Preview**, **Run Default**, **Run...**, **Edit**, **Delete** and **Duplicate** and **Permissions**.

The View HTML and History options are only available if the report has been run at least once.

Viewing the Most Recent Report

To view the most recently generated report, click the **View HTML** link. This opens a window with the report's name, date generated and date range. A graph is displayed in your default graph style. The data for the graph is displayed below the graph in table format.

If you initially selected to run the report in a number of formats, you will also have these options listed—for example, **View Text** and **View CSV**.

Report History

Clicking the **History** link opens the **Report History** form. This form allows you to select a previously run report to be viewed. If the report was originally run in a number of formats, you are able to select the format to view. If you only ran the report in one format, only that format is available.

Previewing the Report

To see a preview of the report, click the **Run Preview** link. A progress window appears as the report is generated, and then the report will be displayed automatically. The Run Preview link is not available for reports that require user interaction.

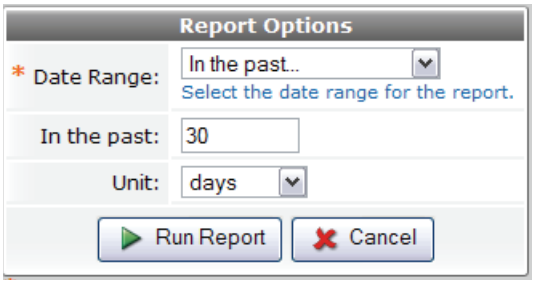
The report preview uses the default format and date range for the report, as displayed next to the report name in the list of reports. The output of the preview run is not stored in the report history, and the Last Run date will not be updated.

Run Default

Clicking the **Run Default** runs the report using all defaults for both format and date range. A progress window appears as the report is generated, and then the report is displayed automatically. The Run Default link is not available for reports that require user interaction. To print the report, click the **Print** icon in your Web browser.

Run

The **Run** option allows you to change the date range of the report before it is run. Choose a time period for the report from the Date Range drop-down list.



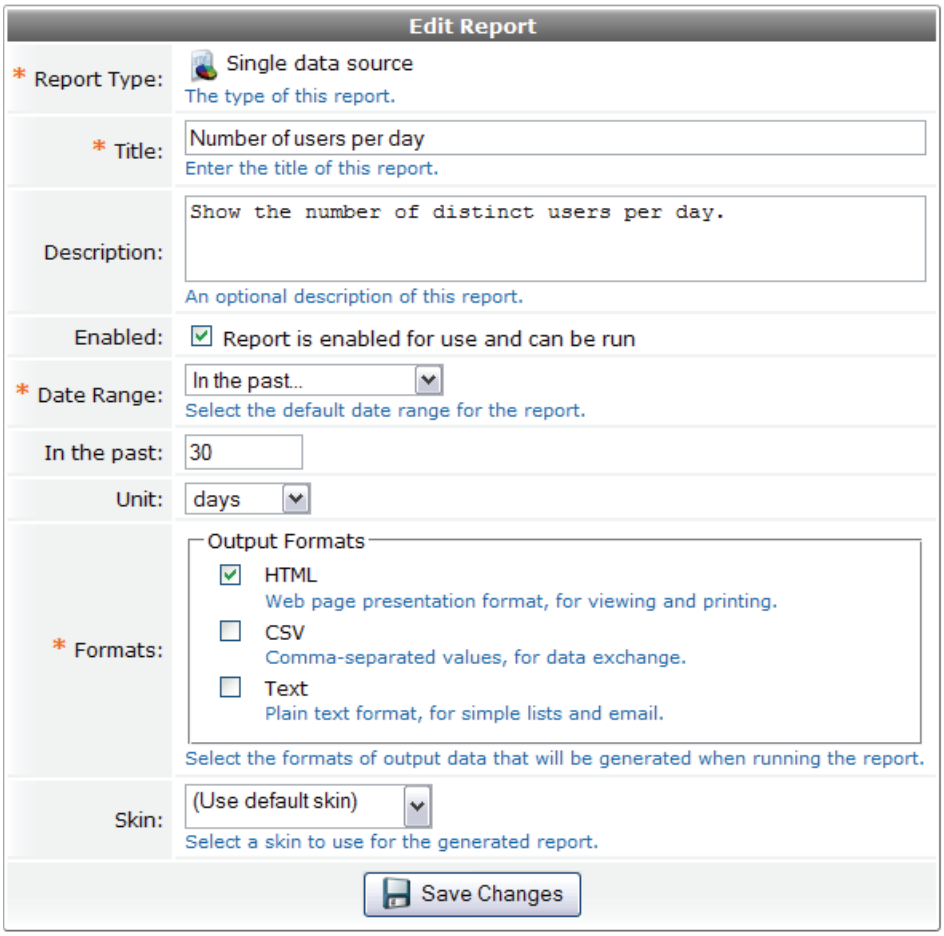
If the report definition includes any additional parameters that have a user interface, these will also be displayed as part of the **Report Options** form.

Click the **Run Report** button to generate the report using the selected parameters. A progress window will appear as the report is generated, and then the report will be displayed automatically. To print the report, click the **Print** icon in your Web browser.

Edit a report

You can edit any of the predefined reports. Clicking the **Edit** link opens the Report Editor window. See "Components of the Report Editor" in this chapter for more details.

You can change the defaults for your report in the Report Editor window by selecting the **Report Type** link.



The Report Type editor allows you to change the defaults for the Date Range and the Formats for the report you have selected. If you want to change the default for another report you must also edit that report. Click the **Save Changes** button to have these changes become the new default.

Delete a Report

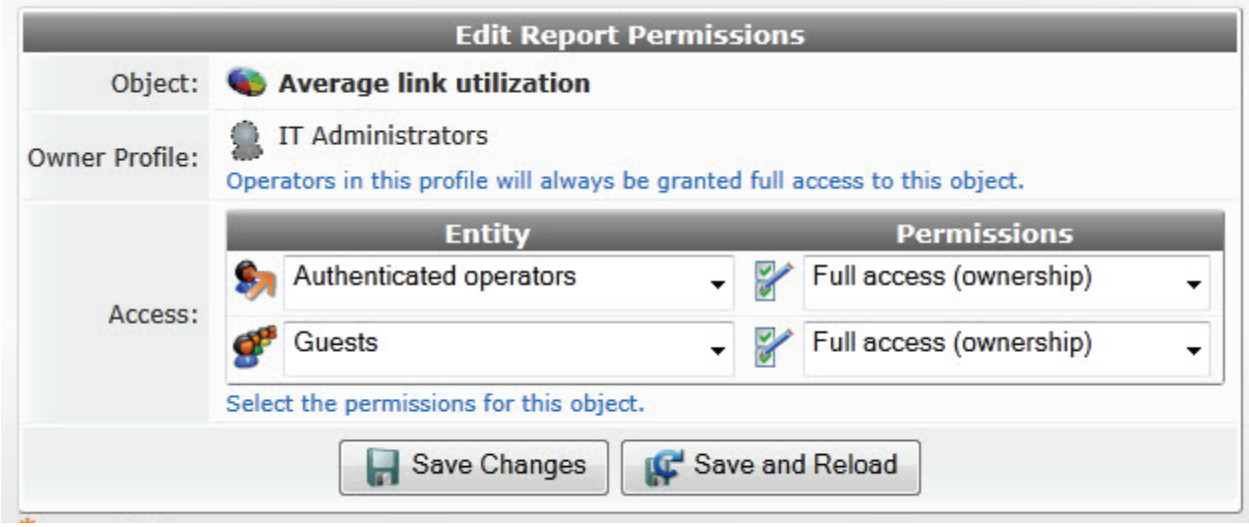
You can delete any predefined reports by selecting the report and clicking the **Delete** link. You are asked to confirm the deletion. Once you delete a report, it is permanently deleted. Use this option with care.

Duplicate a Report

You are able to duplicate a report by clicking on the **Duplicate** icon link. This is an easy way to start creating a new report that is similar to an existing report. See "Report Created by Duplicating an Existing Report" in the Reference chapter for an example.

Permissions

Use the **Permissions** link to edit report premissions . You can change who can use, view, edit or delete the report. The Permissions link is only displayed if the current operator has the Object Permissions privilege. This privilege is located in the Administrator group of privileges.



The permissions defined on this page apply to the report identified in the "Object" line.

The owner profile always has full access to the report.

To control access to this report by other entities, add or modify the entries in the "Access" list. To add an entry to the list, or remove an entry from the list, click one of the icons in the row. A **Delete** icon and an **Add** icon will then be displayed for that row.

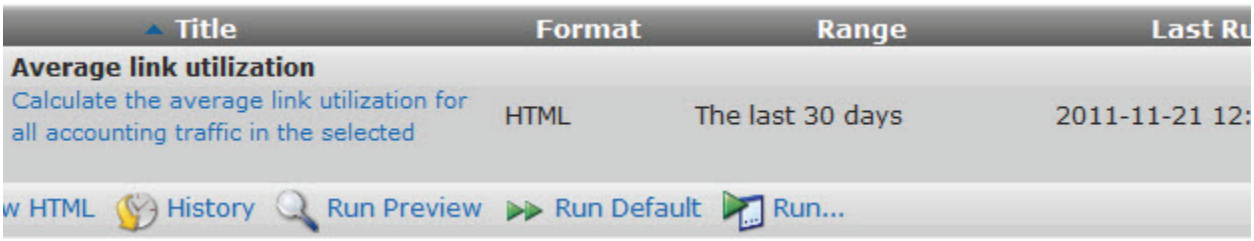
Select one of the following entities in the Entity drop-down list:

- **Operator Profiles** – a specific operator profile may be selected. The corresponding permissions apply to all operators with that operator profile.
- Other Entities
  - **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.

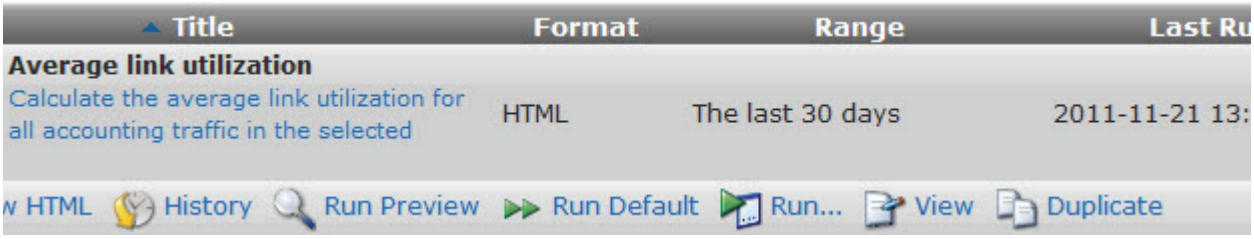
The permissions for the selected entity can be set using the Permissions drop-down list:

- **No access** – the report is not visible on the list, and cannot be used, edited, duplicated, or deleted.

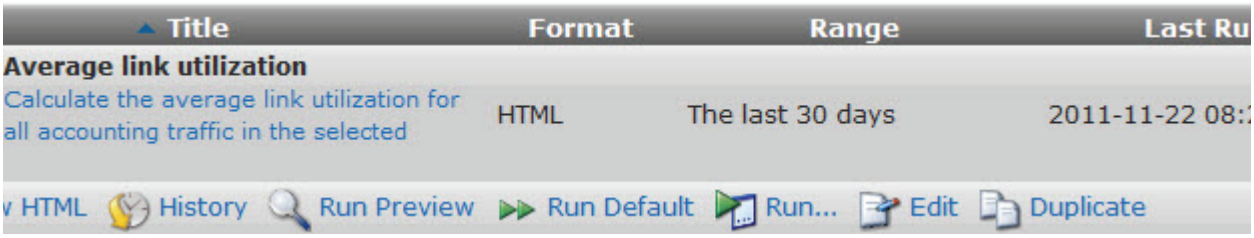
- **Visible-only access** – the report is visible in the list. It can be viewed in HTML but cannot be edited



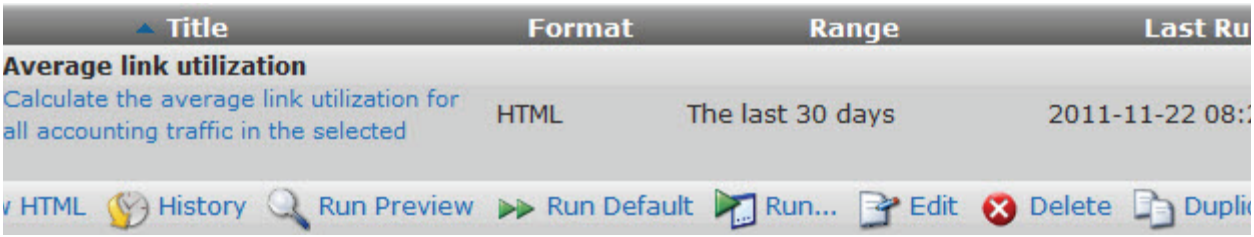
- **Read-only access** – the report is visible in the list and it may be viewed and duplicated. The report cannot be edited or deleted.



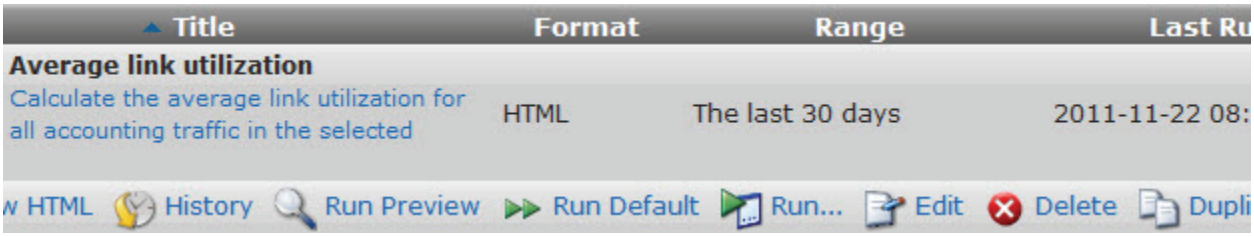
- **Update access** – the report is visible in the list and may be duplicated and edited. The report cannot be deleted and the permissions for the report cannot be modified.



- **Update and delete access** – the report is visible in the list, and may be edited or deleted. The permissions for the report cannot be modified.



- **Full access (ownership)** – the report is visible in the list, and may be edited or deleted. Permissions can be changed when you have Full Access, but this also requires that you have the **Administrator > Object Permissions** privilege set in your operator profile.

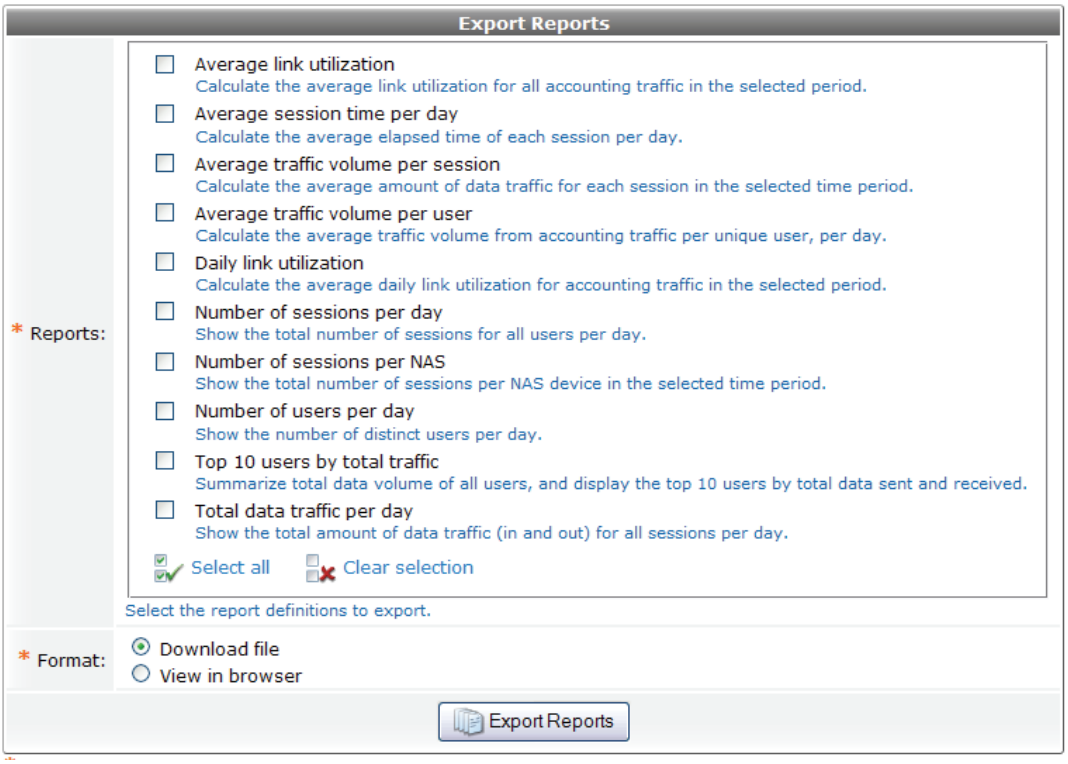


Exporting Report Definitions

Report definitions may be exported to a file and later imported. This provides an easy way to move reports from one appliance to another.

Click the **More Options** tab at the top of the report list to access the Export Reports command link. (This link also appears on the **Reporting** start page.)

Use the check boxes to select the reports to export.



If you select the Download file option, clicking the **Export Reports** button will download the selected report definitions to your Web browser. Otherwise, if the View in browser option is selected, the selected report definitions will be displayed as text. This allows you to copy and paste report definitions to another application.

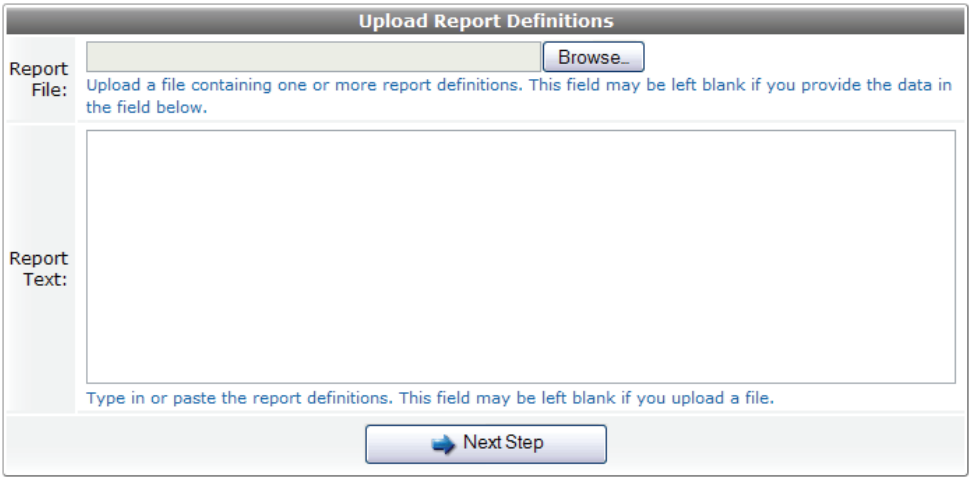
Only the report definition will be exported. The report definition comprises all aspects of the report that can be edited using the Report Editor. The exported data does not include any of the previously run copies of the report, nor does it include the data used to create the reports.

Importing report Definitions

Report definitions may be imported from a file that has been generated with the Export Reports command.

Click the **More Options** tab at the top of the report list to access the Import Reports command link. (This link also appears on the **Reporting** start page.)

You may select a file to upload using your Web browser, or alternatively the report definition may be pasted into the text area provided.



A report definition begins and ends with the lines

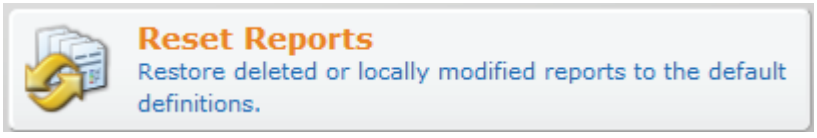
```
-----BEGIN REPORT DEFINITION-----
-----END REPORT DEFINITION-----
```

Click the **Next Step** button to proceed. A list of the available reports for import will be displayed. Use the check boxes to select the reports to import and click the **Import Reports** button to create new reports. Importing a report that already exists will replace the existing report definition.

Resetting Report Definitions

Report definitions may be individually reset to the factory defaults. Use this option if you have modified a report and it is no longer functioning correctly, or if you have accidentally deleted a standard report.

Click the **More Options** tab at the top of the report list to access the **Reset Reports** command link. (This link also appears on the **Reporting** start page.)



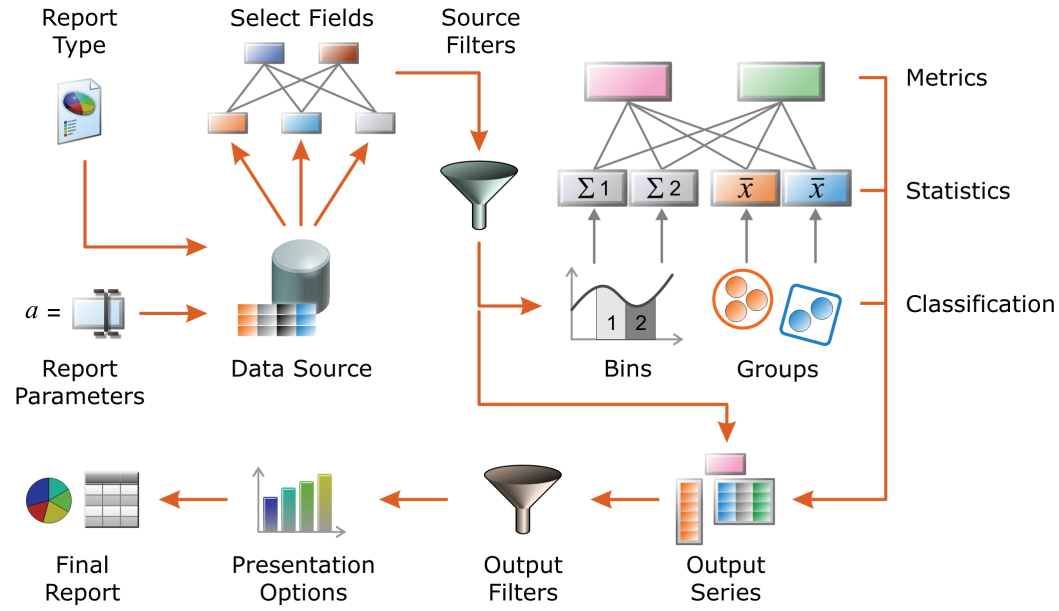
The set of default reports is displayed as a checklist, with each report shown in the list with an indicator if it has been deleted or modified from the default settings.

To restore the default settings for one or more reports, select the reports to reset and click the **Reset Reports** button.

About Custom Reports

The Report Editor is used to build a custom report. The process used to generate a report is shown in the figure below. In this diagram, the arrows represent the flow of data, while the icons represent the processing stages that the data goes through.

Figure 40 Report generation process



Starting from the top left, and working clockwise:

- The **Report Type** (**"Report Type"**) specifies the basic properties for the report.
- **Report Parameters** ("Report Parameters" in this chapter) are used as an input to the report generation process, before any data is selected.
- Report data is taken from the **Data Source** ("Data Source" in this chapter), and by selecting fields of interest ("Select Fields" in this chapter). Some fields are used directly ("source fields"), while some fields are derived from the source fields ("derived fields").
- One or more **Source Filters** ("Source Filters" in this chapter) is used to restrict which data is included in the report.
- In some reports, data is classified and grouped into **Bins** and **Groups** ("Classification Groups"). Using these classification groups allows for summary information to be calculated ("Statistics and Metrics" in this chapter).
- The result of the report is one or more **Output Series** ("Output Series" in this chapter), which can contain data from the source fields, derived fields, or the statistic and metric fields calculated from the classification groups.
- **Output Filters** ("Output Filters" in this chapter) can be used to select specific data to output from the report.
- The report itself consists of charts, tables and text content that are arranged using the **Presentation Options** ("Presentation Options" in this chapter) to yield the **Final Report** ("Final Report" in this chapter).

The data classification steps in the top right corner of the diagram are detailed in in this chapter. **See "Report History"** and **"Groups"** in this chapter. Understanding how to use bins and groups will allow you to classify related data records and extract statistics of interest from them.

Data Sources

The available data sources are:

- **Local RADIUS Accounting** – Accounting traffic consists of summary information about visitor sessions, reported by NAS devices to the application. In the RADIUS Accounting data source, each data record corresponds to a single visitor session. The data record contains information such as the start and stop times for the session, the NAS IP address, client IP address and MAC address, and statistics such as the total amount of input and output traffic and the length of the session.
- **Local Visitor Accounts** – In this data source, each data record corresponds to a single visitor account. The data record contains all the fields defined for the visitor account, including standard fields such as username, role, and expiration time, as well as any custom fields that have been defined (**See** "Customization of Fields" in the Guest Management chapter).

Binning

Binning is a classification method that converts a continuous measurement into a discrete measurement. For example, converting a time measurement into a date is a 'bin' classification, because all time measurements that are made on any particular date will fall into the same 'bin' when this classification is applied.

Binning can only be applied to numerical values, such as time measurements, traffic measurements, or the duration of a user's session, where the range of possible values is potentially unlimited.

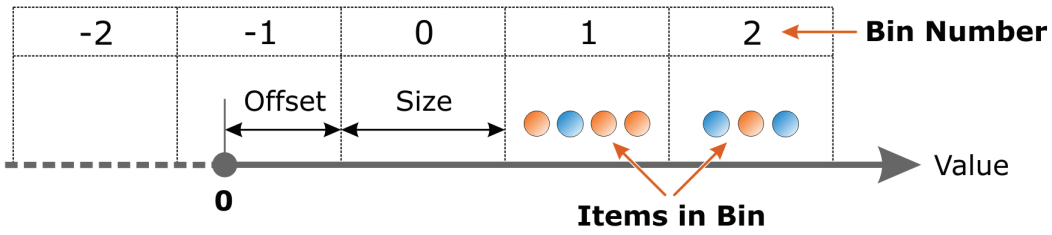
Classifying into bins is achieved by calculating a **bin number** for each item of data. The bin number is a calculation that results in related items of data being collected together. Related pieces of information may have slightly different values (for example, time measurements) but they are considered to be sufficiently the same to be placed in the same bin.

Bin numbers do not need to be consecutive numbers.

The formula used to calculate the bin number is shown in the diagram below.

Figure 41 Bin number calculation

$$Bin\ \# = \left\lfloor \frac{Value - Offset}{Size} \right\rfloor$$



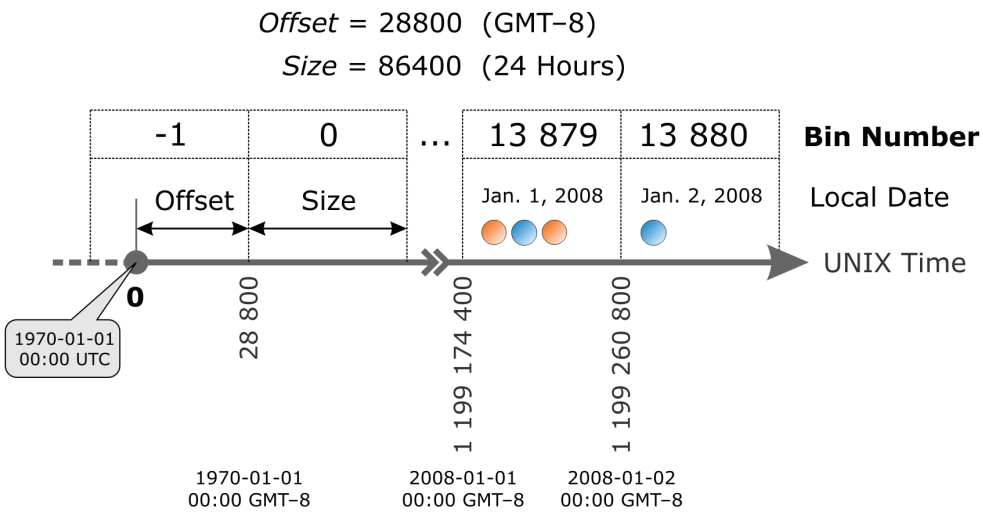
Bin classifications may be created using the report editor. **See** "Groups" in this chapter for a list of the available bin classification methods.

Binning Example – Time Measurements

The following diagram explains how to derive the offset for time bins into days, based on being west of GMT.

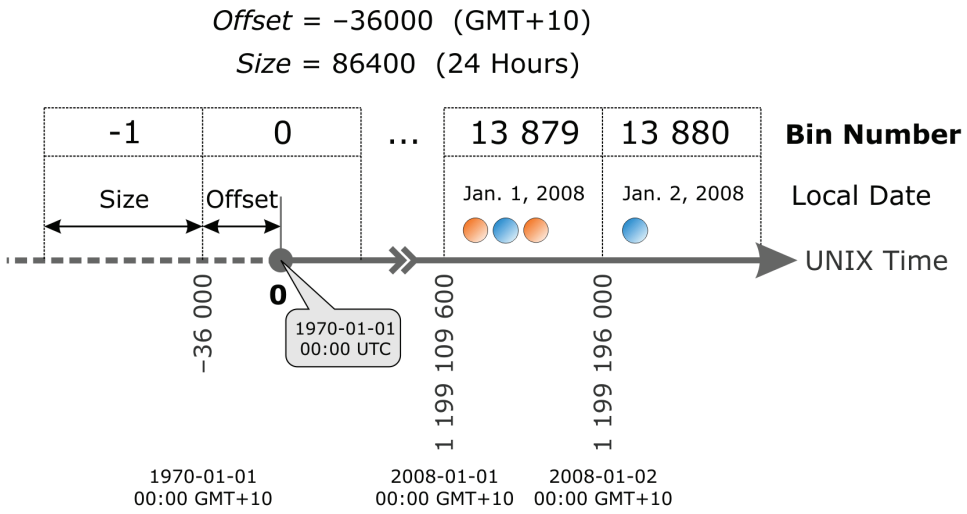
Reporting uses seconds as the time measurement. Therefore, as there are 3600 seconds in an hour, GMT – 8 makes the offset 28800 (3600 * 8).

Figure 42 Reporting – Bin west of GMT



The next diagram is similar but for time zones that are east of GMT

Figure 43 Reporting – Bin east of GMT



This process may be automated by entering an expression as the value for the time zone offset. The correct expression to use for the Bin Offset is:

```
<?= -date("Z")
```

Explanation: The PHP `date()` function returns the time zone offset in seconds when passed the "Z" format string. Because this is a positive value for east of GMT, and a negative value for west of GMT, the value is negated.

Groups

Grouping is a classification method that applies to discrete values. For example, collecting together data records that have the same username is a group classification.

Some time measurements can be grouped; for example, grouping all time measurements based on the hour of the day, or day of the week, is a group classification rather than a bin classification, as the set of values is discrete.

As in bin classifications, the group classification results in related items of data being collected together. The difference is that all the related items must have the same group value to be placed in the same group.

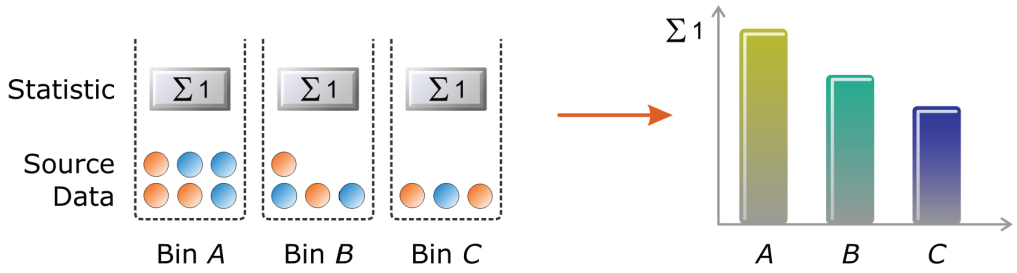
Group classifications may be created using the report editor. **See "Groups"** in this chapter for a list of the available group classification methods.

Statistics from Classification Groups

The classification groups that you define in a report will determine what type of statistics that can be derived for that report. This is shown in the following diagrams.

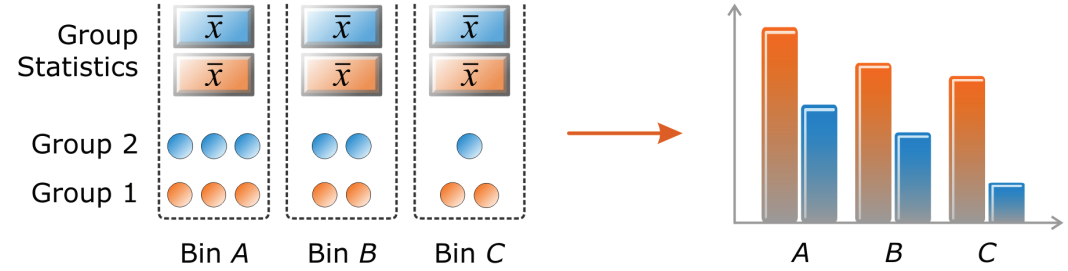
The following figure shows how statistics are calculated per bin when bins are present but groups are not present. For example, if each bin represents a different date, and the source data is a traffic measurement, then the statistic here could be the total amount of traffic per day. **See Figure 44**.

Figure 44 Reporting – Bin statistics without groups



The next figure shows statistics calculated per group when both bins and groups are present. For example, if each bin represents a different date, the source data is a traffic measurement, and the grouping is done by username, then the group statistic here is "traffic per user", and the end result is "traffic per user per day".

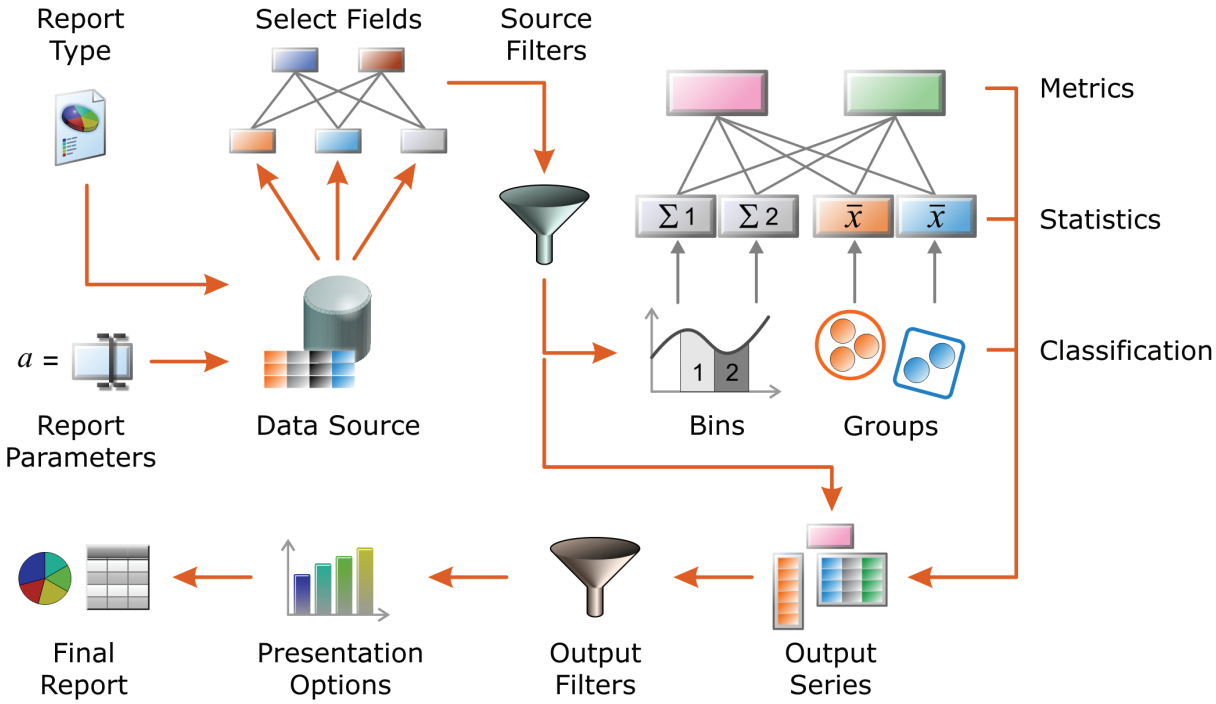
Figure 45 Reporting – Bin statistics with groups



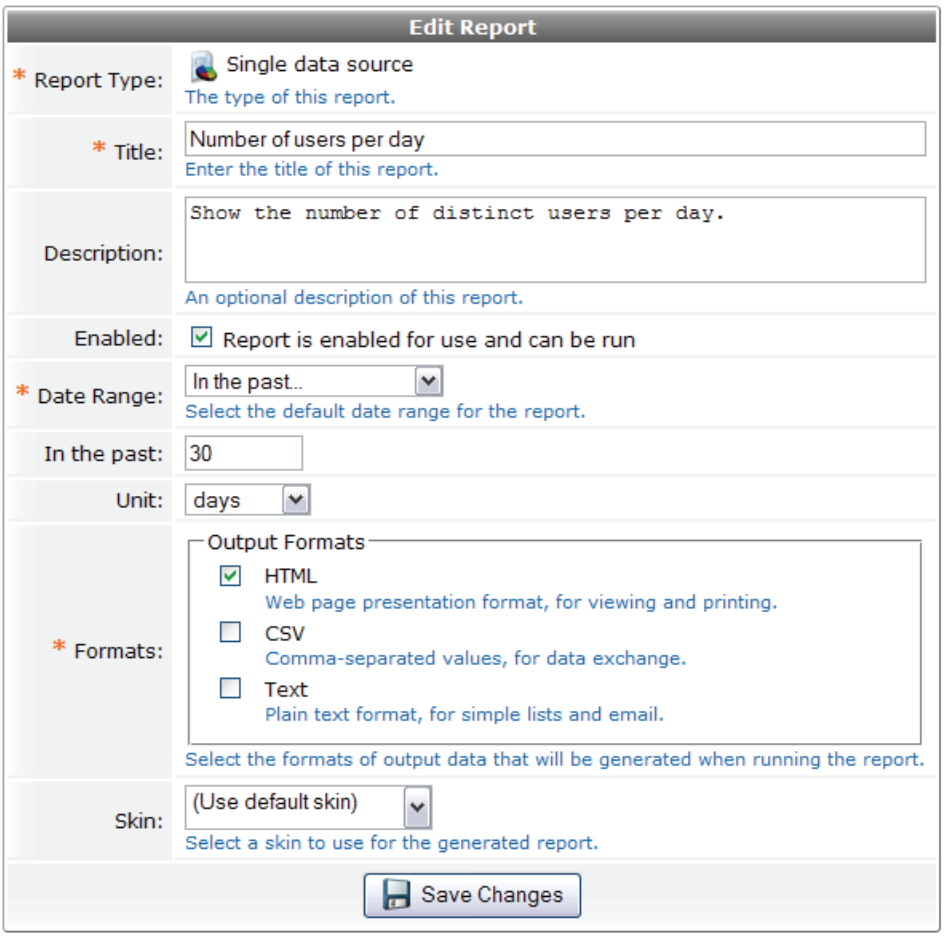
Components of the Report Editor

To create a new report using the Report Editor (shown above), start at the top left and go clockwise, following the arrows, until you have a final report.

Figure 46 *Components of the Report Editor*



Report Type



The Report Type link opens a window where you type a distinct name or Title for the report. You can add additional information in the **Description** field. This could be used to explain the purpose of the report.

While you are working on creating the report you could leave the **Enabled** field unchecked. When you want the report to be available for use, mark the Enabled check box.

You should set a default Date Range for the report. The available options are listed under the drop down menu. You are able to change the Unit for this date range to seconds, minutes, hours, weeks, months or years.

You must select one or more of the Output Formats. When the report is run, it will be generated in each of these formats.

A skin for the generated report may be selected. This skin will be used when a HTML formatted report is generated. The **(No skin)** option may be selected to use a blank template, while the **(Use default skin)** option will use the skin that is currently marked as enabled in the Plugin Manager.

Click the  **Save Changes** button to return to the Report Editor.

The selections you make in the **Edit Report** form will become the defaults used when running this report.

Report Parameters

Report parameters are fixed values defined at the start of a report run.

The value of a parameter may be obtained from the operator as input before running the report, or may be a fixed internal value that is set by the report designer.

A report parameter can be used in many places throughout the report including:

- In an expression used to calculate the value of a derived field
- As a value used in a source filter (range, match or list)
- As a value used in data classification (discrete bins)
- In an expression used to calculate a metric for the report
- As a component of an output series
- In an expression used to calculate a component of an output series
- As part of an output filter
- As text displayed in a presentation block
- As a formatting option for a chart or table

Each parameter has a name that is unique within the report. You can also attach a description to the parameter for use by the report designer.

To use a report parameter as a replacement for a field value, select the parameter from the list of fields.

To use a report parameter in a PHP expression, use the syntax `$parameter` – where the name of the parameter is preceded with a dollar sign $. All the power of PHP expressions can be used to work with the value of this parameter.

These are the places in the report where PHP expressions are used:

- Derived field expressions
- Metric field expressions
- Output series field expressions
- Advanced custom expressions for filters

These are the places in the report where template syntax may be used:

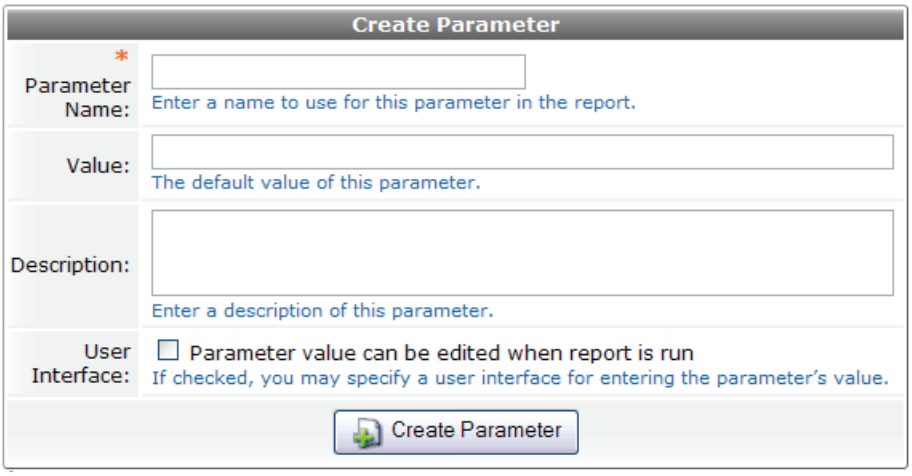
- Properties for source and output filters (range, match and list values)

- Properties for classification methods (bin size and offset)
- Properties for output series (limit and remainder category)
- Properties for individual fields within an output series (header)
- Properties for presentation blocks (container CSS style)
- Properties for table cells within a presentation block (CSS style)
- Within text presentation blocks

In these cases the report editor may simply indicate that a value is required. To use the value of a report parameter in a template, use the syntax `{$parameter}`. Standard template syntax, such as modifiers and substitutions, are available to modify the display of the parameter. See "Smarty Template Syntax" in this chapter for more information about template syntax. Some examples are given below:

- `{$parameter|strtoupper}` Substitutes the uppercase version of the parameter
- `{$parameter|default:"text"}` Substitutes the parameter, or "text" if the parameter is blank or not set
- `{if $parameter}true{else}false{/if}` Substitutes the word "true" or "false" depending on the value of the parameter

To create a parameter click the **Create Parameter** tab at the top of the Edit Parameters list view. The **Create Parameter** form will be displayed.



Parameters share the same namespace as the other types of field within the report (source fields, derived fields, statistic fields and metric fields). Choose a Parameter Name that is unique in the report.

Enter a value for the parameter in the **Value** field. This value will be substituted elsewhere in the report where the parameter is used.

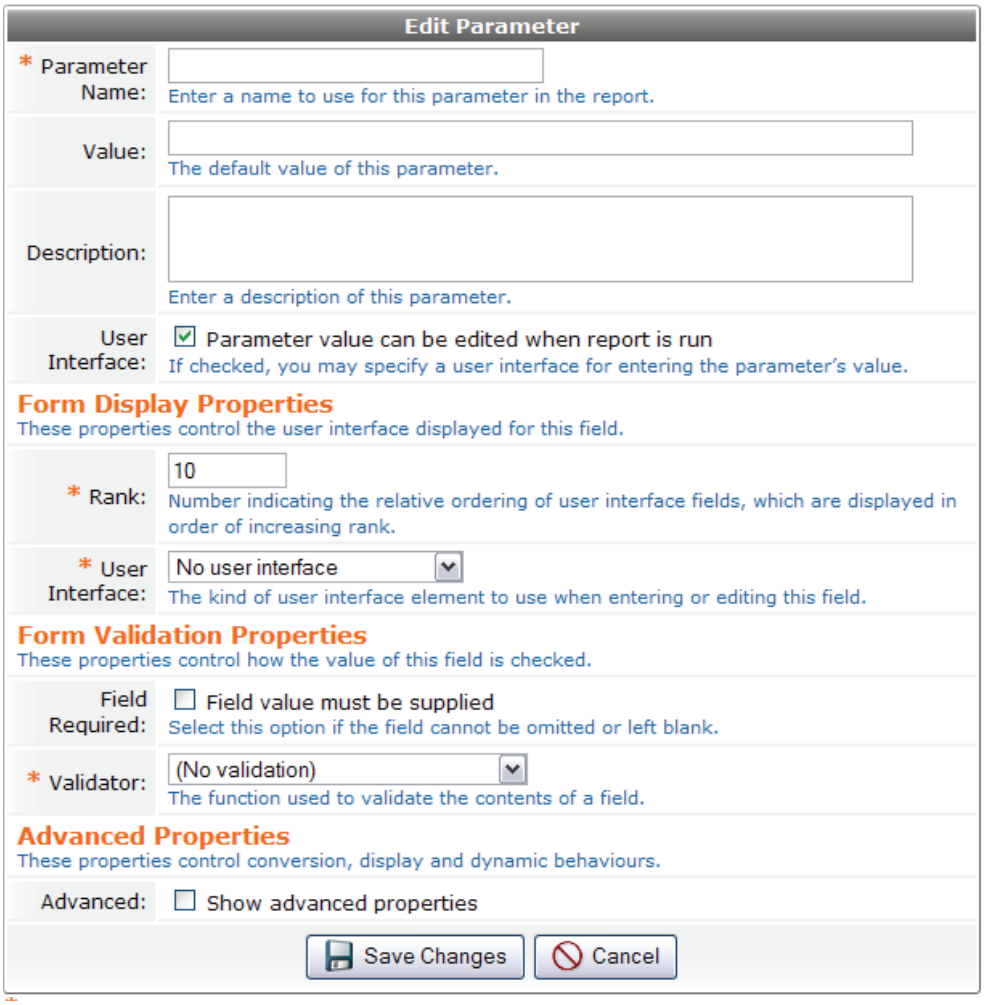
You are able to type a description of this parameter in the **Description** field.

If the value of the parameter should be obtained from the operator as input before running the report, select the User Interface check box.

Click the **Create Parameter** button to add this parameter to the report. You can create as many parameters as you need.

If the parameter should have a user interface, the **Edit Parameter** form will be displayed after clicking the **Create Parameter** button.

Parameter User Interface Editing

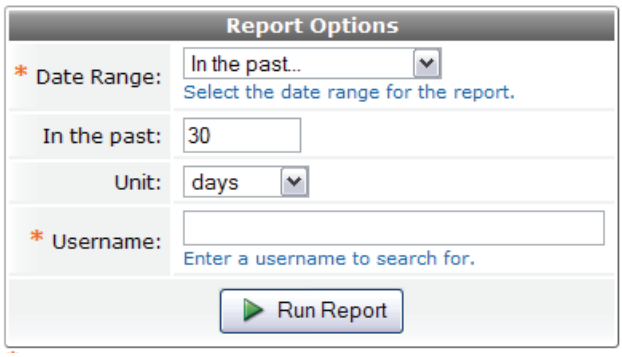


The **Edit Parameter** form is used to specify the default value for a parameter as well as the type of user interface to use for this parameter.

If **No user interface** is selected, then the parameter will have a fixed value and cannot be edited before the report is run.

Otherwise, if another type of user interface element is selected, clicking the **Run...** icon link from the list of reports will display a **Run Options** form that includes an additional user interface element that corresponds to the parameter. In this way the value for a parameter may be selected by the operator before the report is generated.

For example, to generate a report with information about a specific username, you could define a parameter **in_username** that presents a text field to the operator, as shown in the figure below.



The initial value displayed on this form for a report parameter may be specified as the Value for the parameter.

The  **Run Preview** and  **Run Default** icon links will be available for a report if all parameters have an acceptable default value. This is determined by the validation properties for each parameter. If no validation properties are specified, all parameter values are considered to be valid.

To require an operator to make a selection for a parameter, you must specify how to validate the parameter, and you should also specify a default value that is not valid according to the validation properties. When this is done, the Run Preview and Run Default links will be unavailable, and appropriate parameter values must be specified by the operator before the report can be generated. A message will be displayed in the report editor indicating that this is the case.

The options for the form display, form validation and advanced properties are similar to customizing forms in Guest Manager. See "Form Display Properties" in this chapter for information about form display properties. See "Form Validation Properties" for form validation properties, or "Advanced Form Field Properties" for advanced properties.

Data Source

You must select a data source for the report using the **Select Data Source** form. You should also select the fields that are required by the report.

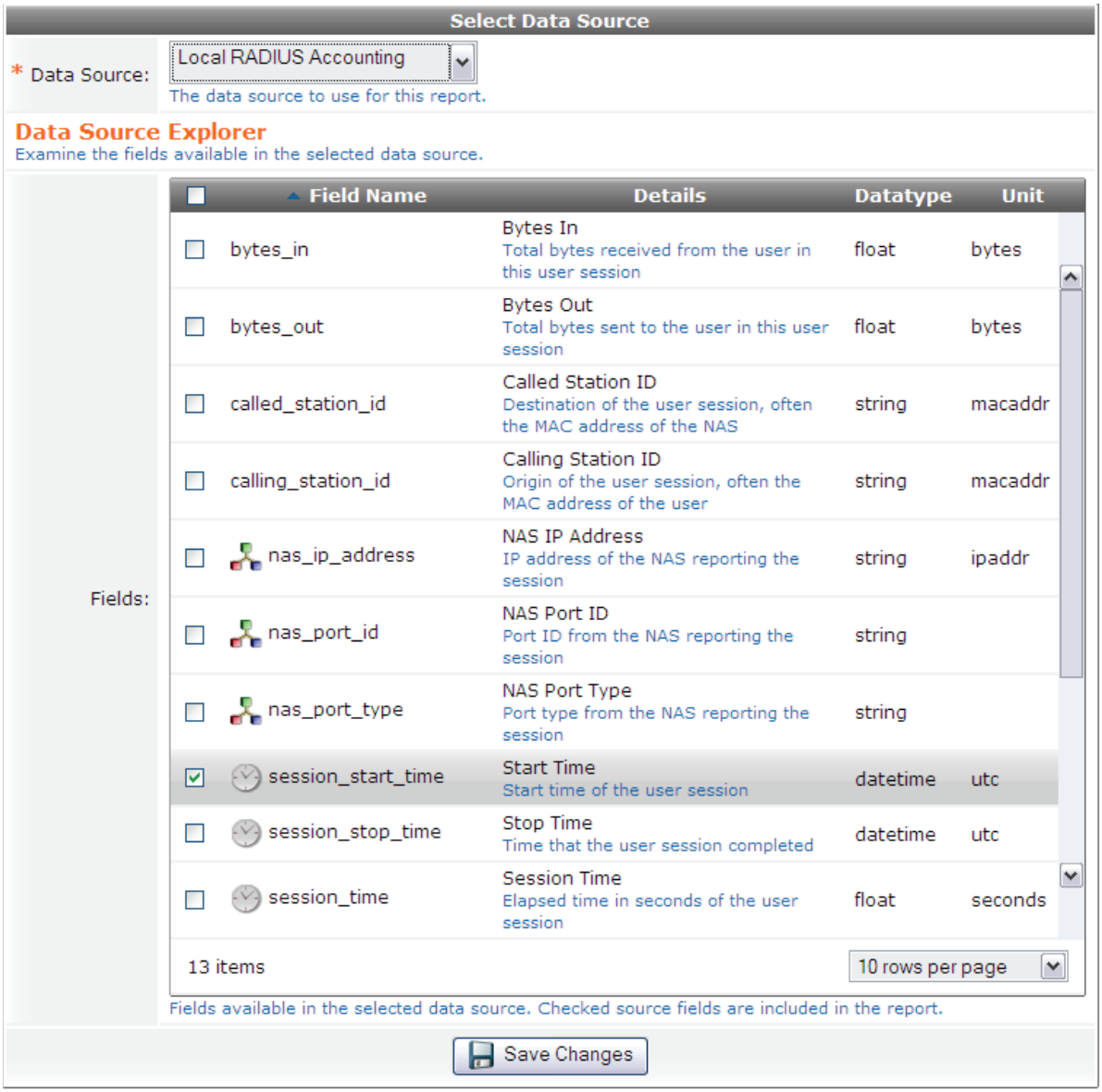
Different fields will be displayed, depending on which data source has been selected. **See "Data Sources"** in this chapter for details about the data sources that are available for use.

To select a field for inclusion in the report, mark the check box on the left hand side next to the field. You are able to select multiple fields in this window. The report is generated based on the fields that you select.

One of the selected fields must be a date/time field.

If you are building a new report by using the Create Report link, the fields you select here will be used to automatically construct an output series in the report. In this case, **Create Report: Step 2** will be displayed at the top of the page.

Returning to the **Select Data Source** form after creating a report will not automatically generate a corresponding output series for the selected fields. This means that selecting a field in the data source will not automatically add it to the output of the report; you must specify how to classify and format the data before it can be displayed in the generated report.



Click the **Save Changes** button to return to the Report Editor.

Select Fields

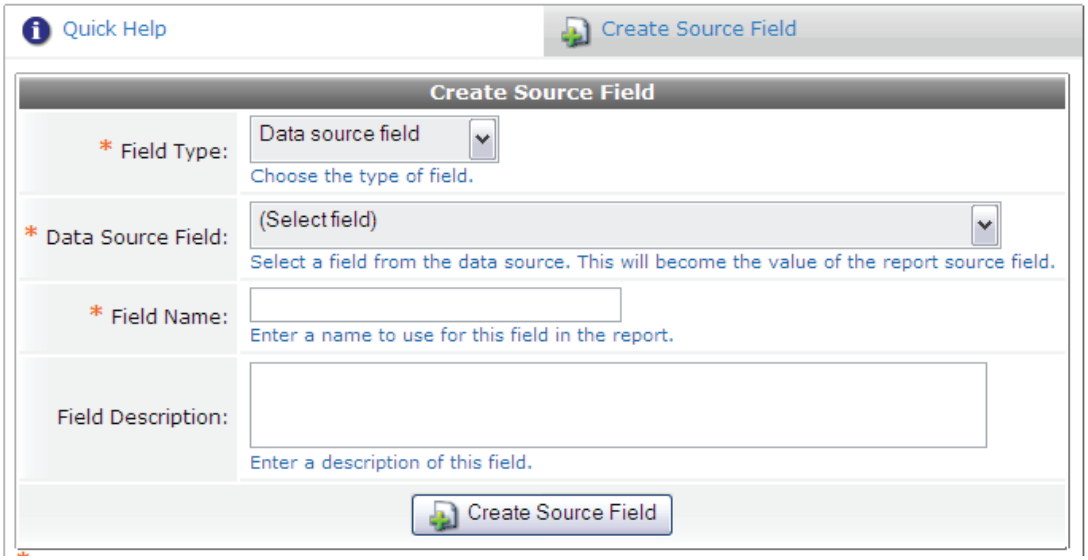
If you have not selected fields in the **Data Source** form, you must select the required source fields here. Fields can be defined one at a time by clicking the **Create Source Field** tab.

Source fields are the basic building blocks from which the rest of the report is constructed. You should add source fields for any item of data on which you want to filter; any items that must be aggregated or grouped together; or any item over which statistics are to be calculated.

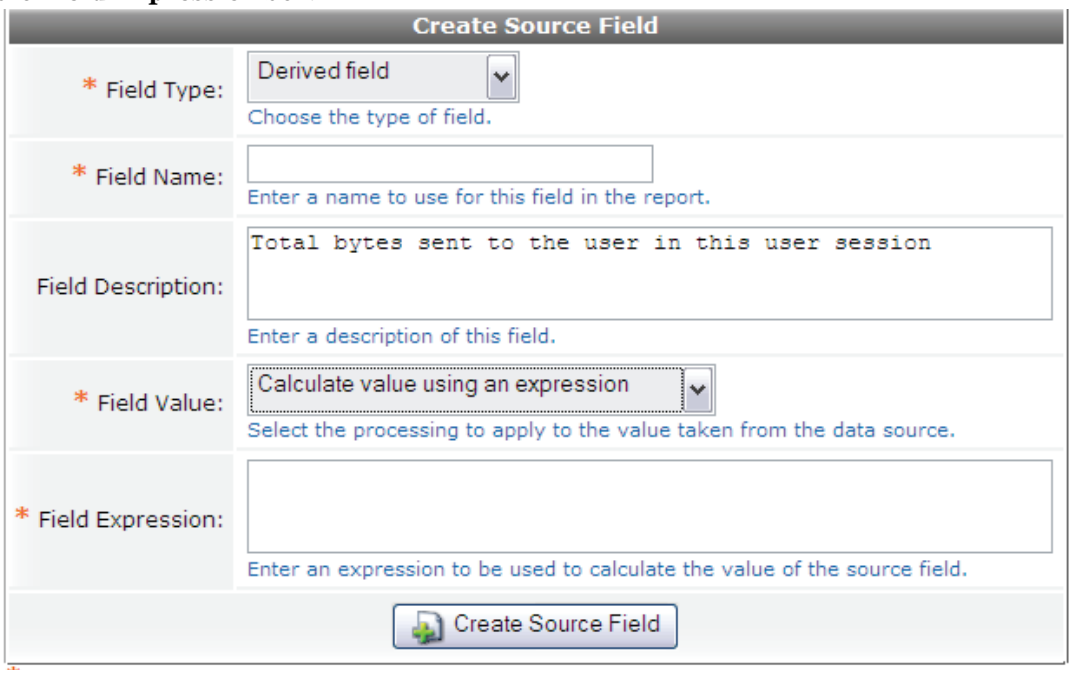
Source fields are of two kinds:

- **Data source fields** are individual items of data taken from the data source for the report. This is the smallest fundamental unit of data available in the report.
- **Derived fields** are source fields that are created from other data source fields or derived fields. A derived field is one that can be calculated for each data record selected from the data source.

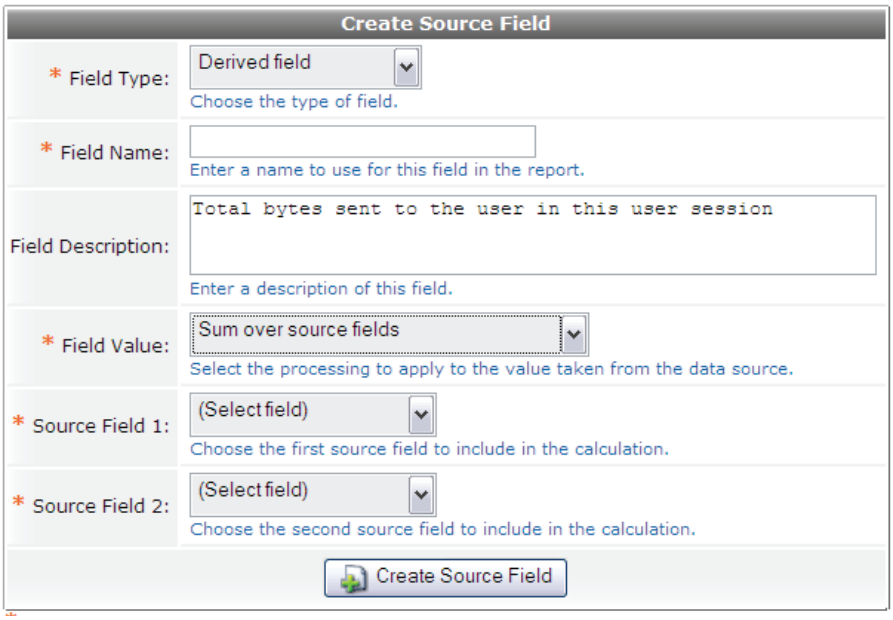
Each source field has a name that is unique within the report. You can also attach a description to the field for use by the report designer. If you select a field from the **Data Source Field** drop down list, that field name is automatically placed in the **Field Name** area. It can be changed if you want.



As derived fields do not exist in the Data Source, you will need to give each field a unique name. You are also required to give the field a value. This can be by calculating a value using a PHP expression entered in the **Field Expression** box.



If you select to calculate a value by summing over source fields, you are required to nominate the fields to be summed.



Click the **Create Source Field** button to create the source or derived field in the report.

Source Filters

Source filters are applied to the data source fields to determine whether a data record will be included for processing in the report. The statistics, metrics and output data of the report can only be generated from source data that has passed through the source filters.

You should define source filters to specify what parts of the input data you are interested in.

The first source filter has a special property. When a report is run, the time range for the report is calculated and is set as the minimum and maximum values for the range of the first source filter. This allows the time range for a particular report to be easily specified when a report is run (for example, by selecting the “last month” option for the report range). When running a report, you can also select specific date and time values for the start and end of the report, which will become the minimum and maximum values for the first source filter.

You should ensure that the first source filter is applied to a time field, in order to maintain this expected behavior of the report.

The remaining source filters are ordered, which means these filters will always be applied in the same order to each data record.

You can reorder the filters to obtain precise control over exactly which data will be included in the report.

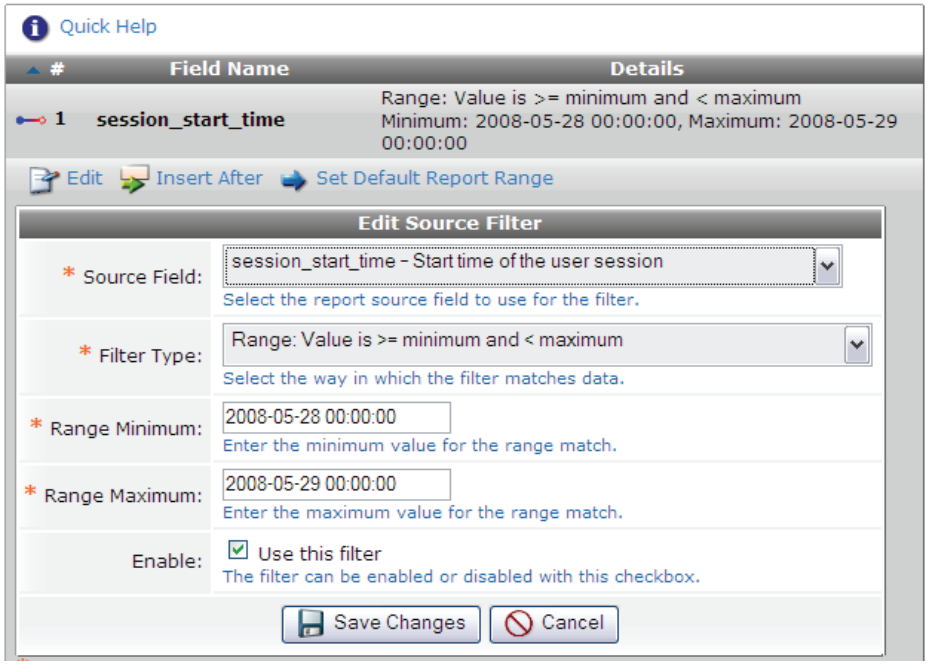
Source filters are of three basic kinds:

- **Range** filters check to see if the data value falls within a certain range.
- **Match** filters check if the data value matches a particular condition, which could be a regular expression or other match value.
- **List** filters check to see if the data value is found in a list.

As one of the selected fields is a date/time field, this is automatically set as the first source filter for you.

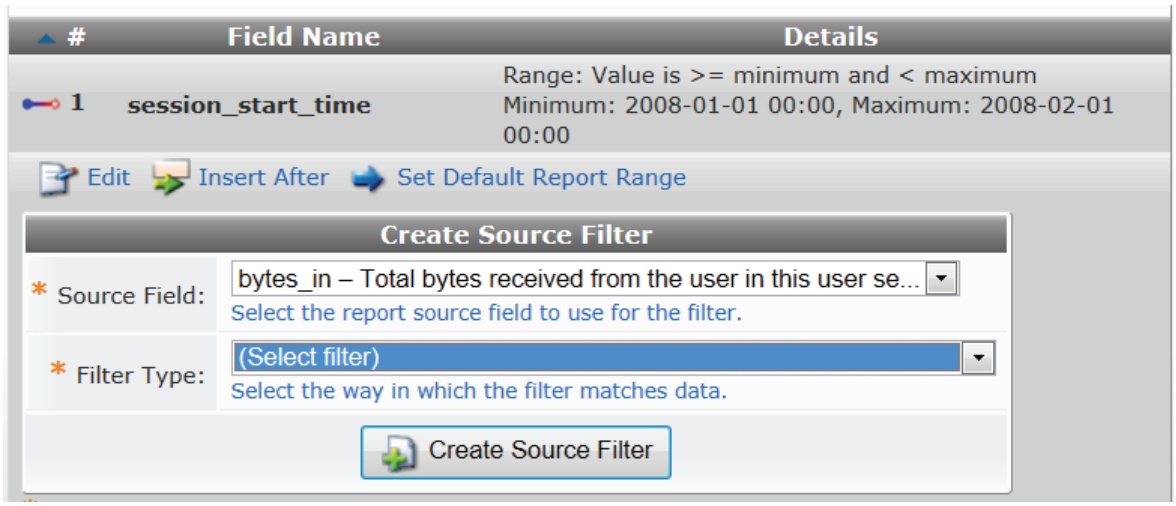
To add additional filters, click the first source filter. An action row is displayed with **Edit** and **Insert After** links. There is also a **Set Default Report Range** option for the first date/time filter.

The **Edit** link allows you to alter the options for the source filter as well as being able to disable the filter.



Click the **Save Changes** button to keep any changes you have made.

The **Insert After** link allows you to create additional filters.



You are required to select a field from the **Source Field** drop down list. This displays a list of the fields that you previously created in the **Data Source** or the **Select Fields** sections of the Report Editor.

You must then select the filter from the **Filter Type** drop down list. The following options are available:

- List: Value is not one of a list
- List: Value is not one of a list (case sensitive)
- List: Value is one of a list
- List: Value is one of a list (case sensitive)
- Match: Value does not match regular expression
- Match: Value does not match regular expression (case sensitive)
- Match: Value matches regular expression
- Match: Value matches regular expression (case sensitive)
- Match: Value is equal to
- Match: Value is equal to (case sensitive)
- Match: Value is not equal to
- Match: Value is not equal to (case sensitive)
- Range: Value is > minimum and < maximum
- Range: Value is > minimum and <= maximum
- Range: Value is >= minimum and < maximum
- Range: Value is >= minimum and <= maximum

Additional options are displayed depending on the filter type – list, match or range. Complete the form by entering appropriate options for use by the filter.

Click the **Create Source Filter** button to add this filter.

Classification Groups

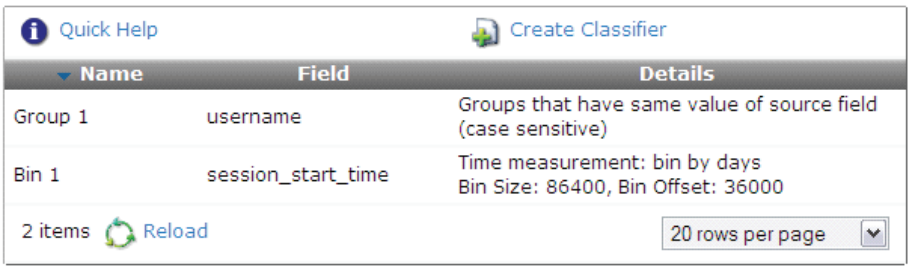
Classification groups are ways of collecting together groups of related input data records.

Often, the purpose of a report is to discover any underlying patterns or trends in the data. This can usually be done by looking at the raw data of the report, subdividing it into various groups of related data, and then analyzing the groups using statistics and graphs to identify the desired features.

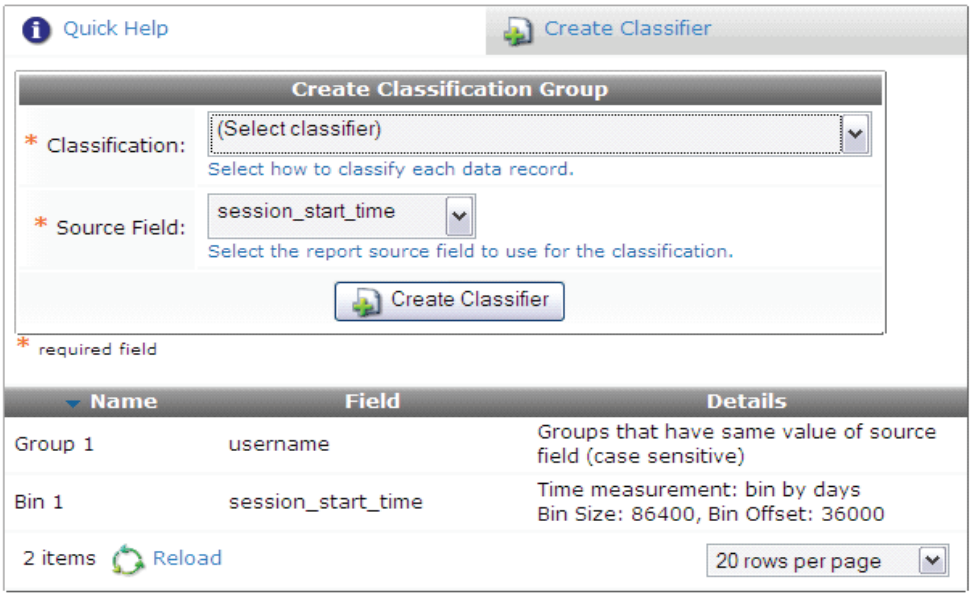
Classification groups perform the task of grouping related input data into sets, which makes it possible to calculate statistics over the items of interest.

There are two types of classification groups:

- **Bins** are classification methods that convert a continuous measurement into a discrete measurement. For example, converting a time measurement into a date is a 'bin' classification, because all time measurements that are made on any particular date will fall into the same 'bin' when this classification is applied. Binning applies to numerical values only, such as time measurements, data traffic measurements, or the duration of a user's session, where the range of possible values is potentially unlimited. **See "Data Sources"** in this chapter for more information about bin classifications.
- **Groups** are classification methods that apply to discrete values. For example, collecting together data records that have the same username is a group classification, as is grouping based on just the first letter of the username. Some time measurements can be grouped; for example, grouping all time measurements based on the hour of the day, or day of the week, is a group classification rather than a bin classification, because the set of possible values is fixed. **See "Groups"** in this chapter for more information about group classifications.



To create a bin or a classification group, click the **Create Classifier** tab in the Edit Classification Groups list view.



You are required to choose the classification method and the Source Field to use for the classification.

NOTE

The **Create Classifier** tab can be accessed from the Classification, Bins or Groups options in the Report Editor.

The available classification methods are explained below:

- **Discrete bins from start and stop values** – **See "Data Sources"** in this chapter for a bin number formula description. The bin classification requires two source fields from a data record. The bin formula is applied to both source field values to obtain start and stop bin numbers. The data record is classified with each bin number between the start and stop numbers, inclusive of the endpoints of the range. The bin offset is used to account for time zones. See "Binning Example – Time Measurements" in this chapter for a description.
- **Discrete bins from value of source field** – See "Data Sources" in this chapter for a bin classification description. The bin classification method applies the bin number formula, described in the , to the value of the source field to calculate a bin number for the data record.
- **Groups that have same value of source field** – This group classification method collects together all data records that have the same value for the specified source field, ignoring case.
- **Groups that have same value of source field (case sensitive)** – This group classification method collects together all data records that have the same value for the specified source field.

- **Time measurement: bin by days** – See "Binning Example – Time Measurements" in this chapter for the bin classification method description. The bin classification method uses the specified date/time field to calculate a day number. Times that fall within the same day are assigned the same bin number. The bin offset is used to account for time zones as explained in the .
- **Time measurement: bin by hours** – This bin classification method uses the specified date/time field to calculate an hour number. Times that fall within the same hour are assigned the same bin number.
- **Time measurement: bin by months** – This bin classification method uses the specified date/time field to calculate a year and month number. Multiple months may be grouped together by specifying a bin size greater than 1; for example, to bin by quarters of the year, use 3 for the bin size. Times that fall within the same month or group of months are assigned the same bin number.
- **Time measurement: bin by weeks** – This bin classification method uses the specified date/time field to calculate a week number. Times that fall within the same week are assigned the same bin number.
- **Time measurement: group by day of the month** – This group classification uses the specified date/time field to calculate the day of the month from 1 to 31. This is used as the group number, which collects together all data records that have the same day of the month.
- **Time measurement: group by day of the week** – This group classification uses the specified date/time field to calculate the day of the week, from 0 to 6 where 0 is Sunday and 6 is Saturday. This is used as the group number, which collects together all data records that have the same day of the week.
- **Time measurement: group by hour of the day** – This group classification uses the specified date/time field to calculate the hour of day, from 0 to 23 where 0 is midnight, 12 is midday and 23 is 11 pm. This is used as the group number, which collects together all data records that have the same hour of the day.
- **Time measurement: group by month of the year** – This group classification uses the specified date/time field to calculate the month of the year, from 1 to 12 where 1 is January and 12 is December. This is used as the group number, which collects together all data records that have the same month of the year.

The remaining options in the form will change depending on your selection. See "Resetting Report Definitions" in this chapter for more information about binning and grouping classification methods.

Click the **Create Classifier** button to define the classification group in the report.

Statistics and Metrics

Statistics are fields with values that are calculated from a group of source fields. For example, the total sum of all fields in a particular group would be a statistic field.

Define statistic fields for any item of data over which you want to calculate some kind of summary information, such as a count, sum or average.

To select which classification group to use for a statistic or metric field, consider which items you want to calculate across. This is called a 'dimension' of the report. To calculate a single statistic for all the items in a particular group, select that group as the classification group. To calculate a single statistic over all the items in the report, select the 'All data' dimension of the report.

There is a close relationship between statistics and classification groups. In general, you should define classification groups to define how you want to break up the report data, then define statistic fields to extract the desired information about those groups.

Metrics are fields with values calculated from other statistics. For example, converting a total sum to a cost by multiplying by a rate would be a metric field.

Define metric fields to calculate quantities that are related to the report statistics, such as averages, costs or performance measurements.

To derive a metric from one or more statistics, the metric must be calculated using the same dimension of the report as for the statistics.

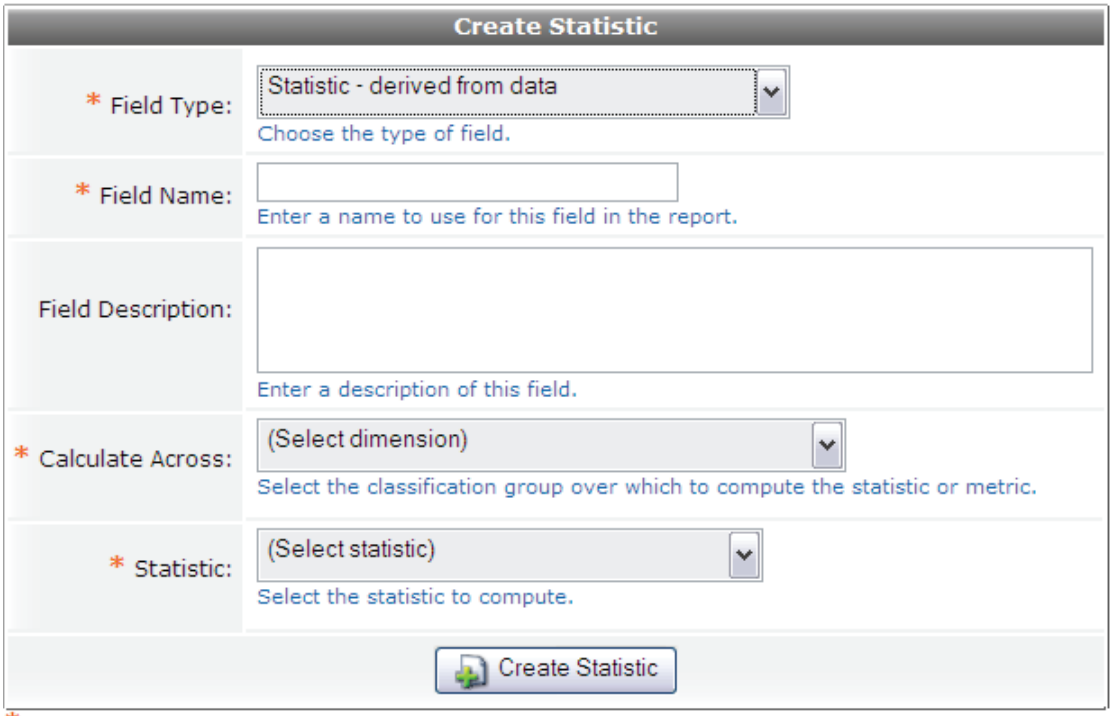
Like the statistic fields, metrics share a close relationship with the report's classification groups. When designing a report, consider the metrics that you would like to generate, and work backwards to determine the statistics you will need in order to calculate each metric and the classification groups will be needed to calculate each statistic.

Each statistic and metric field has a name that is unique within the report. You can also attach a description to the field for use by the report designer.

When designing the structure of the report, it may help to consider these questions:

- *What is the metric supposed to tell me?* (Indicates the field name and description.)
- *Is the metric a single value, or a collection of values?* (Indicates if the metric's dimension is 'All data', or another classification group.)
- If a collection of values – what is the common property that each value shares? (Indicates the structure of the classification group.)
- *What is the underlying data that is being summarized?* (Indicates the type of statistic or metric, and the source fields to consider.)
- *How is the metric calculated from the underlying data?* (Indicates the metric expression, or statistic computation method.)

To create a statistic or a metric, click the **Create Statistic** tab at the top of the Edit Statistics list view.



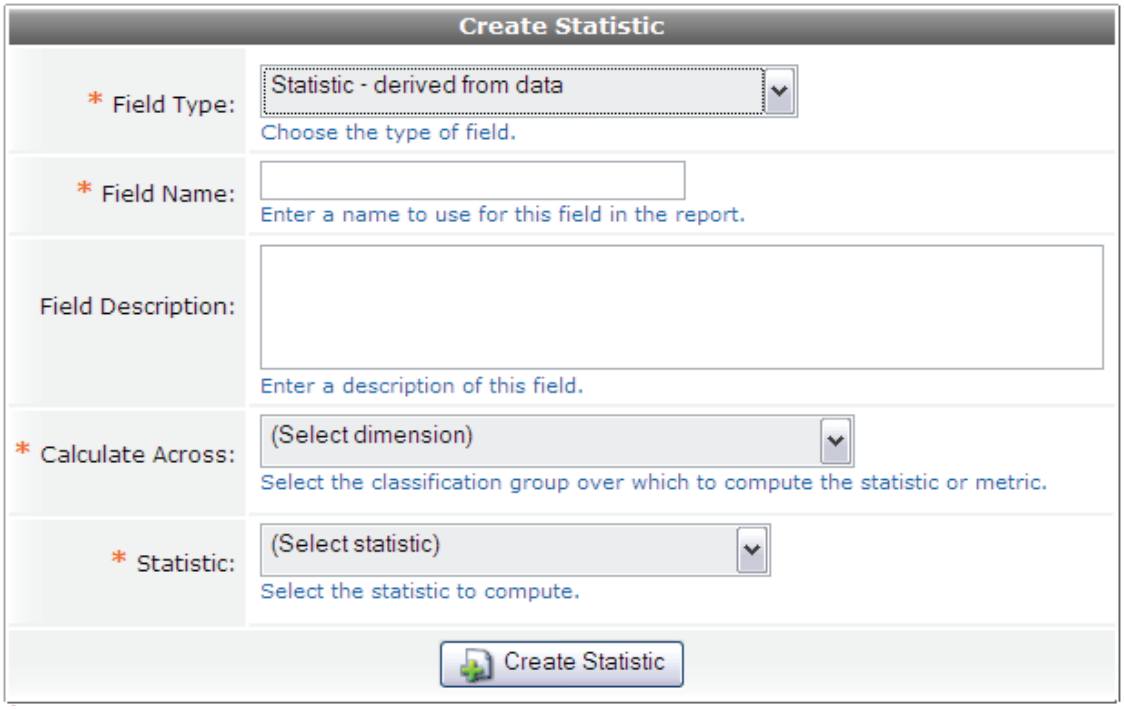
The **Field Type** parameter determines whether you are creating a statistic or a metric. If you are creating a statistic for the report, you must enter a field name. This cannot be a name of an existing field or parameter. You are also required to enter how this statistic is to be calculated. This is specified in the **Calculate Across** field.

The type of statistic is then selected from the **Statistic** drop down list, which is one of the following options:

- **Average value** – the average value of the source field over the selected classification group is calculated
- **Maximum value** – the maximum value of the source field over the selected classification group is calculated

- **Median value** – the median (middle) value of the source field over the selected classification group is calculated
- **Minimum value** – the minimum value of the source field over the selected classification group is calculated
- **Number of bins** – the number of different bin classification groups is calculated
- **Number of distinct values** – the number of distinct values that the source field takes over the selected classification group is calculated
- **Number of groups** – the total number of classification groups in all bins is calculated
- **Number of values in a particular group** – the total number of items in a specified classification group is calculated
- **Sum of values** – the sum of all values of the source field over the selected classification group is calculated

The form is slightly different if you select to create a metric.



The **Field Type** parameter must be changed to **Computed metric** and the Field Name must be unique. You should select what data the metric is to be calculated over in the Calculate Across field.

The type of metric can be one of:

- **Add (value 1 + value 2)** – the values are added
- **Average value** – the average value of the statistic field over the selected report dimension is calculated
- **Divide (value 1 ÷ value 2)** – the values are divided
- **Maximum value** – the maximum value of the statistic field over the selected report dimension is calculated
- **Median value** – the median (middle) value of the statistic field over the selected report dimension is calculated
- **Minimum value** – the minimum value of the statistic field over the selected report dimension is calculated
- **Multiply (value 1 × value 2)** – the values are multiplied

- **Number of distinct values** – the number of distinct values that the statistic field takes over the selected report dimension is calculated
- **Subtract (value 1 – value 2)** – the values are subtracted
- **Sum of values** – the sum of all values of the statistic field over the selected report dimension is calculated
- **Use an expression to calculate value** – a PHP expression is used to calculate a value for the metric over the selected report dimension from one or more statistic fields

Value 1 and Value 2 list the fields previously created in the report. Unless you are using an expression to calculate the metric, you are required to select the fields for Value 1 and Value 2.

Click the **Create Statistic** button to create the statistic or metric field in the report.

Output Series

A report has one or more output series, which contain the data tables generated from the input data and statistics calculations in the report.

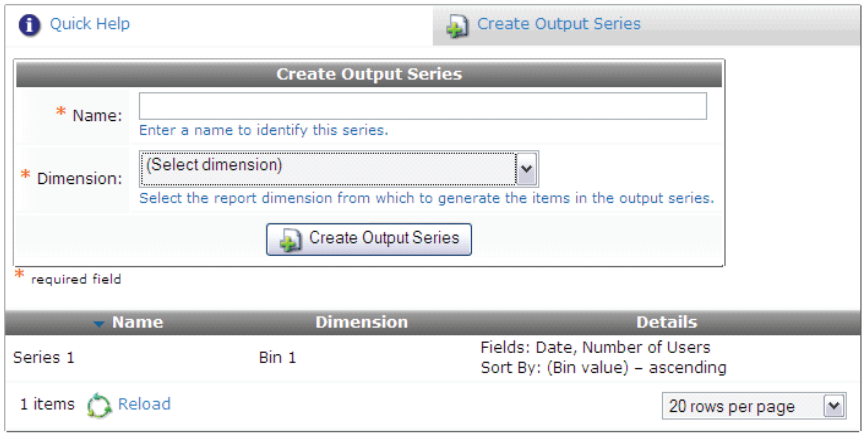
An output series is used by the output filters and presentation blocks defined in the report. Each output series can have multiple fields within it; the fields within the output series can also perform basic calculations and formatting on the data to be output.

For each output series, one item in the series is generated for each item in the selected 'dimension' of the report. For example, the report might define a group which contains sets of related input records; this group is a dimension of the report. A statistic can be defined in that dimension that is computed for each group, across all of the input data in each set. An output series for that dimension can include the statistic calculated for each group set, but cannot include the original data (as there might be more than one data record in each group).

As another example, consider the same report with a group definition and a statistic calculated in that dimension of the report. An output series for the 'Source data' dimension of the report can include a field for the statistic calculated in each group; this may produce duplicate copies of the statistic in the output series, because it will be included for each group item that has the statistic, and there may be multiple group items used to calculate the statistic.

You should define the report's output series according to how you want to collect and organize the input data and the calculated statistics for display. To generate a report containing a table or graph of data, you should define an output series that contains the fields that are to be displayed.

Click the **Create Output Series** tab at the top of the Edit Output Series list view to create an output series in the report.

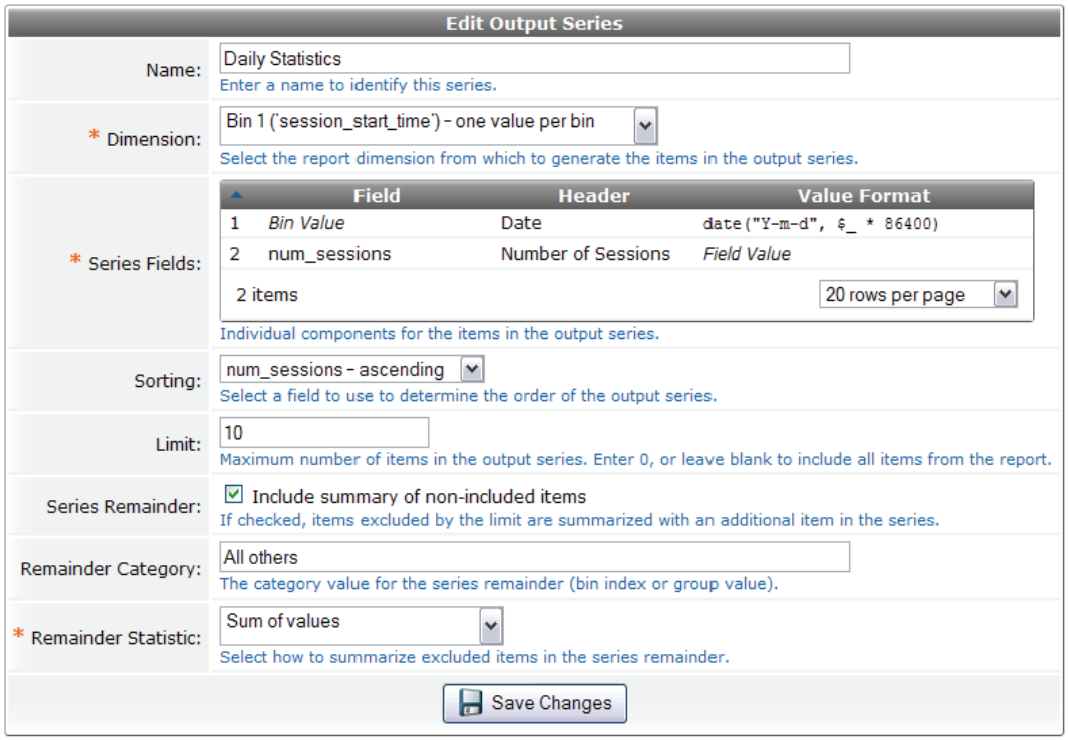


You are required to enter a unique name for this output series. You must also select the Dimension to be used. This could be the source data or one of the classification groups defined in the report.

Click the **Create Output Series** button to add the output series definition to the report. The **Edit Output Series** form will then be displayed to allow the components of the output series to be defined.

Output Series Fields

The **Edit Output Series** form is used to define the components and properties of an output series.



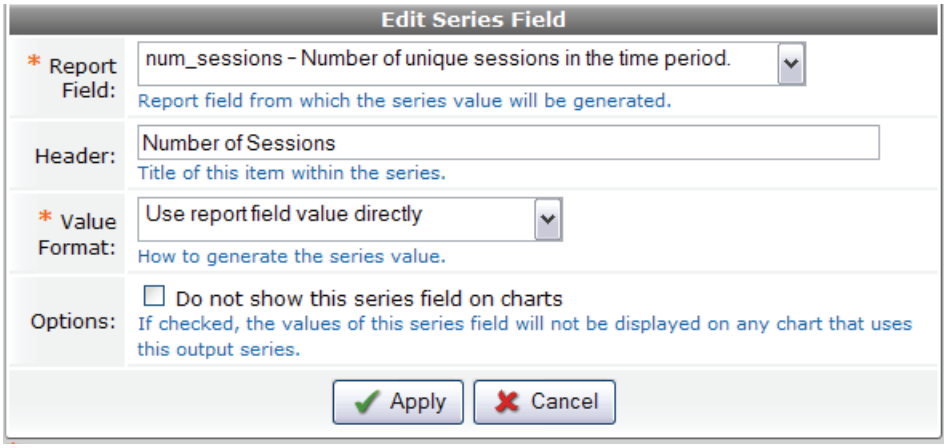
The list of series fields will highlight any invalid field names with a red border. Fields may be marked as invalid because they are not available for the selected output series dimension or because they have been deleted from the report definition.

The order in which you select output fields is significant, because table and chart presentation blocks will display the fields of an output series in order. You may reorder the fields by using the **Move Up** and **Move Down** links. To insert a new field into the output series, select an existing field and click either the **Insert Before** or **Insert After** links.

An output series may be sorted in ascending or descending order by selecting the appropriate option in the **Sorting** drop-down list.

If you also specify a value for the Limit, you can create an output series that contains only the “Top X” or “Bottom X” items. In this case, you may select the **Include summary of non-included items** check box to add a “remainder” row to the output series that summarizes all the remaining items in a single entry.

To edit an output series field, click the **Edit** link for the field. The **Edit Series** field opens, as shown below.



The Header is displayed in tables and charts that use this output series. Use a short description of the values contained in this field.

The Value Format specifies how to generate the value for the output series field. You can specify an expression to calculate the value; in the expression, use the variable `$_` to obtain the value of the report field for this output series.

In most cases it is not necessary to perform data formatting for the fields in the output series, as this is normally achieved in the report's presentation blocks. Use a value expression only if the actual value to be displayed should be modified (for example, converting from bytes to megabytes), or if the underlying format of the value should be changed (for example, converting from a bin number to a date).

Select the **Do not show this series field on charts** check box to prevent the display of the series field on charts. This option is useful if the same output series is used in two presentation blocks, one being a chart showing summary data and the other being a table showing detailed statistics.

Output Filters

Output filters are applied to the output series defined in the report to determine whether a particular item will be included in the output of the report. The presentation blocks of the report can only include the output data that has passed through the output filters.

You should define output filters to specify what parts of the output data you are interested in looking at. You can also define output filters to specify what output data should be excluded from the report.

Output filters can filter on either unformatted source data or formatted output data. Unformatted source data is the data used to generate the output series; depending on the dimension of the output series, this may include either raw source data and derived fields or statistic and metric fields. Formatted output data is the actual content of the output series after any data processing has been applied in the output series definition.

Use filtering based on unformatted source data to exclude output series items based on a certain data field, statistic or metric value in the data. Use filtering based on the formatted output series to exclude output data based on group or bin values, as these typically need to be formatted before they are of use.

The output filters are ordered, which means the filters will always be applied in the same order to each item of the output series.

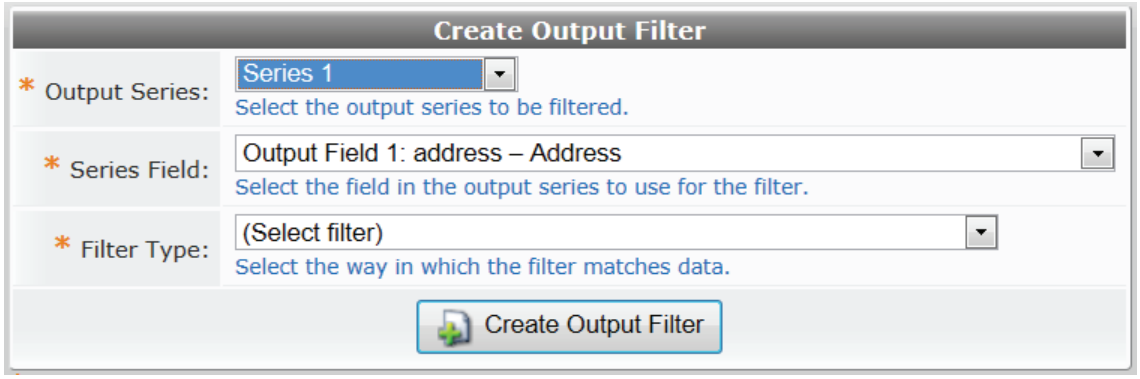
You can reorder the filters to obtain precise control over exactly which data will be included in the report's output.

Output filters are of three basic kinds:

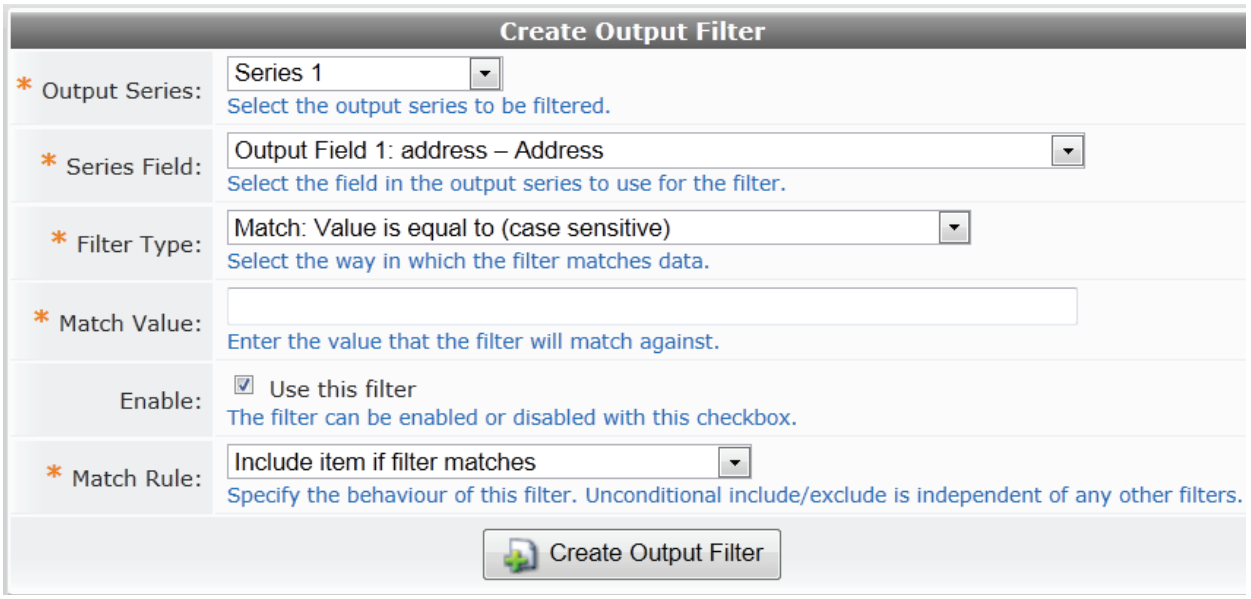
- **Range** filters check to see if a value falls within a certain range.

- **Match** filters check if a value matches a particular condition, which could be a regular expression or other match value.
- **List** filters check to see if a value is found in a list.

Click the **Create output filter** link to create an output filter.



Select the output series you want to filter in order to view the remaining filter options.



You can select any of the source fields that would be available to the output series, or any of the fields in the output series. This allows output filtering to be performed based on either the report data store, or the output series data.

The types of output filter that are available are the same as used in the source filters. **See "Source Filters"** in this chapter for details about the types of filter that are available.

The Match Rule allows you to construct more complex filtering rules. You can choose from the following matching rules:

- **Include item if filter matches** – If the filter matches the item in the output series, the item will be included. The remaining filters will be applied in order.
- **Exclude item if filter matches** – If the filter matches the item in the output series, the item will not be included. The remaining filters will be applied in order.
- **Unconditionally include item if filter matches** – If the filter matches the item in the output series, the item will always be included in the output. No further filters will be applied to the data once this filter has matched.

- **Unconditionally exclude item if filter matches** – If the filter matches the item in the output series, the item will never be included in the output. No further filters will be applied to the data once this filter has matched.

Click the **Create Output Filter** button to add the new output filter to the report definition.

Presentation Options

The Presentation Options provide you with a number of choices regarding the final presentation of your report.

The presentation blocks of the report define the visual appearance of the report, such as what data to display and how to display it.

There are three different types of presentation block:

- **Chart** presentations allow an output series to be shown graphically using different styles of graph. (For details, **See** **"Chart Presentations"** in this chapter.)
- **Table** presentations list the contents of an output series in a formatted table. (For details, **See** **"Table Presentations"** in this chapter.)
- **Text** presentations are blocks of text included in the report. You may insert the values of metrics or perform custom processing to include the output data from the report in the text. For details, **See** **"Text Presentations"** in this chapter.)

Presentation blocks are included in the final report in the order they are defined.

Chart Presentations

A chart presentation block displays the values of an output series graphically. Charts are only displayed in reports where the HTML output format is selected. Charts are not supported in CSV or plain text reports.

The chart is displayed within a HTML ** ** container element. The styles applied to this element may be specified. For example, to align the chart with the center of the page, use the container style `text-align: center;`

Most of the chart options are used to control the visual appearance of the chart. You can specify layout options, chart colors and opacity, line widths and styles, font size, axis formatting options, and more.

Different types of chart are supported, including:

- Line
- Pie
- Pie 3-D
- Column
- Stacked Column
- Floating Column
- Column 3-D
- Stacked Column 3-D
- Parallel Column 3-D
- Bar
- Stacked Bar
- Floating Bar
- Area
- Stacked Area
- Candlestick

- Scatter
- Polar

In general, the first field in the output series is used as the category values for the chart. The second and subsequent fields are used as the values to display on the chart.

The Pie and Pie 3-D charts support only a single data point for each category value. A pie chart is used to compare the relative proportions of different values in a single data series.

The Floating Column and Floating Bar charts require two data points for each category value. The data points are the high and low values for each category (in that order).

The Candlestick chart requires four data points for each category value. The data points are the maximum, minimum, open and close value for each category (in that order).

The Scatter chart allows plotting of one or more data series consisting of (x, y) pairs. This chart requires that the category values alternate between x and y coordinates.

Table Presentations

A table presentation block displays the value of an output series in a formatted table.

For reports generated using the HTML output format, you may specify the table's alignment relative to the page and any styles that should be applied to the table.

The table may be displayed in one of two ways. Assuming the output series dimension covers three values (A, B and C), the default table layout will displays the output series fields organized by columns:

Table 30 *Default Table Layouts*

Field 1, value A1	Field 1, value B1	Field 1, value C1
Field 2, value A_2	Field 2, value B_2	Field 2, value C_2
Field 3, value A_3	Field 3, value B_3	Field 3, value C_3

If you select the **Transpose table** check box, the columns and rows will be interchanged, which results in the following layout:

Table 31 *Transposed Table Layouts*

Field 1, value A1	Field 2, value A2	Field 3, value A3
Field 1, value B_1	Field 2, value B_2	Field 3, value B_3
Field 1, value C_1	Field 2, value C_2	Field 3, value C_3

Transposed tables are recommended if the output series will contain more than a few values, as in the default layout the table will end up containing more columns than rows, making it more difficult to read.

Text Presentations

A text presentation block may be used to insert template code into the generated report. The template for the text presentation block is evaluated when the report output is generated. See "Smarty Template Syntax" in the Reference chapter for details about the template syntax that is supported.

The default reports include a standard header block for generated reports using the syntax:

```
{include file=report_template_header.html}
```

This standard header includes the report title, the time at which the report was run, and the date range included in the report.

The variables available for use in the template include any of the parameters defined in the report, as well as the following special variables:

Table 32 *Template Variables*

Variable	Description
$_data	Data store for this report instance; **See** "Report Preview with Debugging" in this chapter for information about the structure of this variable
$_format	Name of format of this report instance ("CSV", "HTML", "Text")
$_info	Information about the report run
$_options	Miscellaneous options for report generation
$_report_id	ID of the report
$_report	Report definition
$_report.desc	Description of the report
$_report.structure	Report structure definition; describes the fields, filters, classification groups, output series and presentation blocks that make up the report
$_report.title	Title of the report
$_skin_id	Skin ID to use for presentation (set to false if no skin is selected, or if the format is not HTML)
$_timestamp	Timestamp of this report instance

Final Report

You are able to view the final report by clicking on the Final Report option. The report is displayed in a new window.

If the report has not met your expectations, you are able to return to the Report Editor by closing the final report window. Changes can then be made in the appropriate area of the Report Editor.

Creating Reports

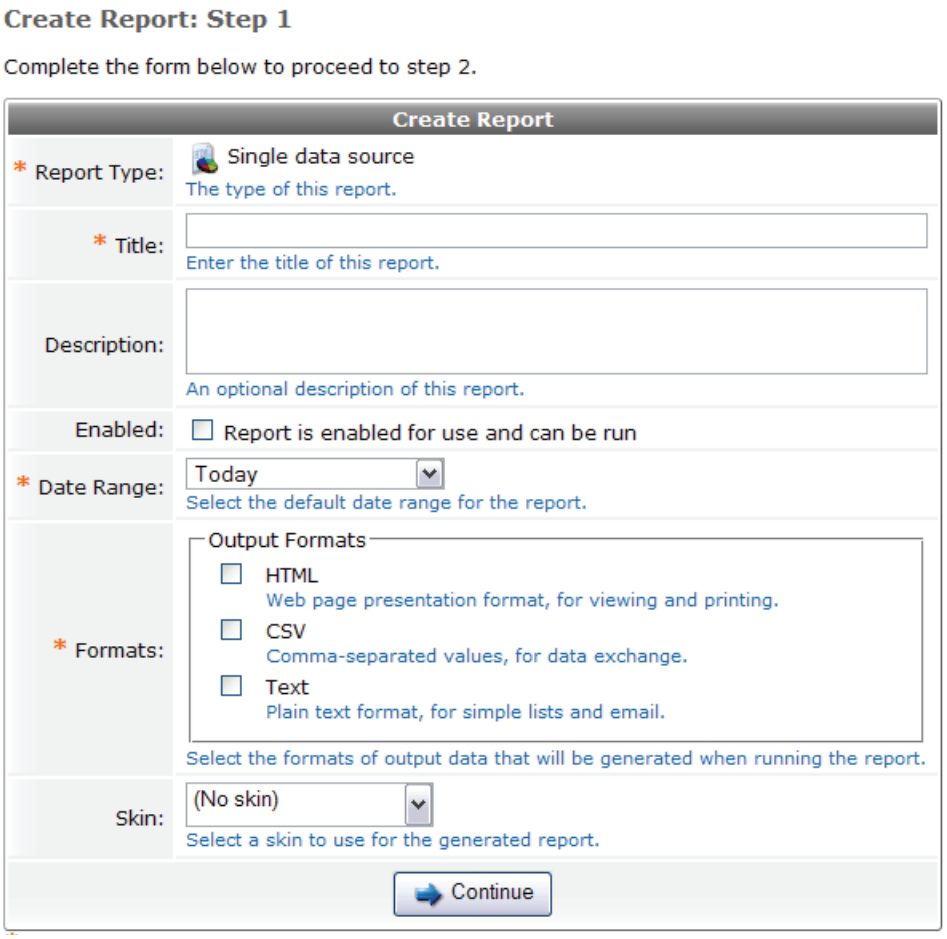
You can create a report by clicking the Report Manager's **Create New Report** command link on the **Reporting start** page.

Using this command link creates a basic data report for the specified time range, and for the specified data fields.

The report editor may then be used to further customize the report by defining new filters, classification groups and output series.

Creating the Report – Step 1

The following form will be displayed when the **Create New Report** link is clicked.



This is the same form that you would obtain if you clicked the Report Type option in the Report Editor. **See "Report Type"** in this chapter for more details about this form.

Click the **Continue** button to move to Step 2.

Creating the Report – Step 2

In step 2, the **Select Data Source** form is displayed.

This is the same form that you would obtain if you clicked the **Data Source** option in the Report Editor. See "Data Sources" in this chapter for more details about this form.

When you are first creating a report, the fields you select here will be used to automatically construct an output series in the report. The output series will be for the Data dimension of the report and will include all the fields selected in step 2. This allows you to create simple reports that list the available data without additional processing. You can then use this basic report to define additional filters, classification groups, output series and presentation blocks to generate summarized data of interest to you.

Click the **Save Changes** button to continue to the Report Editor.

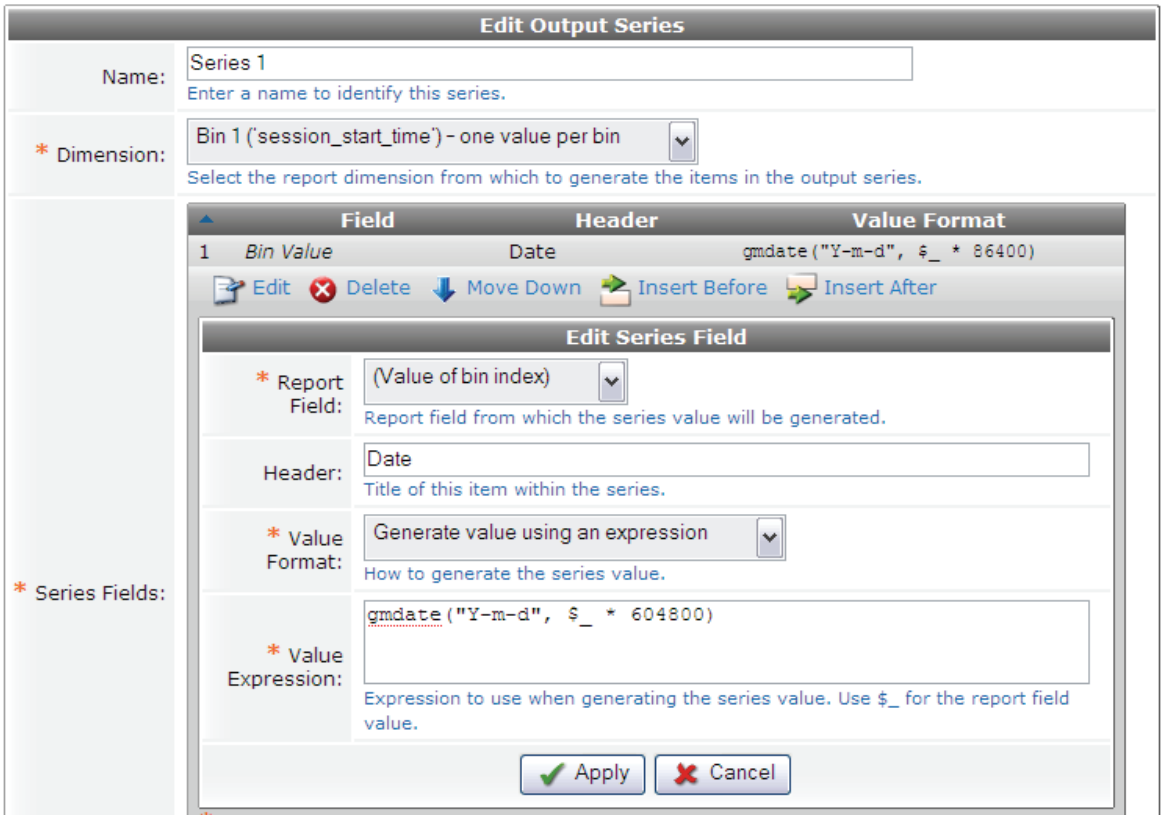
Creating Sample Reports

Report Based on Modifying an Existing Report

This sample involves modifying the predefined Number of users per day report to report on the number of users per week.

1. Select the "Number of users per day" report.
2. Click the **Edit** link. This opens the Report Editor.
3. Click Report Type in the Report Editor, as you need to change the title of the report to "Number of users per week". Because you want to report on weekly data, the date range should also be changed to a figure that is divisible by 7. To see the last 6 weeks of user numbers, enter **42** for the date range.
4. Click the **Save Changes** button to return to the Report Editor.
5. Click the Classification option in the Report Editor. The Bin classification needs to be changed from days to weeks. This is done by clicking on the Bin and then clicking the **Edit** button.
6. The Classification method should be changed to **Time measurement: bin by weeks**. The Bin Offset may be changed to suit your time zone, **See "Binning Example – Time Measurements"** in this chapter for more information.
7. Click the **Save Changes** button.
8. Click the **Back to report editor** link to return to the Report Editor.

Click the Output Series option because you need to change the formula to calculate in weeks instead of days. This means changing the expression to multiply by 604800, as shown in the screen below.



Click the **Apply** button to make your changes take effect.

Click the **Save Changes** button at the bottom of the window to save the changes to the output series.

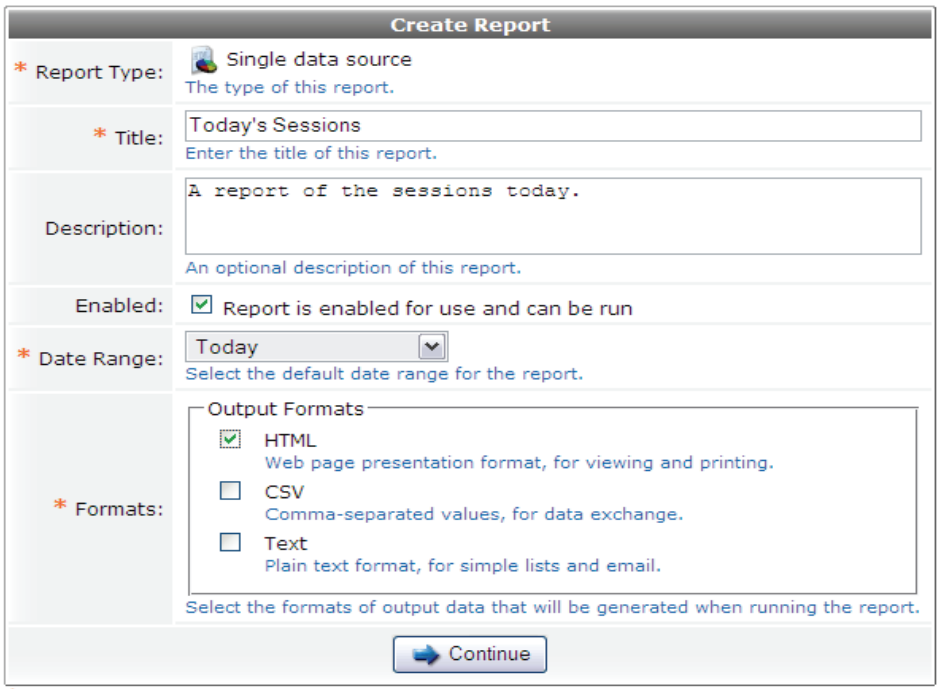
Click the **Back to report editor** link to return to the Report Editor.

Click **Final Report** to run the report and verify the changes you have made.

Report Created from Report Manager using Create New Report

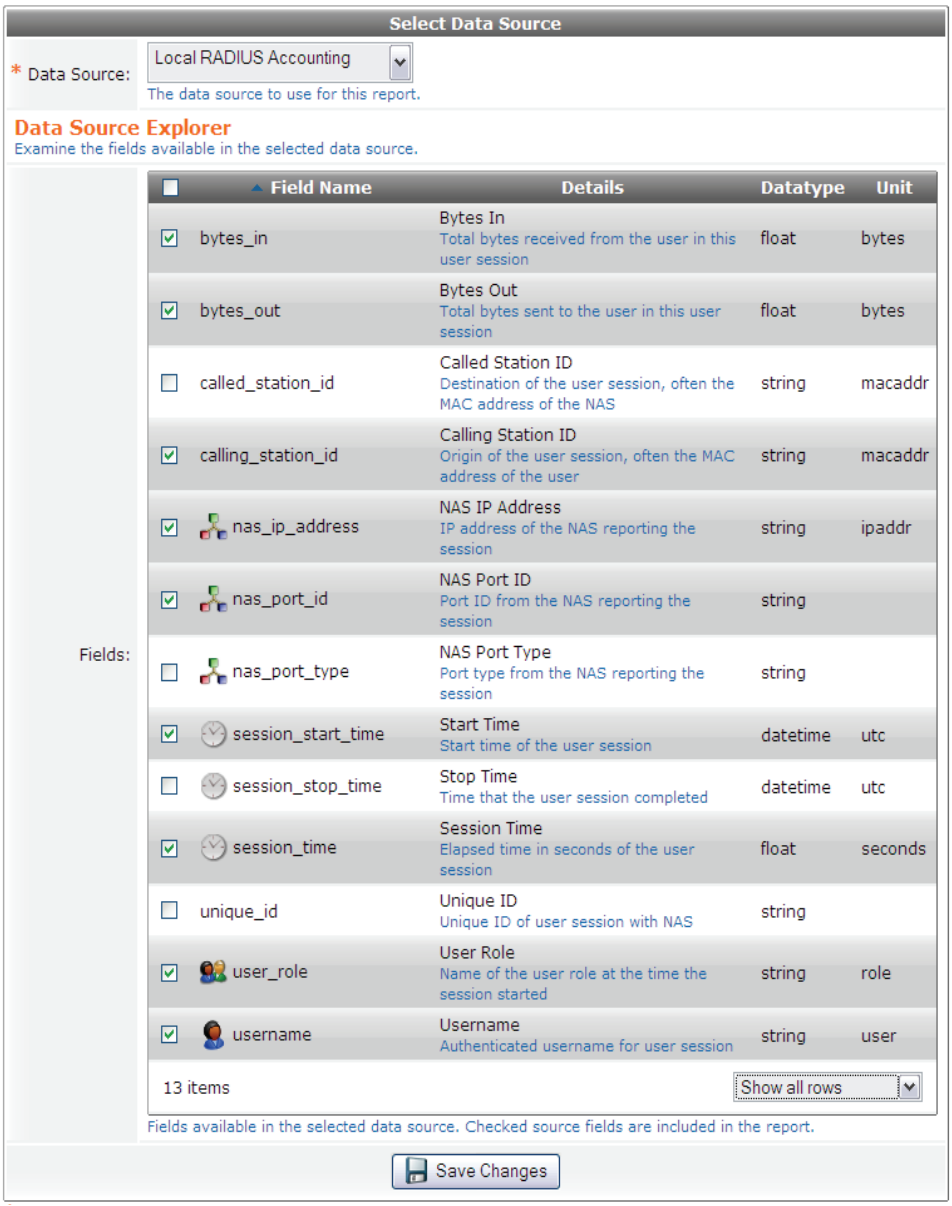
To create a report that lists today's user sessions, follow this process.

1. To create a new report without it being based on an existing report, click **Create New Report**.
2. You must give the report a Title. For this report, **Today's Sessions** would be an appropriate name.
3. Enable the report by marking the Enabled check box.
4. Ensure that the Date Range is Today and select an Output Format. These changes are shown in the screen below.



5. Click the **Continue** button to move to Step 2.

6. Select the required fields in Step 2. For this report the fields are shown in the screen below. These are the fields of interest for the report.



7. Click the **Save Changes** button to have the report created. The Report Editor screen is displayed.
8. If you click the Final Report option in the Report Editor you can see the report as it is after these two steps.

Today's Sessions

Report generated at 2008-05-29 14:31:43

Date range: **Today** (2008-05-29 00:00:00 to 2008-05-29 14:31:43)

Bytes In	Bytes Out	Calling Station ID	NAS IP Address	NAS Port ID	Start Time	Session Time	User Role	Username
7,929	278,825	00-17-31-47-DD-23	192.168.88.13	21	2008-05-29 00:45:39+09	1,926	Guest	demo6018@example.com
951,112	21,906,354	00-17-31-38-49-13	192.168.88.12	19	2008-05-29 01:10:32+09	29,002	Contractor	demo0177@example.com
416,399	12,542,501	00-17-31-CF-58-9D	192.168.88.12	3	2008-05-29 05:31:44+09	23,886	Contractor	demo1600@example.com
104,467	725,507	00-17-31-A8-32-B6	192.168.88.12	2	2008-05-29 11:41:42+09	5,457	Contractor	demo2363@example.com
183,424	3,753,684	00-17-31-75-77-9E	192.168.88.12	18	2008-05-29 11:54:33+09	28,337	Employee	demo5425@example.com

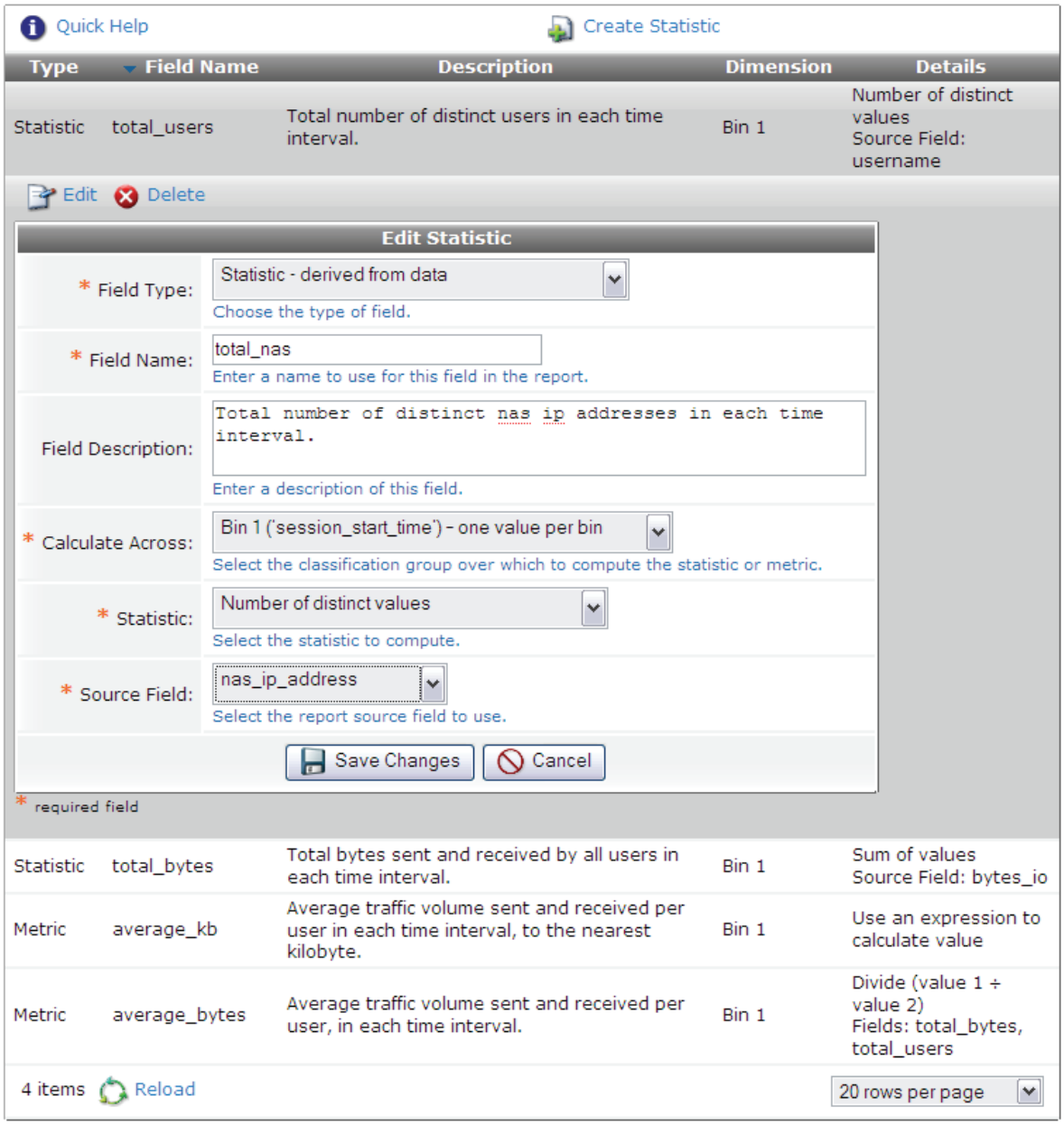
9. You can continue to further enhance this report using the Report Editor. To change the formatting of the table you would use the Presentation Options; to remove a column you would use the Output Series option; to restrict the data in the table you would use a filter, for example, a source filter to limit by NAS IP address; a classification group would enable you to carry out statistical analysis, for example, grouping by NAS IP address.

Report Created by Duplicating an Existing Report

To create an Average Traffic Volume per NAS report by duplicating the Average Traffic Volume per User report, you would need to do the following.

1. Select the **Average traffic volume per user** report from the list of reports.
2. Click the **Duplicate** link. This creates a copy of the report which will be titled **Copy of Average Traffic Volume per User**.
3. Click the **Copy of Average Traffic Volume per User** report.
4. Click the **Edit** link to open the Report Editor.
5. Click **Report Type** in the Report Editor. You need to change the name of the report and its description. The new report will be called “Average traffic volume per NAS”.
6. Click the **Save Changes** button to return to the Report Editor.
7. Click **Data Source** in the Report Editor. Ensure that you have the correct fields selected. For this new report you need to select the **nas_ip_address** field. You may also want to deselect the **username** field as it will no longer be used.
8. Click the **Save Changes** button to return to the Report Editor.
9. Click **Statistics** in the Report Editor. The **total_users** field needs to be changed to reflect the change in the report. You may also want to alter the field description.
10. Click the **total_users** field and then click the **Edit** link.

11. The Source Field will be changed to **nas_ip_address**, as this report is to calculate the average traffic by NAS rather than the average traffic by user. The field will also be renamed to **total_nas** to reflect the new value it will contain. These changes are shown in the screen below.



12. Click the **Save Changes** button.
13. Because the **total_users** field is no longer available in the report, the **average_bytes** field must be updated to refer to the **total_nas** field instead. Click the **average_bytes** field, and then click the **Edit** link. Change Value 2 to **total_nas**.
14. Click the **Save Changes** button.
15. Click the **Back to report editor** link to return to the Report Editor.
16. Click **Output Series** in the Report Editor. Select Series 1. The description should be changed. Click the **Edit** link and then click the **average_kb** row.
17. Click the **Edit** link. The Header should be changed to read “NAS Average Traffic (KB)”.
18. Click the **Apply** button.
19. Click the **Save Changes** button at the bottom of the window to save the changes to the output series.

20. Click the **Back to report editor** link to return to the Report Editor.

21. As there are no further changes required, click the **Final Report** icon to preview your new report.

Report Troubleshooting

Report Preview with Debugging

If you are experiencing problems with your report, you can receive help with the Report Diagnostics. The diagnostics run the report and show you the internal data that is being used to generate the contents of the final report.

The report data store contains all the source data records, organized by classification group, as well as the statistics and metrics calculated from this data.

The report's output series and presentation blocks are generated from the contents of the data store, so if you are not getting the results you expect from the report, this could be because the data store either does not contain the right data, or does not contain the right classification groups. Examining the data store will help you find the cause of the problem.

No Classification Groups

When there are no classification groups, the report data store is a simple list of the source data.

```
array (
  0 => first data record
  1 => second data record
  ...
)
```

Classification Using Either Bins or Groups

When using either bins or groups, the report data store is indexed by the bin or group number, then the bin or group value.

```
array (
  0 => /* bin or group 0 */
  array (
    123 => /* bin or group value: 123 */
    array (
      0 => first data record
      1 => second data record
      ...
    ),
    234 => /* bin or group value: 234 */
    array (
      /* bin items */
    )
  ),
  1 => /* bin or group 1 */
  ...
)
```

Classification Using Both Bins and Groups

When using both bins and groups, the report data store is indexed first by bin and then by group.

```
array (
  0 => /* bin 0 */
  array (
    123 => /* bin value: 123 */
    array (
```

```
      0 => /* group 0 */
      array (
        'a' => /* group value: 'a' */
        array (
          0 => first data record
          1 => second data record
          ...
        ),
      ),
    ),
    234 => /* bin value: 234 */
    array (
      /* bin items organized by group */
    )
  ),
  1 => /* bin 1 */
  ...
)
```

Troubleshooting Tips

The following tips may be useful to you when developing new reports.

- **Draw a diagram** – Make a sketch of any charts or tables you want to include in the report. Identifying the necessary contents will help you to select the right data source fields, classification groups and output series.
- **Examine similar reports** – When creating a new report, look at the structure of the predefined reports in order to find a similar report.
- **Ensure you have a time source field** – The first input filter is always used to restrict the time range of the report to an interval that is specified by the user. You must therefore select a time field from the data source to be able to do this filtering.
- **Use only one classification group** – Multiple bin and group classification groups can be defined, but this can complicate the report's structure unnecessarily. To build an easily understood and maintainable report, stick to a single classification bin or group, or the combination of a single bin with a single group.
- **Remove unnecessary fields** – Each record from the data source will have a value for each of the data source fields and derived fields stored in the report data store. When looking at moderate to large data sets, you should remove fields that are not used anywhere in the report. This will improve the speed of the report.
- **Reduce amount of data** – When developing a new report, you may find the process easier if you select a small set of data to use. For example, choose one specific date for the range of the report in the report editor. This will allow you to develop the basic structure of the report. Once you have defined the structure, you can increase the amount of data in the report and shift your focus to the output formatting options.

The Administrator module provides tools used by a network administrator to perform both the initial configuration and ongoing maintenance of ClearPass Guest.

Accessing Administrator

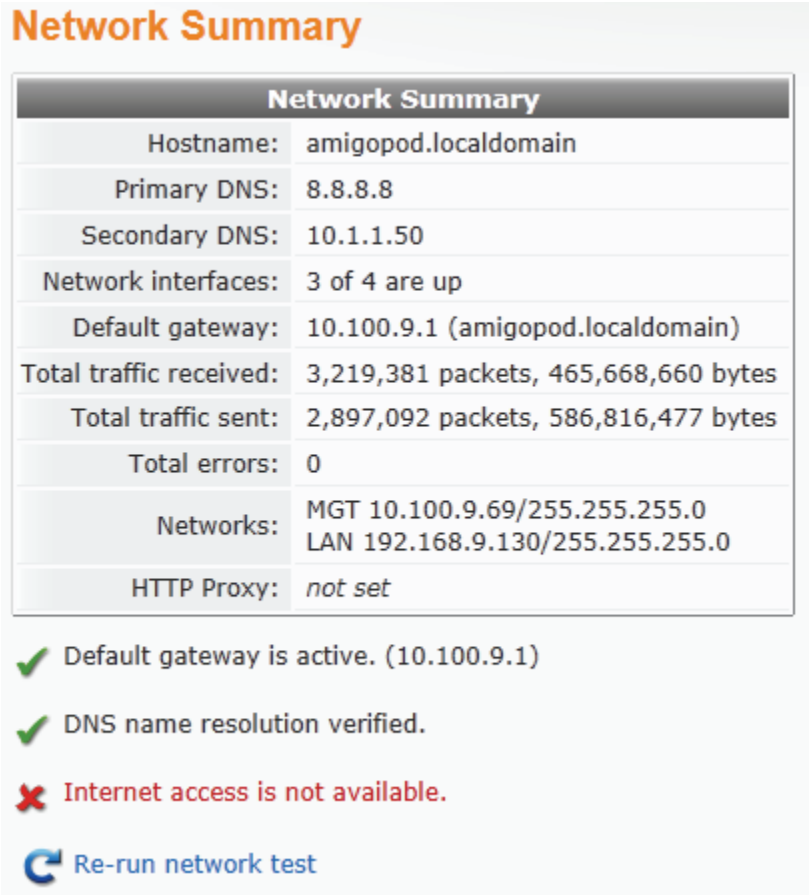
Use the Administrator command link on the home page to access the system administration features.

Alternatively, use the Administrator navigation menu to jump directly to any of the system administration features.

Network Setup

The Network Setup command allows you to configure the system's network interfaces and other related network parameters. To access network setup and configuration tasks, choose **Administrator > Network Setup** in the left menu.

A summary of the system's current network configuration is displayed on the Network Setup page, and the results of the network connectivity test are shown below the summary. Additional commands on the Network Setup page let you navigate to various network configuration tasks.



Configuring Integration with Other ClearPass Servers

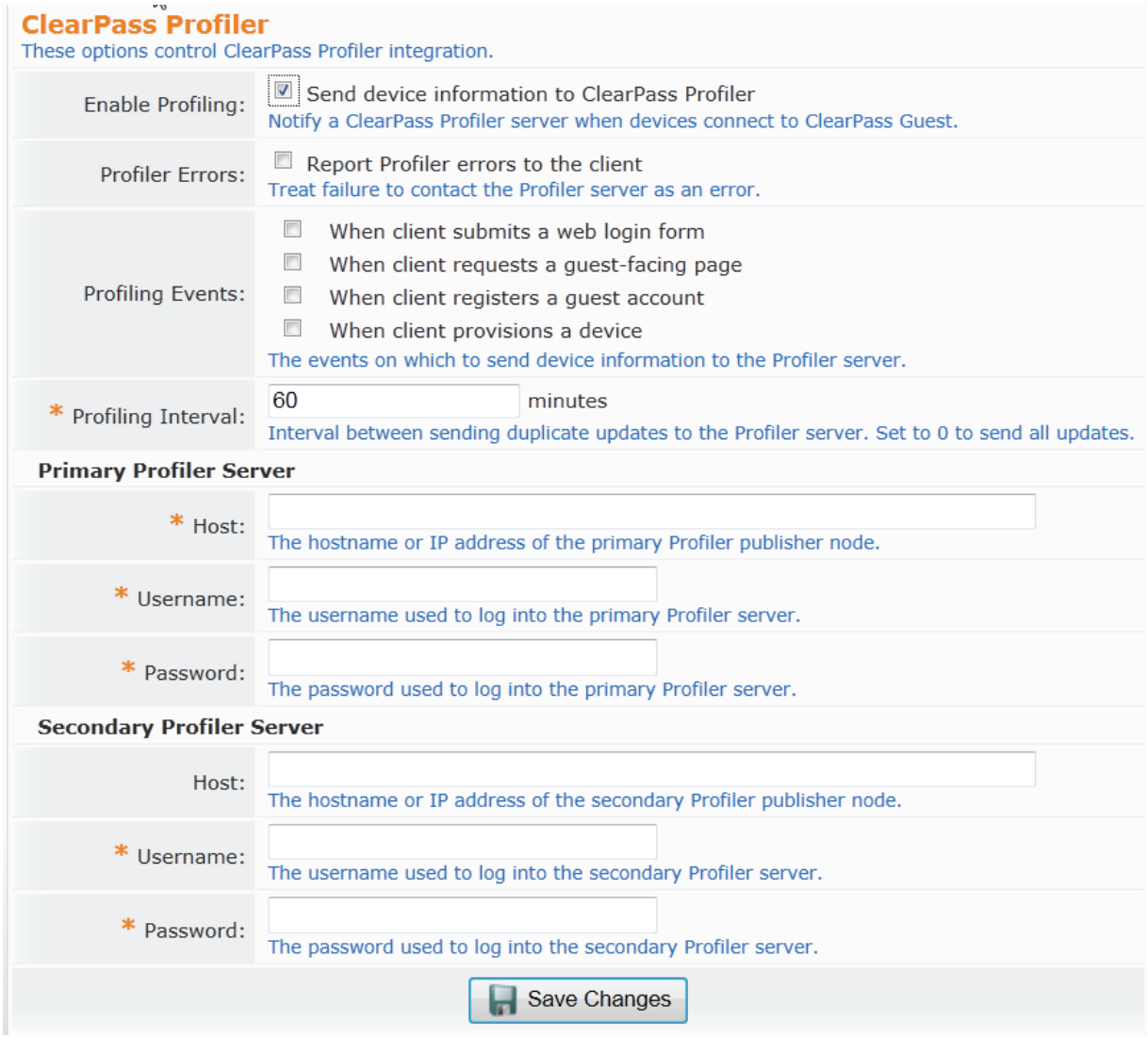
The Administrator module lets you configure integration with ClearPass Profiler and Policy Manager servers.

To configure integration with ClearPass servers:

1. Go to **Administrator > Network Setup > ClearPass**. The Manage ClearPass Servers form opens.

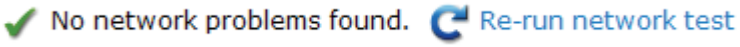
2. To configure integration with ClearPass Policy Manager, mark the **Enable Policy Manager** check box. The form expands to include options for specifying the Policy Manager hostname, username, and password.

3. To configure integration with ClearPass Profiler, mark the **Enable Profiling** check box. The form expands to include options for sending device error, event, and profile interval information, as well as the hostname, username, and password for the primary and secondary Profiler servers.



Automatic Network Diagnostics

When you view or edit the appliance's network configuration on the Network Setup, HTTP Proxy, Network Diagnostics, or Network Interfaces page, an automatic network connectivity test determines the current status of the network, and the results of the diagnostic are displayed.

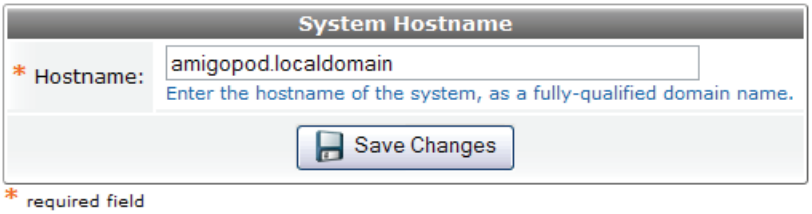


The problems that can be detected with this built-in diagnostic include:

- No default gateway set
- Default gateway is not responding to ICMP echo request
- DNS name resolution is not available
- System services need to be restarted to verify DNS
- HTTP proxy access is not available
- Internet access is not available

Viewing or Setting System Hostname

The system hostname is a fully-qualified domain name. By default, this is set to **clearpass-guest.localdomain**, but you may specify another valid domain name.



NOTE

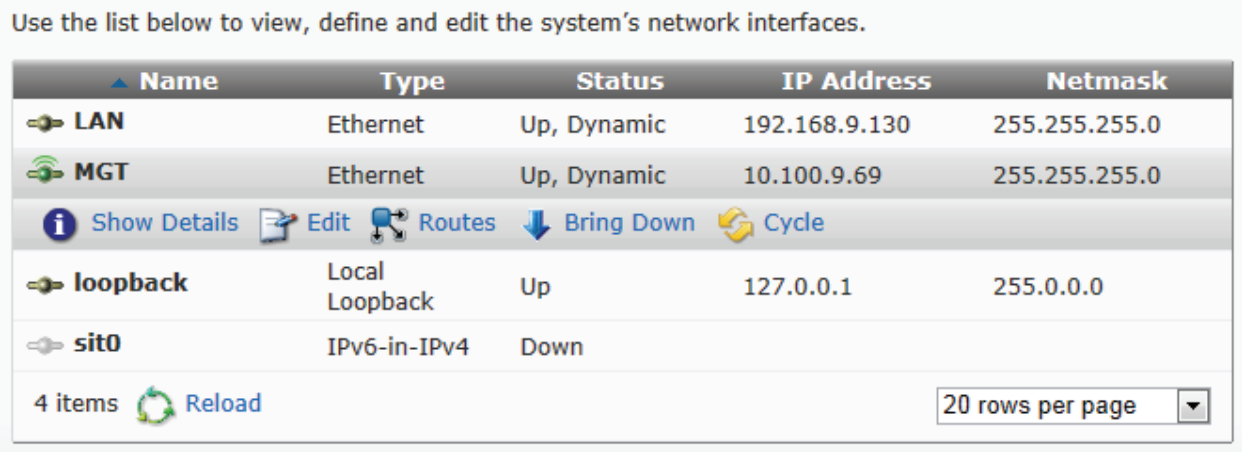
The system hostname should match the common name of the installed SSL certificate. If these names do not match, then HTTPS access to the appliance may result in security warnings from your Web browser.

A valid hostname is a domain name that contains two or more components separated by a period (.). Hostname parameters are:

- Each component of the hostname must not exceed 63 characters
- The total length of the hostname must not exceed 255 characters
- Only letters, numbers, and the hyphen (-) and period (.) characters are allowed
- Hostnames may start with numbers, and may contain only numbers

Viewing Network Interface Settings

The Network Interfaces List lets you view details and configure settings for the system's network interfaces. You can enable and disable network interfaces; change the IP address, static routing, or other configuration items for an interface; and add or remove new network interfaces. To open this page, choose **Administrator > Network Setup > Network Interfaces**.



The icons for each network interface indicate its state:

- **Down** – Network interface is disabled
- **Up** – Network interface is enabled
- **Default** – Network interface is enabled, and the current default gateway uses this network interface

Click a network interface in the list to select it. You can then choose from the following actions:

- **Show Details** – Display detailed information and statistics about a network interface.

- **Edit** – Change the configuration of a network interface, including IP address, DNS settings, or Ethernet settings. **See** **"Changing Network Interface Settings"** in the Adminstrator Tasks chapter for details.
- **Delete** – Remove a network interface. Manually created network interfaces may be deleted—for example, tunnel, VLAN, or secondary interfaces. The standard system network interfaces cannot be deleted.
- **Routes** – Define static routes that specify the gateway IP addresses for other networks.
- **Bring Down** – Disables the network interface.
- **Bring Up** – Enables the network interface.

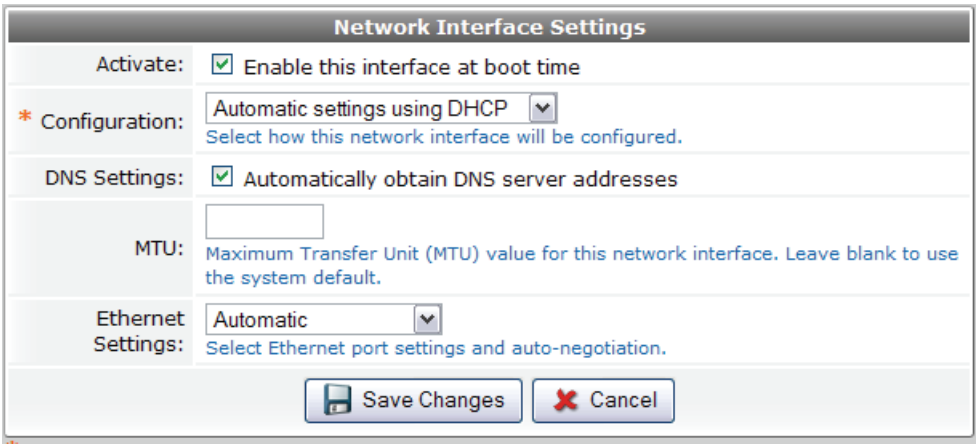
Changing Network Interface Settings

The **Network Interface Settings** form can be used to configure network addressing and other properties of the network interface.

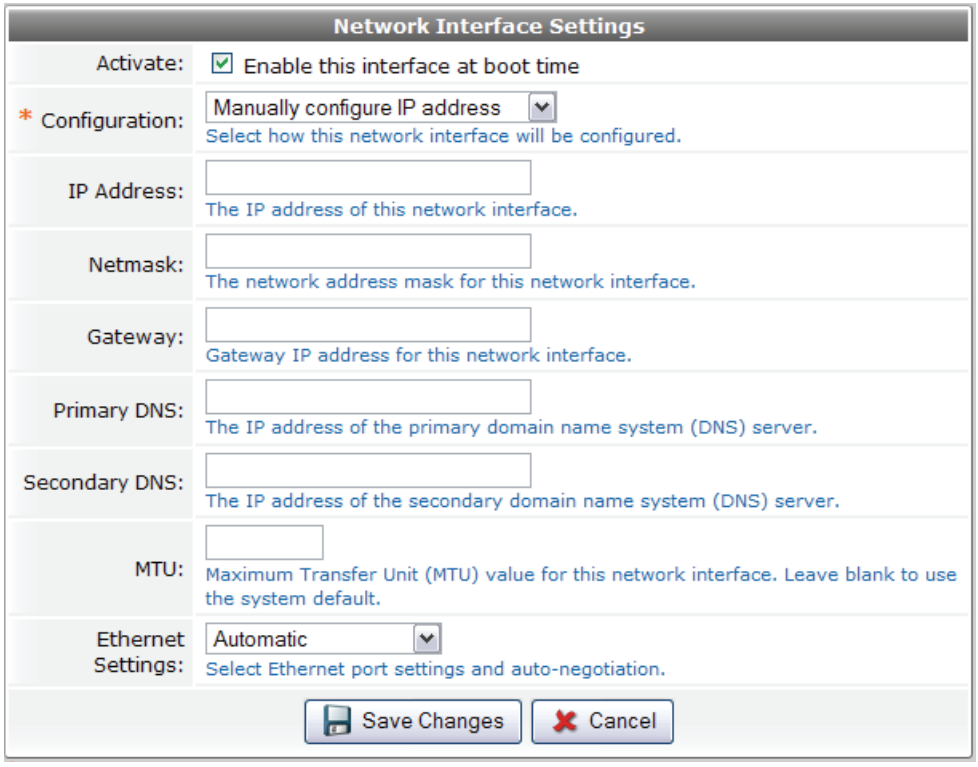
To change the configuration of a network interface, choose **Administrator > Network Setup > Network Interfaces** to display the Network Interfaces List. Click the network interface's row in the list, then click the **Edit** command. The row expands to provide configuration options.

Use the Configuration drop-down list to select the IP address configuration method for the network interface. LAN and MGT network interfaces may be configured for automatic settings using DHCP or BOOTP, or can be manually configured for an IP address. When you choose one of these settings from the Configuration drop-down list, additional options are displayed.

- To configure the network interface using DHCP, select **Automatic settings using DHCP**. When using automatic settings, you can also mark the **Automatically obtain DNS server addresses** check box to use DNS server information provided by the DHCP server.



- To specify an IP address for the network interface, select **Manually configure IP address**. The following form is displayed for IP address details.

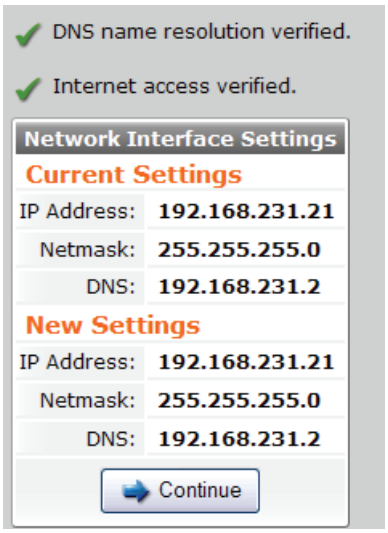


The MTU field allows you to specify the Maximum Transfer Unit size in bytes for the network interface. While standard Ethernet uses a MTU of 1500 bytes, you may find it necessary to reduce the MTU slightly in some network topologies. ClearPass Guest uses a default MTU of 1476 bytes unless otherwise specified in this form.

The Ethernet Settings field specifies the physical layer link parameters to use for this network interface. You may select one of the following:

- **Automatic** uses link auto-negotiation to determine the best available speed. This is the recommended setting.
- 1000 Mbit, full duplex
- 100 Mbit, full or half duplex
- 10 Mbit, full or half duplex

Click the **Save Changes** button to update the network interface with the specified settings. The new settings will be tested and the results of the test displayed.



- If DNS name resolution is not working, the system will be unable to perform many common tasks. To resolve this issue, check the DNS server settings for the network interface. If you are using DHCP, check that your DHCP server provides DNS server information, and enable this option for the network interface. If you are assigning network addresses manually, check that you have provided the correct DNS server addresses.
- If DNS name resolution is working, but Internet access is not available, the system will not be able to check for updates. To resolve this issue, check that the correct gateway address is configured.

Click the **Continue** button to apply the new network settings. If the appliance's IP address has changed, you will be automatically redirected to the new IP address. If the computer you are using to configure the appliance does not have suitable network settings to access the new IP address, the redirect will fail. You can update your computer's network settings and then click the Refresh icon in your Web browser to reconnect.

About Default Gateway Settings

When more than one default gateway is set, the interface with the lowest "metric" takes priority.

The default metric for each network interface is set as follows:

Table 33 *Default Interface Settings*

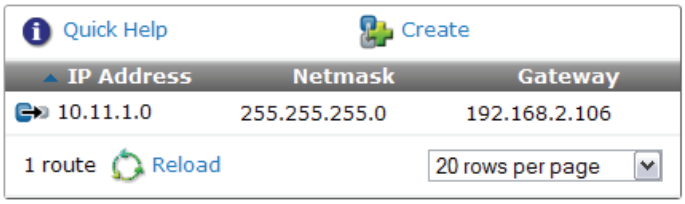
Interface	Adapter Name	Default Metric
MGT	eth0	1
LAN	eth1	11

These values cannot be changed through the **Network Interface Settings** form.

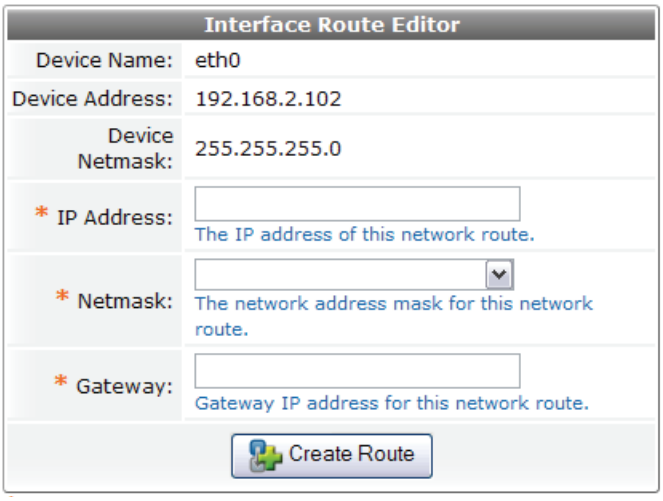
In practice, this means that any default gateway set for the MGT port will be used by default. To use a default gateway configured for the LAN port, a default gateway for the MGT port must not be configured.

Managing Static Routes

In the Network Interfaces list view, click the network interface to edit, and then click **Routes**. The Network Interface Routes list view will be displayed.



Click the **Create** tab to add a new static route. You must specify the network address of the destination network as an IP address and netmask, and the gateway for the destination network. The gateway IP address must be reachable directly from the network interface.



Click the **Create Route** button to add the route. Changes made to the routing table entries are applied immediately.

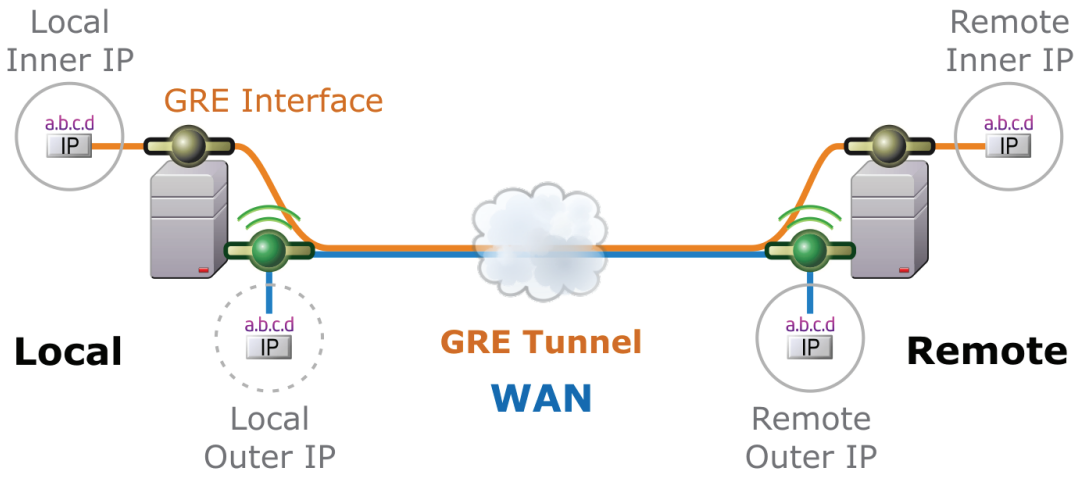
To manage existing routing entries, click the entry in the table. The **Edit** link may be used to modify the settings for a routing entry. Click **Delete** to remove a routing entry. Click **Test Gateway** to verify that the gateway IP address is reachable via an ICMP ping.

Creating a Tunnel Network Interface

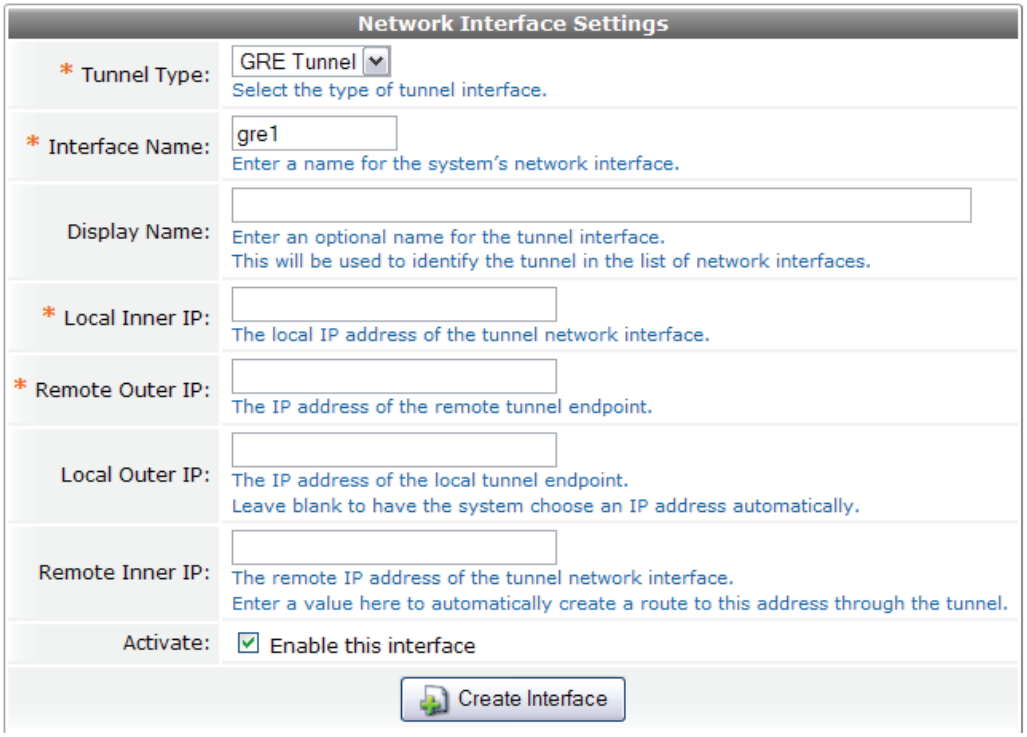
ClearPass Guest supports creating a generic routing encapsulation (GRE) tunnel. This protocol can be used to create a virtual point-to-point link over a standard IP network or the Internet.

The following figure shows how the local and remote servers are connected using the tunnel, and where the inner and outer IP addresses for the tunnel are used. **See** **Figure 47**.

Figure 47 *Network diagram showing IP addressing for a GRE tunnel*



To create a GRE tunnel, navigate to the Network Interfaces page and click the **Create a tunnel network interface** link. The **Network Interface Settings** form is displayed.



The Interface Name is the system's internal name for this tunnel interface. A default value is supplied, which may be used without modification. A Display Name may be specified to identify the connection in the list of network interfaces.

The IP address settings for the GRE tunnel must be specified in order for it to be created successfully.

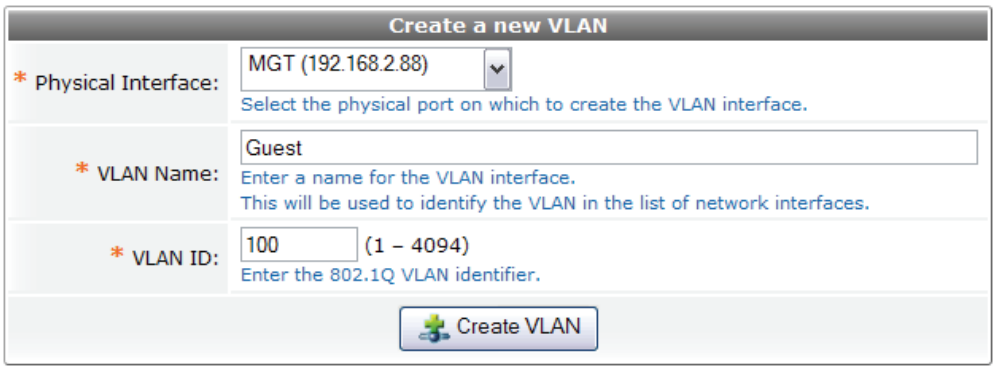
Select the **Enable this interface** check box to activate the tunnel interface immediately after it has been created.

Click the **Create Interface** button to add the new tunnel interface.

Creating a VLAN Interface

Navigate to **Administrator > Network Setup > Network Interfaces** to view the list of interfaces currently configured on the system.

Use the **Create a VLAN interface** link to create a new network interface with a specific VLAN tag. The **Create a New VLAN** form is displayed.



In this form, select the physical interface through which the VLAN traffic will be routed, and enter a name for the VLAN and the corresponding VLAN ID. Use a descriptive name for the VLAN Name field, as this is only used by administrators to identify the network interface. The corresponding VLAN ID is used by the network infrastructure to identify a specific virtual LAN. You can enter a value between 1 and 4094 inclusive. The VLAN ID cannot be changed after the VLAN interface has been created. To specify a different VLAN IDs, you will need to create a new VLAN interface.

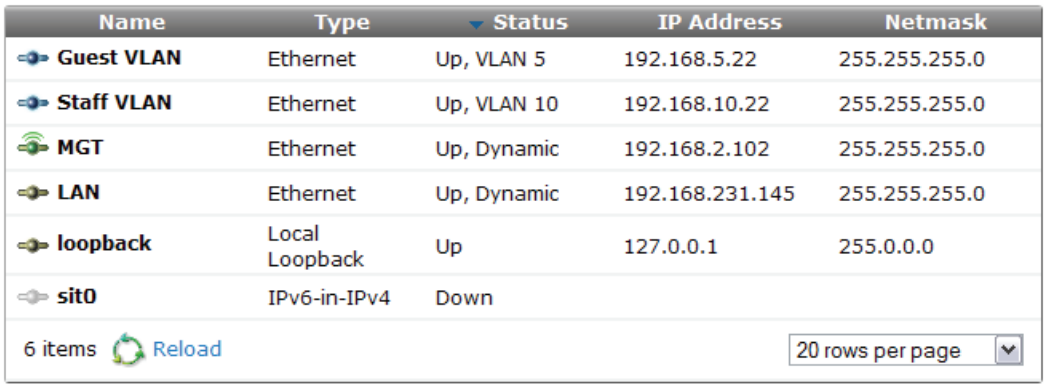
Click the **Create VLAN** button to create a new network interface with the corresponding VLAN identifier.

Your network infrastructure must support tagged 802.1Q packets on the physical interface selected. VLAN ID 1 is often reserved for use by certain network management components; avoid using this ID unless you know it will not conflict with a VLAN already defined in your network.

Managing VLAN Interfaces

After creating a VLAN interface, you will be returned to the Network Interfaces list view to edit the properties of the new interface.

VLAN network interfaces have the same properties as a physical network interface. Refer to this guide or the online help for additional details about setting the properties for the interface.

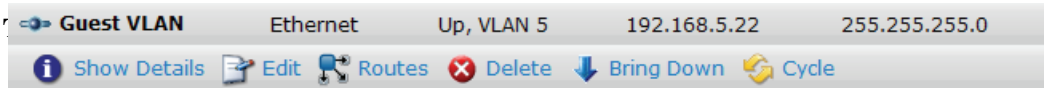


The VLAN Name that is displayed in the list of network interfaces may be modified here. **See "Changing Network Interface Settings"** in this chapter for details about the remaining network interface settings, which may be configured for a VLAN interface in the same way as a physical network interface.

VLAN interfaces are distinguished from other network interfaces with blue icons. The possible states for the system's network interfaces are summarized in the table below

Table 34 *Network Interface States*

Interface State	Physical	VLAN
Active (up)		
Active with default gateway		
Inactive (down)		

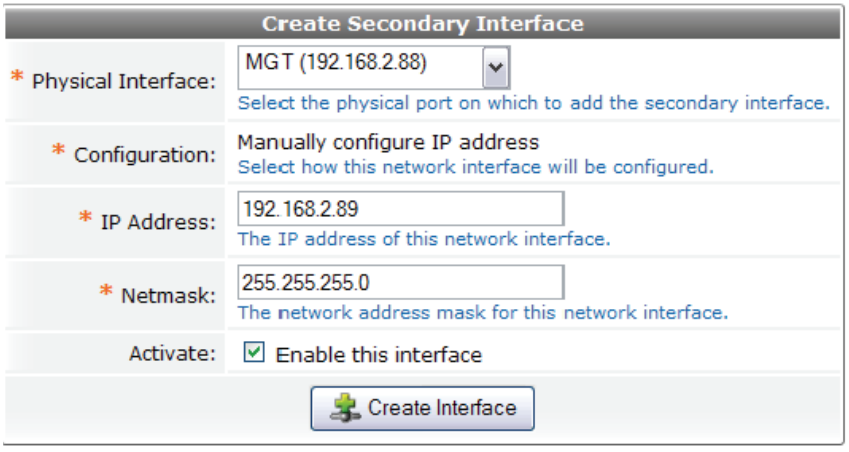


- **Show Details** – Displays detailed information and statistics about the network interface.
- **Edit** – Change the configuration of the VLAN interface, including IP address, DNS settings, MTU, and whether to enable the interface when the system starts.
- **Routes** – Define static routes that specify the gateway IP addresses for other networks.
- **Delete** – Removes the VLAN interface.
- **Bring Up** – Enables the VLAN interface.
- **Bring Down** – Disables the VLAN interface.
- **Cycle** – Disables and re-enables the VLAN interface. This operation may be used to renew a DHCP lease.

Creating a Secondary Network Interface

A secondary network interface is a secondary IP address assigned to a physical network interface. The secondary network interface is displayed as a separate logical network interface.

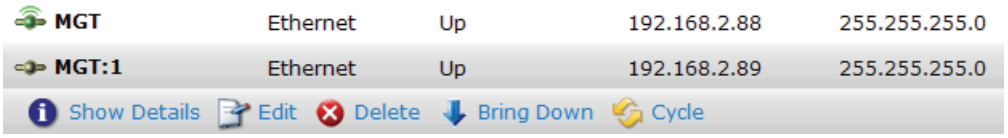
From the Network Interfaces page, click the **Create a secondary network interface** link. The **Create Secondary Interface** form will be displayed.



A secondary IP address must be a statically configured IP address. It is not possible to configure more than one IP address using DHCP on the same network interface.

Click the **Create Interface** button to create a new secondary interface with the specified IP address. The network interface will appear in the list and will be automatically brought up.

Secondary network interfaces have the same name as the underlying physical interface, with a suffix such as ":1", ":2" and so on for each subsequent IP address created.

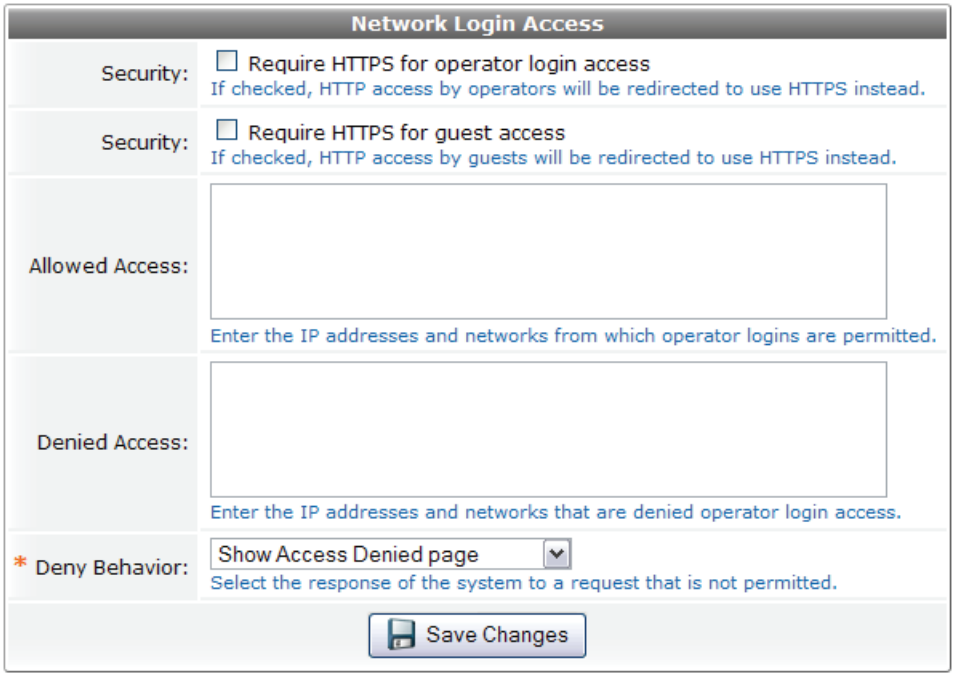


All secondary interfaces will be brought down if the corresponding physical interface is brought down.

Login Access Control

Authentication and role based access control is used to identify operators and their level of access to the system. The default login access settings require HTTPS for both operators and guests.

For security reasons, it may be desirable to prevent guests from obtaining login access to the administrator user interface. This may be achieved by first ensuring that guests and operators are using different network address ranges, and then defining those networks in the **Network Login Access** form. To access this form, navigate to **Administrator > Network Setup** then click the **Network Login Access** command link.



The login access rules that have been defined will only apply to the components of the system that require an operator login. Guest specific pages that do not require an operator login are not affected by any allow/deny rules and are always available, regardless of the IP address used to access them.

The **Network Login Access** form also controls the access restrictions used for SSH console access, if it is enabled. **See "Changing Network Security Settings"** in this chapter for more information about remote console access via SSH.

The 'Allowed Access' and 'Denied Access' fields are access control lists that determine if an operator is permitted to view the login page. You can specify multiple IP addresses and networks, one per line, using the following syntax:

- **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

The 'Deny Behavior' drop-down list may be used to specify the action to take when access is denied.

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 **0.0.0.0/0**.

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 list, then the client will be denied access. If the matching rule is in the Allowed Access list, then the client will be permitted access.

If the Allowed Access list is empty, all access will be allowed, except to clients with an IP address that matches any of the entries in the Denied Access list. This behavior is equivalent to adding the entry **0.0.0.0/0** to the Allowed Access list.

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 **0.0.0.0/0** to the Denied Access list.

For example, assuming that visitors are assigned IP addresses in the **10.1.0.0/16** network, and operators are using the **192.168.88.0/24** network:

- If the 'Allowed' list is empty and the 'Denied' list contains **10.1.0.0/16**, operator logins will be permitted to all IP addresses other than those on the guest network.

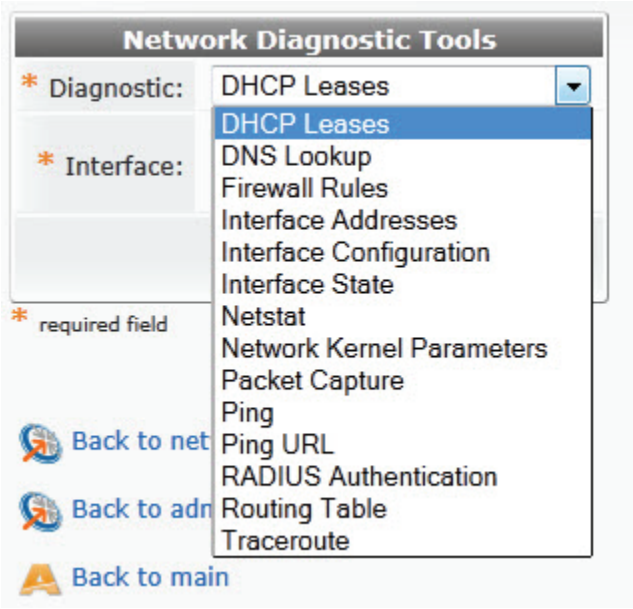
For greater security, the operator logins may be restricted more explicitly:

- If the 'Allowed' list is set to **192.168.88.0/24**, and the 'Denied' list is set to **0.0.0.0/0**, operators may only access the system from the specified network.
- Guest self-registration is still permitted regardless of guest IP address.

The 'Deny Behavior' drop-down list may be used to specify the action to take when access is denied.

Network Diagnostic Tools

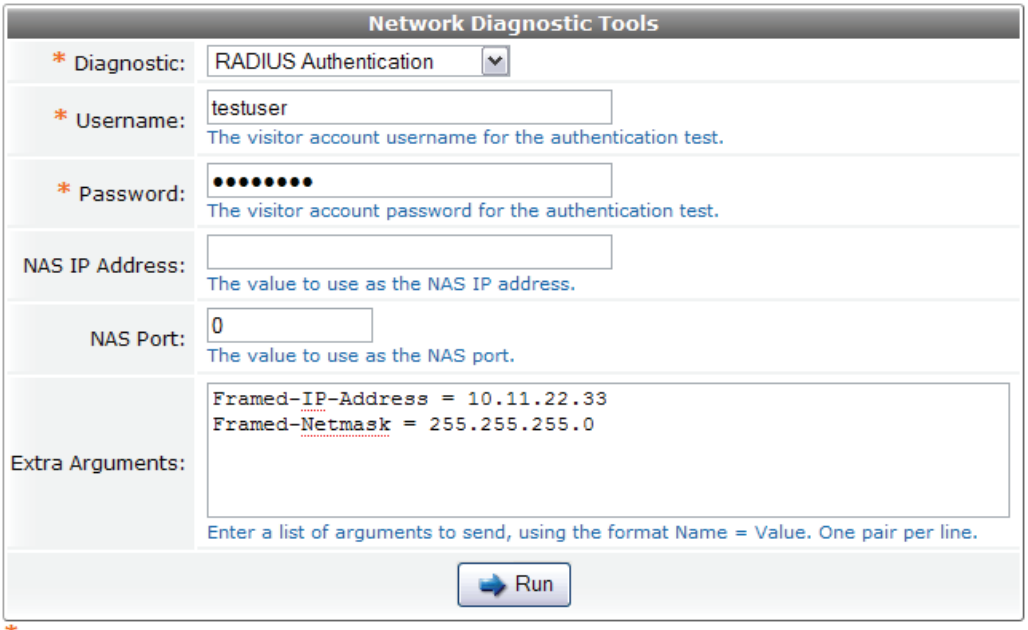
A number of built-in diagnostic tools are available to verify different aspects of your network's configuration. To view these tools, navigate to **Administrator > Network Setup,** then click the **Network Diagnostics** command link.



Select a diagnostic from the drop-down list. Depending on the diagnostic you have selected, additional parameters will also be available:

- **DHCP Leases** – Select a network interface to view the DHCP lease information for that interface.
- **DNS Lookup** – Enter a hostname to perform a domain name lookup and display the results.
- **Firewall Rules** – Displays the iptables firewall rules that are currently in effect.
- **Interface Addresses**– Displays all active IP addresses and interface details.
- **Interface Configuration** – Select a network interface to view the system settings for that interface. The information displayed includes physical layer parameters such as port auto-negotiation, speed, duplex, packet and byte counters; data link layer parameters including the hardware address; and network layer parameters including IPv4 and IPv6 addresses.
- **Interface State** – Displays a summary of all network interfaces and the internal state of each interface.
- **Netstat** – Displays a list of currently open TCP and UDP sockets.
- **Network Kernel Parameters** – Displays a list of system configuration settings related to networking. If required, these settings can be changed using the system configuration parameters (sysctl) editor; **See** **"Changing Network Security Settings"** for details.
- **Packet Capture** – Sets up packet capturing. **See** **"Network Diagnostics – Packet Capturing"** for more information.
- **Ping** – Enter a hostname or IP address to test connectivity using an ICMP echo request. The test will take approximately 5 seconds to run.
- **Ping URL** – Enter a URL to test connectivity using a HTTP request. Only the headers for the specified Internet resource are retrieved. This test can be used to verify Internet connectivity, or that your HTTP proxy settings are correct.
- **RADIUS Authentication** – Enter a username and password to test the results of a RADIUS Access-Request. Values for the NAS-IP-Address and NAS-Port RADIUS attributes may be specified using this

form. Additional RADIUS attributes may also be included by adding `Attribute-Name = Value` pairs in the Extra Arguments field; see the example below.

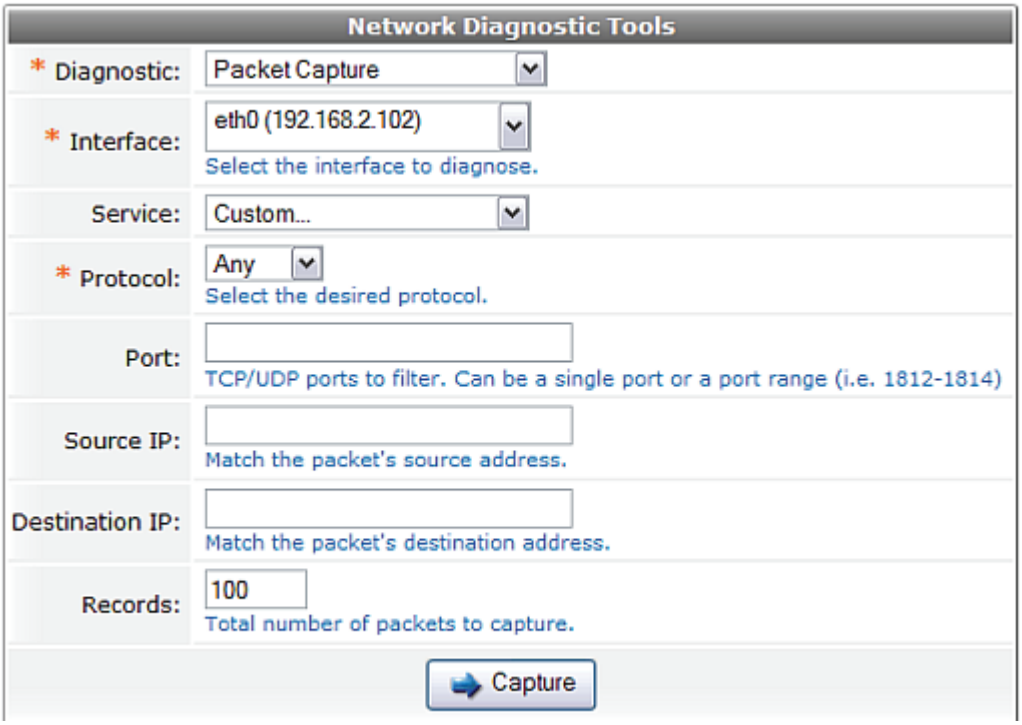



```
Sending Access-Request of id 226 to 127.0.0.1 port 1812
    User-Name = "testuser"
    User-Password = "password"
    Framed-IP-Address = 10.11.22.33
    Framed-Netmask = 255.255.255.0
rad_recv: Access-Accept packet from host 127.0.0.1:1812, id=226,
```

- **Routing Table** – Displays the current IPv4 routing table. The list shows the static, network addresses and default routes configured for the system.
- **Traceroute** – Enter a hostname or IP address to determine the route that packets traverse to that host. The test may take a considerable amount of time (30 seconds or more), depending on network conditions.

Network Diagnostics – Packet Capturing

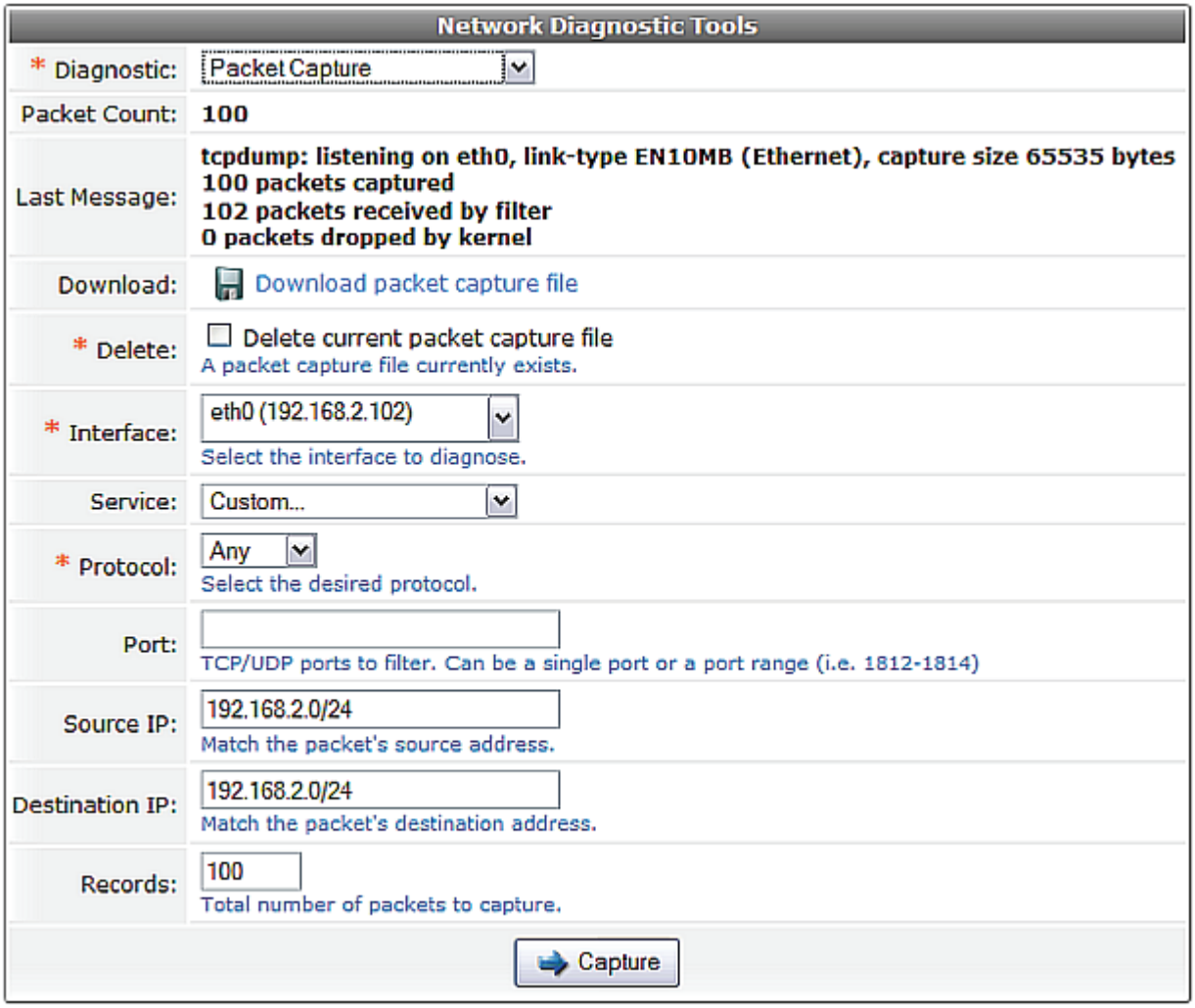
The Packet Capture network diagnostic can be used to capture network traffic for in-depth debugging of network issues. To access the Network Diagnostics tools for Packet Capturing, click the **Network Diagnostics** command link on the **Administrator > Network Setup** page.



Select the network interface and, if required, enter filtering parameters to restrict the type and number of packets to be captured. The maximum size of a packet capture is 100,000 packets.

You can enter network addresses in the Source IP and Destination IP fields by using an IP address and a network address length; for example, **192.168.2.0/24**.

Click the **Capture** button to begin the packet capture operation. While packet capturing is in effect, the status of the packet capture is displayed as part of the **Network Diagnostics** form.



Once the packet capture has completed, the status is updated, and a link to **Download packet capture file** is available. Click this link to download a packet capture file, which may be analyzed using the Wireshark utility or another tool capable of reading the "pcap" file format.

To delete the saved file, select the **Delete current packet capture file** check box and click the **Delete** button.

To start another packet capture, modify the filtering parameters if required and click the **Capture** button.

Network Hosts

The built-in hosts file may be edited, to make resolving hostnames easier in certain situations, or to work around DNS issues that may be present in a complex network. To manage and view the current host configuration, click the **Network Hosts** command link on the **Administrator > Network Setup** page.

The hosts file is a simple text file that associates IP addresses with hostnames. Each line of the file should contain one IP address.

Both IPv4 and IPv6 addresses may be entered.

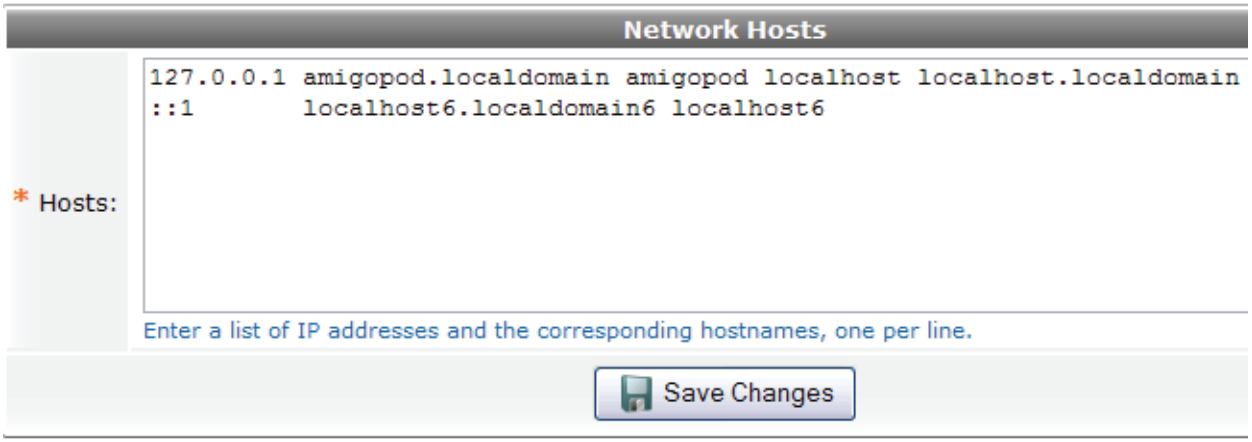
Comments may be entered on lines that begin with a **#** character.

For each host a single line should be present with the following information:

```
IP_address canonical_hostname [aliases...]
```

The fields on each line are separated by any number of blanks or tab characters. Any text from a **#** character to the end of the line is a comment, and is ignored.

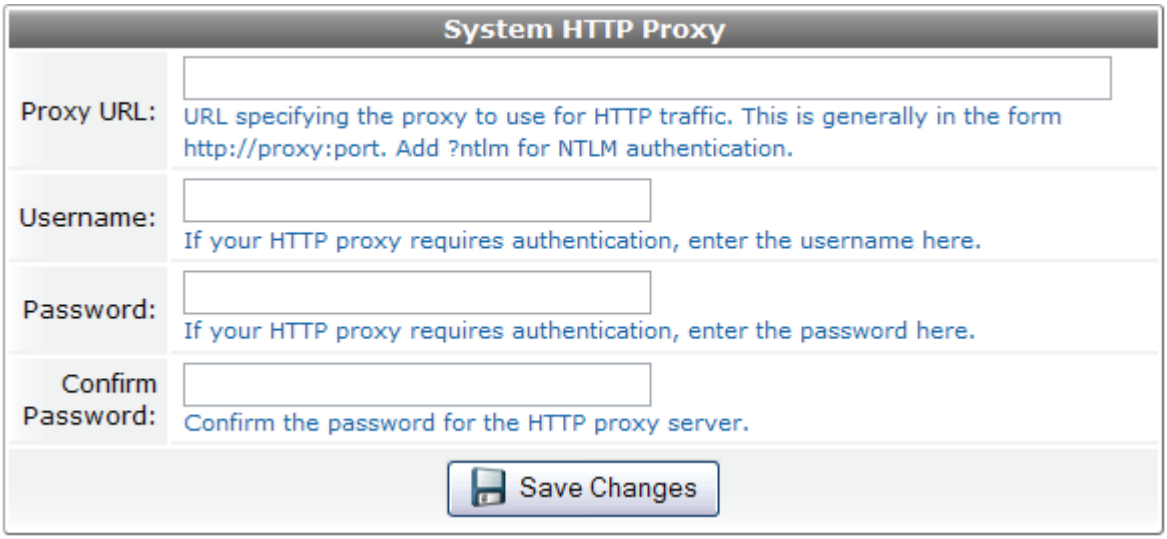
Hostnames may contain only alphanumeric characters, minus signs ("-"), and periods ("."). A hostname must begin with an alphabetic character and end with an alphanumeric character.



After making changes in the Hosts field, click the **Save Changes** button to update the system's hosts file.

HTTP Proxy Configuration

If your network requires the use of a HTTP proxy to access the internet, the proxy's details should be entered on this form. To manage and view the current HTTP Proxy configuration click the **HTTP Proxy** command link on the **Administrator > Network Setup** page.



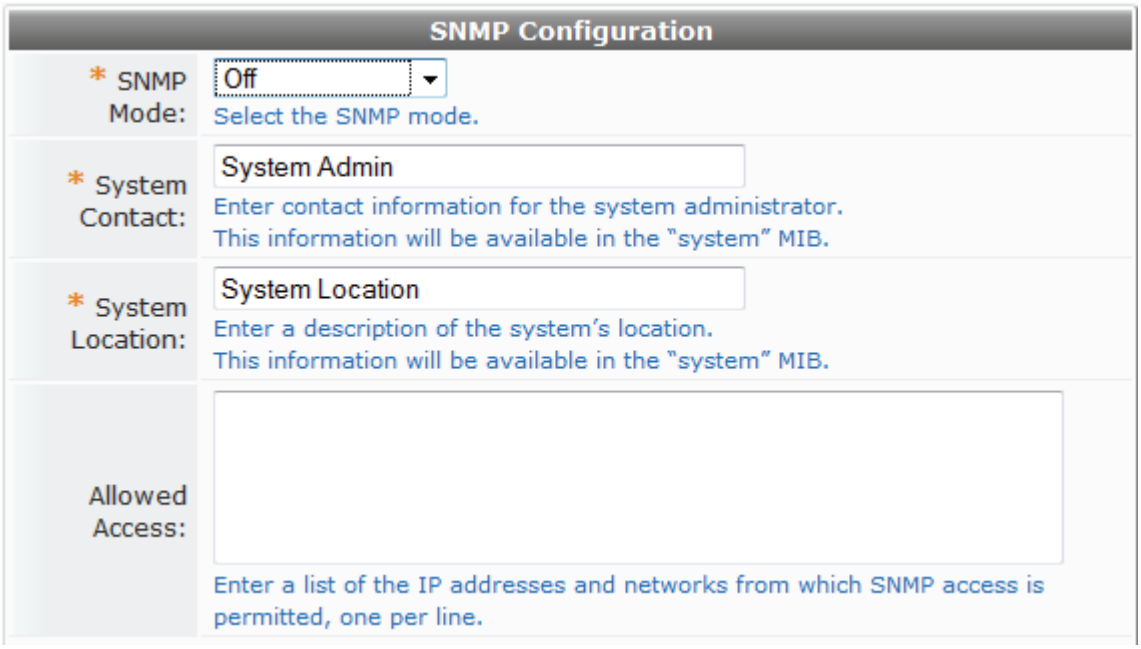
Common port numbers for HTTP proxy access are 3128 and 8080. These port numbers can be specified in the Proxy URL. For example, **http://192.168.88.30:3128/** is a valid proxy URL with a port specification. The default port is 80 if not otherwise specified.

For proxies that require authentication, a username and password must also be supplied.

SNMP Configuration

The Simple Network Management Protocol (SNMP) may be used to obtain system information and perform management tasks in a distributed network environment. To manage and view the current SNMP configuration click the **SNMP Configuration** command link on the **Administrator > Network Setup** page.

The **SNMP Setup** form is used to configure the system's SNMP server and enable SNMP access.



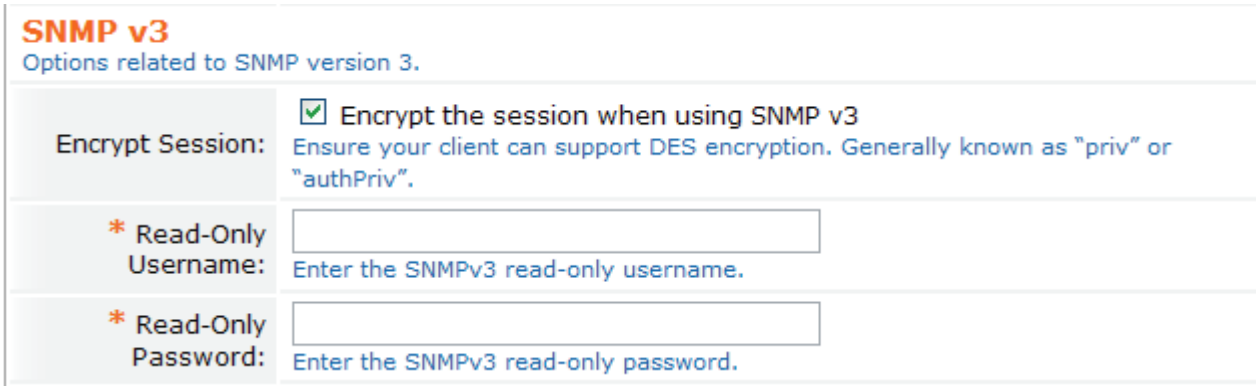
To enable SNMP access, one of the available modes must be selected. Version 2c, version 3, or both versions may be enabled.

The System Contact and System Location parameters are basic SNMP "system" MIB parameters that are frequently used to identify network equipment. **See "Supported MIBs"** in this chapter for a list of supported MIBs.

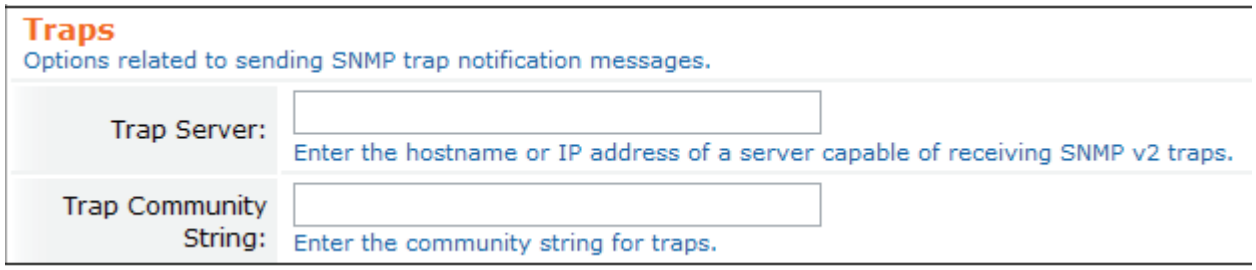
To restrict access to the SNMP server, a list of IP address and networks may be provided from which SNMP access will be permitted. Network addresses may be specified using either a network prefix length (for example, **1.2.3.4/24**) or a network mask (for example, **1.2.3.4/255.255.255.0**).

If the Allowed Access field is left blank, all IP addresses will be able to perform SNMP queries. It is recommended that you enter either the IP address of your network management station or the network address of your management network in order to prevent guest access to the SNMP server.

SNMP version 2c has only one configuration option, which is the name of the community string. SNMP clients must provide this value in order to access the server. The default community string is **public**.



SNMP version 3 adds authentication and encryption capabilities to the protocol. You must supply a set of credentials to be used for SNMP v3 access. You can also select whether encryption should be used.



Traps are notification messages sent when certain conditions are reached. A trap server and community string may be provided. Currently there are no defined SNMP trap messages.

Click the **Save Changes** button to apply the new SNMP server settings. The settings will take effect immediately.

Supported MIBs

The SNMP server currently supports the following MIBs:

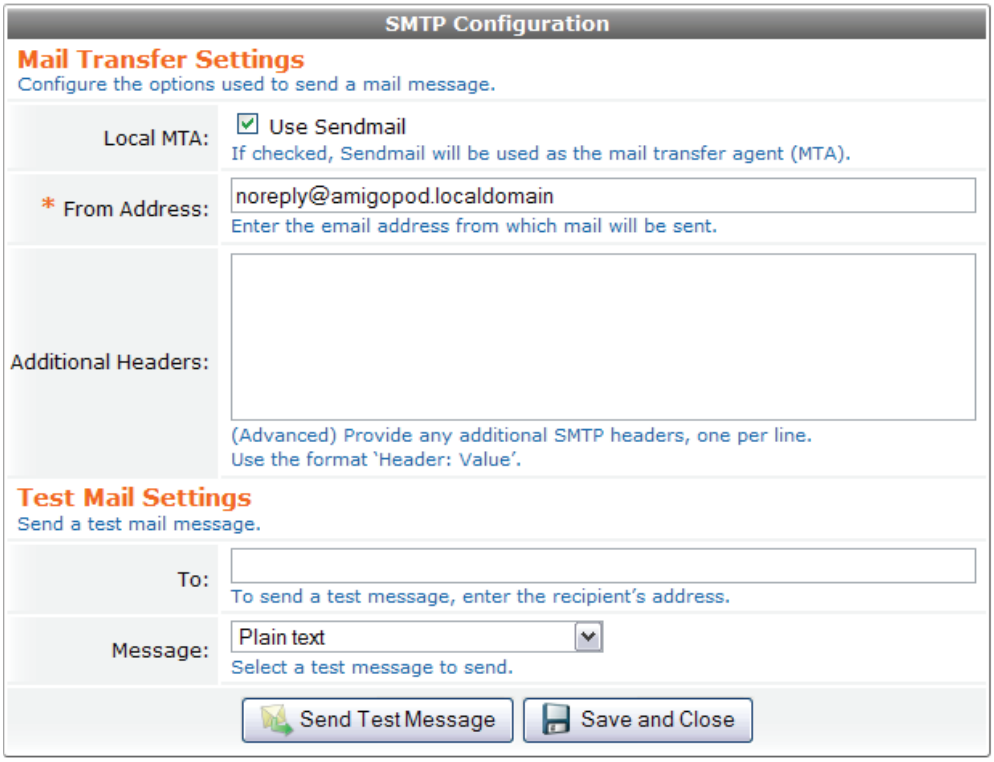
- DISMAN-EVENT-MIB
- HOST-RESOURCES-MIB
- IF-MIB
- IP-FORWARD-MIB
- IP-MIB
- IPV6-MIB
- MTA-MIB
- NET-SNMP-AGENT-MIB
- NET-SNMP-EXTEND-MIB
- NOTIFICATION-LOG-MIB
- RFC1213-MIB
- SNMP-FRAMEWORK-MIB
- SNMP-MPD-MIB
- SNMP-TARGET-MIB
- SNMP-USER-BASED-SM-MIB
- SNMPv2-MIB

- SNMP-VIEW-BASED-ACM-MIB
- TCP-MIB
- UCD-DISKIO-MIB
- UCD-DLMOD-MIB
- UCD-SNMP-MIB
- UDP-MIB

SMTP Configuration

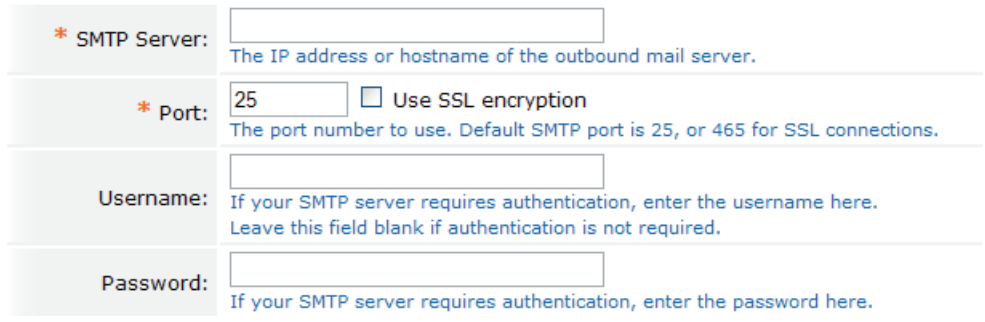
The **SMTP Configuration** form is used to provide system default settings used when sending email messages. To manage and view the current SMTP configuration click the **SMTP Configuration** command link on the **Administrator > Network Setup** page.

See "SMTP Services" in the Guest Management chapter for additional configuration options for SMTP services.



The built-in Sendmail mail transfer agent may be used to deliver email directly. This option requires that the server have outbound internet access using port 25.

Alternatively, you may configure an outbound mail server to which messages will be delivered. This option does not require outbound internet access. You can also specify the credentials to use if your mail server requires authentication.



The From Address must be specified. This is the sender of the email and will be visible to all email recipients. It is recommended that you provide a valid email address so that guests receiving email receipts are able to contact you.

When using the SMTP Server option, the following special header values are recognized:

- **X-Smtp-Timeout** – Sets the timeout for SMTP server operations in seconds (minimum 5; the default is system defined)
- **X-Smtp-Debug** – Set to 1 to enable a debugging mode, where log messages are displayed on the test screen. **Note:** Do not use this setting in a production environment.

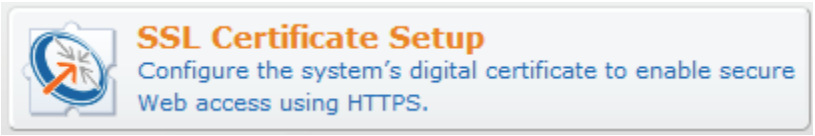
Click the **Send Test Message** button to send an email to a test email address in the selected format. This can be used to verify the SMTP configuration, as well as check the delivery of HTML formatted emails.

Click the **Save and Close** button to save the updated SMTP configuration.

SSL Certificate

The Secure Sockets Layer (SSL) is a cryptographic protocol that enables secure communications across a potentially insecure network. The security guarantees offered by the protocol include both privacy (so that the content of communications cannot be intercepted or modified), and authentication (so that the identity of the server can be verified). The public key infrastructure (PKI) that provides these guarantees is based on the X.509 standard for digital certificates.

To manage and view SSL certificates, click the **SSL Certificate Setup** command link on the **Administrator > Network Setup** page.



If you already have a valid digital certificate for this server, it may be uploaded and used directly. The **SSL Certificate Install** command is used to do this. See "SSL Certificate" in this chapter for details.

If you do not have a digital certificate, you must first create a certificate signing request using the **SSL Certificate Request** command. The certificate signing request should then be provided to a certification authority, which will create the actual digital certificate. See "Requesting an SSL Certificate" in this chapter for more details.

Requesting an SSL Certificate

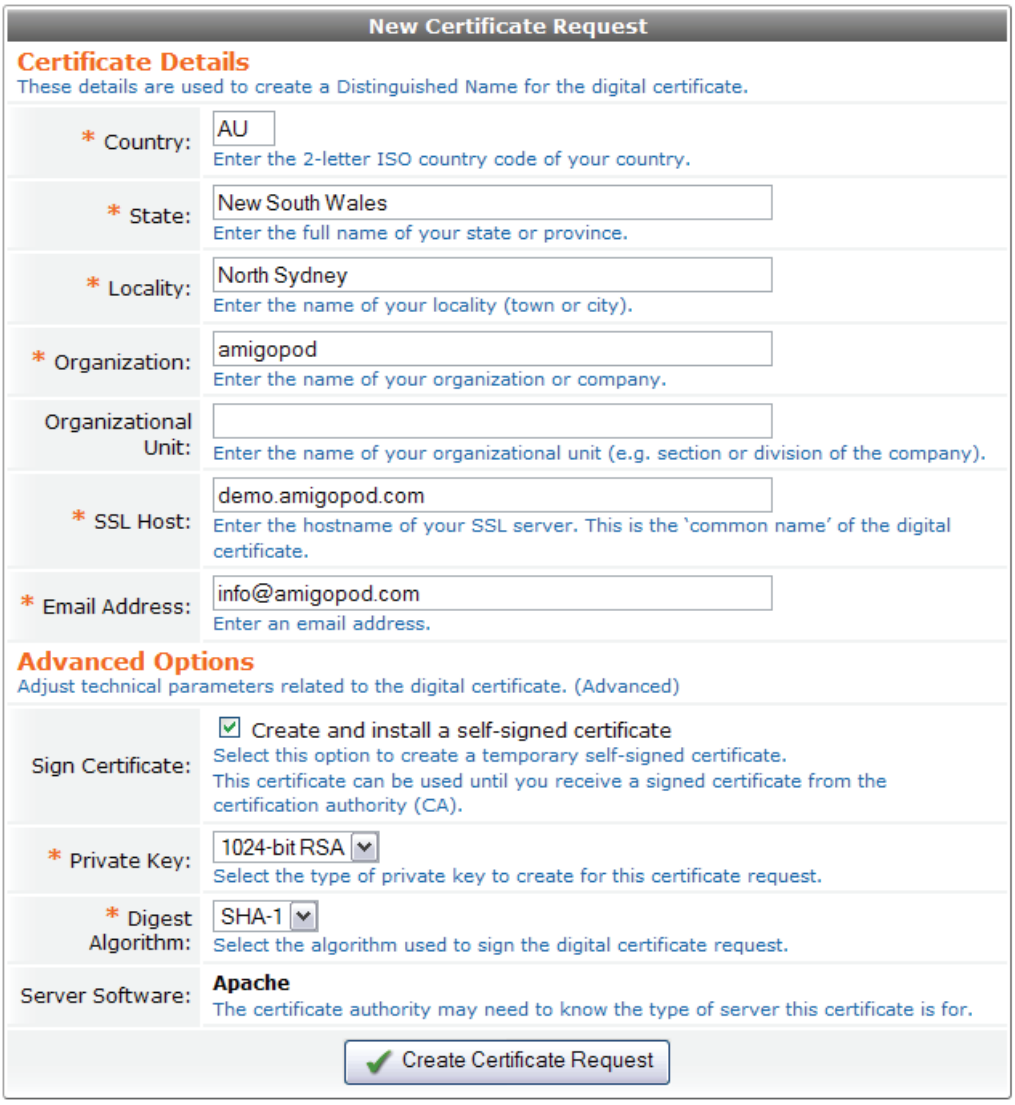
Use the **New Certificate Request** form to create a new certificate signing request.

If you have already created a certificate signing request, the **New Certificate Request** form will not be displayed. You are presented with these options instead:

- **Download the current server certificate** – Downloads the current SSL certificate to your Web browser. This command can be used to back up an installed SSL certificate.
- **Install a signed certificate** – See "Installing an SSL Certificate" in this chapter for details on installing an SSL certificate.
- **Create a new CSR** – Displays the New Certificate Request form and allows you to start over.

You can also use the **New Certificate Request** form to create and install a self-signed certificate for the SSL hostname you specify. Self-signed certificates allow for the connection to the server to be secured, but Web browsers will display security warnings as the issuer of the certificate is not trusted.

A completed sample certificate request is shown below.



Click the ✔ **Create Certificate Request** button to generate the certificate signing request.

The certificate signing request is displayed in a text field in the browser. This can be used to copy and paste the request directly to a certificate authority that supports this form of request submission.

Alternatively, you may click the **Download the current CSR** link to download a **.csr** file to your browser. This file should be sent to your certificate authority to be signed and converted into a digital certificate.

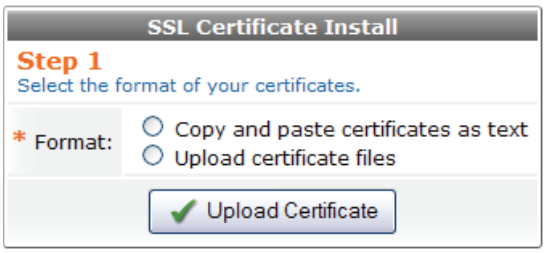
Some certificate authorities will also request the type of server that the certificate is to be used for, or will make the certificate available in several different formats. You should choose a certificate for the “Apache” Web server.

Changing the SSL certificate requires the system’s Web server to be restarted. You will be prompted to do this with the message “system services need to be restarted due to configuration changes.”

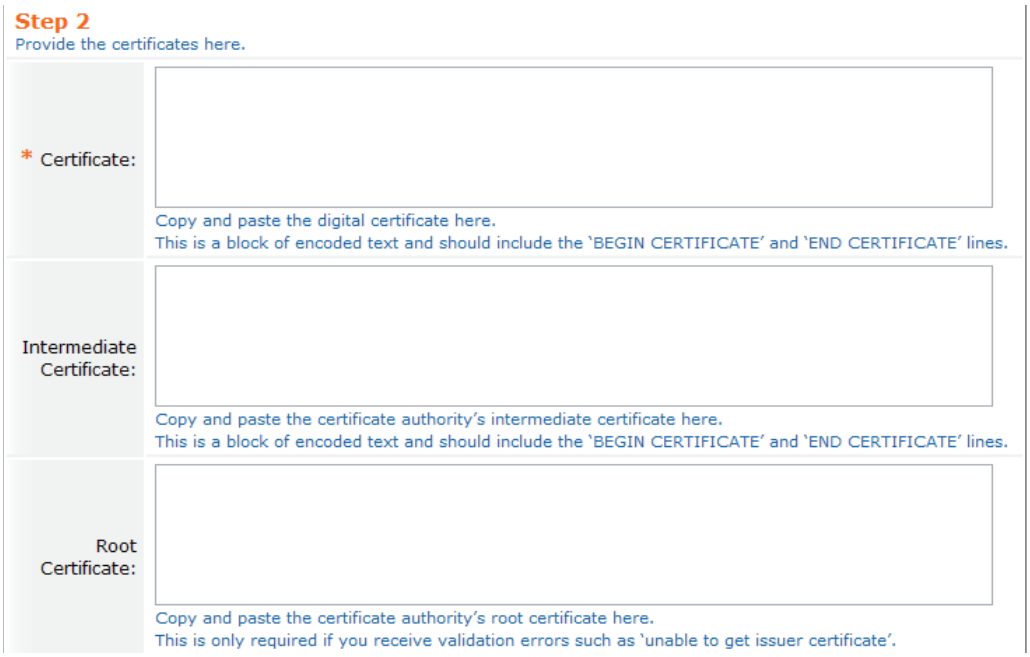
Installing an SSL Certificate

To install an SSL certificate, use the **SSL Certificate Install** form.

The process for installing an SSL certificate has been simplified. In the first step, select whether you will be copying and pasting the certificate as plain text, or uploading the certificate from a file.



In the second step, you must provide between one and three items of information:



- The **Certificate** field must contain the digital certificate. This can be a file containing a base-64 representation of the certificate, or it can be a block of text that contains the certificate.

  Your certificate authority will provide this certificate to you. If required, select the Apache format to ensure that you receive the certificate in the correct format (PEM, or a base-64 encoded version of the certificate).

  When copying and pasting a certificate, ensure that you include the beginning and ending lines of the certificate; these are -----BEGIN CERTIFICATE----- and -----END CERTIFICATE-----.

- The **Intermediate Certificate** is optional, but is typically required for many public certificate authorities. The reason for this is that the certificate authority's root certificate is not used to sign your certificate directly; rather, the root certificate is used to issue one or more intermediate certificates, which are then used to sign the issued certificates.

  Your certificate authority will provide this certificate to you. Check your certificate authority's "How To" instructions for details on obtaining the intermediate certificate. Often, it is available from the same page where you downloaded your certificate.

- The **Root Certificate** is optional, and is not required for many public certificate authorities. When you install your server's certificate, the certificate and its issuing intermediate certificate will be verified against a list of **trusted root** certificates, many of which are pre-installed.

  You will need to provide a root certificate only if you receive a validation error when attempting to install your certificate.

This validation error is typically displayed as a message that includes the statement "unable to get local issuer certificate".

To resolve this error, first check that you have provided the correct intermediate certificate. If the problem persists, check with your certificate authority for the appropriate root certificate to use.

As an optional third step, if you have a private key that corresponds to the SSL certificate, it may be specified separately. This is only required if you did not generate the certificate signing request on the server.

Click the ✔ **Upload Certificate** button to install the new SSL certificate.

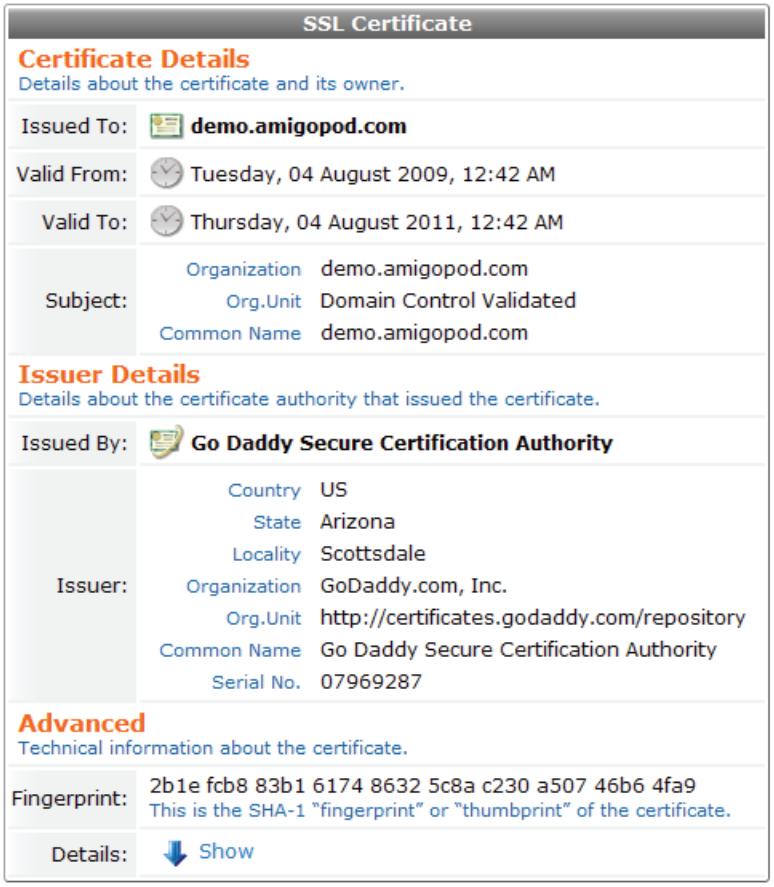
NOTE

Changing the SSL certificate requires the system's Web server to be restarted. You will be prompted to do this with the message "System services need to be restarted due to configuration changes."

Displaying the Current SSL Certificate

After a certificate has been installed (either a self-signed certificate created with the certificate signing request, or a certificate issued by a certification authority), you may use the **SSL Certificate Details** link on the **Adminstrator > Network Setup** page to display detailed information about the certificate.

The **SSL Certificate** form displays details about the certificate, its issuer, and technical information about the certificate. Click the **Show** link at the bottom of the form to view advanced information and details about the certificate.



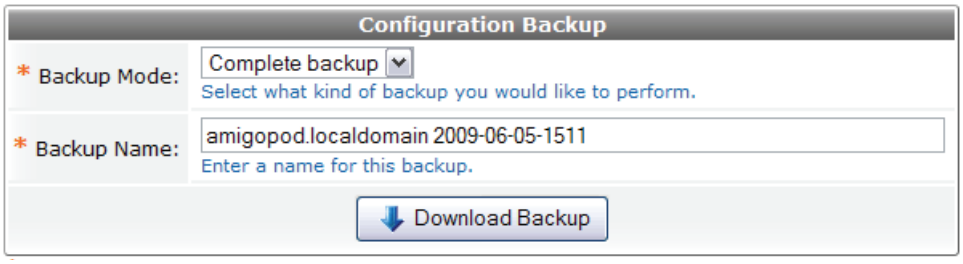
Backup and Restore

Click the **Backup & Restore** command link on the Administrator start page to make backups of the appliance's current configuration as well as restore a previous backup.

It is recommended that you make a complete configuration backup of the system after completing a deployment and after making configuration changes. The scheduled backup command described in the Import and export visitor accounts can be of use to ensure that the system's configuration can be restored in case of hardware failure or an unintended change to the configuration.

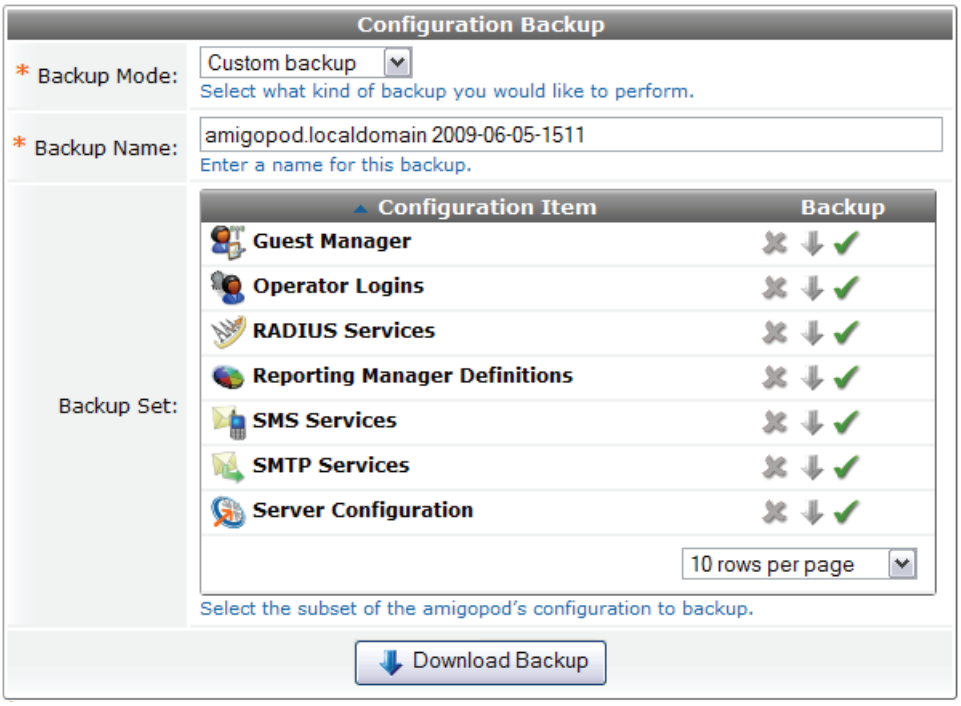
Backing Up Appliance Configuration

The **Configuration Ba.ckup** command allows you to back up the current configuration of ClearPass Guest. You can do either a complete backup (default) or a custom backup.



The complete backup does not require any input from you unless you want to alter the backup filename. Click the **Download Backup** button to begin the backup. You will be prompted by your Web browser to save the backup file

You are also able to do a custom backup.



The custom backup allows you to choose which configuration items of the system should be backed up. Within each area (Guest Manager, Operator Logins, RADIUS Services, Reporting Manager Definitions and

Server Configuration), you can select to back up the entire area or only a particular part of that area. To access the components within an area, click the down arrow .

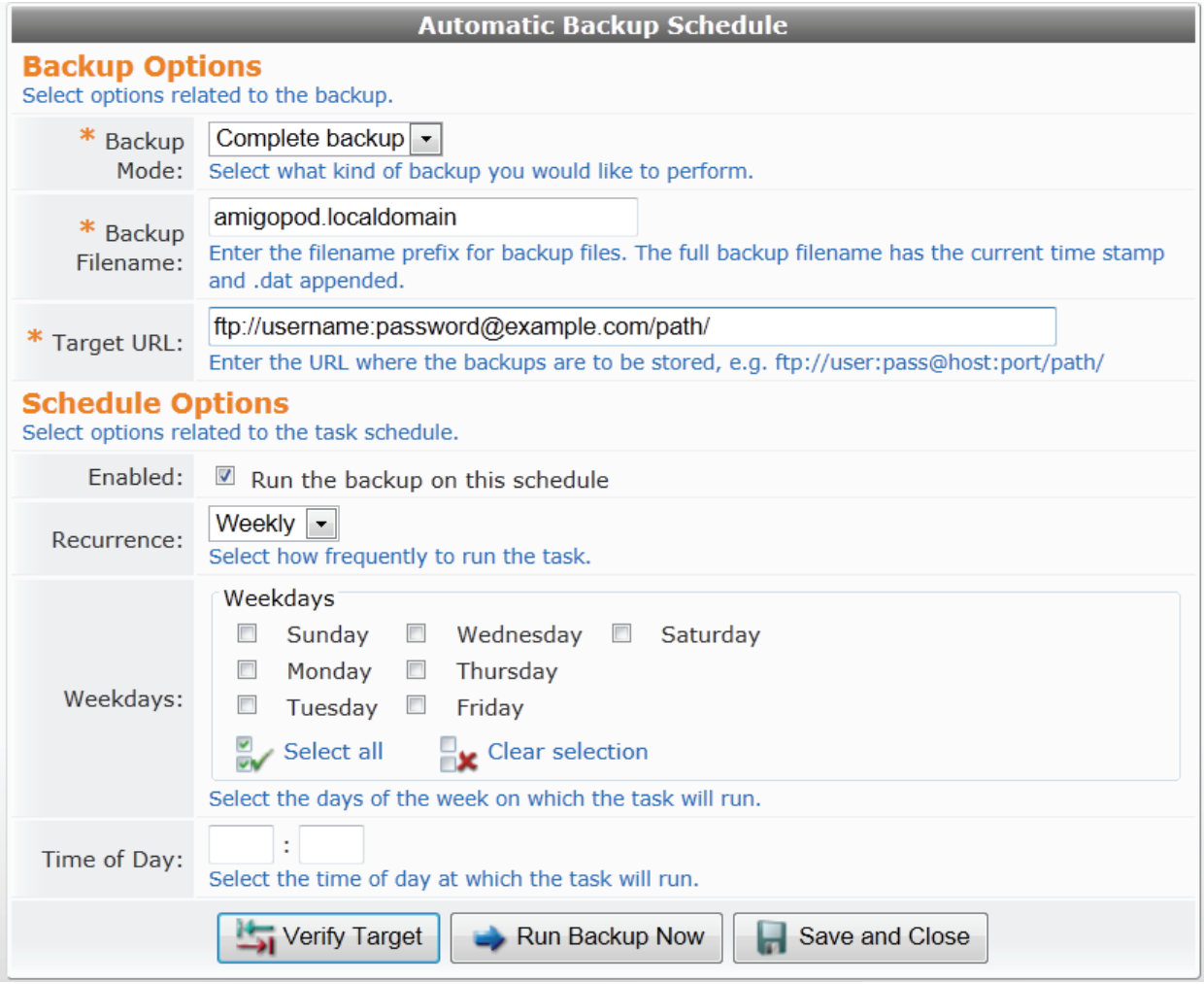
There are five possible states for each area, described below:

1. **Complete backup** – The tick mark is highlighted: . The components of the area are not displayed, but the entire area and all of its components will be backed up.
2. **Partial backup** – The down arrow is highlighted: . The components of the area are displayed; those that are marked with a tick will be backed up, and those that are marked with a cross will not be backed up.
3. **Partial/complete backup** – Both the down arrow and tick marks are highlighted: . The components of the area are displayed, and any that have not been specifically marked for no backup will be changed to a complete backup.
4. **Partial/no backup** – Both the down arrow and cross marks are highlighted: . The components of the area are displayed, and any that have not been specifically marked for a complete backup will be changed to no backup.
5. **No backup** – The cross is highlighted: . The components of the area are not displayed, and will not be backed up.

Click the **Download Backup** button to start the backup. You will be prompted by your Web browser to save the backup file.

Scheduling Automatic Backups

Click the **Backup Schedule** command on the **Administrator > Backup & Restore** page to schedule an automatic backup. You should schedule backups on a regular basis.



You are able to select either a complete or custom backup to run on the schedule. The options available are the same as for the manual backup.

You are required to enter a prefix for the backup filename. The backup name is used as the basis for the name of the backup file. The current time and date is used to identify different backups, in the format YYYYMMDD-hhmmss. For example, with the backup name 'backup', the backup filename will be **backup.20080101-123456.dat**.

The target URL specifies where the automatic backups are stored. The following URL schemes are supported:

- FTP: Use the syntax ftp://user:password@example.com/path/to/backups/
- FTP over SSL: Use the syntax ftps://user:password@example.com/path/to/backups/
- SMB: Use the syntax smb://user:password@server/share/path/to/backups/

Additional protocol-specific options can be specified as the query string component of the URL (**?query-string**).

The available options are:

- **FTP** options
  - **create-dirs**: create directories remotely if required
  - **limit-rate=N**: limit transfer speed to N bytes per second
  - **pasv**: enable PASV mode (default)
  - **port**: enable PORT mode

- **proxy***: proxy related arguments
- **quote=CMD**: send custom command to FTP server
- **require-ssl**: require SSL connection for success

- **SMB** options
  - **kerberos**: use Kerberos authentication (Active Directory)
  - **domain=NAME** or **workgroup=NAME**: set the workgroup to NAME
  - **debug**: generate additional debugging messages which are logged to the application log

Multiple options should be separated with semicolons. Special characters (such as space) can be URL encoded with the standard %XX syntax as described in RFC 1738.

Example target URLs:

ftp://example.com:4567/path?create-dirs;require-ssl;limit-rate=100k

smb://myuser:mypassword@domain.example.com/backup/server%20backups/

Click the **Verify Target** button to create a test file in the backup directory. Use this command to verify that you have entered the target URL correctly, and the remote server is able to accept backup files.

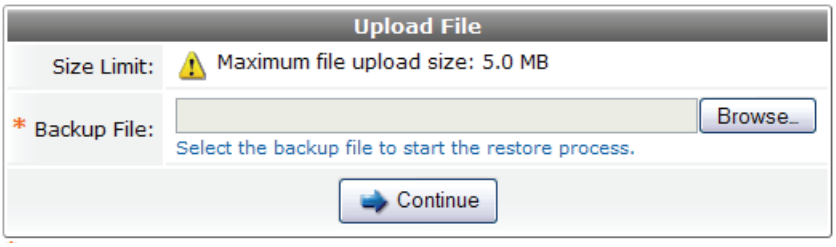
Click the **Run Backup Now** button to run the scheduled backup immediately. A progress window is displayed as the backup is run.

Click the **Save and Close** button to save the new backup schedule and return to the Backup & Restore page.

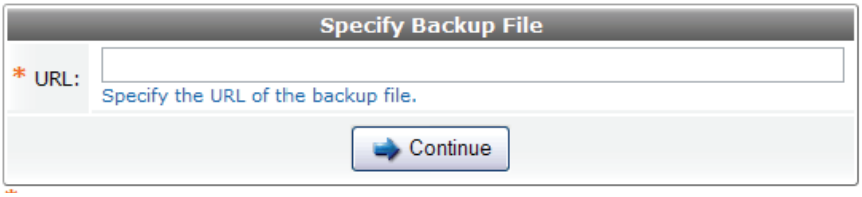
Restoring a Backup

To restore a backup, click the **Configuration Restore** command link on the **Administrator > Backup & Restore** page. This procedure has six steps.

1. Enter the name of the backup file. You are able to browse to locate the required file.

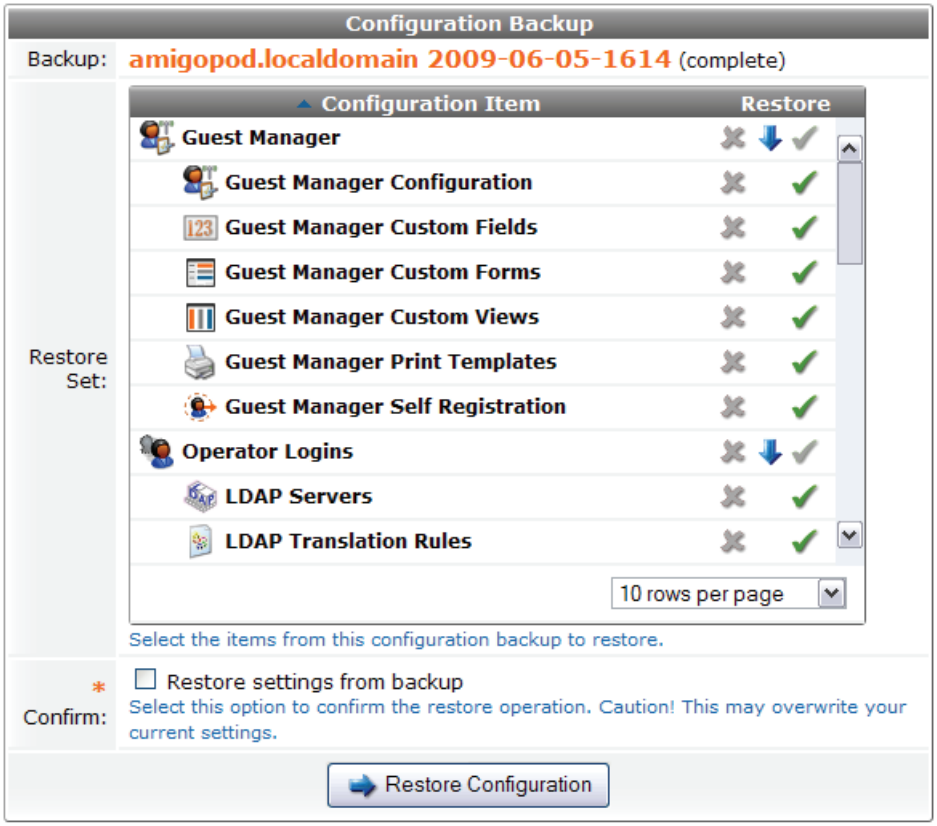


   If the backup file is larger than the maximum file upload size, you cannot upload the backup file using your Web browser. In this case, click the **Restore a backup from a URL** link, and provide a URL that refers to the backup file that is to be restored.



2. Click the **Continue** button.
3. You are then required to select the items that you want to restore. By default, most options are automatically selected, however certain server configuration options will not be automatically restored, such as the server's network interface configuration and subscription IDs. To perform a complete

restore, be sure to select the appropriate items by clicking the tick icon for each configuration item to restore.



4. Mark the **Restore settings from backup** check box. Be aware that it is possible to overwrite any local configuration changes that have been made since the backup was created.
5. Click the **Restore Configuration** button for the restore to commence. A progress window is shown for the restore operation.

6. You are presented with a 'System restore operation completed successfully' message.

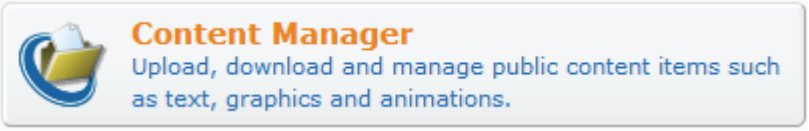
If any problems were found during the system restore, a diagnostic message will be displayed indicating the error. More details about the error will be available in the application log.

One or more warning messages will be displayed if there is a difference in software version numbers between the system at the time of the backup, and the restore system. This warning is issued because the software version number cannot be changed by the restore process to the same version at the time of the backup. However, this does not necessarily indicate a problem with the restore.

Content Manager

The Content Manager allows you to upload content items to ClearPass Guest. Content items are assets such as text, images, and animations that are made available for guest access using the application's built-in Web

server. To access the Content Manager, click the **Content Manager** command link on the **Customization** start page.



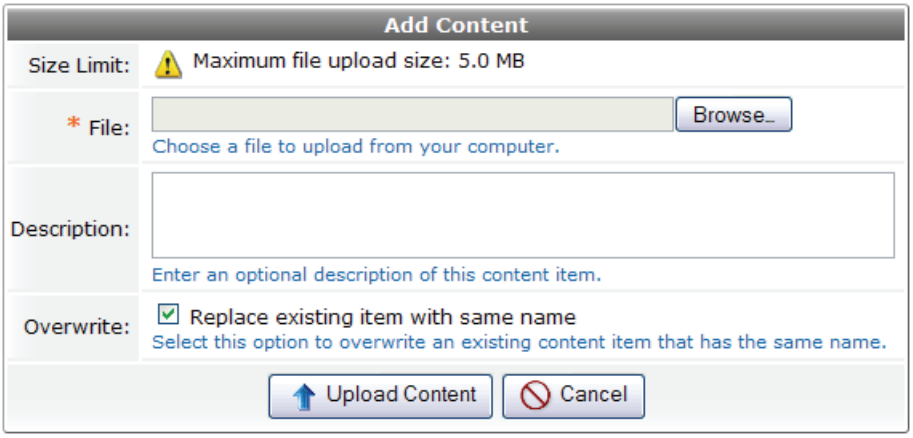
You can add content items by using your Web browser to upload them. You can also copy a content item stored on another Web server by downloading it.

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 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://192.168.88.88/public/logo.jpg**.

Uploading Content

You are able to add a new content item using your Web browser by clicking the **Upload New Content** tab. The **Add Content** form will be displayed.

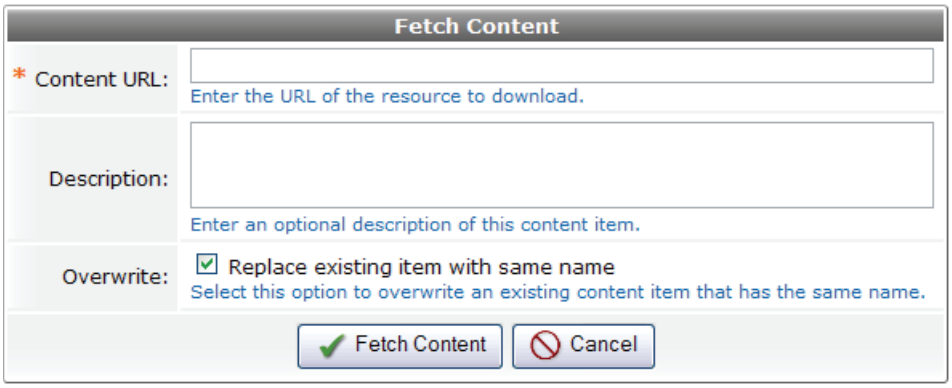


You can upload single content files, multiple content asset files and folders, or a Web deployment archive. To upload multiple assets, first compress the files as a “tarball” or zip file, then browse to it in the File field. Allowed file formats are .tgz, .tar.gz, .tb2, .tar.bz2, or .zip. When you have 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.

After you have completed the form, click the **Upload Content** button to have the file uploaded. The file is then displayed in the list view and will be placed in the **public** directory on the Web server. You are then able to reference this file when creating custom HTML templates.

Downloading Content

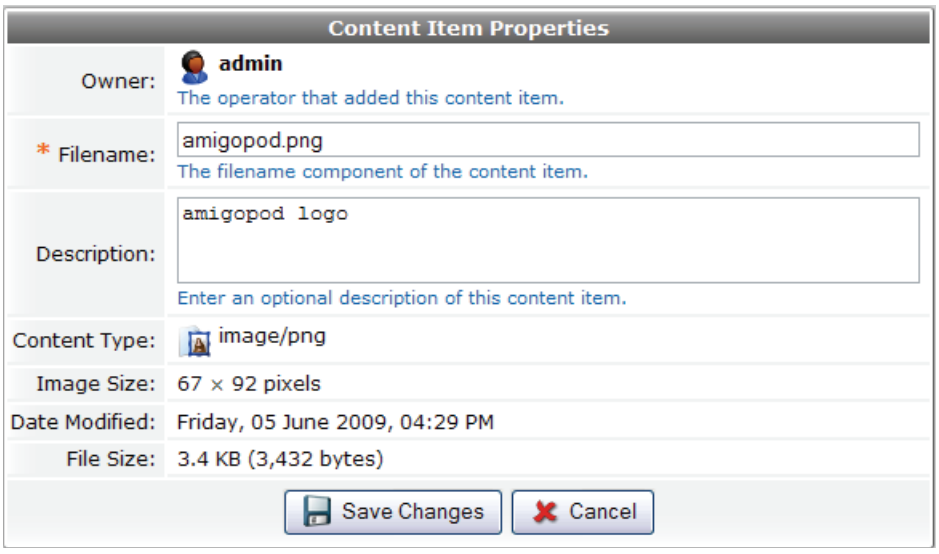
To download a file from the Internet for use in ClearPass Guest, click on the **Download New Content** tab. The **Fetch Content** form is displayed.



After you have completed the form, click the **Fetch Content** button to have the file downloaded. The file is placed in the **public** directory on the Web server. You are then able to reference this file when creating custom HTML templates.

Additional Content Actions

The **Properties** link allows you to view and edit the properties of the item. Editable properties include the content item's filename and description. Read-only properties include the content type, modification time, file size, and other content-specific properties such as the image's size.



You are able to delete the content item using the **Delete** link. You will be asked to confirm the deletion.

You can rename the content item using the **Rename** link.

Click the **Download** link to save a copy of the content item using your Web browser.

You are able to open a new window to view the item using the **View Content** link.

The **Quick View** link can be used to display certain types of content inline, such as images and text. This link is not available for all content types.

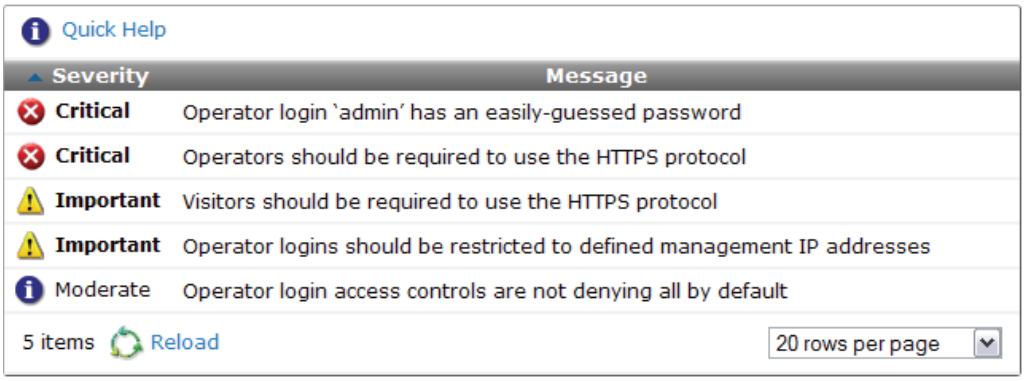
Security Manager

ClearPass Guest has a built-in audit capability that can analyze the configuration of the application and check for common security problems.

Performing a Security Audit

Use the **Check Security** command link on the **Administrator > Security Manager** page to start a security audit of the system.

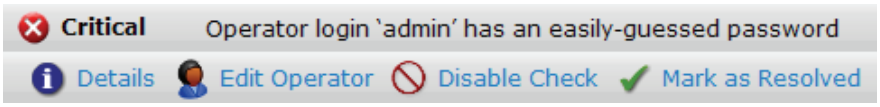
A security assessment will be performed and a report will be displayed containing the recommendations from the security assessment.



Reviewing Security Audit Results

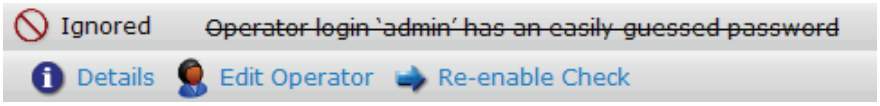
For each of the security recommendations presented, you can choose to accept the recommendation, ignore the recommendation, or disable the recommendation.

A **Details** link may be provided, containing more information about this security message or guidance on a recommended fix.



Use the links provided to review the appliance's configuration, and make modifications where necessary. In some cases, a suggested configuration is supplied with the recommendation; in this cases, click the **Fix this Problem** link to apply the changes.

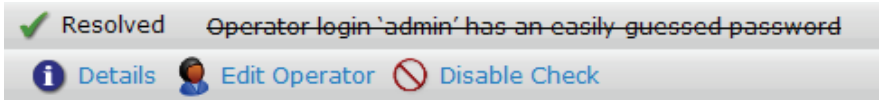
To disable a security check, and prevent it from reappearing in future security audits, click the **Disable Check** icon link.



NOTE

Disabled recommendations will not be shown in future security audits. Make sure that you are comfortable with the security implications of this decision. A message that has been disabled can be re-enabled while you are still viewing the security recommendations. Alternatively, all previously disabled security checks can be re-enabled by clicking the **Re-enable all checks and run the security audit again** link below the list view.

If you have taken steps to correct a security problem, a message can be marked as resolved by clicking the **Mark as Resolved** link. When this is done, the status of the message will change to Resolved:



Marking a message as **Resolved** does not disable the corresponding security check. Future security audits will still perform this check, and will generate the same warning message if the same security problem still exists. For this reason, the Resolved status is intended only for use as a "checklist" of items requiring

attention. Use the **Disable Check** link to prevent the security audit from raising warnings about a specific security condition.

Changing Network Security Settings

Use the **Network Security** command link to check the current settings for remote console access.

ClearPass Guest has a command line interface(CLI) which may be accessed using the appliance console or SSH.

Typical usage scenarios where command line access might be used are:

- Changing the initial network configuration of the appliance
- Resetting the appliance to factory default settings
- Resetting a forgotten 'admin' operator login password
- Rebooting the appliance
- Enabling or disabling remote SSH access

Command line access is not required to perform any normal configuration or management tasks, and should never be required after the initial setup has been completed.

For this reason, SSH access has been disabled by default. It is recommended to leave this network service disabled unless you have specific requirements to the contrary.

Network access restrictions for SSH console access may be specified using the **Network Login Access** form for operator logins. This can be used to ensure that guests do not have SSH console access, even if it is enabled for operators; See "Creating a VLAN Interface" in this chapter for details on configuring the access control list for operators.

Resetting the Root Password

The root password is required to log into the appliance's console user interface (either directly at the console, or remotely via SSH). See "Console Login" in the Setup Guide chapter for an explanation.

The default root password for the appliance is **admin**.

During the initial setup wizard, the root password is updated to correspond to the administrator's password.

Once you have set the initial root password, future changes to the administrator password **will not** change the appliance's root password.

In order to recover from a forgotten root password, you must have administrative access to the graphical user interface. Navigate to **Administrator > Security Manager**, click the **Network Security** command link, and then click the **Reset Root Password** link at the bottom of the page.

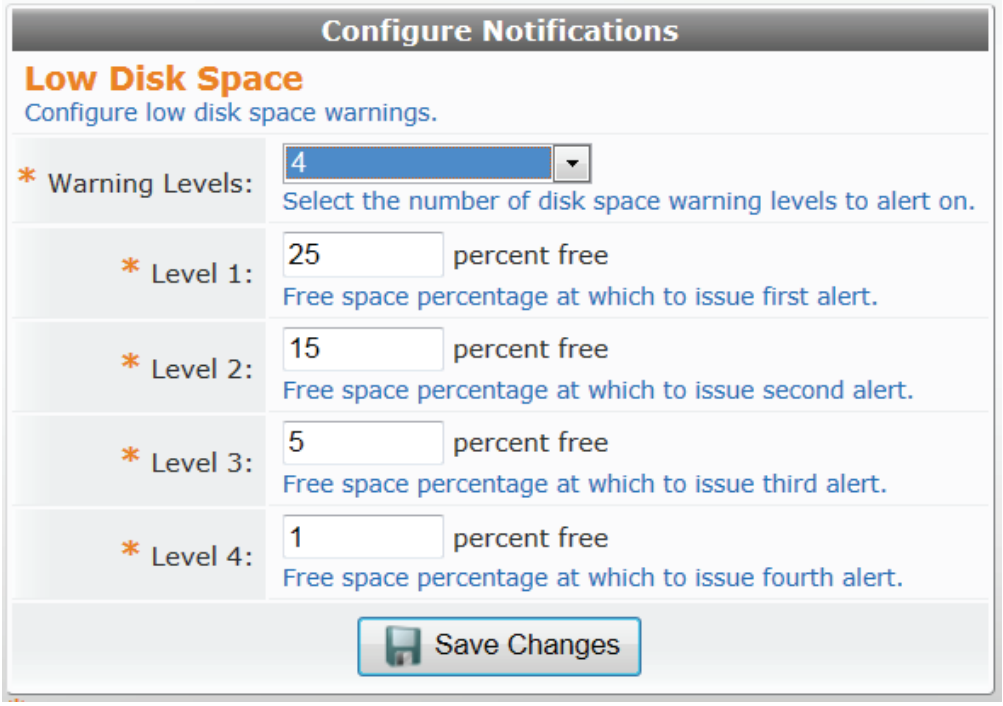
Provide your current operator password, and confirm the new root password by entering it in the appropriate fields. Click the **Set Password** button to have the new root password take effect.

The **Reset Root Password** form is only available to operators with both the Plugin Manager and Network Setup privileges.

Notifications

Operators with the IT Administrator profile can choose to receive warning notifications by email when disk space is low. You can configure notification frequency according to remaining disk space, or disable notifications.

1. To configure notifications, go to **Administrator > Notifications**. The Configure Notifications page opens.



2. In the **Warning Levels** drop-down list, specify the maximum number of alerts to receive. If you do not want to receive notifications, choose **0-Disable warnings**.
3. If you enabled warnings, in the **Level 1** field, enter the amount of remaining disk space at which the first notification should be sent.
4. If you specified more than one alert level in the Warning Levels field, use the Level 2 through Level 4 fields to specify the percent of remaining disk space at which each alert should be sent, then click the **Save Changes** button.

OS Updates

The server's operating system software is automatically maintained by the Plugin Manager. You can check for and install software updates using the process. See "Adding or Updating New Plugins" in this chapter for details.

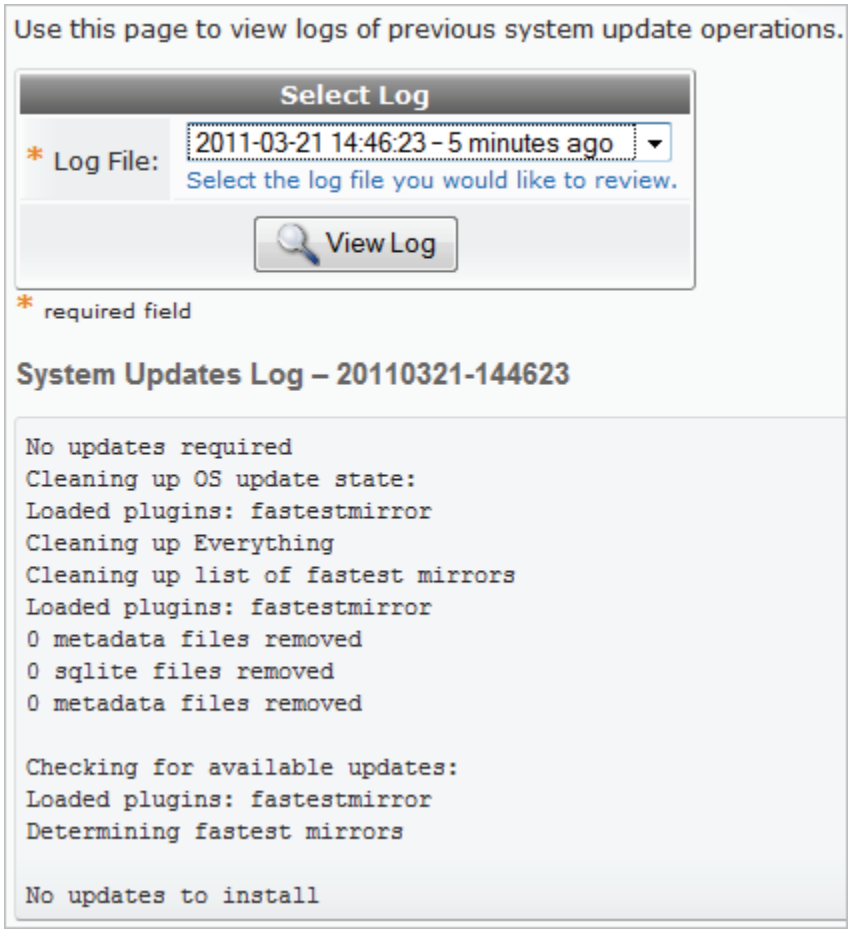
In some situations, manual OS updates may be required. Click the **Manual OS Updates** link to perform manual system maintenance tasks.

Manual Operating System Updates

Use the **Check For System Updates** command link to start a background check for any updates that may be available. If the system makes any changes, it automatically displays the most recent log file in the **System Updates Log** window.

Reviewing the Operating System Update Log

Use the **System Updates Log** command link to view log files from previous system update operations. To view log files from previous system update operations, click the **Log File** drop-down list, select the log file you want to display, then click **View Log**.



Determining Installed Operating System Packages

Use the Advanced view of the System Information page to display a list of the installed operating system packages, together with the corresponding version numbers.

Plugin Manager

Plugins are the software components that fit together to make your Web application. The Plugin Manager allows you to manage subscriptions, list available plugins, add new plugins, and check for updates to the installed plugins.

To access Plugin Manager tasks, navigate to **Administrator > Plugin Manager.** The Available Plugins page is displayed. Plugins are listed by category and include:

- Standard application plugins—Provide corresponding functionality for interactive use by operators
- Kernel plugins—Provide the basic framework for the application
- License plugins—Authorize access to features of the application
- Operator plugins—Conrol access to the Web application
- Skin plugins—Provide the style for the application's visual appearance
- Transaction processor plugins—Provide services primarily reserved for internal use by the software and are not exposed in the user interface

Plugins cannot be updated while High Availability is running. Because exact synchronization of the two servers is required for High Availability Services, you must first destroy the clusters, then re-create the

clusters after the plugins are updated. Please see Destroying a Cluster and Cluster Setup in the High Availability Services chapter.

Managing Subscriptions

A subscription ID is a unique number used to identify your software license and any custom software modules that are part of your ClearPass Guest solution. To view current subscription IDs, navigate to **Administrator > Plugin Manager,** then click **Manage Subscriptions**. The ClearPass Guest Subscription page opens.

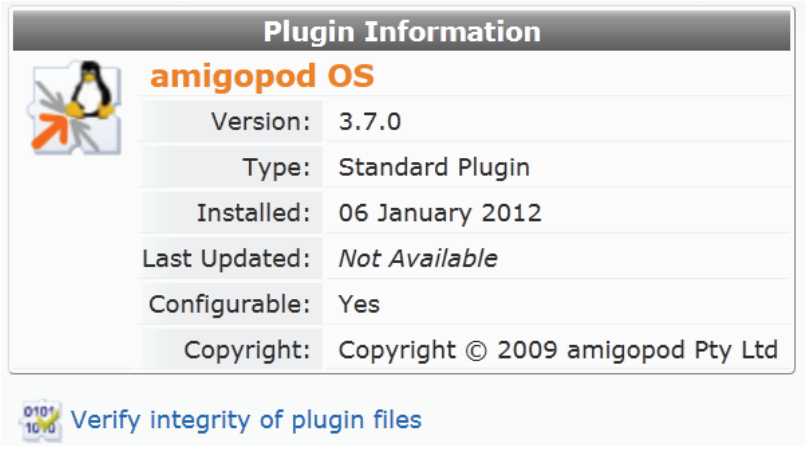
Comments can be added in front of the subscription ID if you place the subscription ID inside parentheses, for example, Hotspot Plugin (abc123-abc123-abc123-abc123-abc123) This allows you to keep track of which subscription ID is for which plugin. The above subscription would be for the Hotspot Plugin.

Viewing Available Plugins

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 and lets you manage them. Depending on the plugin, options in the list let you view details, configure, enable or disable, or remove the plugin. To view the list of available plugins, choose **Administrator > Plugin Manager > Manage Plugins**. The Available Plugins page opens.

Click a plugin's **Configuration** link to view or modify its settings. See "Configuring Plugins" in this chapter for details about the configuration settings.

The **About** link displays information about the plugin, including the installation date and update date. The About page for the Kernel and Administrator plugins also includes links to verify the integrity of all plugin files, or perform an application check.



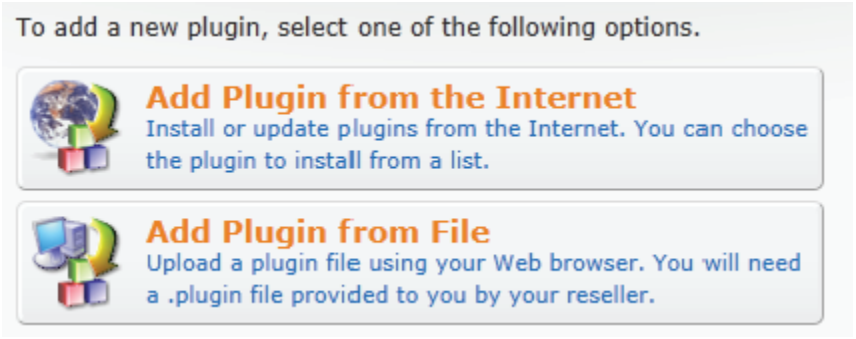
Use the **Disable**, **Enable** and **Remove** links to make changes to the available features of the application.

Plugins cannot be disabled or removed if other enabled plugins are dependent on them. An error message will be displayed if an operation is attempted that would leave the application in an inconsistent state.

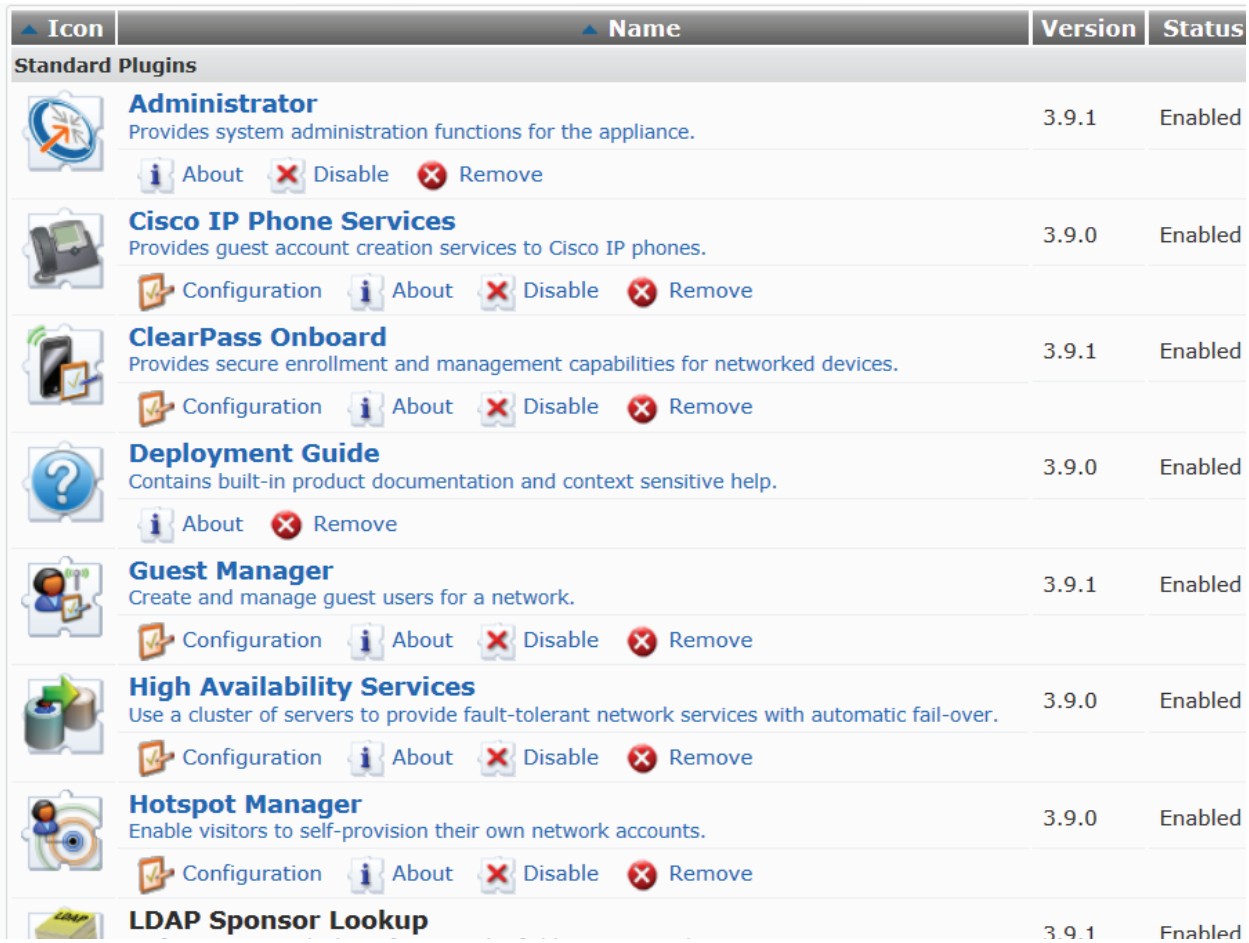
Adding or Updating New Plugins

You can add or update plugins either from the Internet or from a file provided to you by email.

- If your new plugin was emailed to you as a file, navigate to **Administrator > Plugin Manager > Add New Plugin**. On the Add New Plugin page, choose the Add Plugin from File command, then browse to the file to upload it. The Add New Plugin page also provides the option to choose the internet download method.



- To upload plugins or updates from the internet, navigate to **Administrator > Plugin Manager** and choose the Check for Updates command. The Add New Plugins page opens. Use this page to select the plugins or updates you want to install.



The default view of the Add New Plugins page lists all available updates and plugins that are not yet installed on your system. You can configure the list to display all plugins (including those already installed on the system) or just new plugins and updates. To change the list, click the **Display All Plugins** or **Display Changed Plugins** link.The default selections include all new plugins and any updated plugins that are available. To install the default selections, click the **Finish** button to download and install the selected plugins.

When you select multiple available updates on the Add New Plugins page and click the Finish button, the system updates them sequentially. If an update for one plugin cannot be completed—for example, due to low disk space—the update for that plugin is cancelled. The other updates are not affected, and the system continues to process the rest of the plugin updates in the queue.

NOTE

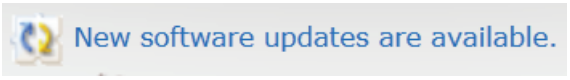
Plugins cannot be updated while High Availability is running, as exact synchronization of the two servers is required for High Availability Services. Please see Destroying a Clusterand Cluster Setupin the High Availability Services chapter.

Configuring Plugin Update Notifications

To have the system automatically check for plugin updates and provide notification when they are available, go to the **Administrator > Plugin Manager** page and click the **Configure Update Checks** command. The Check for Plugin Updates page opens.

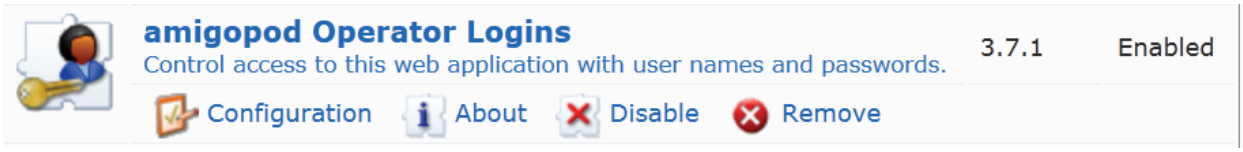
You can use the Plugin Updates form on this page to specify how often you want to be notified of plugin updates. The notification frequency may be set to daily, weekly, monthly, or disabled (the default).

When new updates are available, the following notification message is displayed at the top of the page. This message is only displayed to administrators.

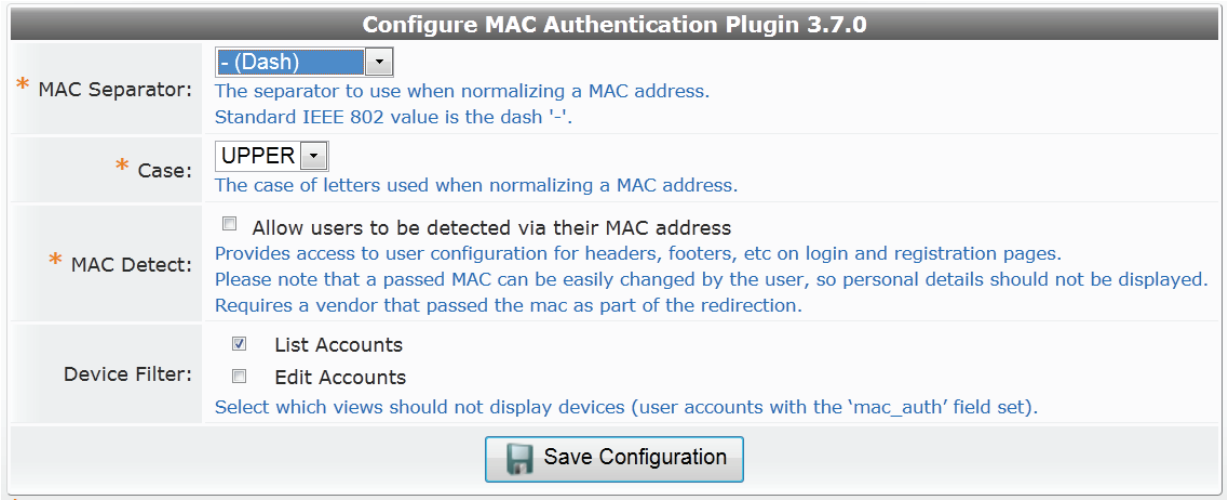


Configuring Plugins

You can configure most standard, kernel, and skin plugins. To view or change a plugin's configuration, go to the **Administrator > Plugin Manager** page and click the **List Available Plugins** command. Depending on the plugin, options in the Available Plugins list let you view details, configure, enable or disable, or remove the plugin. Plugins cannot be disabled or removed if other enabled plugins are dependent on them. An error message is displayed if an operation is attempted that would leave the application in an inconsistent state.



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.



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.

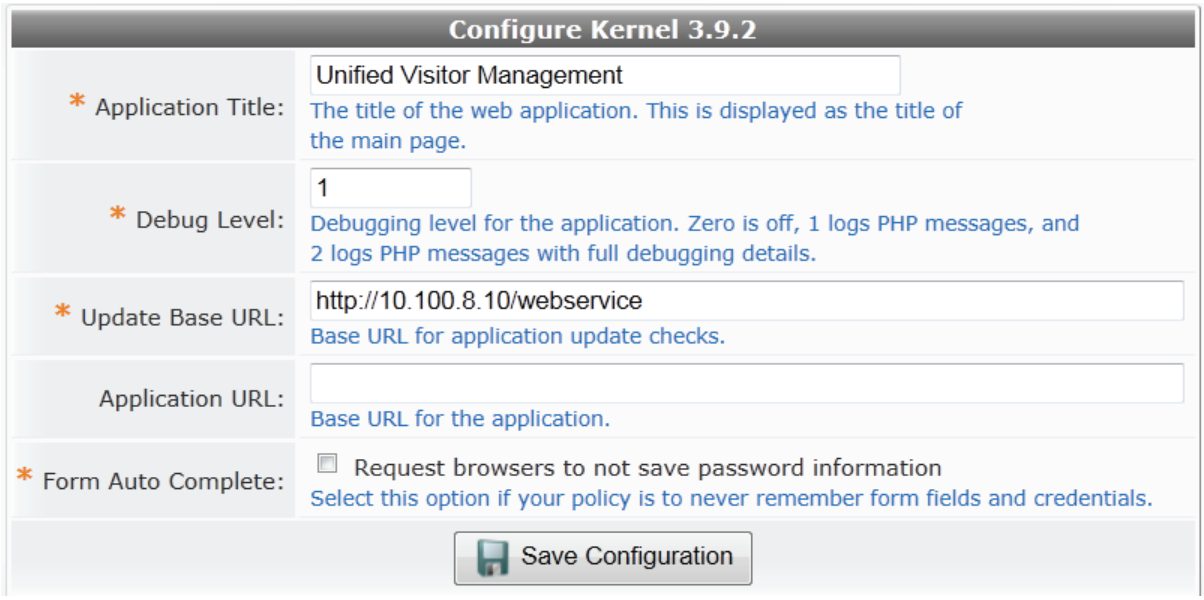
In most cases, plugin configuration settings do not need to be modified directly. Use the customization options available elsewhere in the application to make configuration changes.

For more information about plugin configuration:

- **Kernel**— See "Configuring the Kernel Plugin" in this chapter
- **Operator Logins**— See "Security Manager" in this chapter
- **Operating System**— See "Security Manager" in this chapter
- **RADIUS Services**— See "Server Configuration" in the RADIUS Services chapter
- **Aruba ClearPass Skin—** See "Configuring the Aruba ClearPass Skin Plugin" in this chapter
- **Guest Manager**— See "Default Settings for Account Creation" in the Guest Management chapter
- **SMS Services**— See "Sending an SMS" in the Guest Management chapter
- **SMTP Services**— **See "SMTP Services"** in the Guest Management chapter
- **MAC Authentication**— See "MAC Authentication in ClearPass Guest" in the Guest Management chapter

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.

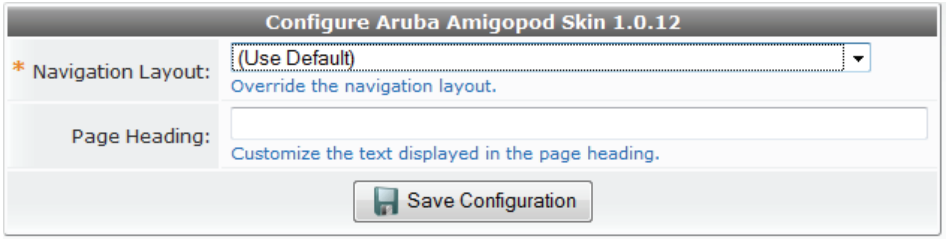


1. To change the application's title, enter the new name in the **Application Title** field (for example, your company name) to display that text as the title of your Web application. Click **Save Configuration**.
2. TheKernel plugin's **Debug Level**, **Update Base URL** and **Application URL** options should not be modified unless you are instructed to do so by Aruba support.
3. To turn off autocomplete on forms, mark the check box in the **Form Auto Complete** row. This disables credentials caching.
4. To restore the plugin's configuration to the original settings, click the **Restore default configuration** link below the form. 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.
5. 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.

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, 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.

1. To modify the standard Aruba ClearPass skin plugin, click its **Configuration** link on the Available Plugins page.



2. The default navigation layout is “expanded.” To change the behavior of the navigation menu, click the **Navigation Layout** drop-down list and select a different expansion level for menu items.
3. The **Page Heading** field allows you to enter additional heading text to be displayed at the very top of the page.

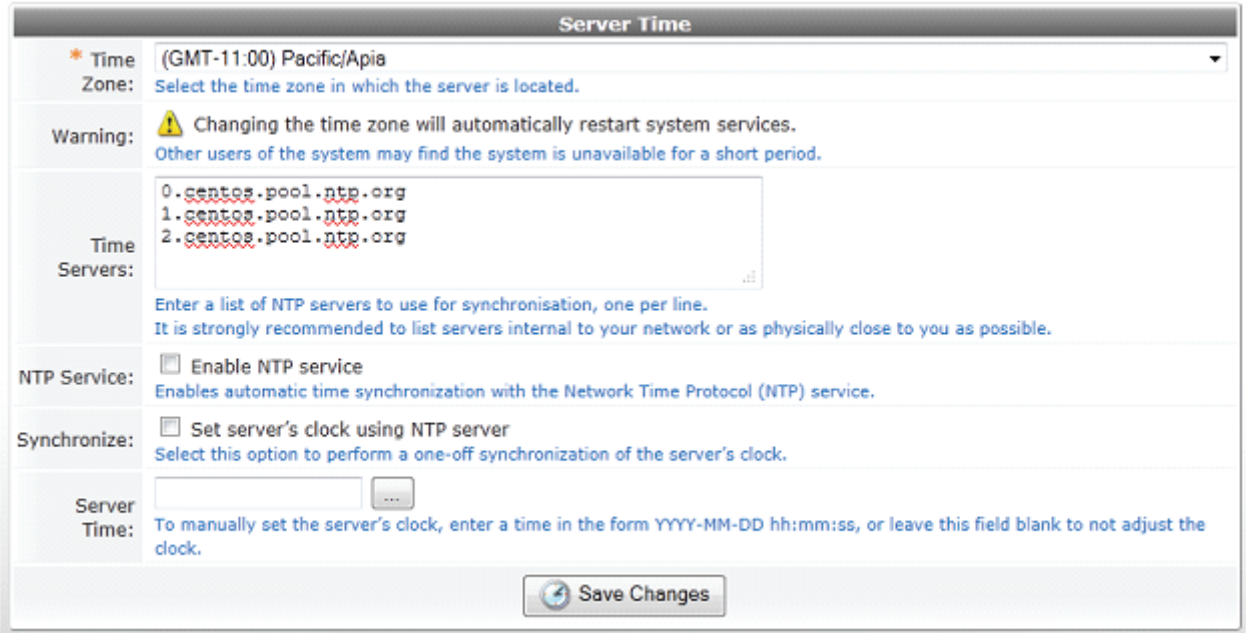
The default skin used by the ClearPass Guest application is the one that is enabled in the Plugin Manager. To change the default skin globally, navigate to the plugin list and click the **Enable** link for the skin you would like to use as the default. When you install a new custom skin, it is automatically 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” in the Operator Logins chapter.
- To use a different skin for an individual operator login, see “Local Operator Authentication” in the Operator Logins chapter.
- To have the login page use a different skin than the rest of the application, see “Operator Logins Configuration” in the Operator Logins chapter.
- To specify a skin for a customized guest self-registration page, see “Configuring Basic Properties for Self-Registration” in the Guest Management chapter.

Server Time

The **Server Time** form allows you to configure the time and date properties of the ClearPass Guest interface.



To ensure that authentication, authorization, and accounting (AAA) is performed correctly, it is vital that the server maintains the correct time of day at all times. It is strongly recommended that you configure one or more NTP servers to automatically synchronize the server's time.

NTP can interfere with timekeeping in virtual machines. The default virtual machine configuration will automatically synchronize its time with the host server, and so you should not configure NTP if you are using virtualization for ClearPass Guest. However, make sure that the host is configured to keep its clock in sync with a suitable time source.

If one is available, it is strongly recommended that you use an NTP server that is available on your local network. This will improve timekeeping and will eliminate the need for additional Internet traffic for the time server.

To use a public NTP server, enter the following hostnames:

```
0.pool.ntp.org
1.pool.ntp.org
2.pool.ntp.org
```

You can also use NTP pool servers located in your region. For more information, refer to the NTP Pool Project Web site: http://www.pool.ntp.org.

Select the **Set server's clock using NTP server** check box to perform a single clock synchronization with the specified time servers. The synchronization will take place when you click the Save Changes button.

You should provide a local NTP server. Do not use the default setting as this may be unreliable.

To set the server's time manually, enter a value in the Server Time field using the recommended format, or click the **...** button to display a date/time chooser.

Click the **Save Changes** button to apply the new time and date settings.

If the server's clock is running slow, changing the server's time may cause your current login to expire. In this case you will need to log in again after clicking the Save Changes button.

System Control

The **System Control** commands on the **Administrator > System Control** page allow you to:

- Shut down the server immediately.
- Reboot the system which stops all services while the reboot is taking place.
- Restart the system services without stopping the server. This would usually be done after a plugin installation if required, or if performing other system changes such as installing a new SSL certificate or changing the server's time zone.
- Schedule a reboot or shutdown operation to take place at a future point in time.
- Configure the database and advanced system settings
- Configure system-level log files
- Configure Web servers and Web applications.

Changing System Configuration Parameters

The **System Configuration** form allows "sysctl" parameters to be modified. These parameters may be used to adjust advanced networking and kernel options and control other system properties that apply at the operating system level.

Changing kernel options to incorrect values can result in a non-functional system. For this reason it is recommended not to change these values unless you are advised by Aruba support, or you have carefully tested the result of the change in a controlled environment.

Click the **Save Changes** button to apply the new configuration parameters. The settings will be applied to the operating system immediately, but in some cases the new settings will not take effect until the system is rebooted. For this reason, it is recommended that you always reboot after modifying any of these parameters.

System Log Configuration

The **System Log Configuration** form allows you to modify options related to locally stored system log files, including the HTTP access log, HTTP error log, and the general-purpose system message log. You can also define a remote syslog server to which log messages will be sent, and specify which syslog messages should be sent.

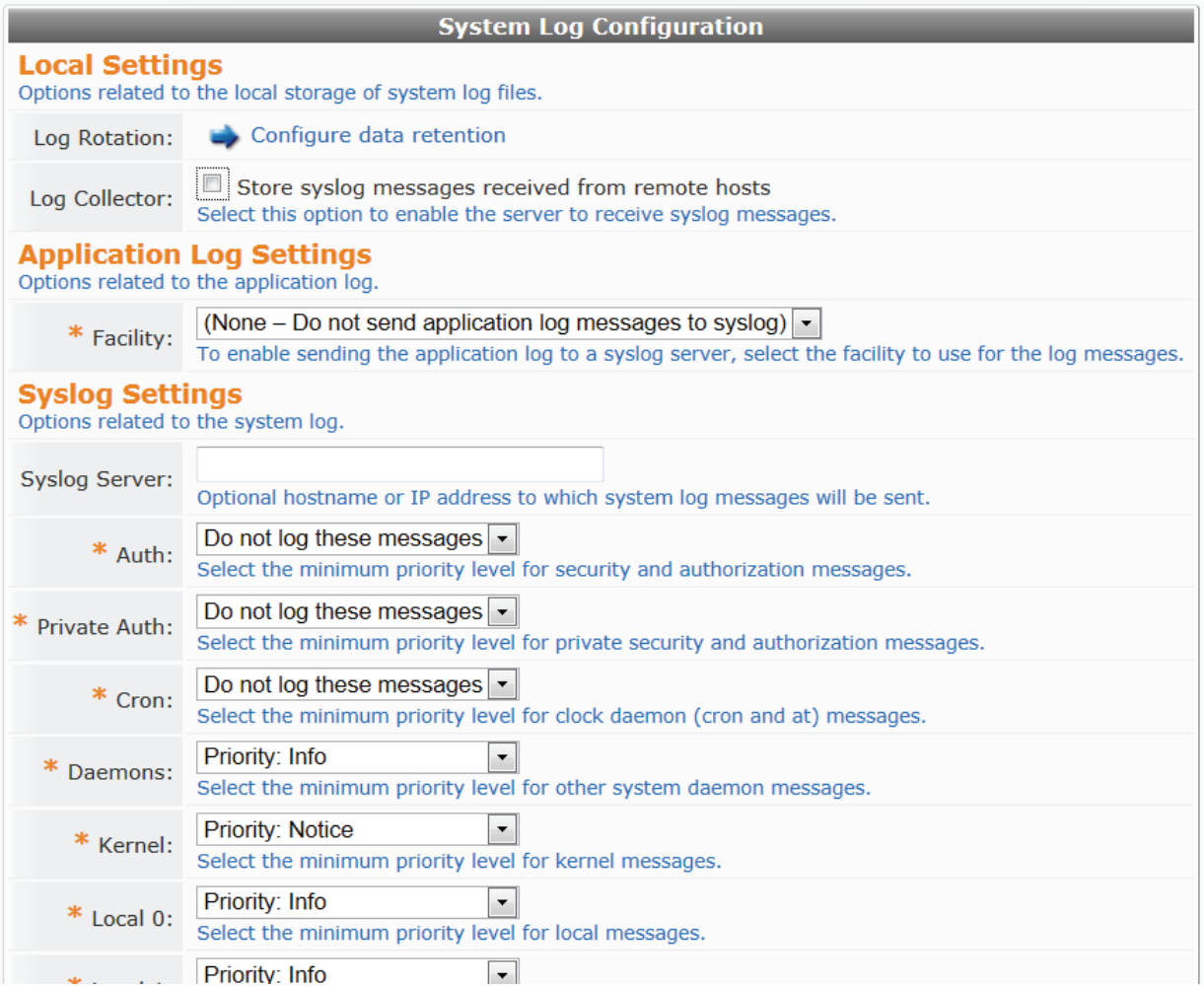
The syslog protocol is used to send log messages from one system to a syslog server (also known as a 'collector'). Log messages are grouped according to both facility and priority.

The following priority levels are defined in the protocol:

- 0—Emergency: system is unusable
- 1—Alert: action must be taken immediately
- 2—Critical: critical conditions
- 3—Error: error conditions
- 4—Warning: warning conditions

- 5—Notice: normal but significant condition
- 6—Informational: informational messages
- 7—Debug: debug-level messages

When a syslog server has been defined, messages matching the rules defined here are sent to the syslog server. The syslog protocol uses UDP port 514.



Log Rotation: Configuring Data Retention

To configure the number of weeks to retain records for data, log files, disabled accounts, and mobile device certificates, click the **Configure data retention** link in **Log Rotation** row. The Data Retention Policy page opens. Log files are rotated and expired logs are cleared according to the database maintenance schedule you define. See Managing Data Retention.

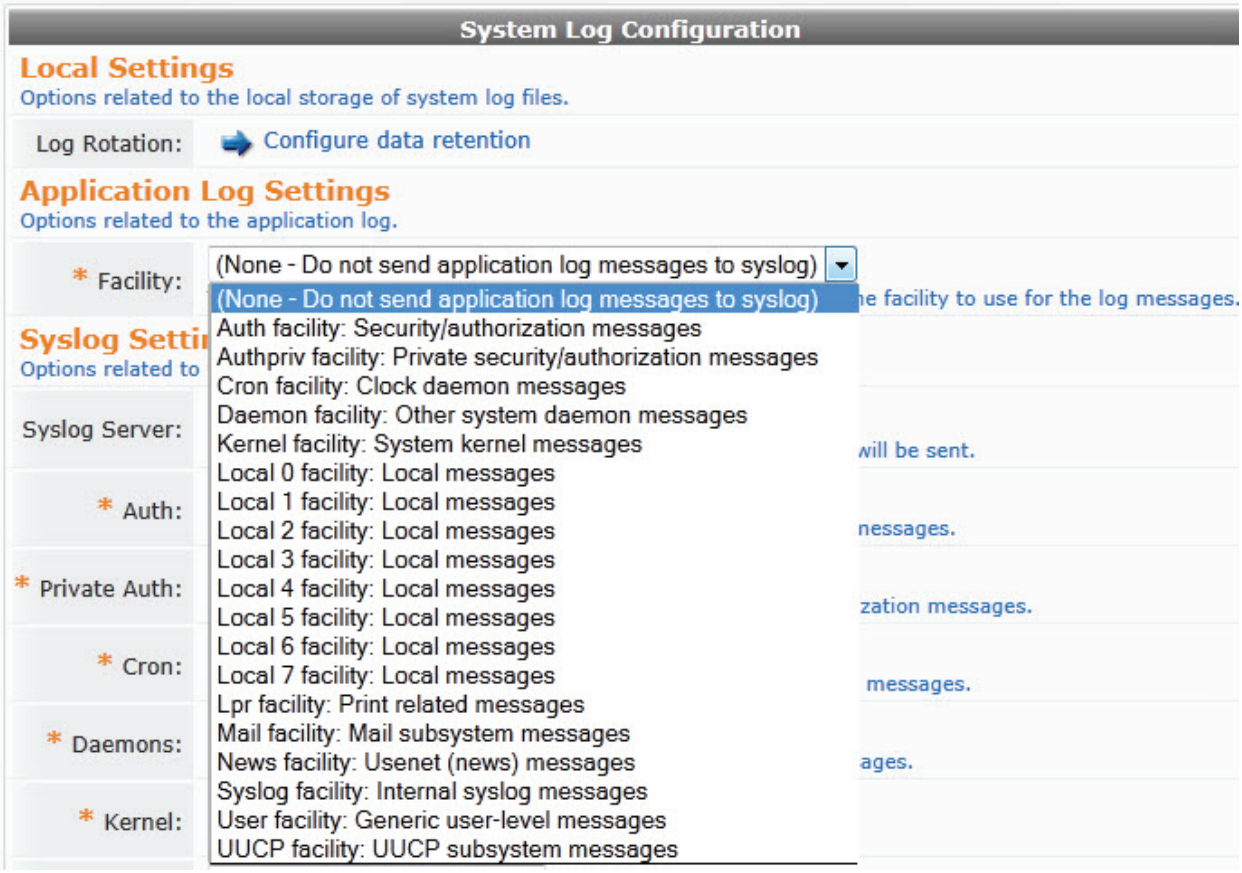
Log Collector: Storing Incoming Syslog Messages

Your ClearPass Guest server can also act as a syslog server. To configure the ClearPass Guest server to receive syslog messages sent by remote hosts in the network, mark the check box in the **Log Collector** row. The **Allowed Access** row is added. You can specify IP addresses and networks from which messages may be received, or allow syslog messages to be received from any IP address.

Storing incoming syslog messages can use a lot of disk space. If you choose the log collector option, be sure to set appropriate data retention limits and enable low disk space notifications.

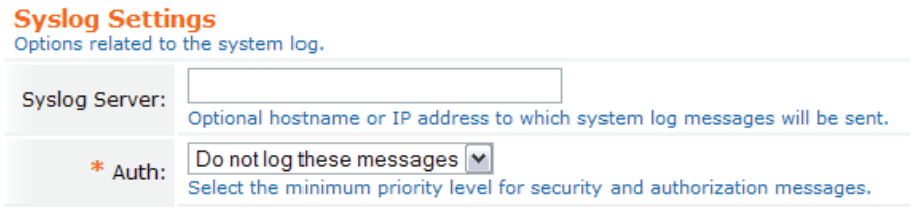
Facility: Redirecting Application Log Messages

To redirect log messages from the application log to the syslog, select an option from the **Facility** field drop-down menu. The default option **None – Do not send application log messages to syslog** stores all application-generated messages in the separate application log. If you select a specific syslog facility, the minimum priority level for the corresponding syslog facility determines whether the syslog message is forwarded to the remote collector.



For details on defining a database maintenance schedule, See "Changing Database Configuration Parameters" in this chapter.

For high-traffic sites that are maintaining many weeks of log files, enter a non-zero value for Disk Space to ensure that the log files cannot fill up the system's disk. If the disk space check is enabled, the server's free disk space is checked daily at midnight, and if it is below the specified threshold, old log files are deleted to free up space.



The syslog protocol is used to send log messages from one system to a syslog server (also known as a 'collector'). The syslog protocol uses UDP port 514. Log messages are grouped according to both facility and priority.

System log messages can be sent to multiple syslog collectors. In the **Syslog Server** row of the System Log Configuration page, you may enter multiple syslog collectors as a comma-separated list of hostnames or IP addresses.

When a syslog server has been defined, messages that match the rules defined in this form will be sent to the specified syslog server.

The following priority levels are defined in the syslog protocol, which is fully specified in RFC 3164:

Table 35 *Sylog Priority Levels*

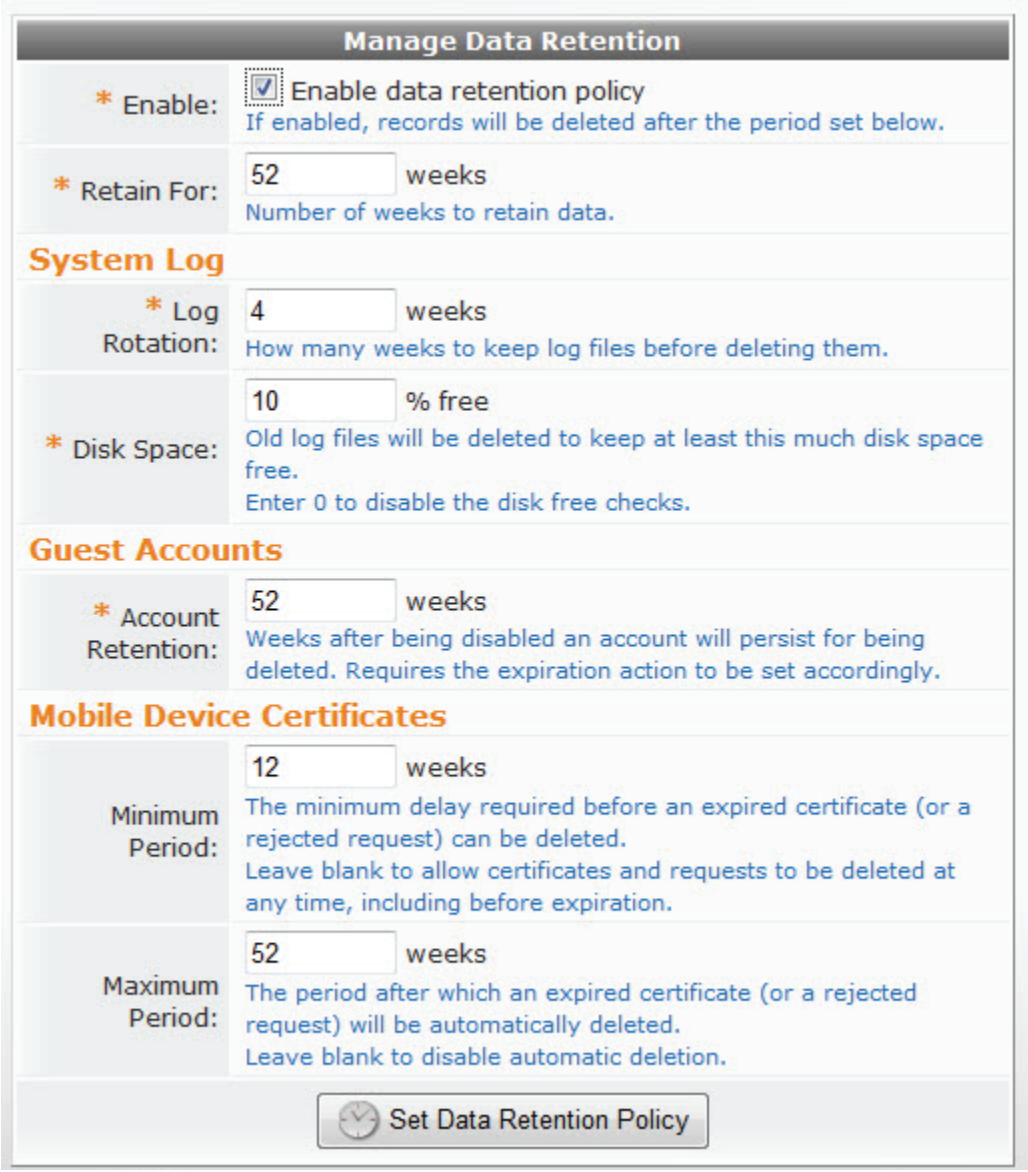
Level	Name	Meaning
0	Emergency	System is unusable
1	Alert	Action must be taken immediately
2	Critical	Critical conditions that warrant urgent attention
3	Error	Error conditions that should be investigated more closely
4	Warning	Warning conditions that may need to be investigated more closely
5	Notice	Normal but significant condition
6	Informational	Informational messages
7	Debug	Debugging messages

Click the **Save Changes** button to apply the new system log parameters. The changes will take effect immediately.

Managing Data Retention

The Data Retention Policy page (**Administrator > System Control > Data Retention**) lets you manage historical data by archiving or deleting it. For a data retention policy to take effect, you must schedule and enable database maintenance. To do this, go to **Administrator > System Control > Database Config**.

Figure 48 *Data Retention Policy page*



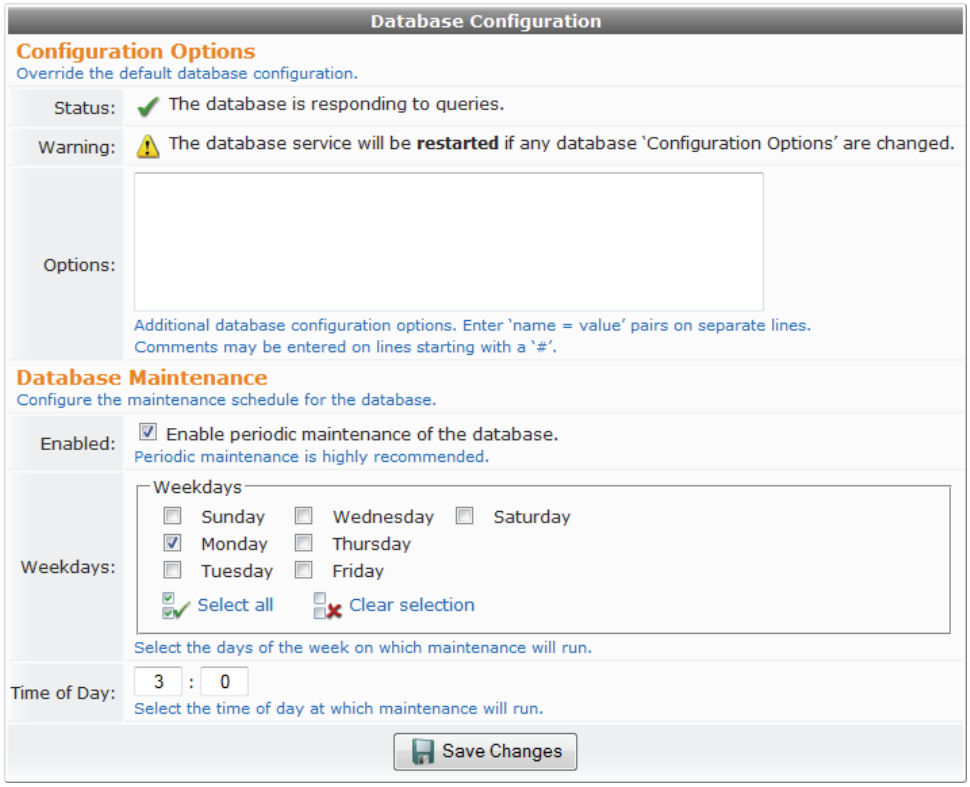
Select **Enable** to enable the the data retention policy opton and enter how many weeks in the **Log Rotation** field to indicated how many weeks you want log files kept before they are deleted.

You can specify how many weeks a guest account persists after the account is disabled in the **Guest Accounts** field.

For mobile device certificates, select the minimum delay, in weeks, required before an expired certificate or rejected request can be deleted. The maximum period is the number of weeks after which an expired certificate is automatically deleted.

Changing Database Configuration Parameters

The **Database Configuration** form allows you to configure the system's database and manage its maintenance schedule. Access this form by navigating to **System Control > Database Config**.

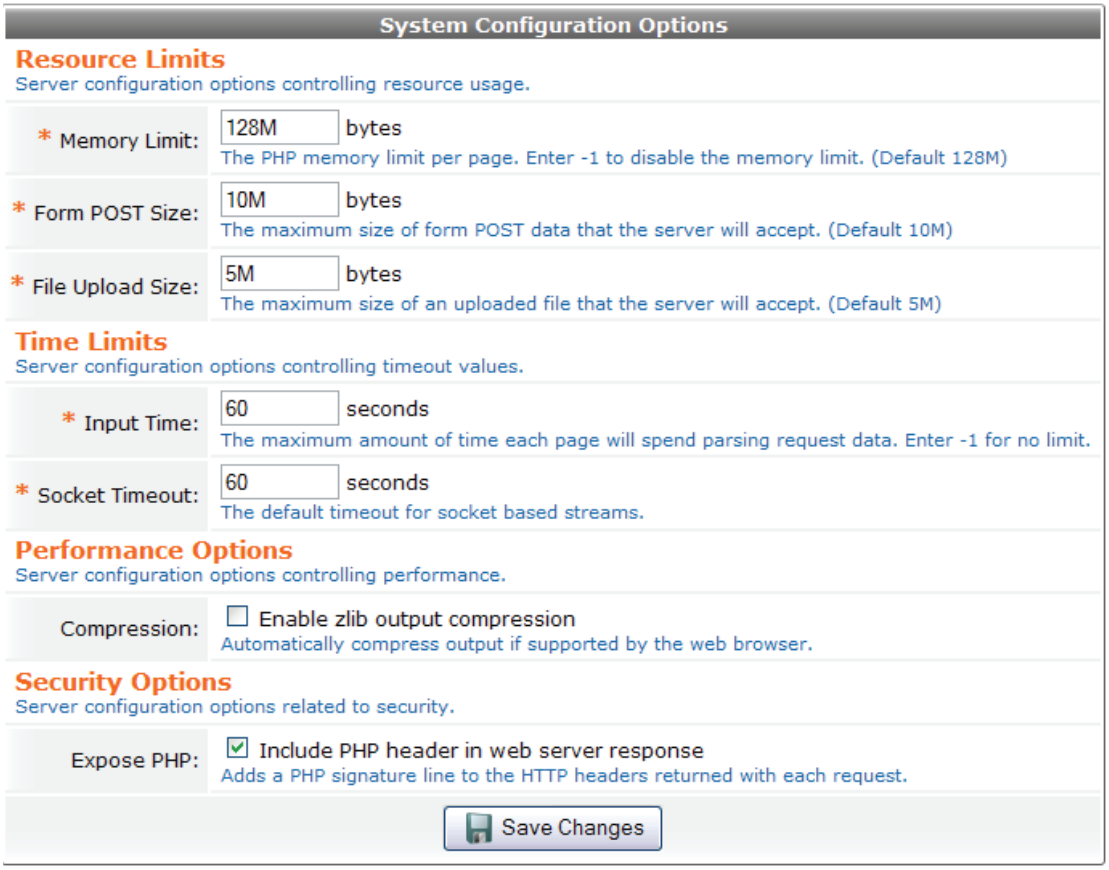


The **Options** field is a text field that accepts multiple **name = value** pairs. You can also add comments by entering lines starting with a **#** character.

The Database Maintenance of this form allows you to adjust the time (or times) at which the system will run maintenance tasks and remove expired log files. You should adjust the maintenance schedule to coincide with those times when your system is least in use. A periodic maintenance schedule is highly recommended. You should not disable periodic maintenance unless you have a specific requirement.

Changing Web Application Configuration

Certain performance and security options may be configured that affect the operation of the Web application user interface. Use the **Web Application Co nfiguration** command link to adjust these configuration parameters.



The **Memory Limit** may be increased to allow larger reports to be run on the system.

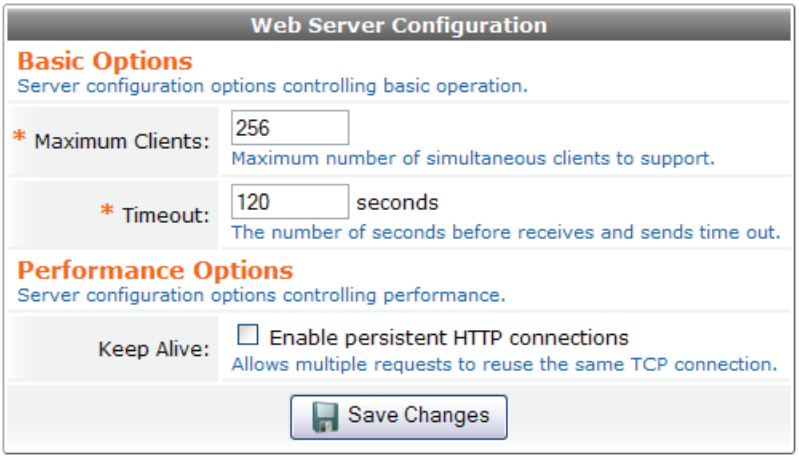
The **File Upload Size** may be increased to allow larger content items to be uploaded, or larger backup files to be restored.

Use the **Enable zlib output compression** check box to compress output sent to the Web server. This option may provide faster loading pages, particularly on slow networks, but may also increase the CPU load on the server.

Click the **Save Changes** button to apply the new Web application configuration parameters. Changing the parameters requires the Web server to be restarted, which will be performed immediately. Other users of the system may find the system is unavailable for a short period while the restart takes place.

Changing Web Server Configuration

High-traffic deployments may need to adjust certain performance options related to the system's Web server. Use the Web Server Configuration command link to adjust these configuration parameters.



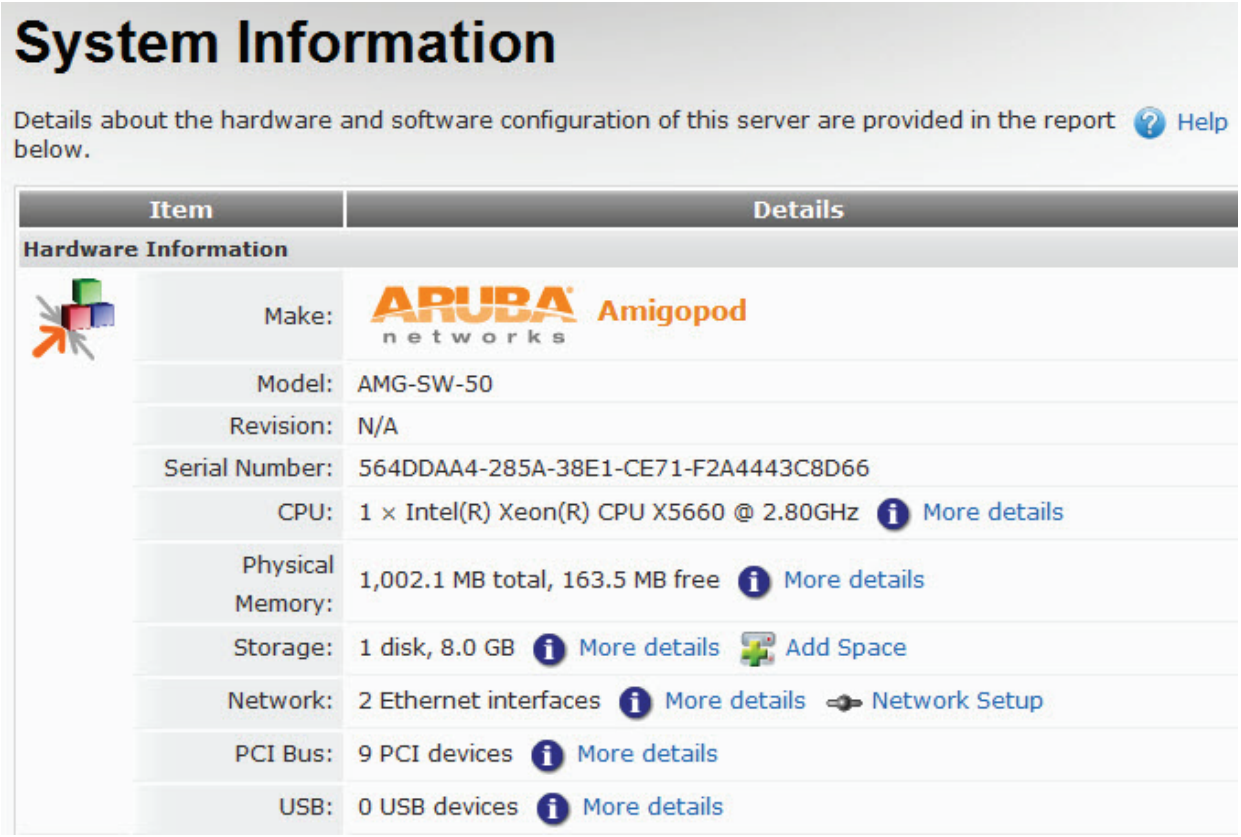
The **Maximum Clients** option specifies the maximum number of clients that may simultaneously be making HTTP requests. The default value should only need to be increased for high-traffic sites.

Persistent HTTP connections (also known as pipelining) may be enabled using the **Enable persistent HTTP connections** check box. This feature is only supported for HTTP 1.1 compliant clients.

Click the **Save Changes** button to apply the new Web server configuration parameters. Changing the parameters requires the Web server to be restarted, which will be performed immediately. Other users of the system may find the system is unavailable for a short period while the restart takes place.

System Information

The System Information link on the **Administrator > System Information** page provides a summary of hardware, operating system and software information, as well as a snapshot of the current state of the system.



This report can be downloaded for support purposes.

Adding Disk Space

Storage capacity can be increased on VMware-based deployments. To increase available storage, click the **Add Space** option on the **System Information** screen. TheAdding Disk Space screen appears. Follow instructions on this page.

Add Disk Space

How To Add Disk Space

If you need to increase the server's available storage capacity, follow these steps:

1. Ensure that you have a complete backup of the server.
   Configuration Backup
2. Add a new disk to the server.

   For **VMware ESXi** and **VMware Player**:
   - Edit the settings of the virtual machine, and then click **Add...** to add new hardware.
   - Using the Add Hardware Wizard, create a new SCSI disk and add it to the virtual machine.
   - Once you have completed the wizard, refresh this page.
     Refresh

   For **VMware Fusion**:
   - You must power off the virtual machine before you can edit its settings.
   - Once you have added a new disk, power on the virtual machine.
   - After the virtual machine has restarted, refresh this page.
     Refresh

   Do not change the size of any existing disk in the virtual machine.
   This is not a supported operation and could lead to data loss.

   If you are using another virtualization product, refer to the appropriate documentation for instructions on modifying the virtual machine's configuration.

3. You can repeat this process in the future to add more disk space as required.

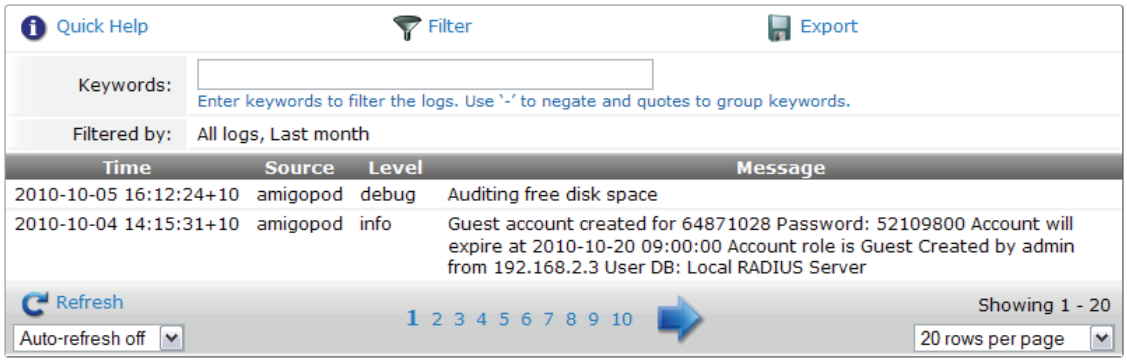
Add Disk Space

Use this form to add more disk space to the server.

System Log

The system log viewer available on the **Support > System Logs** page displays messages that have been generated from multiple different sources:

- **Application Logs**—messages generated by the ClearPass Guest application.
- **HTTP Logs**—messages generated by the Apache Web Server.
- **RADIUS Logs**—messages generated by the RADIUS server during authentication, authorization or accounting.
- **System Logs**—messages generated by the system and various internal processes within it. Depending on the plugins you have installed, additional message sources may also be included in the system log viewer.



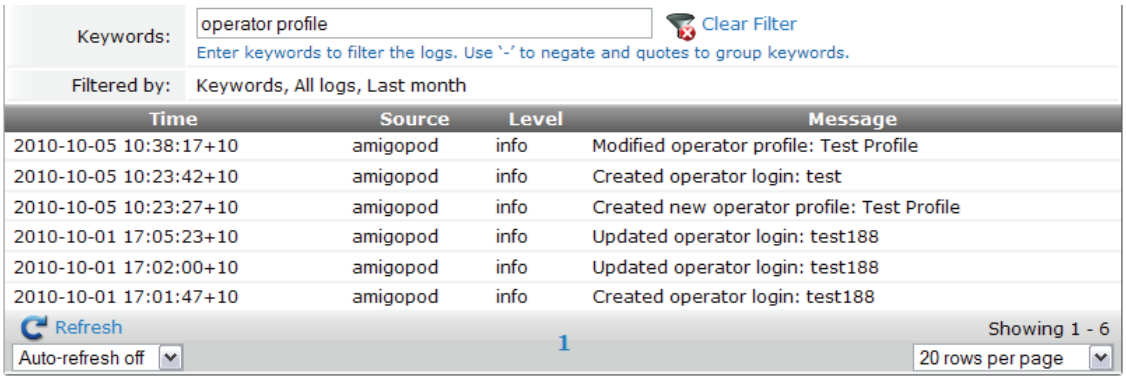
The information shown in the table is a summary of the log message. Click a log entry in the table to view the details of the log message.

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.

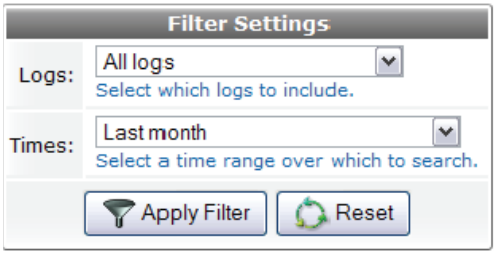
Use the **Refresh** link, or the Auto-refresh drop-down list, to keep the displayed log messages up to date.

Filtering the System Log

Use the Keywords field to perform a keyword search. Only the log messages that match the keywords entered are displayed. Click the **Clear Filter** link to restore the default view.



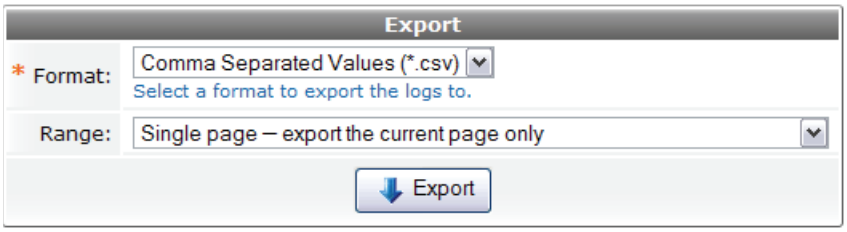
Use the **Filter** tab to control advanced filtering settings, such as which logs to search and the time period to display:



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.

Exporting the System Log

Use the **Export** tab to save a copy of the system logs, in one of several formats.



Select one of the following formats from the Format drop-down list:

- **Comma Separated Values (*.csv)** – the data contains a header row with five exported fields:

  ```
  timestamp,source,level,message,detail
  ```

- **HTML document (*.html)** – the exported data is contained in a table with four columns: Time, Source, Level, Message
- **Tab Separated Values (*.tsv)** – the data contains a header row with five exported fields:

  ```
  timestamp source level message detail
  ```

- **Text file (*.txt)** – the data contains a line for each log message, including the timestamp, source, level and message. The details follow on lines that start with a space.

  ```
  [2010-10-04 14:15:31+10] ClearPass Guest info Guest account created for 98084707
  ```

- **XML document (*.xml)** – the exported data is contained within the `<system-logs>` element's `<records>` element.

Use the Range option and the Download Limit field to specify whether the current page or all matching log messages are included in the export.

Viewing the Application Log

The events and messages generated by the application are displayed in a table on the **Support > Application Log** page.

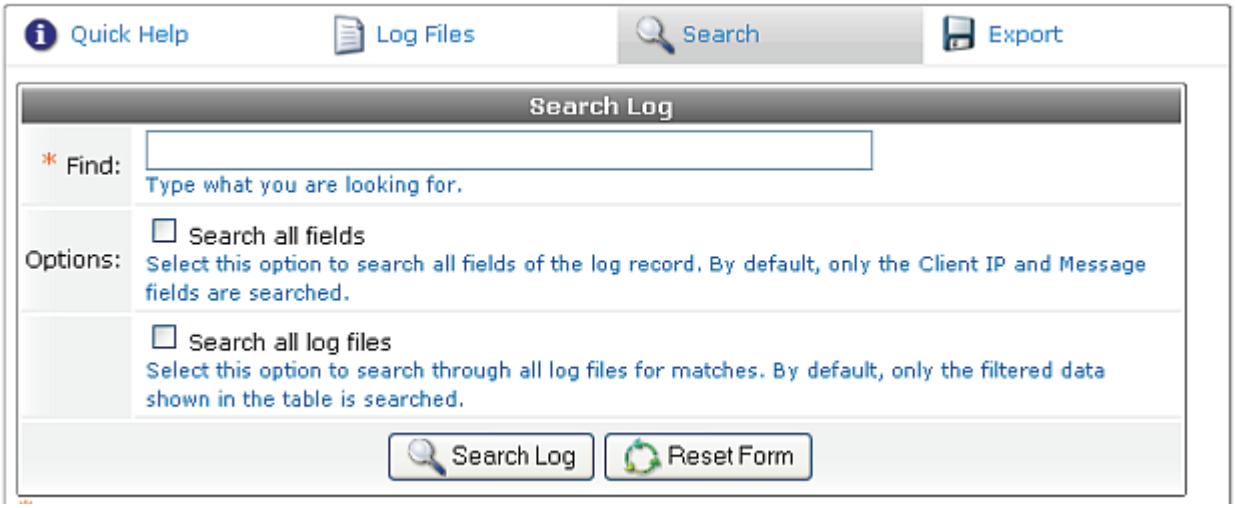
The System Logs viewer is recommended for viewing and searching all system logs, including the application log. A link to the system log viewer is provided at the bottom of the Application Log table.

In the Application Log view, you can click an event for in-depth information about it. You can double-click the row of the log entry to close it.

The Application Log lists the events and messages for the current month. To view events and messages from previous months, select the month from the drop-down list displayed at the top of the table when you click the **Log Files** tab.

Searching the Application Log

You are able to search for particular log records using the form displayed when you click the **Search** tab.



Click the **Reset Form** button to clear the search and return to displaying all records in the log.

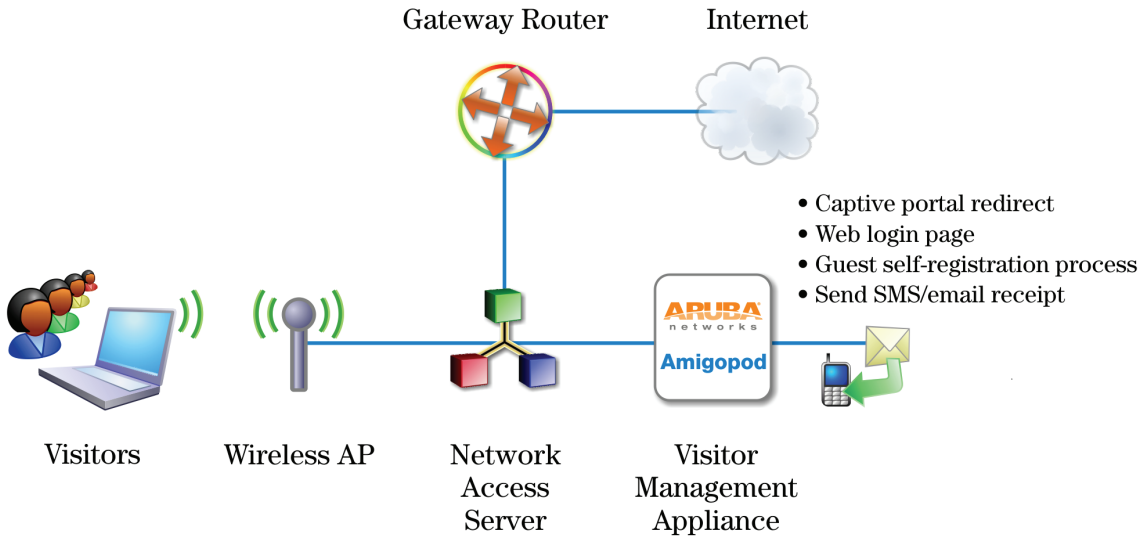
Exporting the Application Log

Use the **Export** tab to save the log in other formats, including HTML, text, CSV, TSV and XML. You can select options to print, email or download the data.

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.

The following diagram shows how the process of customer self provisioning works.

Figure 49 *Guest self-provisioning*



- Your customer associates to a local access point and is redirected by a captive portal to the login page.
- Existing customers may log in with their Hotspot username and password to start browsing.
- New customers click the **Hotspot Sign-up** link.
- On page 1, the customer selects one of the Hotspot plans you have created.
- On page 2, the customer enters their personal details, including credit card information if purchasing access.
- The customer's transaction is processed, and if approved their visitor account is created according to the appropriate Hotspot plan.
- On page 3, the customer receives an invoice containing confirmation of their transaction and the details of their newly created visitor account.
- The customer is automatically logged in with their username and password, providing instant Hotspot access.

Manage Hotspot Sign-up

You can enable visitor access self provisioning by navigating to **Customization > Hotspot Manager** and selecting the **Manage Hotspot Sign-up** command. This allows you to change user interface options and set global preferences for the self-provisioning of visitor accounts.

The **Enable visitor access self-provisioning** check box must be ticked for self-provisioning to be available.

The **Require HTTPS** field, when enabled, redirects guests to an HTTPS connection for greater security.

The **Service Not Available** Message allows a HTML message to be displayed to visitors if self-provisioning has been disabled. **See "Smarty Template Syntax"** in the Reference chapter for details about the template syntax you may use to format this message.

Click the **Save Changes** button after you have entered all the required data.

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.spiffywidgets.com/hotspot_plan.php.

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.spiffywidgets.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.

Look and Feel

The skin of a Web site is its external look and feel. It can be thought of as a container that holds the application, its style sheet (font size and color for example), its header and footer and so forth.

The default skin used by ClearPass Guest is the one that is enabled in the Plugin Manager. The skin is seen by all users on the login page.

SMS Services

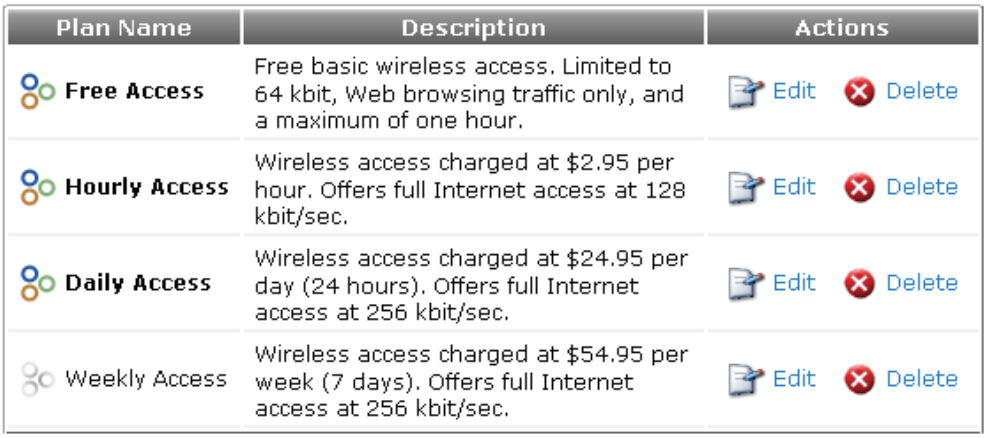
Configure the following settings in the **SMS Services** section of the **Hotspot Preferences** form to override the default SMS settings with your own custom configuration.

- **SMS Receipt**: Click this drop-down list to select the template you want to use for SMS receipts. The default value is **SMS Receipt**.
- **Phone Number Field**: Click this drop down list and identify the field that contains the visitor's phone number. The default value is **visitor_phone**.
- **Auto**-Send Field: Click this drop-down list and select the field which, when configured with any string or non-zero value, will trigger the automatic sending of an SMS receipt. The default value of this field is **auto_send_sms**.

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.

You can customize which plans are available for selection, and any of the details of a plan, such as its description, cost to purchase, allocated role and what sort of username will be provided to customers.



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

Above is the list of default plans provided by the application. Plans that you have enabled have their name in bold with the following icon: . Plans that have not been enabled do not have names in bold and their icon is a little different: . You are able to edit these plans, delete these plans as well as add your own plans. Once a plan has been deleted it is not possible to undo the deletion.

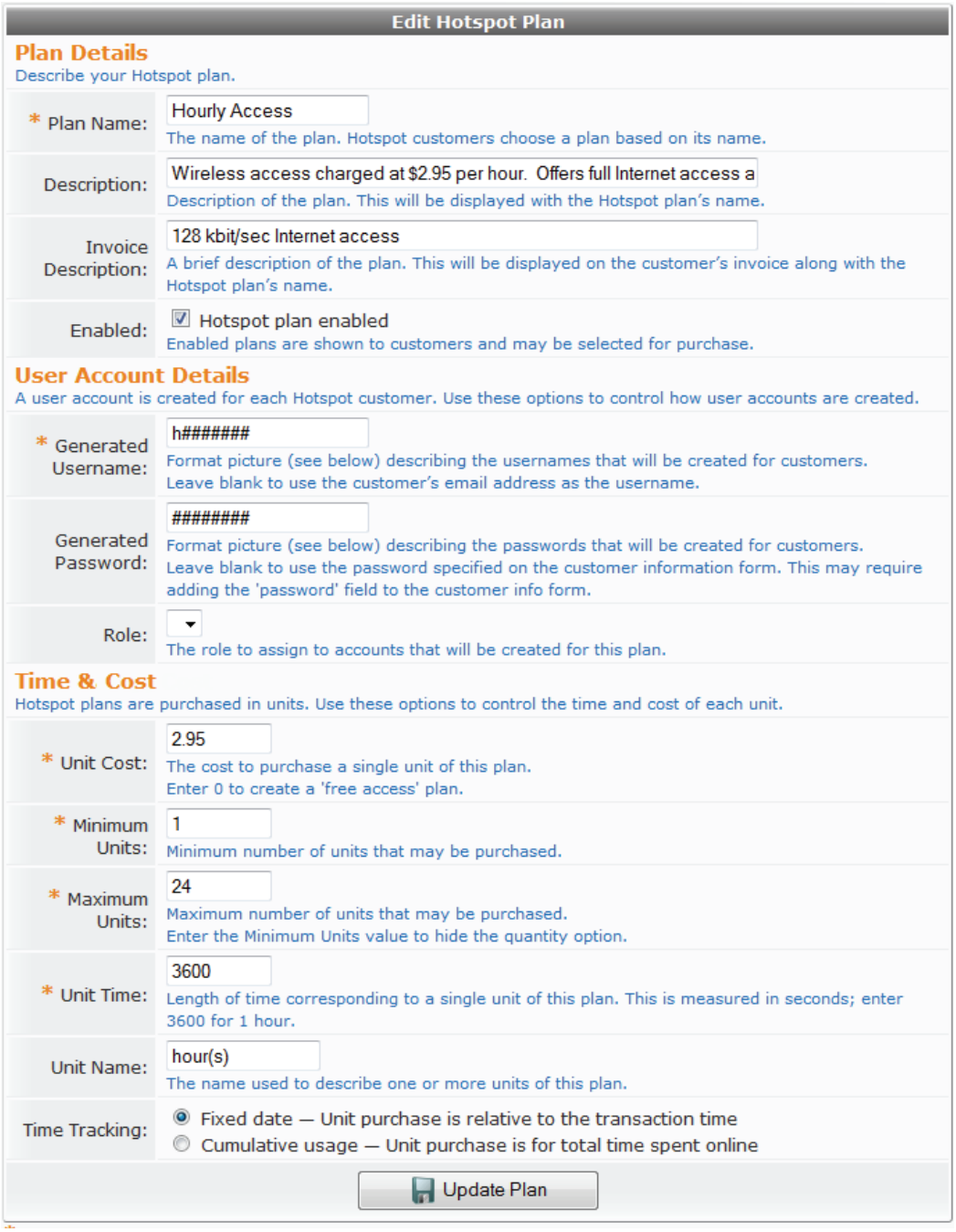
Modifying an Existing Plan

Click the **Edit** link next to a plan to modify it. The **Edit Hotspot Plan** appears.

You may alter the fields to meet the requirements of your company.

Creating New Plans

Custom hotspot plans are added by clicking the **Create Hotspot plan** button. The following form is displayed.



Click the **Create Plan** button to create this plan for use by your Hotspot visitors.

See "Format Picture String Symbols" in the Reference chapter for a list of the special characters that may be used in the Generated Username and Generated Password format strings.

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:

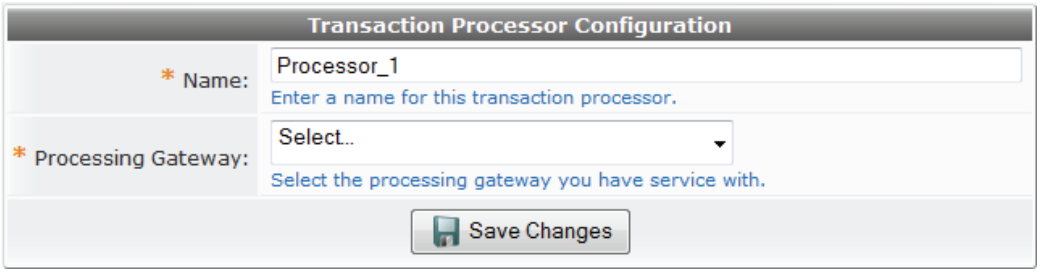
- Authorize.Net AIM
- CyberSource

- eWAY
- Netregistry
- Paypal
- WorldPay

ClearPass Guest also includes a Demo transaction processor that you can use to create hotspot forms and test hotspot transactions.

Creating a New Transaction Processor

To define a new transaction processor, navigate to **Customization > Hotspot Manager**, click **Manage Transaction Processors**, then select **New Transaction Processor**.



In the **Name** field, enter a name for the transaction processor.

Click **the processing gateway** drop-down list and select the gateway with which you have a service account to display additional configuration fields for that gateway type. Each transaction processing gateway type requires unique merchant identification, password and configuration information. 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 Existing Transaction Processors

Once you define a transaction processor, it will appear in the transaction processor list. When you select an individual processors in the list, the list displays a menu that allows you to perform the following actions:

- **Edit** – changes the properties of the specified transaction processor
- **Delete** – removes the processor from the Transaction Processors list
- **Duplicate** – creates a copy of a transaction processor
- **Show Usage** – opens a window in the Transaction Processors list that shows if the profile is in use, and lists any hotspots associated with that transaction processor. Each entry in this window appears as a link to the **General Hotspot References** form that lets you change the transaction processor associated with that hotspot.

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 by using the **Manage Hotspot Customer Information** command.

See "Duplicating Forms and Views" in the Guest Management chapter for information about the form field editor which may be used to make changes to the customer information form.

Managing Hotspot Invoice

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.

The Invoice Title must be written in HTML. See "Basic HTML Syntax" in the Reference chapter for details about basic HTML syntax.

You are able to use Smarty functions on this page. See "Smarty Template Syntax" in the Reference chapter for further information on these.

You are able to insert content items such as logos or prepared text. See "Customizing Self Provisioned Access" in the Guest Management chapter for details on how to do this.

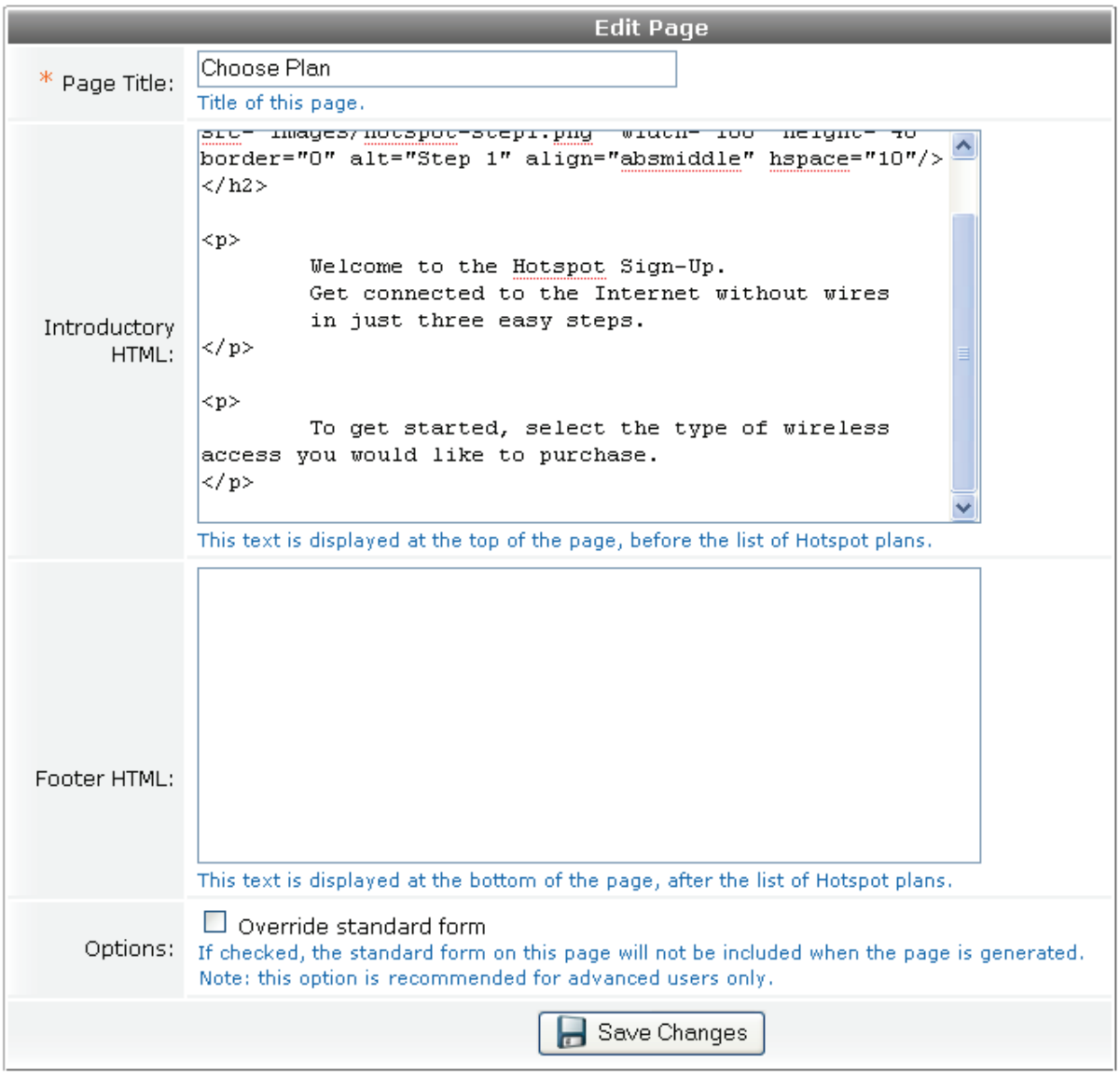
Click the **Save Changes** button after you have entered all the required data.

Customize User Interface

Each aspect of the user interface your Hotspot customers see can be customized.

Customize Page One

Page one of the guest self-provisioning process requires that the guest selects a plan. You are able to customize how this page is displayed to the guest.



You are able to give this page a title, some introductory text and a footer. The Introduction and the Footer are HTML text that may use template syntax, See "Smarty Template Syntax" in the Reference chapter.

Customize Page Two

On page 2, you can make changes to 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.

Edit Page

* Page Title:	Your Details Title of this page.

Introductory HTML:	`<h2>`
	`Hotspot Sign-Up <img class="nwa_hotspot_step" src="images/hotspot-step2.png" width="100" height="48" border="0" alt="Step 2" align="absmiddle" hspace="10"/>`
	`</h2>`
	
	`<p>`
	`To create your wireless account, please enter your details below.`
	`</p>`
	This text is displayed at the top of the page, before the form for the user's details.

Footer HTML:	`<h2>`
	`Important Information`
	`</h2>`
	
	`{nwa_icontext type="info" class=" "}`
	`<span class="nwaImportant">Note:</span>`
	`We collect your personal information in order to provide you with`
	`wireless network service. Your personal details are kept strictly`
	`confidential at all times.`
	`(<a href="#" target="HotspotPopup" onclick="alert('Sorry, this feature has been disabled in the demo.');return false;">Read our privacy`
	This text is displayed at the bottom of the page, after the form for the user's details.

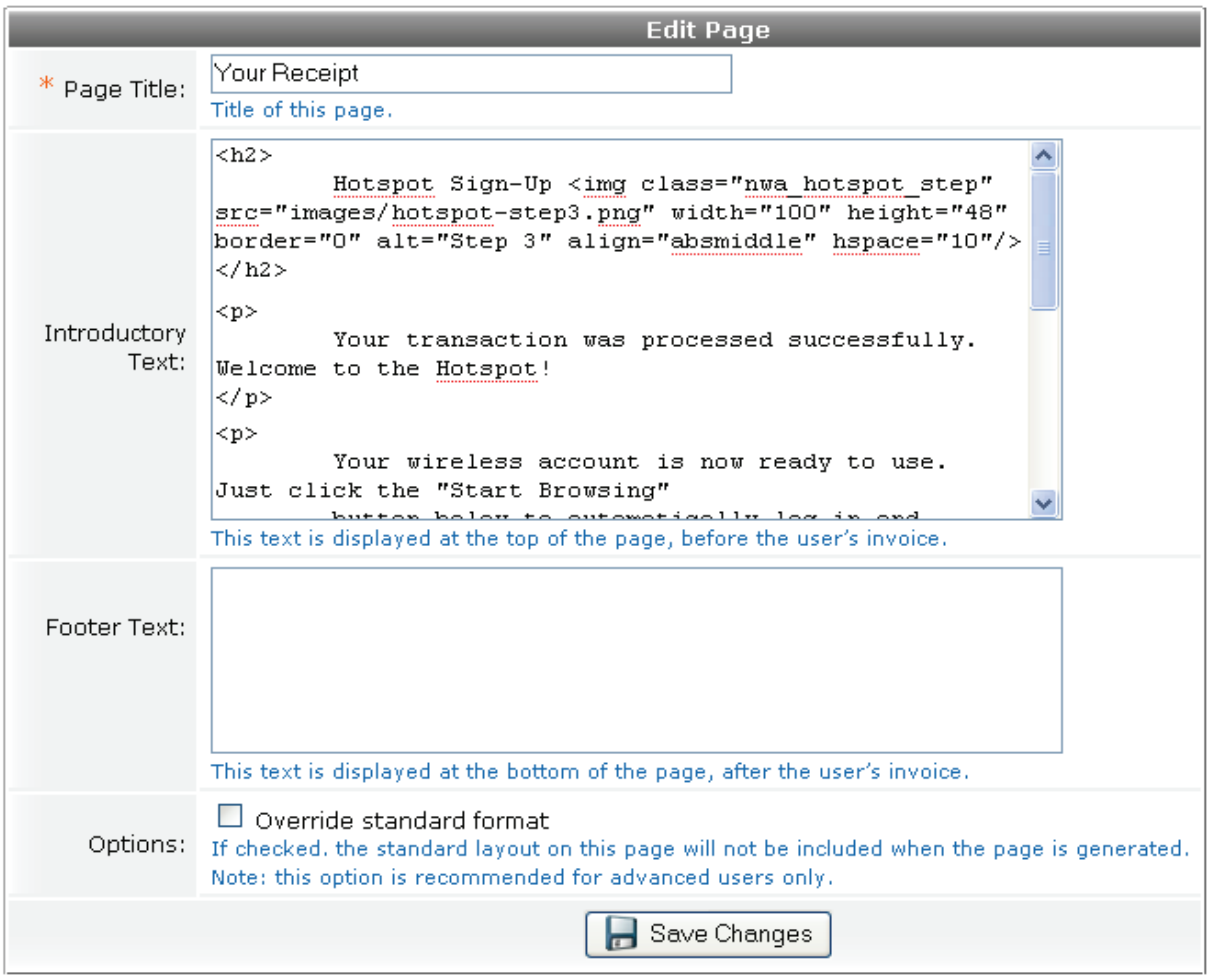
Transaction Header HTML:	`<h2>`
	`Hotspot Sign-Up <img class="nwa_hotspot_step" src="images/hotspot-step2.png" width="100" height="48" border="0" alt="Step 2" align="absmiddle" hspace="10"/>`
	`</h2>`
	
	`<p>`
	`Please wait while your transaction is being processed...`
	`</p>`
	When a transaction is in progress, this text is displayed at the top of the page, before the progress notification area.

Transaction Footer HTML:	When a transaction is in progress, this text is displayed at the bottom of the page, after the progress notification area.
Options:	☐ Override standard form 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.

See "Smarty Template Syntax" in the Reference chapter for details about the template syntax you may use to format the content on this page.

Customize Page Three

You can make changes to the content of page 3, where the customer receives an invoice containing confirmation of their transaction and the details of their newly created wireless account.



See "Smarty Template Syntax" in the Reference chapter for details about the template syntax you may use to format the content on this page.

View Hotspot User Interface

The Hotspot manager allows you to view and test Hotspot self-provisioning pages, as well as log in to and view the Hotspot self-service portal that allows customers to view their current account expiration date, purchase time extensions, log out of the Hotspot or change their user password.

To access either of these user pages, navigate to **Customization > Hotspot manager** and select the **Self-Provisioning** or **Self-Service** links in the left navigation menu.

The goal of a highly available system is to continue to provide network services even if a hardware failure occurs.

High Availability Services provides the tools required to achieve this goal. These tools include service clustering, fault tolerance, database replication, configuration replication, automatic failover and automatic recovery.

You must have two ClearPass Guest servers with the High Availability Services plugin installed in order to use these features.

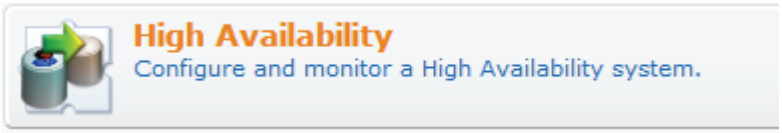
See "About High Availability Systems" in this chapter for an introduction to High Availability Services including a detailed explanation of how it works.

See "Cluster Status" in this chapter for an explanation of the cluster status messages.

See "Recovering From a Failure" in this chapter for the procedures to use if you need to recover a failed cluster.

Accessing High Availability

Use the **High Availability** command link available from the **Administrator** start page to access the clustering and replication features.



Alternatively, use the High Availability navigation menu to jump directly to any of the high availability features.

About High Availability Systems

Terminology & Concepts

A **cluster** consists of a primary node and a secondary node, configured so that a failure of either node will not prevent the cluster as a whole from performing its normal functions.

The **primary node** is the active server in a cluster. The cluster's network services are always delivered by the primary node.

The **secondary node** is the backup server in a cluster. If the primary node fails, the secondary automatically takes over and continues delivering network service.

Fault tolerance is the ability of a server cluster to continue operating if either the primary or secondary node experiences a hardware failure.

Failover is the process by which the secondary node assumes control of the cluster once the primary node has failed.

A cluster's **virtual IP address** is a unique IP address that will always be assigned to the primary node of the cluster. In order to take advantage of the cluster's fault tolerance, all clients that use the cluster must use the cluster's virtual IP address, rather than each node's IP address.

Replication is the process of ensuring that the secondary node maintains an exact copy of the primary node's database contents and configuration. Replication is used to ensure that if a failover is required, the secondary node can continue to deliver an uninterrupted service to clients of the cluster.

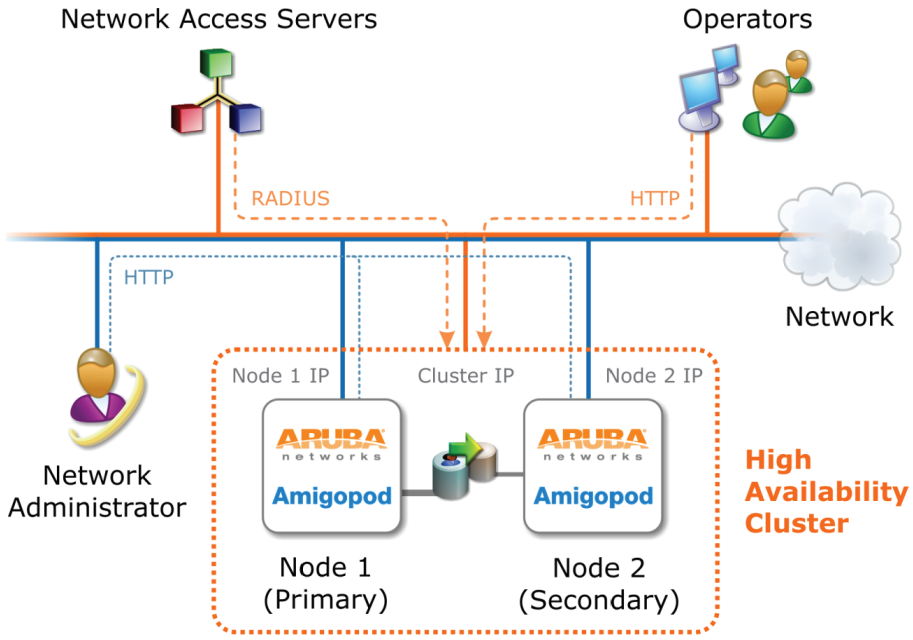
See "About High Availability Systems" for the following settings and procedure..

- Keep-alive
- Database replication.
- Configuration replication
- Downtime threshold

Network Architecture

The figure below shows the network architecture for a high availability cluster.

Figure 50 Network architecture of high availability cluster



The key points to note about this architecture are:

- The RADIUS and Web server protocols (HTTP and HTTPS) are supported by the cluster.
- The cluster has three IP addresses: each node has its own IP address, and there is a virtual IP address for the cluster which will always be assigned to the primary node in the cluster.
- For the cluster to provide failover redundancy, all network access servers and operators must use the cluster's IP address.
- The network administrator should use the node IP addresses to perform system administration tasks on each node, including managing the cluster itself.
- The cluster relies on DNS for name lookup. Each node must have a unique hostname, and each node must be able to resolve the other node's IP address by performing a DNS lookup.

The nodes in the cluster must be connected to the same local network. Use high quality network cables and reliable switching equipment to ensure the nodes have an uninterrupted network connection.

NOTE

There should be no routers, gateways, firewalls, or network address translation (NAT) between the two nodes. Having nodes in different physical locations is not recommended and is not a supported configuration for the cluster.

Deploying an SSL Certificate

Special consideration needs to be given to deployments that require SSL access to the cluster.

The Common Name (CN) of an SSL certificate must match the hostname of the site being visited. Certificates that do not meet this requirement may still be used to secure the connection, but a browser security warning is displayed. In modern browsers this warning is intended to deter users from what may be a potentially serious "man in the middle" attack. Non-technical visitors should not be expected to analyze and interpret these messages.

Where SSL access is a requirement, the recommended approach is to issue the certificate for the hostname of the cluster's virtual IP address, and install the same certificate on both nodes.

This approach ensures that all operator and visitor access to the cluster is secured with a certificate that matches the hostname and IP address, avoiding any unnecessary browser security warnings.

NOTE

When using this approach, the administrator will receive browser security warnings about the certificate hostname mismatch if he accesses each node individually.

Normal Cluster Operation

When the cluster is operating normally, the cluster status will be:

The cluster is running normally.

In this state, the primary node is assigned the cluster IP address and is responsible for delivering network services to clients. Each node is also continuously performing failure detection, database replication and configuration replication, as explained below.

Failure Detection

Failure detection is accomplished using a **keep-alive test**. The primary and secondary nodes verify that each is able to communicate with the other node by sending network requests and answering with a response. This takes place at the Keep Alive Rate specified in the cluster configuration, which by default is once every 2 seconds.

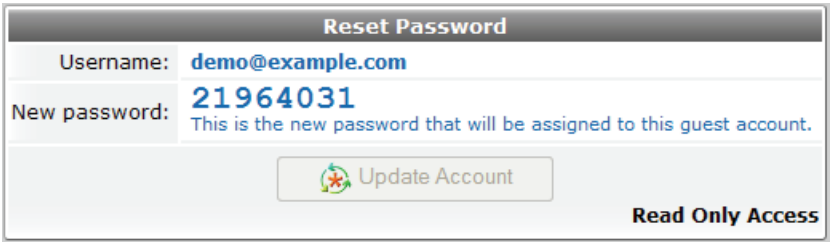
If several consecutive keep-alive tests have failed, the cluster determines that a failure has occurred. A cluster failover may then take place, depending on which node has failed. **See "Primary Node Failure"** in this chapter for information about a primary node failure, or **"Secondary Node Failure"** for information about a secondary node failure.

To avoid any network service interruptions, it is important that the nodes maintain an uninterrupted network connection.

Database Replication

Database replication occurs continuously in a normally operating cluster. All database modifications, including new guest accounts, changes to existing guest accounts, RADIUS roles, NAS servers, and RADIUS accounting information, are replicated from the primary node to the secondary node. The replication delay will depend on the volume of database updates and system load but is generally only a few seconds.

Replicating the database contents ensures that in the event of a primary node failure, the secondary node is up to date and can continue to deliver the same network services to clients. While the primary node is online, the secondary node's database can only be updated with replication changes from the primary node. No other database changes can take place on the secondary node. Because of this, any form that requires a database update will be disabled and shown as "Read Only Access" on the secondary node.



Ensure that you always access the cluster using the virtual IP address when performing any database updates, such as creating new guest accounts or performing RADIUS authentication. This is required so that the changes will be performed on the primary node and then replicated to the secondary node.

Configuration Replication

Configuration replication also occurs continuously within the cluster, but takes place at a slower rate due to the reduced frequency of configuration updates. This rate is the Config Sync rate specified in the cluster configuration, which by default is once every minute.

The configuration items that are replicated include:

- Configuration for installed plugins (**See "Configuring Plugins"** in the Administrator Tasks chapter)
- Fields defined in Guest Manager (See "Customization of Fields" in the Guest Managment chapter)
- Forms and views defined in Guest Manager (See "Customization of Forms and Views" in the Guest Managment chapter)
- Guest self-registration pages (See "Customizing Self Provisioned Access" in the Guest Managment chapter)
- Instances of reports that have previously been run (See "Report History" in the Report Management chapter)
- LDAP authentication servers and translation rules (See "LDAP Operator Authentication" in the Operator Logins chapter)
- Network login access configuration (See "Creating a VLAN Interface" in the Administrator Tasks chapter)
- Operator login configuration (See "Operator Logins Configuration" in the Operator Logins chapter)
- Operator logins (See "Local Operator Authentication" in the Operator Logins chapter)
- Operator profiles (See "Operator Profiles" in the Operator Logins chapter)
- Print templates defined in Guest Manager (See "Editing Guest Receipt Page Properties" in the Guest Management chapter)
- Publicly-accessible Web server items in Content Manager (See "Content Manager" in the Administrator Tasks chapter)
- RADIUS server configuration (See "Server Configuration" in the RADIUS Services chapter)
- Report definitions (See "Viewing Reports" the Reports chapter)
- SMS service configuration (See "Editing Guest Receipt Page Properties" in the Guest Management chapter)
- SMTP server configuration (See "SMTP Configuration" in the Administrator Tasks chapter)
- SMTP settings for email receipts (See "Email Receipt Options" in the Guest Management chapter)

- SNMP server settings (See "SNMP Configuration" in the Administrator Tasks chapter)
- The set of currently installed plugins (See "Plugin Manager" in the Administrator Tasks chapter)
- Web Login pages (See "Web Logins" in the RADIUS Services chapter)

Certain configuration items are not replicated. These are:

- HTTP Proxy settings ("HTTP Proxy Configuration" in the Administrator Tasks chapter)
- Network interface configuration ("Viewing Network Interface Settings" in the Administrator Tasks chapter)
- RADIUS dictionary entries (See "Dictionary" in the RADIUS Services chapter)
- SSL certificate settings (See "SSL Certificate" in the Administrator Tasks chapter)
- Subscription IDs in Plugin Manager (See "Managing Subscriptions" in the Administrator Tasks chapter)
- System hostname (See "Viewing or Setting System Hostname" in the Administrator Tasks chapter)

Primary Node Failure

If the cluster's primary node fails, the cluster status will be displayed on the secondary node as:

The secondary node is running, but the primary node is down or stopped.

While the primary node is down, the cluster is in a failed state and cannot deliver network services. If the primary node recovers within the downtime threshold, the cluster will automatically return to the normal state and network service will be restored.

An automatic failover will be initiated after the primary node has been offline for the **downtime threshold**, which is 30 seconds by default.

Once failover has occurred, the cluster status will be displayed on the secondary node as:

The secondary node has taken over the cluster services because the primary node is down.

In the failover state, the secondary node will assume control of the cluster and will take over the cluster's IP address. This will restore network service for clients of the cluster. Replication will stop as there is no longer a primary node.

While the primary node is offline, the cluster will no longer be fault-tolerant. A subsequent failure of the secondary node will leave the cluster inoperable.

See "Recovering From a Temporary Outage" in this chapter for instructions on recovering a cluster in this state.

The secondary node has taken over the cluster services. The primary node is back online, but the cluster needs to be recovered.

In this state, the primary node was offline for a period of time greater than the downtime threshold, and then recovered. The cluster has failed over to the secondary node.

In this state, the cluster is not fault-tolerant. A subsequent failure of the secondary node will leave the cluster inoperable.

Recovering the cluster is required for replication to resume and return the cluster to a fault-tolerant state.

See "Recovering From a Temporary Outage" in this chapter for instructions on recovering a cluster in this state.

Secondary Node Failure

If the cluster's secondary node fails, the cluster status will be displayed on the primary node as:

The primary node is running, but the secondary node is down or stopped.

The cluster will continue operating without service interruption. Network services will be unaffected as the cluster's virtual IP address is assigned to the primary node.

While the secondary node is offline, the cluster will no longer be fault-tolerant. A subsequent failure of the primary node will leave the cluster inoperable.

To recover the cluster, the secondary node must be brought back online. If the node has experienced only a temporary outage and has the same cluster configuration, the cluster will automatically repair itself. Replication will update the secondary node with any database or configuration changes that were made on the primary node while the secondary node was offline.

If the secondary node was replaced due to a hardware failure then the cluster must be destroyed and rebuilt. See "Recovering From a Hardware Failure" in this chapter for instructions on recovering a cluster in this state.

Email Notification

In addition to sending syslog messages, ClearPass Guest can also send email alerts to operators with administrator access if a high-availability cluster enters a failover state. This feature requires that each high-availability node have a valid SMTP configuration, and that each operator login is configured with an email address.

Cluster Status

The current status of the cluster is shown at the top of each page that is related to High Availability Services. for an explanation of each possible status, and the recommended action to take, if any.

Table 36 *Cluster Status Descriptions*

Status	Description
	This system is not part of a high availability cluster. • To create a new cluster and make this server the primary node, use the Create New Cluster command. • To join a cluster and make this server the secondary node, use the **Join Cluster** command.
	The cluster is running normally. • Click the View details link to show more information about the cluster. • To perform a scheduled maintenance task, such as a reboot, on the primary node in the cluster, use the Cluster Maintenance command. • **See "Normal Cluster Operation"** in this chapter for more information about normal cluster operations.
	The secondary node has taken over the cluster services because the primary node is down. • A failover has occurred. The cluster must be recovered to resume fault-tolerant operation. • Ensure the primary node is back online.
	The secondary node has taken over the cluster services. The primary node is back online, but the cluster needs to be recovered. • A failover has occurred. The cluster must be recovered to resume fault-tolerant operation. • See "Recovering From a Temporary Outage" in this chapter for the procedure.
	A failure has occurred. • Check the detailed status information. • If this message persists, you may need to rebuild the cluster. See "Recovering From a Hardware Failure" in this chapter.

Table 36 *Cluster Status Descriptions (Continued)*

	The primary node is running, but the secondary node is down or stopped. • The secondary is no longer available. Check the Remote Status on the primary node to determine the cause of the problem. • To clear the error condition, bring the secondary node back online. The cluster will return to fault-tolerant mode automatically. • If the secondary node needs to be replaced, the cluster must be rebuilt. See "Recovering From a Hardware Failure" in this chapter.
	The secondary node is running, but the primary node is down or stopped. • The primary is no longer available. Check the Remote Status on the secondary node to determine the cause of the problem. • The cluster IP address is inaccessible and network services are unavailable. • Automatic failover will take place after the downtime threshold has been exceeded.
	The cluster services are starting. Check the detailed status information.
	The primary node is running, but a problem has been detected. Check the detailed status information.
	The primary node is running, but the secondary node is reporting a problem. Check the detailed status information.
	The cluster is recovering from a failure. Check the detailed status information.
	The cluster is currently being initialized. Check the detailed status information.
	Status call timed out. Server may be down. This message may be displayed if the node cannot be contacted. There may be a network issue affecting your management workstation, or the node may be offline. • Refresh your Web browser to check the connection to the node. If the problem persists, check the cluster status on the other node.

Cluster Setup

Before you begin, review this checklist to ensure you are prepared to set up a cluster:

- You have two servers available.
- Each server is powered up and connected to the same local area network.
- Each server has a unique hostname.
- Each server has a valid subscription ID and has been updated using the Plugin Manager. Ensure that the High Availability Services plugin has been installed along with any available plugin updates.
- You are logged in as the administrator on each server.
- You have determined the desired network configuration (virtual IP address) for the cluster.

Click the **Create New Cluster** command link on the **Administrator > High Availability > Cluster Configuration** page to begin the process of creating a new cluster.

Prepare Primary Node

Use the **Cluster Configuration** form to enter the basic network and control parameters for the cluster.

If you have not already set a unique hostname for this server, you can do so here. Each node in the cluster must have a unique hostname. You can selec a single virtual IP address by entering one IP address in the Virtual IP Address field, or specify more than one virtual IP by entering a comma-separated list of multiple IP addresses.

Each node in the cluster must be able to resolve the other node by using a DNS lookup. This is verified during the cluster initialization. In practice, this means that you must configure your local DNS or DHCP server with appropriate entries for each node.

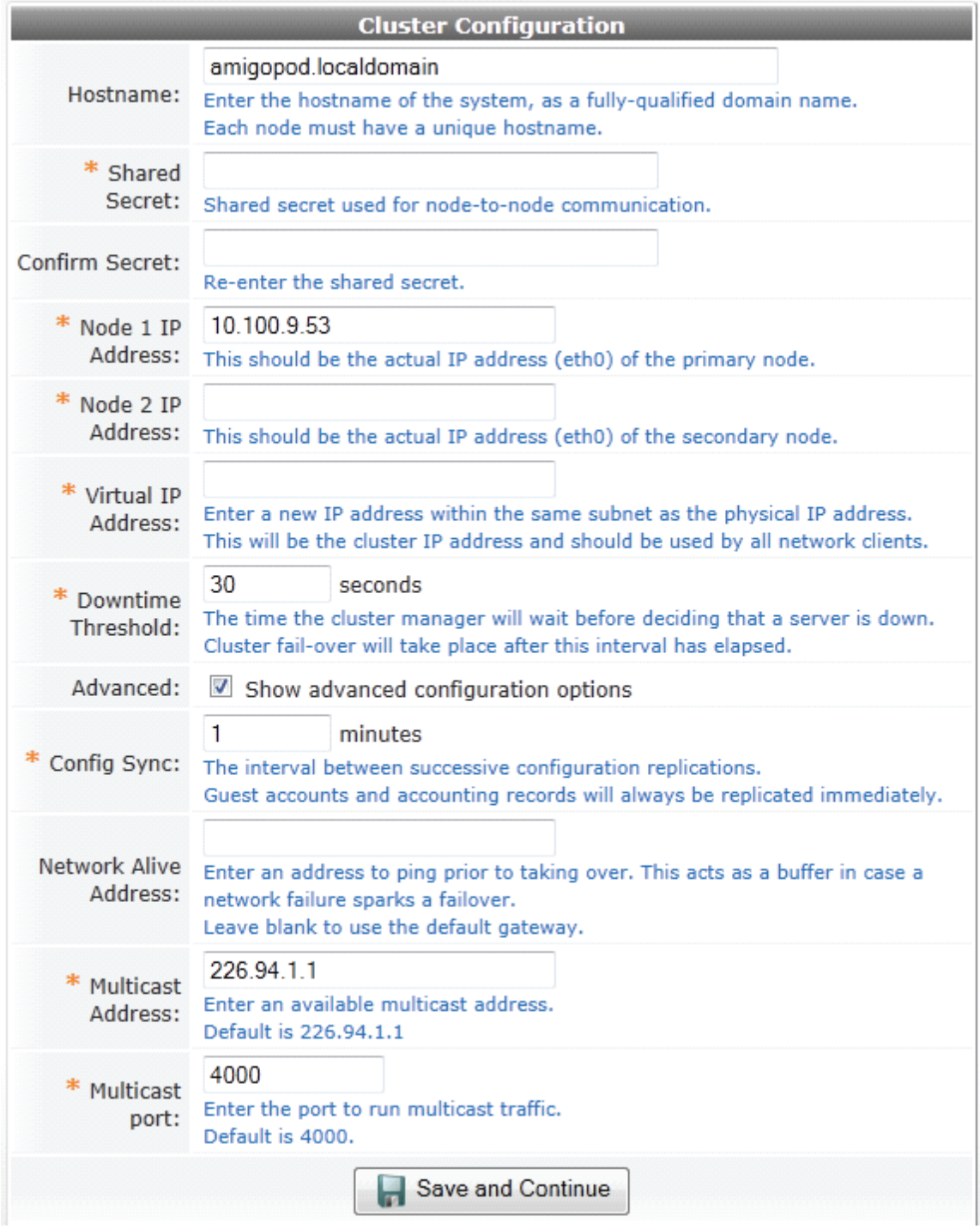
You must enter a shared secret for this cluster. The shared secret is used to authenticate the messages sent between the nodes in the cluster.

For the **downtime threshold** parameter, **See "Primary Node Failure"** in this chapter.

High Availability Services requires an IPv4 multicast address and port number. By default these values are 226.94.1.1 on UDP port 4000. If this address and port combination overlaps an existing solution on your network, you can adjust them when initializing the cluster configuration. If this multicast address is already in use, the cluster initialization will not work and you will need to choose a different address. Click the **Advanced** check box and enter an appropriate multicast address and port. These values will be automatically synchronized on the secondary node.

Click the **Save and Continue** button to prepare the primary node.

Any switch equipment the ClearPass Guest appliances are connected to should also be configured to allow IPv4 multicast traffic.



If you have not already set a unique hostname for this server, you can do so here. Each node in the cluster must have a unique hostname. A valid hostname is a domain name that contains two or more components separated by a period (.). Hostname parameters are as follows:

- Each component of the hostname must not exceed 63 characters
- The total length of the hostname must not exceed 255 characters
- Only letters, numbers, and the hyphen (-) and period (.) characters are allowed
- Hostnames may start with numbers, and may contain only numbers

You can select a single virtual IP address by entering one IP address in the Virtual IP Address field, or specify than one virtual IP by entering a comma-separated list of multiple IP addresses.

NOTE

Each node in the cluster must be able to resolve the other node by using a DNS lookup. This is verified during the cluster initialization. In practice, this means that you must configure your local DNS or DHCP server with appropriate entries for each node.

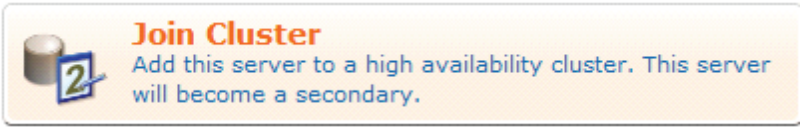
You must enter a shared secret for this cluster. The shared secret is used to authenticate the messages sent between the nodes in the cluster.

For an explanation of the **downtime threshold** parameter. See "Primary Node Failure" in this chaper.

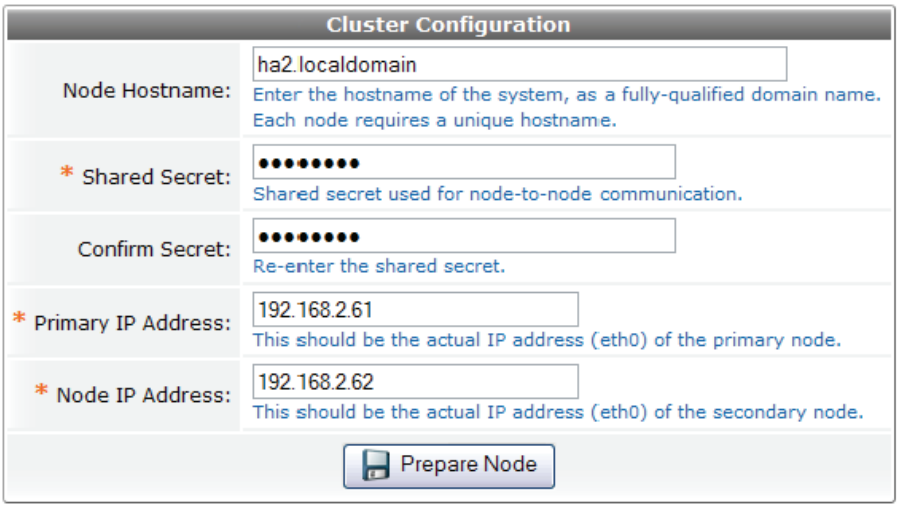
Click the **Save and Continue** button to prepare the primary node.

Prepare Secondary Node

To prepare the secondary node, log in to that node and click the **Join Cluster** command link.



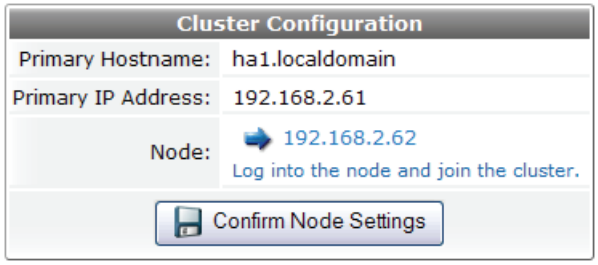
Use the **Cluster Configuration** form to enter the shared secret for the cluster and the IP address of the primary node.



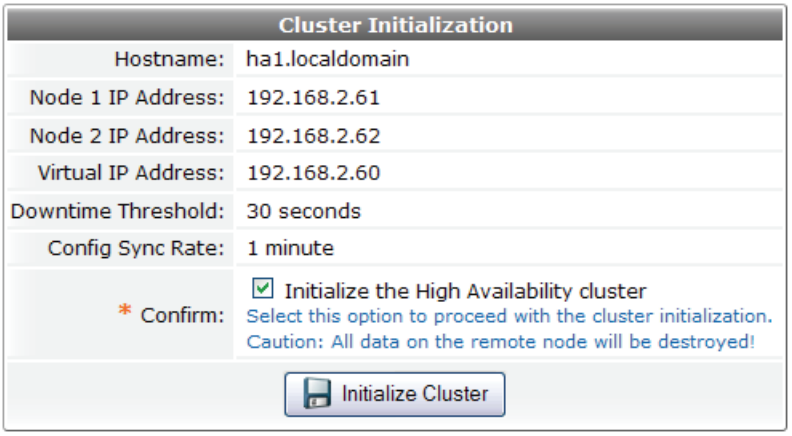
Click the **Prepare Node** button to save and verify the settings for the secondary node.

Cluster Initialization

To complete the setup of the cluster, return to the primary node after preparing the secondary node and click the **Confirm Node Settings** button.



The **Cluster Initialization** form is displayed.



Select the check box and click the **Initialize Cluster** button to proceed.

NOTE

During the cluster initialization process, the entire contents of the RADIUS database (including guest accounts, user roles, and accounting history) and all configuration settings of the primary node will be replicated to the secondary node. The existing database contents and configuration settings on the secondary node will be destroyed. It is very important to ensure that you have selected the correct node as the primary node, particularly if you are rebuilding the cluster. If in doubt, it is recommended that you perform a complete backup of both nodes prior to initializing the cluster.

Several status messages and a progress meter will be displayed while the cluster is initialized, which may take several minutes depending on the amount of data to be replicated.

Once the initialization process completes, you will be returned to the High Availability start page, where the cluster status will be displayed as:
The cluster is running normally.

Cluster Deployment

After setting up a cluster, you must make appropriate configuration changes for your network to take advantage of the cluster's fault tolerance.

The principal configuration change required is to replace the IP address of a single ClearPass Guest server with the virtual IP address of the cluster.

- NAS devices and other RADIUS clients should be configured with the cluster IP address.
- Operators should use the cluster's IP address when provisioning guest accounts.
- Configure NAS devices to redirect visitors to the cluster's IP address for Web login pages. Only the IP address in the redirection URL should be changed; the remainder of the redirection URL should not be altered.

The network administrator should use the node IP addresses to perform system administration tasks on each node, including managing the cluster itself.

Cluster Maintenance

Use the **Cluster Maintenance** command link to access maintenance functions related to the cluster.

The maintenance commands that are available on this page will depend on the current state of the cluster as well as which node you are logged into.

NOTE

Some maintenance commands are only available on the secondary node. Other commands may change the active state of the cluster. For this reason it is recommended that cluster maintenance should only be performed by logging into a specific node in the cluster using its IP address.

Recovering From a Failure

From a cluster maintenance perspective, there are two kinds of failure:

- A **temporary outage** is an event or condition that causes the cluster to failover to the secondary node. Clearing the condition allows the cluster's primary node to resume operations in essentially the same state as before the outage.
- A **hardware failure** is a fault that to correct requires rebuilding or replacing one of the nodes of the cluster.

The table below lists some system failure modes and the corresponding cluster maintenance that is required.

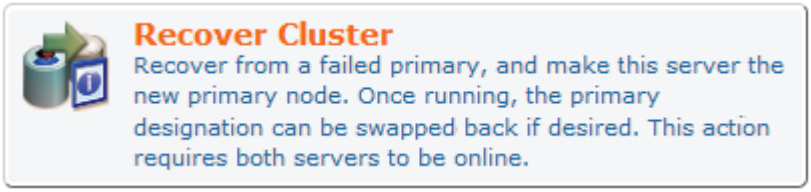
Table 37 *Failure Modes*

Failure Mode	Maintenance
Software failure – system crash, reboot or hardware reset	Temporary outage
Power failure	Temporary outage
Network failure – cables or switching equipment	Temporary outage
Network failure – appliance network interface	Hardware failure
Hardware failure – other internal appliance hardware	Hardware failure
Data loss or corruption	Hardware failure

Recovering From a Temporary Outage

Use this procedure to repair the cluster and return to a normal operating state:

1. This procedure assumes that the primary node has experienced a temporary outage, and the cluster has failed over to the secondary node.
2. Ensure that the primary node and the secondary node are both online.
3. Log into the secondary node. (Due to failover, this node will be assigned the cluster's virtual IP address.)
4. Click Cluster Maintenance, and then click the **Recover Cluster** command link.



5. A progress meter is displayed while the cluster is recovered. The cluster's virtual IP address will be temporarily unavailable while the recovery takes place.
6. Recovery is complete. The secondary node is now the new primary node for the cluster. The cluster is back in a fault-tolerant mode of operation.

The Recover Cluster command will only work if the node that failed is brought back online with the same cluster configuration. This is normally the case in all temporary outages. See **"Recovering From a Hardware Failure"** in this chaper, in this case, for a description of how to recover the cluster.

NOTE

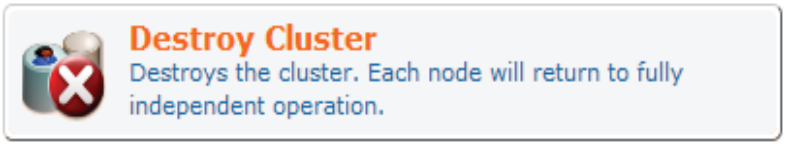
The **Recover Cluster** action is available from *either* node, and will make that node the new primary node for the cluster. To return the primary node back to its original status as the primary node in the cluster, you can use the **Swap Primary Servers** command. **See "Performing Scheduled Maintenance"** in this chaper for an explanation.

Recovering From a Hardware Failure

If the failed node has been replaced, the cluster configuration will no longer be present on that node. To recover the cluster, first ensure that the replaced node is ready to rejoin the cluster, then destroy the cluster and recreate it.

Use the following procedure to rebuild the cluster:

1. This procedure assumes that the primary node has failed and has been replaced.
2. Configure the network settings, subscription IDs and hostname for the replacement primary node.
3. Ensure that the replacement primary node and the secondary node are both online.
4. Log into the secondary node. (Due to failover, this node will be assigned the cluster's virtual IP address.)
5. Click Cluster Maintenance, and then click the **Destroy Cluster** command link.



6. A progress meter is displayed while the cluster is destroyed. The virtual IP address of the cluster will be unavailable until the cluster is reinitialized.
7. Click the **Create New Cluster** command link.
8. Recreate the cluster. **See "Cluster Setup"** in this chapter for a description of the process. Note that the new cluster's primary node must be the former cluster's secondary node that you are presently logged into.
9. When the cluster is initialized, the database and configuration is replicated to the replacement primary node.
10. Recovery is complete. The cluster's virtual IP address is now available, and the secondary node is now the new primary node for the cluster. The cluster is back in a fault-tolerant mode of operation.

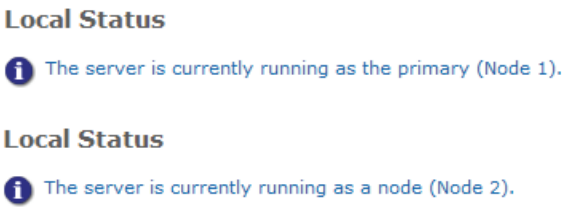
A similar procedure can be used to rebuild the cluster in the event of a secondary node suffering a hardware failure.

Performing Scheduled Maintenance

Routine maintenance tasks such as a server reboot or shutdown may occasionally be required for a server that is part of a cluster.

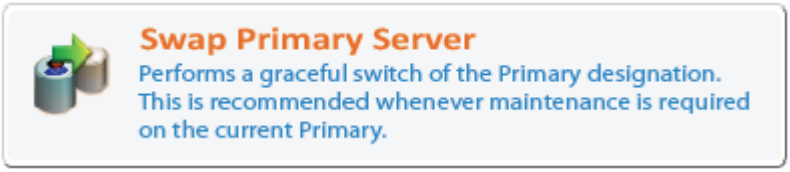
These tasks may be performed by ensuring that the server is the secondary node in the cluster. If the secondary node goes offline, the primary node will be unaffected and the cluster will continue to provide network services without interruption. When the secondary node comes back online, the cluster will be automatically rebuilt and replication will resume.

To check the current status of a node, log into that node and click the **Show details** link displayed with the cluster status on the High Availability page. The node's current status is displayed under the **Local Status** heading.



Use this procedure to make the current primary node the secondary node:

1. Log into the current secondary node of the cluster.
2. Click Cluster Maintenance, and then click the **Swap Primary Server** command link.



3. A progress meter is displayed while the primary node is switched. The cluster's virtual IP address will be temporarily unavailable while the swap takes place.
4. The swap is complete. The secondary node is now the new primary node for the cluster. The cluster is back in a fault-tolerant mode of operation.
5. Perform any required maintenance on the new secondary node.

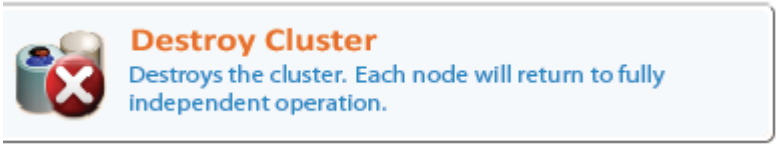
Updating Plugins

Plugins cannot be updated while High Availability is running. Because exact synchronization of the two servers is required for High Availability Services, you must first destroy the cluster, then re-create the cluster after the plugins are updated. See Destroying a Cluster and Cluster Setup in this chapter.

For information on updating plugins, see Plugin Manager in the Administrator Tasks chapter.

Destroying a Cluster

The **Destroy Cluster** command link is used to shut down a cluster and return to independent nodes. Avoid using this command when you are accessing the cluster using its virtual IP address, as the virtual IP address will no longer be available when the cluster has been destroyed.



Immediately after the cluster is destroyed, both nodes will have the same database and configuration state. However, changes on one node will no longer be replicated to the other node as the cluster is no longer functioning.

Cluster Troubleshooting

When building a cluster, use the recommended values for the downtime threshold, keep-alive rate and configuration sync rate. You should only change these values if you have a specific requirement and have verified that different values can be used to meet that requirement.

To avoid unexpected failover of the cluster, ensure that the network connection to the nodes of the cluster is always available. Use high quality network equipment, including cables, and secure physical access to the servers to prevent accidental dislodgement of cables.

If network access to the cluster is intermittent, this may indicate a possible hardware failure on the current primary node. In this situation, you may either use the Swap Primary Server command to make the secondary node the new primary node, or you can cause the cluster to failover to the secondary by disconnecting the primary node.

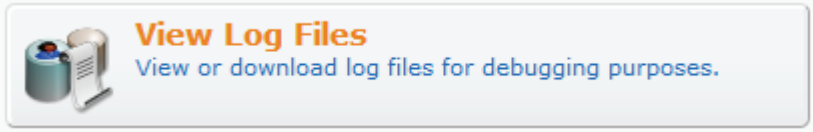
Brief network outages are permissible and will not cause failover, provided that the network outage is shorter than the downtime threshold of the cluster.

During a failover from the primary to the secondary node, the network services provided by the cluster will be unavailable. The time that the cluster will be offline is bounded by the downtime threshold. This can be used to calculate the expected availability of the cluster.

The **Restart Cluster Services** and **Stop Cluster Services** command links on the Cluster Maintenance page may be used to test failover conditions by simulating a cluster failure.

Avoid using these commands when you are accessing the cluster using its virtual IP address, as the virtual IP address may become unavailable.

The **View Log Files** command link allows the internal state of the cluster to be viewed.



This may be useful if debugging a problem related to the cluster. The log files may be exported to a zip file. If you require support about a cluster-related problem, include a copy of the exported cluster log files with your support request.

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, ** **. 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, ** **.

Use the following standard HTML tags in customization:

Table 38 *Standard HTML Tags*

Item	HTML Syntax
Basic Content	
Heading level 1	`<h1>Main Heading</h1>`
Heading level 2	`<h2>Subheading</h2>`
Heading level 3	`<h3>Section heading</h3>`
Regular paragraph text	`<p>Paragraph text</p>`
Line break	` ` ` ` – equivalent syntax (XHTML)

Bullet list	`<ul>`
	`  <li>List item text</li>`
	`</ul>`

Numbered list	`<ol>`
	`  <li>List item text</li>`
	`</ol>`

Text Formatting	
Bold text	`<b>words to be made bold</b>` `<strong>equivalent syntax</strong>`
Italic	`<i>words to be made italic</i>` `<em>equivalent syntax</em>`
Underline	`<u>words to underline</u>`
Typewriter text	`<tt>Shown in fixed-width font</tt>`
Styled text (inline)	`<span style="…">Uses CSS formatting</span>` `<span class="…">Uses predefined style</span>`

Table 38 *Standard HTML Tags (Continued)*

Styled text (block)	`<div style="…">Uses CSS formatting</div>` `<div class="…">Uses predefined style</div>`
Hypertext	
Hyperlink	`<a href="url">Link text to click on</a>`
Inline image	`<img src="url">` `<img src="url" />` – XHTML equivalent
Floating image	`<img src="url" align="left">`

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.

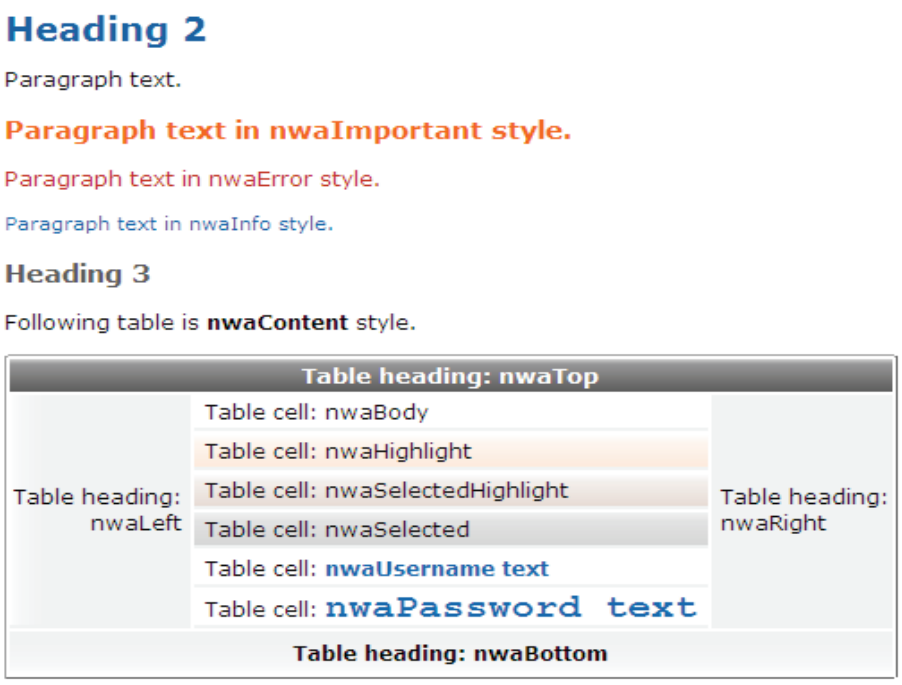


Table 39 *Formatting Classes*

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

Table 39 *Formatting Classes (Continued)*

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
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"}
```

Note that 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* ***}**. Note that this is different from a 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. Note that 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}
```

Note that 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

Note that 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|nwadateformat:"%Y-%m-%d"}
```

See "Date/Time Format Syntax" in this chapter for detailed information on the date/time format modifiers. **See Table 40.**

Table 40 *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)
nwadateformat	Date/time formatting; see **"nwadateformat Modifier"** in this chapter for details about this modifier function

Table 40 *Smarty Modifiers (Continued)*

Modifier	Description
nwatimeformat	Date/time formatting; see **"Date/Time Format String Reference"** in this chapter 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 NwaMoneyFormat() function; see "NwaMoneyFormat" in this chapter 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. Note that no HTML entity escaping is performed when inserting content using this function.

nwa_icontext

`{nwa_icontext} … {/nwa_icontext}`

Smarty registered block function. Generates a block of text with a marker icon displayed in the top left.

Usage examples:

```
{nwa_icontext icon="images/icon-info22.png"}Text to display{/nwa_icontext}
{nwa_icontext type="info"}Information block{/nwa_icontext}
```

- 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 ‘nwaIndent’ 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. See “GetCallingStationTraffic()” .

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. This should be one of the functions listed in the “Standard RADIUS Request Functions”section. 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:

- GetTraffic($criteria, $from_time, $to_time = null, $in_out = null)
- GetTime($criteria, $from_time, $to_time = null)
- GetSessions($criteria, $from_time, $to_time = null)
- GetCallingStationTraffic($callingstationid, $from_time, $to_time = null, $in_out = null, $mac_format = null)
- GetUserTraffic($username, $from_time, $to_time = null, $in_out = null)
- GetIpAddressTraffic($ip_addr, $from_time = null, $to_time = null, $in_out = null)
- GetCallingStationTime($callingstationid, $from_time, $to_time = null, $mac_format = null)
- GetUserTime($username, $from_time, $to_time = null)
- GetIpAddressTime($ip_addr, $from_time = null, $to_time = null)
- GetCallingStationSessions($callingstationid, $from_time, $to_time = null, $mac_format = null)
- GetUserSessions($username, $from_time, $to_time = null)
- GetIpAddressSessions($ip_addr, $from_time = null, $to_time = null)

- GetUserActiveSessions($username, $callingstationid = null)
- GetCurrentSession($criteria)
- GetUserCurrentSession($username)
- GetIpAddressCurrentSession($ip_addr = null)
- GetCallingStationCurrentSession($callingstationid, $mac_format = null)
- GetSessionTimeRemaining($username, $format = “relative”)
- ChangeToRole($username, $role_name)

The $criteria array consists of of one or more criteria on which to perform a databased search. This array is used for advanced cases where pre-defined helper functions do not provide required flexiblity.

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 one of two supported methods:

- `{nwa_assign var=_GET.get_variable value=...}`
- `{nwa_assign var=smarty.get.get_variable value=...}`

The variables that can be accessed this way are _GET (smarty.get), _POST (smarty.post), _REQUEST (smarty.request), _SESSION (smarty.session), _COOKIE (smarty.cookies), and _ENV (smarty.env).

Assigning to values in _SESSION will persist the value for the next page load in the session.

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 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 41 *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. Note 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

There are two basic modifiers available for you to use in ClearPass Guest: nwadateformat and nwatimeformat.

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 42 *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, %I:%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	%I:%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" 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 nwadateformat modifier. See "nwadateformat Modifier" in this chapter.

Date/Time Format String Reference

Table 43 *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)
%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

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 (**"NwaParseCsv"**) 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"** in this chapter.

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 44 *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" and "NwaVLookup".

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), "I" and "l" (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 45 *NwaVLookup Options*

Option	Description
$value	The value to look 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.

Note the following differences from Excel VLOOKUP:

- Column indexes are 0-based.
- Column indexes can also be strings.

See "NwaParseCsv" and "NwaCsvCache".

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 **word1***XX***word2**. 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

GuestManager Standard Fields

The table below describes standard fields available for the GuestManager form.

Table 46 *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 **do_schedule** and **schedule_time** fields, and may be one of the following: • Account will be enabled at *date and time* • 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 NwaCaptchaIsValid 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: `array('generator' => 'time')`
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.
creator_name	String. Name of the creator of the account. This field does not have a default value. Also, See “sponsor_name” .

Table 46 *GuestManager Standard Fields (Continued)*

Field	Description
do_expire	Integer that specifies the action to take when the expire time of the account is reached. See "expire_time" . • 0—Account will not expire • 1—Disable • 2—Disable and logout • 3—Delete • 4—Delete and logout "Disable" indicates that the enabled field will be set to 0, which will prevent further authorizations using this account. "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"** in the Guest Management chapter for more information.
do_schedule	Boolean flag indicating if the account should be enabled at schedule_time. Set this field to 0 to disable automatic activation of the account at the activation time. Set this field to 1, and provide a valid time in the schedule_time field, to automatically enable the account at the specified activation time. See "schedule_time" .
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 change_expiration or guest_edit 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 change_expiration or guest_edit forms.
dynamic_is_expired	Boolean flag indicating if the user account has already expired. This field is available when modifying an account using the change_expiration or guest_edit 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 (dynamic_is_expired is false), or if the account has expired (dynamic_is_expired is true). This field is available when modifying an account using the change_expiration or guest_edit 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 change_expiration and guest_enable forms. The value is generated from the **do_expire**, **expire_time**, **expire_postlogin** and **expire_usage** fields, and may be one of the following: • Account will expire at *date and time*, or *interval* after first login, or after *interval* total usage • Account will expire at *date and time* or *interval* after first login • Account will expire at *date and time* or after *interval* total usage • Account will expire at *date and time* • Expires *interval* after first login or after *interval* total usage • Expires *interval* after first login • Expires after *interval* total usage • No expiration time set

Table 46 *GuestManager Standard Fields (Continued)*

Field	Description
expire_time	Integer. Time at which the account will expire. The expiration time should be specified as a UNIX timestamp. 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.
expire_usage	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.
http_user_agent	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.
id	String. Internal user ID used to identify the guest account to the system.
ip_address	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: `<?= $user["ip_address"]`
modify_expire_postlogin	String Value indicating how to modify the **expire_postlogin** field. This field is only of use when editing a visitor account. It may be set to one of the following values: • "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. This field controls account modifications; it is not stored with the visitor account.
modify_expire_time	String. Value indicating how to modify the **expire_time** field. This field may be provided when creating or editing a visitor account. It may be set to one of the following values: • "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; • "expire_after" to set the expiration time to the current time, plus the number of hours in the **expire_after** field; • "plus *X*" or "minus *X*", where *X* is a time measurement, to extend or reduce the expiration time by *X* (hours, but may have a "ywdhms" suffix to indicate years, weeks, days, hours, minutes, seconds respectively); • A time measurement "*X*", to set the expiration time to the current time plus *X*; • Any other value to leave expire_time unmodified. This field controls account creation and modification behavior; it is not stored with created or modified visitor accounts.

Table 46 *GuestManager Standard Fields (Continued)*

Field	Description
modify_expire_usage	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: • "expire_usage" to set the cumulative usage expiration timer to the value in the expire_usage field; • "plus ***X***" or "minus ***X***", where ***X*** is a time measurement, to extend or reduce the cumulative usage expiration timer by ***X*** (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. This field controls account modifications; it is not stored with the visitor account.
modify_password	String. Value indicating how to modify the account password. • 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. This field controls account creation and modification behavior; it is not stored with created or modified visitor accounts.
modify_schedule_time	String. Value indicating how to modify the **schedule_time** field. It may be one of the following values: • "none" to disable the account activation time; • "now" to activate the account immediately; • "schedule_time" to use the activation time specified in the **schedule_time** form field (normally a UNIX time, but may be 0 to disable activation time); • "schedule_after" to set the activation time to the current time plus the number of hours in the **schedule_after** field; • "plus *X*", where *X* is a time measurement, to extend the activation time by *X*. 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 '+X', 'pX', 'plusX', 'add X', 'addX', or 'aX'. Example: to delay activation time by 2 days, use the value **+2d**. • "minus *X*", where *X* is a time measurement, to reduce the activation time by *X*. See above for details about specifying a time measurement. Alternatively, this operation may be written equivalently as '-X', 'mX', 'minusX', 'sub X', 'subX', or 'sX'. Example: to bring forward activation time by 12 hours, use the value **-12h**. • 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 **schedule_time** unmodified. This field controls account creation and modification behavior; it is not stored with created or modified visitor accounts.
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".

Table 46 *GuestManager Standard Fields (Continued)*

Field	Description
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: `<?= $user["netmask"]`
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: • *empty string* – Default behavior; that is, guests are not required to change their password • **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 password_action_recur 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 password_action_recur field) 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. 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.
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”.

Table 46 *GuestManager Standard Fields (Continued)*

Field	Description
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. • 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: • **nwa_digits_password** to create a password using random digits. The length of the password is specified by the random_password_length field. • **nwa_letters_password** to create a password using random lowercase letters (a through z). The length of the password is specified by the random_password_length 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 random_password_length 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 random_password_length 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 specified by the random_password_length field. • **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 random_password_picture field.
random_password_picture	String. The format string to use when creating a random password, if **random_password_method** is set to "nwa_picture_password".
random_username_length	The length, in characters, of randomly generated account usernames. • For nwa_words_password, 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 nwa_picture_password, the **random_username_length** is ignored. • For nwa_sequence, 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.

Table 46 *GuestManager Standard Fields (Continued)*

Field	Description
random_username_method	String. Identifier specifying how usernames are to be created. It may be one of the following identifiers: • **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.
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”** in this chapter 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.
schedule_after	Integer. Time period, in hours, after which the account will be enabled. This field is used when the **modify_schedule_time** field is set to **schedule_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.
schedule_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.

Table 46 *GuestManager Standard Fields (Continued)*

Field	Description
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.
visitor_company	String. The visitor’s company name.
visitor_name	String. The visitor’s full name.
vvisitor_phone	String. The visitor’s contact telephone number.

Hotspot Standard Fields

The table below describes standard fields available for the Hotspot form.

Table 47 *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.

Table 47 *Hotspot Standard Fields (Continued)*

Field	Description
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 48 *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 49 *SMPT 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 *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. 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_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.

Table 49 *SMPT Services Standard Fields (Continued)*

Field	Description
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.
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.i
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 50 *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 51 *Picture String Example Passwords*

Picture String	Sample Password
####	3728
user####	user3728
v^^#__	vQU3nj
@@@@@	Bh7Pm

Form Field Validation Functions

See **"Form Validation Properties"** in this chapter and **"Examples of Form field Validation"** in the Guest Management chapter 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. **See** **"Regular Expressions"** in this chapter for more information about regular expression syntax.
- **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.
- **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 wieth 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.
- **IsValidFutureTimestamp** – Checks that the value is a valid UNIX time referring to a point in the future.
- **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 (-).
- **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.
- **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 52 *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

- **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.
- **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.
- **NwaCaptchaIsValid** – 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.
- **NwaIsValidExpireAfter** – Checks that the value is one of the account expiration time options specified in the Guest Manager configuration.
- **NwaIsValidLifetime** – 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 53 *Form Field Display Functions*

Function	Description
NwaBoolFormat	Formats a Boolean value as a string. • If the argument is 0 or 1, a 0 or 1 is returned for false and true, respectively. • If the argument is a string containing a "|" character, the string is split at the | separator and used for false and true values. • If the argument is an array, the 0 and 1 index values are used for false and true values. Otherwise, the string values "false" and "true" are returned.
NwaByteFormat	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). • If a negative value is supplied, returns the argument (or null if no argument was supplied). • If a non-numeric value is supplied, that value is returned directly.
NwaCurrencyFormat	Formats a numeric value that indicates a monetary amount as a string. If the argument is null or not supplied, the current locale's settings are used to format the monetary value. • The argument may be an array, which will override the current locale's settings (see **NwaNumberFormat** for the list of settings that are used). • 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).

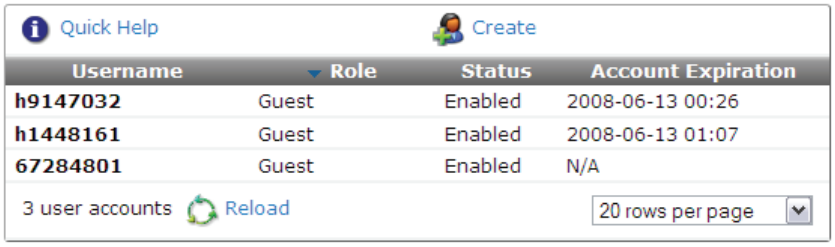
Table 53 *Form Field Display Functions (Continued)*

Function	Description
NwaDateFormat	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 "Date/Time Format Syntax"** in this chapter for a list of available date/time formats, or use one of the following special format strings: • **hhmmss**, **hh:mm:ss** – time of day • **iso8601**, **iso8601t**, **iso-8601**, **iso-8601t** – various ISO 8601 date formats with and without hyphen separators and the time of day • **longdate** – date and time in long form • **displaytime** – time of day • **?:** – returns the string following the ?: if the time value is 0, or uses the format string before the ?: otherwise • **recent** – for example, "2 minutes ago", "3 months ago"
NwaDurationFormat	Converts a time measurement into a description of the corresponding duration. • Format parameters: seconds, minutes, hours, days, weeks. • Any format can be converted to another. • 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. Up to four additional arguments may be supplied to control the conversion: • in_format – The current units of the value being converted (seconds, minutes, hours, days, weeks) • max_format – Controls the max increment you want displayed. • min_format – Controls the min increment you want displayed. Only whole numbers are printed. • default – If set, this value will be returned when the resulting duration (after min_format is taken into account) is 0.
NwaExplodeComma	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.
NwaNumberFormat	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 numerica 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). The specific locale settings used are from **localeconv(),** and are listed below. For *general numeric formatting* : • frac_digits – number of decimal places to display • decimal_point – character to use for decimal point • thousands_sep – character to use for thousands separator For *signs for positive/negative values:* • positive_sign – sign for positive values • p_sign_posn – position of sign for positive values (0..4) • negative_sign – sign for negative values • n_sign_posn – position of sign for negative values (0..4) For *formatting for monetary amounts*: • mon_decimal_point – decimal point character for monetary values • mon_thousands_sep – thousands separator for monetary values • p_sep_by_space – true if a space separates currency symbol from a positive value • p_cs_precedes – true if currency symbol precedes positive value • n_sep_by_space – true if a space separates currency symbol from a negative value • n_cs_precedes – true if currency symbol precedes negative value Additionally, the special value monetary, if true, indicates that a currency value should be formatted, rather than a regular numeric value.

View Display Expression Technical Reference

A page that contains a view is displayed in an operator's Web browser. The view con
tains 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".



In the above view (the **guest_users** view), the four columns displayed correspond to the **username**, **role_name**, **enabled**, and **expire_time** fields.

Table 54 *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 **enabled** 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	
Nwa_BooleanText (*value***,** *if_true***,** *if_false***[,** *if_undefined***])**	Returns the value of *if_true* or *if_false* depending on whether the *value* evaluates to a Boolean true or false, respectively. If the value has an undefined type (in other words. has not been set), and the *if_undefined* parameter was provided, returns *if_undefined*.
Nwa_DateFormat(*value***,** *format***)**	Converts a numerical *value* (UNIX time) to a string using the date and time format string *format*. The format string uses similar syntax to the NwaDateFormat() function. **See "Date/ Time Format String Reference"** in this chapter for a full list of the supported format strings.
Nwa_FloatFormat(*value***,** *decimals***)**	Converts a numerical *value* to a string, with the number of decimal places specified in *decimals*.
Nwa_MinutesToNatural(*value***)**	Converts a numeric *value* measuring a time in minutes to a natural time representation (such as "2 minutes", "3 hours", "11 days").

Table 54 *Display Expressions for Data Formatting (Continued)*

Value	Description
Nwa_NumberFormat(*value***[,** *if_undefined***])** **Nwa_NumberFormat(***value***,** *decimals***)** **Nwa_NumberFormat(***value***,** *decimals***,** *dec_point***,** *thousands_sep***[,** *if_undefined***])**	Converts a numerical value to a string. If the value has an undefined type (in other words, has not been set), and the if_undefined parameter was provided, returns if_undefined. Otherwise, the number is converted to a string using the number of decimal places specified in decimals (default 0), the decimal point character in dec_point (default "."), and the thousands separator character in thousands_sep (default ",").
Nwa_TrimText(*value***,** *length***)**	Trims excessively long strings to a maximum of *length* characters, appending an ellipsis ("…") if the string was trimmed.
Nwa_ValueText(*value***[,** *if_undefined***])**	If the *value* has an undefined type (in other words, has not been set), and the *if_undefined* parameter was provided, returns *if_undefined*, or a HTML non-breaking space (" ") otherwise. Otherwise, the *value* is converted to a string for display.

Standard RADIUS Request Functions

These functions are available for use in condition expressions and value expressions used in the definition of a RADIUS role. **See** **"Adding Authorization Conditions to Attribute Definitions"** in the RADIUS Services chapter for more details about using these functions.

Variables Available in Execution Context

Several PHP variables are available for use at the time the condition expression or value expression is evaluated.

Table 55 *PHP Variables*

Variable	Description
$now	Current UNIX time, as returned by PHP function **time()**
$user	User account structure
$role	Role definition for user
$role_id	Role ID of user account
$timeout	Calculated session timeout for user, in seconds
$attribute	Attribute name (from role definition)
$value	Attribute value (from role definition)

AccessReject()

```
AccessReject()
```

If invoked from a conditional expression, causes the Access-Request to be rejected.

Example usage as part of a condition expression for an attribute:

```
return expression && AccessReject()
```

If the expression evaluates to true, the AccessReject() will cause authorization to be refused. If the expression evaluates to false, the AccessReject() is not called, and authorization process will continue (however, the attribute will not be included in the Access-Accept, as the condition expression has evaluated to false).

EnableDebug()

```
EnableDebug($flag = 1)
```

Enables debugging for the remainder of the processing of this request. The flag may also be set to false or 0 to disable debugging.

Example usage as part of a condition expression for an attribute:

```
return EnableDebug() && expression
```

When debugging is enabled, additional output is generated. This may be visible in the RADIUS Debugger, or in the application log.

DisableDebug()

```
DisableDebug()
```

Disables debugging; equivalent to `EnableDebug(0)`.

GetAttr()

```
GetAttr($attr_name)
```

Returns the value of an attribute supplied with the RADIUS Access-Request. The `$attr_name` argument is the name of the attribute to look up. The attribute name is not case-sensitive. If the attribute was not included with the Access-Request, returns NULL.

Example usage:

- As a condition expression for an attribute:

  ```
  return GetAttr('Calling-Station-Id') == '00-01-02-44-55-66'
  ```

- As an attribute value:

  ```
  <?= GetAttr('Calling-Station-Id')
  ```

ShowAttr()

```
ShowAttr($raw = false)
```

Show the attributes passed with the RADIUS Access-Request. Writes to stderr, so the output can be seen using the RADIUS Debugger. The `$raw` argument, if set, outputs results without translating attribute names. This function is useful to see exactly what a NAS is sending, if debugging an authorization problem.

Example usage:

```
return ShowAttr() && ... // rest of condition
```

MacAddr()

```
MacAddr($mac)
```

Converts a MAC address to a canonical form. Uses standard IEEE 802 form for the MAC address, that is, uppercase hexadecimal digits using hyphen separators (01-23-45-67-89-AB). This function accepts anything that can be interpreted as a MAC address using some fairly liberal guidelines and returns the address in IEEE 802 format as described above. If a match could not be made (for example, empty string, or a string not containing a valid MAC address), returns NULL.

MacEqual()

```
MacEqual($addr1, $addr2)
```

Compares two MAC addresses for equality, using their canonical forms.

Example usage as a condition expression for an attribute:

```
return MacEqual(GetAttr('Calling-Station-Id'), '00-01-02-44-55-66')
```

MacAddrConvert()

```
MacAddrConvert($mac, $mac_format)
```

Converts a MAC address to a specified format. This function accepts anything that can be interpreted as a MAC address using some fairly liberal guidelines and returns the address formatted with the `$mac_format` string.

The `$mac_format` argument should be a sprintf-style format string that expects 6 arguments, which are the octets of the MAC address. For example, the IEEE 802 standard format of uppercase hexadecimal with each octet separated with a hyphen may be represented by the MAC format **%02X-%02X-%02X-%02X-%02X-%02X**. This is also the default value used if `$mac_format` is empty.

GetTraffic()

```
GetTraffic($criteria, $from_time, $to_time = null, $in_out = null)
```

Calculate the sum of traffic counters for accounting records in the database.

NOTE

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(), GetIpAddressTraffic(), or GetUserTraffic().

`$criteria` is the criteria on which to search for matching accounting records. The time interval specified by `$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.

GetTime()

```
GetTime($criteria, $from_time, $to_time = null)
```

Calculate the sum of session times for accounting records in the database.

NOTE

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()" ,** GetIpAddressTime(), or GetUserTime().

`$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.

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()**, **GetIpAddressSessions()**, **GetUserActiveSessions()**, or **GetUserSessions()**.

`$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.

GetCallingStationTraffic()

```
GetCallingStationTraffic($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. Note 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()
```

GetUserTraffic()

```
GetUserTraffic($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()" for details on how to specify the time interval.

GetIpAddressTraffic()

```
GetIpAddressTraffic($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()" for details on how to specify the time interval.

GetCallingStationTime()

```
GetCallingStationTime($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()" for details on how to specify the time interval.

GetUserTime()

```
GetUserTime($from_time, $to_time = null)
```

Calculate sum of session times in a specified time interval.

See "GetTraffic()" for details on how to specify the time interval.

GetIpAddressTime()

```
GetIpAddressTime($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()" for details on how to specify the time interval.

See "GetIpAddressTraffic()" for additional details on the `$ip_addr` argument.

GetCallingStationSessions()

```
GetCallingStationSessions($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()" for details on how to specify the time interval.

GetUserSessions()

```
GetUserSessions($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()" for details on how to specify the time interval.

GetIpAddressSessions()

```
GetIpAddressSessions($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()" for details on how to specify the time interval.

See "GetIpAddressTraffic()" for additional details on the `$ip_addr` argument.

GetUserActiveSessions()

```
GetUserActiveSessions($callingstationid = null)
```

Count 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). If a `$callingstationid` argument is supplied, sessions that match that Calling-Station-Id are excluded from the count of active sessions.

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()**, **GetIpAddressCurrentSession()**, or **GetUserCurrentSession()**. These functions are not available in RADIUS request context, but are available in the HTTP context (using {nwa_radius_query}).

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,
)
```

GetUserCurrentSession()

```
GetUserCurrentSession($username)
```

Looks up the current (most recent) active session for the specified username.

See "GetCurrentSession()" for details of the return value.

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()" for details of the return value.

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()" for details of the return value.

GetUserStationCount()

```
GetUserStationCount($from_time = null, $to_time = null, $exclude_mac = null)
```

Count the total number of unique MAC addresses used in a time interval, for all sessions with the same User-Name attribute as that specified in the RADIUS Access-Request.

If `$exclude_mac` is set, any sessions matching that MAC address are excluded from the count.

This function can be used to link a MAC address to a user on the first time they log in, and subsequently prevent access by the user if using a device other than the original device used.

Examples:

- Link the user MAC address on the first time they log in, and prevent all future access unless the calling-station-id is matched.

  ```
  return GetUserStationCount() > 0 && AccessReject()
  ```

- Fail authorization if the user has used more than 1 different MAC address in the past year. (Note: this does not quite work right as the current session being authorized is not taken into account.)

  ```
  return GetUserStationCount(365*24*60*60) > 1 && AccessReject()
  ```

- The correct way to do the above. Checks the last year of accounting records and permits a user a maximum of 2 different stations.

  ```
  return GetUserStationCount(365*24*60*60, time(),
           GetAttr('calling-station-id')) >= 2 && AccessReject()
  ```

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.

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");
```

RADIUS Server Options

These are the advanced server options that may be configured using the RADIUS Server Options text field. Where applicable, the default value for each configuration option is shown.

The default value will be used if no other value is set in the RADIUS Server Options.

Values for parameters may be quoted using double quotes; backslash escaping is supported within double-quoted strings.

General Configuration

Table 56 *General Configuration Settings*

Value	Description
max_request_time = 30	The maximum time (in seconds) to handle a request. Requests which take more time than this to process may be killed, and a REJECT message is returned.
cleanup_delay = 5	The time to wait (in seconds) before cleaning up a reply which was sent to the NAS. The RADIUS request is normally cached internally for a short period of time, after the reply is sent to the NAS. The reply packet may be lost in the network, and the NAS will not see it. The NAS will then re-send the request, and the server will respond quickly with the cached reply. If this value is set too low, then duplicate requests from the NAS MAY NOT be detected, and will instead be handled as separate requests. If this value is set too high, then the server will cache too many requests, and some new requests may get blocked. (See **max_requests**, below) The useful range of values is 2 to 10
max_requests = 1024	The maximum number of requests which the server keeps track of. This should be 256 multiplied by the number of clients, for example, with 4 clients, this number should be 1024. If this number is too low, then when the server becomes busy, it will not respond to any new requests, until the ‘cleanup_delay’ time has passed, and it has removed the old requests. If this number is set too high, then the server will use a bit more memory for no real benefit. If you aren’t sure what it should be set to, it’s better to set it too high than too low. Setting it to 1000 per client is probably the highest it should be. The useful range of values is 256 and higher.
bind_address = *	Make the server listen on a particular IP address, and send replies out from that address. This directive is most useful for machines with multiple IP addresses on one interface. It can either contain “*”, or an IP address, or a fully qualified Internet domain name.
listen.ipaddr = *not set*	By default, the server uses ‘bind_address’ to listen to all IP addresses on a machine, or just one IP. The ‘port’ configuration is used to select the authentication port used when listening on those addresses. If you want the server to listen on additional addresses, you can use the ‘listen’ section. The IP address on which to listen may be specified as a dotted-quad (1.2.3.4), hostname (radius.example.com) or as a wildcard (*).
listen.port = *not set*	Port number on which to listen. Only applies if ‘listen.ipaddr’ has been set. Allowed values are an integer port number (1812) or 0 to look up the port in /etc/services.

Table 56 *General Configuration Settings (Continued)*

Value	Description
listen.type = not set	Type of packets to listen for. Allowed values are “auth” for authentication packets, and “acct” for accounting packets.
hostname_lookups = off	Log the names of clients or just their IP addresses, for example, www.examle.com (on) or 209.97.207.76 (off). The default is ‘off’ because it would be overall better for the net if people had to knowingly turn this feature on, as enabling it means that each client request will result in AT LEAST one lookup request to the name server. Enabling hostname_lookups will also mean that your server may stop randomly for 30 seconds from time to time, if the DNS requests take too long. Turning hostname lookups off also means that the server won’t block for 30 seconds, if it sees an IP address which has no name associated with it. Allowed values are *no* and *yes*.
log_stripped_names = no	Log the full User-Name attribute, as it was found in the request. Allowed values are *no* and *yes*.
log_auth = yes	Log authentication requests to the log file. Allowed values are *no* and *yes*.
log_auth_badpass = no	Log incorrect passwords with the authentication requests. Allowed values are *no* and *yes*.
log_auth_goodpass = no	Log correct passwords with the authentication requests. Allowed values are *no* and *yes*.
lower_user = no **lower_pass** = no	Convert the username or password to lowercase “before” or “after” attempting to authenticate. If set to “before”, the server will first modify the request and then try to authenticate the user. If set to “after”, the server will first attempt to authenticate using the values provided by the user. If that fails it will reprocess the request after modifying it as you specify below. This is as close as ClearPass Guest can get to case insensitivity. It is the admin’s job to ensure that the username on the auth db side is also lowercase to make this work. Allowed values: before, after, no
nospace_user = no **nospace_pass** = no	Some users like to enter spaces in their username or password incorrectly. To save yourself the tech support call, you can eliminate those spaces here. Allowed values: before, after, no (as for ‘lower_user’ above)
rfc2868_zero_tag = no	Allow the insertion of RFC 2858 tags with a zero value. Normally, zero indicates an unused tag, and in string attributes (for example, Tunnel-Private-Group-Id) a zero tag would be omitted. However, some vendors require the tag to be present even if it is zero. In this case, setting this to ‘yes’ will allow the insertion and use of a zero tag. Default is ‘no’ (RFC 2868 compliant). Allowed values: no, yes
allow_authorize_only = no	Specify this option to enable support for authorization-only RADIUS requests, which have the Service-Type attribute set to the value “Authorize-Only” and do not contain a User-Password attribute. Default is ‘no’. Allowed values: no, yes

Security Configuration

Table 57 *Security Configuration Settings*

Value	Description
security.max_attributes = 200	The maximum number of attributes permitted in a RADIUS packet. Packets which have more than this number of attributes in them will be dropped. If this number is set too low, then no RADIUS packets will be accepted. If this number is set too high, then an attacker may be able to send a small number of packets which will cause the server to use all available memory on the machine. Setting this number to 0 means “allow any number of attributes”.
security.reject_delay = 1	When sending an Access-Reject, it can be delayed for a few seconds. This may help slow down a DoS attack. It also helps to slow down people trying to brute-force crack a user’s password. Setting this number to 0 means “send rejects immediately”. If this number is set higher than ‘cleanup_delay’, then the rejects will be sent at ‘cleanup_delay’ time, when the request is deleted from the internal cache of requests. The range of useful values are 1 to 5.
security.status_server = no	Sets whether or not the server will respond to Status-Server requests. When sent a Status-Server message, the server responds with an Access-Accept packet, containing a Reply-Message attribute, which is a string describing how long the server has been running. Allowed values are *no* and *yes*.

Proxy Configuration

Table 58 *Proxy Configuration Settings*

Value	Description
proxy_requests = yes	Turns proxying of RADIUS requests on or off. The server has proxying turned on by default. If your system is not set up to proxy requests to another server, then you can turn proxying off here. This will save a small amount of resources on the server. If you have proxying turned off, and your configuration files say to proxy a request, then an error message will be logged. Allowed values: no, yes
proxy.synchronous = no	If the NAS re-sends the request to us, we can immediately re-send the proxy request to the end server. To do so, use ‘yes’ here. If this is set to ‘no’, then we send the retries on our own schedule, and ignore any duplicate NAS requests. If you want to have the server send proxy retries ONLY when the NAS sends its retries to the server, then set this to ‘yes’, and set the other proxy configuration parameters to 0 (zero). Additionally, if you want ‘failover’ to work, the server must manage retries and timeouts. Therefore, if this is set to yes, then no failover functionality is possible. Allowed values: no, yes
proxy.retry_delay = 5	The time (in seconds) to wait for a response from the proxy, before re-sending the proxied request. If this time is set too high, then the NAS may re-send the request, or it may give up entirely, and reject the user. If it is set too low, then the RADIUS server which receives the proxy request will get kicked unnecessarily.
proxy.retry_count = 3	The number of retries to send before giving up, and sending a reject message to the NAS.

Table 58 *Proxy Configuration Settings (Continued)*

Value	Description
proxy.dead_time = 120	If the home server does not respond to any of the multiple retries, then the RADIUS server will stop sending it proxy requests, and mark it 'dead'. If there are multiple entries configured for this realm, then the server will failover to the next one listed. If no more are listed, then no requests will be proxied to that realm. After a configurable 'dead_time', in seconds, the RADIUS server will speculatively mark the home server active, and start sending requests to it again. If this dead time is set too low, then you will lose requests, as the server will quickly switch back to the home server, even if it isn't up again. If this dead time is set too high, then the server may take too long to switch back to the primary home server. Realistic values for this number are in the range of minutes to hours (60 to 3600).

SNMP Query Configuration

The SNMP query configuration value is **snmp = no**. To enable SNMP querying of the server, set this directive to 'yes'. Allowed values are *no* and *yes*.

Thread Pool Configuration

Table 59 *Thread Pool Settings*

Value	Description
thread.start_servers = 5	The thread pool is a long-lived group of threads which take turns (round-robin) handling any incoming requests. You probably want to have a few spare threads around, so that high-load situations can be handled immediately. If you don't have any spare threads, then the request handling will be delayed while a new thread is created, and added to the pool. You probably don't want too many spare threads around, otherwise they'll be sitting there taking up resources, and not doing anything productive. The default configuration should be adequate for most situations.
thread.max_servers = 32	Limit on the total number of servers running. If this limit is ever reached, clients will be locked out, so it should not be set too low. It is intended mainly as a brake to keep a runaway server from taking the system with it as it spirals down. You may find that the server is regularly reaching the 'max_servers' number of threads, and that increasing 'max_servers' doesn't seem to make much difference. If this is the case, then the problem is most likely that your back-end databases are taking too long to respond, and are preventing the server from responding in a timely manner. The solution is not to keep increasing the 'max_servers' value, but instead to fix the underlying cause of the problem: slow database, or 'hostname_lookups' set to 'yes'. For more information, see the 'max_request_time' server option.
thread.min_spare_servers = 3 **thread.max_spare_servers** = 10	Server-pool size regulation. Rather than making you guess how many servers you need, the RADIUS server dynamically adapts to the load it sees. That is, it tries to maintain enough servers to handle the current load, plus a few spare servers to handle transient load spikes. It does this by periodically checking how many servers are waiting for a request. If there are fewer than 'min_spare_servers', it creates a new spare. If there are more than 'max_spare_servers', some of the spares die off. The default values are probably OK for most sites.

Table 59 *Thread Pool Settings (Continued)*

Value	Description
thread.max_requests_per_server = 0	Set the maximum number of requests a server should handle before exiting. Zero is a special value meaning “infinity”, or “the servers never exit”.
thread.max_queue_size = 65536	Set the maximum number of incoming requests which may be queued for processing. After the queue reaches this size, new requests are dropped. The default value is recommended for most deployments. Do not change the default value unless you have a specific requirement.

Authentication Module Configuration

Table 60 *Authentication Module Configuration Settings*

Value	Description
module.pap = yes	PAP module to authenticate users based on their stored password.
pap.encryption_scheme = crypt	The PAP module supports multiple encryption schemes: • clear: Clear text • crypt: Unix crypt • md5: MD5 encryption • sha1: SHA1 encryption
module.chap = yes	Authenticates requests containing a CHAP-Password attribute.
module.pam = yes	Pluggable Authentication Modules for Linux.
module.unix = yes	Unix /etc/passwd style authentication.
unix.cache = no	Cache /etc/passwd, /etc/shadow, and /etc/group for authentication. The default is to not cache them. Allowed values: no, yes
unix.cache_reload = 600	If the cache is enabled, reloads its contents every ‘cache_reload’ seconds. Use 0 to disable.
module.mschap = yes	Microsoft CHAP authentication. This module supports MS-CHAP and MS-CHAPv2 authentication. It also enforces the SMB-Account-Ctrl attribute.
mschap.use_mppe = no	If ‘use_mppe’ is set to ‘yes’, the mschap module will add MS-CHAP-MPPE-Keys for MS-CHAPv1 and MS-MPPE-Recv-Key/MS-MPPE-Send-Key for MS-CHAPv2.
mschap.require_encryption = yes	If ‘use_mppe’ is enabled, ‘require_encryption’ makes encryption moderate.
mschap.require_strong = yes	‘require_strong’ always requires 128 bit encryption.
mschap.with_ntdomain_hack = no	Windows sends us a username in the form of DOMAIN\user, but sends the challenge response based on only the user portion. This workaround corrects for that incorrect behavior.

Table 60 *Authentication Module Configuration Settings (Continued)*

Value	Description
mschap.ntlm_auth	The module can perform authentication itself, or use a Windows Domain Controller. This configuration directive tells the module to call the ntlm_auth program, which will do the authentication, and return the NT-Key. Note that you MUST have “winbindd” and “nmbd” running on the local machine for ntlm_auth to work. See the ntlm_auth program documentation for details.

Database Module Configuration

Table 61 *Database Modeule Configuration Settings*

Value	Description
sql.case_insensitive_usernames = 0	Set this option to 1 to match usernames in the local user database without regard to case. This will allows basic RADIUS authentication to work when the case of the username provided by the NAS is different from the case of the username in the local user database. Note that this may have unexpected effects in certain authorization or accounting contexts, or when creating user accounts. This option does not control how external authentication servers perform username matches; these may be case-sensitive or case-insensitive depending on the type of server and its configuration. The default and recommended setting is to perform case-sensitive username matching.
sql.num_sql_socks = 5	The number of SQL connections to make to the database server.
sql.connect_failure_retry_delay = 60	The number of seconds to delay retrying on a failed database connection (per socket).
sql.safe_characters = not set	A list of characters that may be stored in database fields without being escaped. This may be set to the value “all” to indicate all standard ASCII characters. This string should not include any ASCII characters with a value of 128 or more as this could result in a string with an invalid UTF-8 encoding being sent to the database.
sql.simultaneous_stale_time = 86400	The “stale time” determines how much time must elapse without any interim accounting updates before an open session is considered “stale” and will no longer count towards a user’s session limit. Stale sessions are displayed in the Active Sessions list using a different state icon. This parameter is measured in seconds; the default corresponds to a value of 24 hours.
override.session.radutmp = yes	Set this parameter to “yes” to enable session limits in the case where guest accounts are limited to a maximum of one or more concurrent sessions. It is important to ensure that when this configuration option is in effect, the NAS is able to reliably send accounting stop messages. Otherwise, sessions will not be closed and this can lead to the same account being denied access when they are not actually logged in. When this occurs, the user's previous session will be shown as active in the active session list; it can be closed manually here.

EAP Module Configuration

Set the **advanced.eap = 1** option to enable additional EAP types to be selected in the **RADIUS Services** > **Authentication**>**EAP & 802.1X**>**EAP Configuration** form.

The following EAP module options are usually not required, as EAP configuration can be performed using the WebUI. For EAP documentation, **See** **"EAP and 802.1X Authentication and Certificate Management"** in the RADIUS Services chapter for further details.

Table 62 *Optional EAP Module Options*

Function	Description
advanced.eap = 1	Enable additional EAP types in the EAP Configuration form.
module.eap = yes	Extensible Authentication Protocol authentication.
eap.default_eap_type = md5	Invoke the default supported EAP type when EAP-Identity response is received. The incoming EAP messages DO NOT specify which EAP type they will be using, so it MUST be set here. Only one default EAP type may be used at a time. If the EAP-Type attribute is set by another module, then that EAP type takes precedence over the default type configured here.
eap.timer_expire = 60	A list is maintained to correlate EAP-Response packets with EAP-Request packets. After a configurable length of time, entries in the list expire, and are deleted.
eap.ignore_unknown_eap_types = no	There are many EAP types, but the server has support for only a limited subset. If the server receives a request for an EAP type it does not support, then it normally rejects the request. By setting this configuration to "yes", you can tell the server to instead keep processing the request. Another module MUST then be configured to proxy the request to another RADIUS server which supports that EAP type. If another module is NOT configured to handle the request, then the request will still end up being rejected.
eap.cisco_accounting_username_bug = no	Cisco AP1230B firmware 12.2(13)JA1 has a bug. When given a User-Name attribute in an Access-Accept, it copies one more byte than it should. Work around this issue by adding an extra zero byte.
module.eap_md5 = yes	Enables "md5" EAP type. EAP-MD5 authentication is not recommended for wireless connections. It is insecure, and does not provide for dynamic WEP keys.
module.eap_leap = yes	Cisco LEAP. LEAP is not recommended for use in new deployments. Cisco LEAP uses the MS-CHAP algorithm (but not the MS-CHAP attributes) to perform its authentication. As a result, LEAP requires access to the plain-text User-Password, or the NT-Password attributes. "System" authentication is impossible with LEAP.
module.eap_gtc = yes	Generic Token Card. Currently, this is only permitted inside of EAP-TTLS, or EAP-PEAP. The module "challenges" the user with text, and the response from the user is taken to be the User-Password. Proxying the tunneled EAP-GTC session is a bad idea: the users password will go over the wire in plain text, for anyone to see.
eap.gtc.challenge = "Password: "	The default challenge string, which many clients ignore.
eap.gtc.auth_type= PAP	The plain-text response which comes back is put into a User-Password attribute, and passed to another module for authentication. This allows the EAP-GTC response to be checked against plain-text, or encrypted passwords. If you specify "Local" instead of "PAP", then the module will look for a User-Password configured for the request, and do the authentication itself.

Table 62 *Optional EAP Module Options (Continued)*

Function	Description
module.eap_tls = no	Enables EAP-TLS module. The following functions onfigure digital certificates for EAP-TLS. If the private key and certificate are located in the same file, then private_key_file and certificate_file must contain the same filename. • **eap.tls.private_key_password** = *not set* • **eap.tls.private_key_file** = "${raddbdir}/certs/cert-srv.pem" • **eap.tls.certificate_file** = "${raddbdir}/certs/cert-srv.pem" • **eap.tls.dh_file** = "${raddbdir}/certs/dh" • **eap.tls.random_file** = "${raddbdir}/certs/random" • **eap.tls.CA_file** = "${raddbdir}/certs/demoCA/cacert.pem" Trusted root CA list. • **eap.tls.fragment_size** = 1024 This can never exceed the size of a RADIUS packet (4096 bytes), and is preferably half that, to accommodate other attributes in the RADIUS packet. On most APs the maximum packet length is configured between 1500 – 1600. In these cases, fragment size should be 1024 or less. • **eap.tls.include_length** = yes If set to yes, the total length of the message is included in every packet we send. If set to no, total length of the message is included only in the first packet of a fragment series. • **eap.tls.check_crl** = yes Check the Certificate Revocation List. • **eap.tls.check_cert_cn** = *not set* If check_cert_cn is set, the value will be xlat'ed and checked against the CN in the client certificate. If the values do not match, the certificate verification will fail, rejecting the user.
module.eap_ttls = no	The TTLS module implements the EAP-TTLS protocol, which can be described as EAP inside of Diameter, inside of TLS, inside of EAP, inside of RADIUS. The TTLS module needs the TLS module to be installed and configured, in order to use the TLS tunnel inside of the EAP packet. You will still need to configure the TLS module, even if you do not want to deploy EAP-TLS in your network. Users will not be able to request EAP-TLS, as it requires them to have a client certificate. EAP-TTLS does not require a client certificate.**eap.ttls.default_eap_type** = md5 The tunneled EAP session needs a default EAP type which is separate from the one for the non-tunneled EAP module. Inside of the TTLS tunnel, we recommend using EAP-MD5. If the request does not contain an EAP conversation, then this configuration entry is ignored. • **eap.ttls.copy_request_to_tunnel** = no The tunneled authentication request does not usually contain useful attributes like Calling-Station-Id, etc. These attributes are outside of the tunnel, and are normally unavailable to the tunneled authentication request. By setting this configuration entry to 'yes', any attribute which is not in the tunneled authentication request, but which is available outside of the tunnel, is copied to the tunneled request. • **eap.ttls.use_tunneled_reply** = no The reply attributes sent to the NAS are usually based on the name of the user 'outside' of the tunnel (usually 'anonymous'). If you want to send the reply attributes based on the username inside of the tunnel, then set this configuration entry to 'yes', and the reply to the NAS will be taken from the reply to the tunneled request.

Table 62 *Optional EAP Module Options (Continued)*

Function	Description
module.eap_peap= no	PEAP authentication. The PEAP module needs the TLS module to be installed and configured, in order to use the TLS tunnel inside of the EAP packet. You will still need to configure the TLS module, even if you do not want to deploy EAP-TLS in your network. Users will not be able to request EAP-TLS, as it requires them to have a client certificate. EAP-PEAP does not require a client certificate. • **eap.peap.default_eap_type** = mschapv2 The tunneled EAP session needs a default EAP type which is separate from the one for the non-tunneled EAP module. Inside of the TLS/PEAP tunnel, we recommend using EAP-MS-CHAPv2. • **module.eap_mschapv2** = yes Enable the EAP MS-CHAPv2 sub-module. In order for this sub-module to work, the main 'mschap' module must also be configured. This module is the Microsoft implementation of MS-CHAPv2 in EAP. There is another (incompatible) implementation of MS-CHAPv2 in EAP by Cisco, which is not currently supported.

LDAP Module Configuration

The following LDAP module options are usually not required, as LDAP server configuration can be performed using the WebUI. **See "Configuring an LDAP EAS"** in the RADIUS Services chapter for further details.

Table 63 *LDAP Module Settings*

Setting	Description
module.ldap = no	Lightweight Directory Access Protocol (LDAP). This module definition allows you to use LDAP for authorization and authentication (Auth-Type := LDAP).
ldap.server = ldap.example.com	Set the LDAP server hostname/ip address. You can also pass an LDAP URL like ldap://localhost. That way you can also specify alternative ldap schemas like ldaps:// or ldapi://. The port directive will be ignored in this case.
ldap.port = 389	LDAP server port. If LDAP server port is set to 636 (ldaps), SSL connection is enforced. This feature is useful for LDAP servers which support SSL, but don't do TLS negotiation (like Novell eDirectory).
ldap.edir_account_policy_check = yes	Applies Novell's account policy checks (authorization) when authenticating a user via LDAP lookup in the eDirectory. The default setting is "yes". To disable the Novell account policy checks, set this option to "no", in which case all authorization will be performed by the RADIUS server. Required for Novell eDirectory support. When defining this attribute for an individual Novell eDirectory LDAP server, remove the "ldap." prefix from the attribute name.

Table 63 *LDAP Module Settings (Continued)*

Setting	Description
ldap.password_attribute = “nspmPassword”	To support Novell eDirectory Universal Password, this option must be set to “nspmPassword”. Retrieves the user’s plain-text password from the directory and uses in the RADIUS server for user authentication. Universal Password requires a secure connection to the LDAP server. Required for Novell eDirectory support. When defining this attribute for an individual Novell eDirectory LDAP server, remove the “ldap.” prefix from the attribute name.
ldap.password_header = “{clear}”	To extract the user’s plain-text password via Novell Universal Password, this value must be set to “{clear}”. The value for this attribute must be lowercase. Universal Password requires a secure connection to the LDAP server. Required for Novell eDirectory support. When defining this attribute for an individual Novell eDirectory LDAP server, remove the “ldap.” prefix from the attribute name.
ldap.net_timeout = 1	Number of seconds to wait for a response from the LDAP server (network failures).
l**dap.timeout** = 4	Number of seconds to wait for the LDAP query to finish.
ldap.timelimit = 3	Number of seconds the LDAP server has to process the query (server-side time limit).
ldap.ldap_debug = 0	Debug flags for LDAP SDK (see OpenLDAP documentation) Example: (LDAP_DEBUG_FILTER + LDAP_DEBUG_CONNS) ldap.ldap_debug = 0x0028
ldap.identity = *not set*	The DN under which LDAP searches are done.
ldap.password = *not set*	Password which authenticates the identity DN. If not set, the default is to perform an anonymous bind, with no password required. NOTE: this implies that searches will be done over an unencrypted connection!
ldap.basedn	**ldap.filter**= "o=My Org,c=UA" Base of LDAP searches.
ldap.filter	**ldap.filter** = "uid=%{Stripped-User-Name:-%{User-Name}}" The LDAP search filter, to locate user object using the name supplied by client during the RADIUS authentication process.
ldap.base_filter = *not set*	The LDAP search filter used for base scope searches, like when searching for the default or regular profiles.
ldap.start_tls = no	When set to “yes”, the StartTLS extended operation is used to enable TLS transport encryption.
ldap.tls_mode = no	When set to “yes”, or if the server port is 636, we try to connect with TLS. Start TLS should be preferred; ‘tls_mode’ is provided only for LDAP servers like Active Directory which do not support it.
ldap.tls_cacertfile = *not set*	A PEM-encoded file that contains the CA Certificates that you trust.
ldap.tls_cacertdir = *not set*	Path to a directory of CA Certificates that you trust, the directory must be in “hash format” (see: openssl verify).

Table 63 *LDAP Module Settings (Continued)*

Setting	Description
ldap.tls_certfile = *not set*	The PEM Encoded certificate file that should be presented to clients that connect. ldap.tls_keyfile = *not set* The PEM Encoded private key that should be used to encrypt the session.
ldap.tls_randfile = *not set*	A file containing random data to seed the OpenSSL PRNG. Not needed if your OpenSSL is already properly random.
ldap.tls_require_cert = *not set*	Certificate Verification requirements. Can be “never” (don’t even bother trying), “allow” (try, but don’t fail if the certificate can't be verified), or “demand” (fail if the certificate doesn’t verify).
ldap.default_profile = *not set*	DN of a LDAP object, which contains default RADIUS attributes. If not set, use only user specific attributes or attributes, supplied by other modules.
ldap.profile_attribute = *not set*	Name of a user object attribute, which contains DN of radiusProfile object for this user. If unset, use only user specific attributes or attributes, supplied by other modules.
ldap.access_attrused_for_allow = yes	Determines if the access attribute (described below) will be used to allow access (meaning if it exists then user remote access will be allowed) or to deny access.
ldap.access_attr = dialupAccess	If attribute is specified, the LDAP module checks for its existence in the user object. If access_attr_used_for_allow is set to yes, and the attribute exists, the user is allowed to get remote access. If the attribute exists and is set to FALSE, the user is denied remote access. If the attribute does not exist, the user is denied remote access by default. If access_attr_used_for_allow is set to no, and the attribute exists, the user is denied remote access. If it does not exist, the user is allowed remote access.
ldap.password_header = *not set*	If the user password is available we add it to the check items (to assist in CHAP), stripping any headers first. The password_header directive is NOT case insensitive.
ldap.password_attribute = *not set*	Define the attribute which contains the user password.
ldap.groupname_attribute = *not set*	The attribute containing group name in the LDAP server. It is used to search groups by name.
ldap.compare_check_items = no	Specifies if the module will do a comparison on the check items extracted from the ldap with the corresponding items present in the incoming request.
ldap.do_xlat = yes	Specifies if the module will do an xlat on the radius attributes extracted from the ldap database. Also, the attribute operators will be honored. If the directive is set to ‘no’ then we will fall back to the pairadd() function which will just add the attributes at the end of the corresponding attribute list (check or reply items). This can be used to fall back to 0.8.1 behavior without changing the LDAP data or to gain a little performance if the LDAP data is rather simple (no special operators)

Table 63 *LDAP Module Settings (Continued)*

Setting	Description
ldap.groupmembership_filter = *not set*	The filter to search for group membership of a particular user after we have found the DN for the group. Example filter: (|(&(objectClass=GroupOfNames)(member=%{Ldap-UserDn}))(&(objectClass=GroupOfUniqueNames)(uniquemember=%{Ldap-UserDn})))
ldap.groupmembership_attribute = not set	The attribute in the user entry that states the group the user belongs to. The attribute can either contain the group name or the group DN. If it contains the group DN, groupmembership_attribute will also be used to find the group's name. The attribute will be used after a search based on the groupname_attribute and groupmembership_filter has failed. If unset, the module does not search for a group based on attributes in the user entry.

Rewrite Module Configuration

The **attr_rewrite** module can be used to perform pattern matching and replacement tasks on RADIUS attributes contained in an Access-Request message.

See "Server Configuration" in the RADIUS Services chapter for examples showing how to use the attr_rewrite module.

Multiple attr_rewrite modules can be declared. Use the syntax to create an attr_rewrite module named *name*:

```
module.attr_rewrite.name.attribute = "..."
module.attr_rewrite.name.searchin = packet
module.attr_rewrite.name.searchfor = "..."
module.attr_rewrite.name.replacewith = "..."
```

Use this syntax to instantiate the modules, and specify the numerical order in which the processing should be done (0, 1, 2, etc.):

```
authorize.after_preprocess.0.name = module1
authorize.after_preprocess.1.name = module2
```

The following table describes the rewrite module attributes and settings.

Table 64 *Rewrite Module Configuration Settings*

Value	Description
module.attr_rewrite.*name*.attribute = *not set*	Specifies the name of the RADIUS attribute for which rewriting will be performed.
module.attr_rewrite.*name*.searchin = packet	Specifies which attribute list is to be searched: may be "packet", "reply", "proxy", "proxy_reply" or "config". The default of "packet" indicates the Access-Request message; use a value of "reply" to rewrite attributes in either the Access-Accept or Access-Reject message.

Table 64 *Rewrite Module Configuration Settings (Continued)*

Value	Description
module.attr_rewrite.*name*.searchfor = *not set*	A regular expression to use when determining if the attribute should be matched. **See** "Regular Expressions" in this chapter for information about the supported syntax for regular expressions.
module.attr_rewrite.*name*.replacewith = *not set*	The replacement value which will be used for the attribute value, if the attribute matches the "searchfor" regular expression. Backreferences to the matching components of the "searchfor" regular expression are supported: **%{0}** will contain the string for the entire regular expression match, and **%{1}** through **%{8}** contain the contents of the 1st through the 8th matching parenthesized groups. If the "new_attribute" item is set to yes, then this value is used as the contents of a new attribute.
module.attr_rewrite.*name*.ignore_case = no	If set to yes, matches the "searchfor" regular expression in a case-insensitive way. The default behavior is to match case-sensitively.
module.attr_rewrite.*name*.new_attribute = no	If set to yes, a new attribute will be created, containing the value of the "replacewith" item. The new attribute will be added to the "searchin" item (packet, reply, proxy, proxy_reply or config). In this case, the "searchfor", "ignore_case" and "max_matches" items are ignored.
module.attr_rewrite.*name*.max_matches = 10	The maximum number of regular expression matches to be processed for the attribute.
module.attr_rewrite.*name*.append = no	If set to yes, then the "replacewith" string will be appended to the original attribute value. The default of "no" causes the entire attribute value to be replaced.

List of Standard Radius Attributes

Authentication Attributes

These are the attributes the NAS uses in authentication packets and expects to get back in authentication replies. These can be used in matching rules.

- **User-Name**: This attribute indicates the name of the user to be authenticated or accounted. It is used in Access-Request and Accounting packets.
- **Password**: This attribute indicates the password of the user to be authenticated, or the user's input following an Access-Challenge. It is only used in Access-Request packets.
- **CHAP-Password**: This attribute indicates the response value provided by a PPP Challenge-Handshake Authentication Protocol (CHAP) user in response to the challenge. It is only used in Access-Request packets.
- **NAS-IP-Address**: This attribute indicates the IP address of the NAS which is requesting authentication of the user. It is only used in Access-Request packets.
- **NAS-Port-Id**: This attribute indicates the physical port number of the NAS which is authenticating the user. It is only used in Access-Request packets. Note that this is using "port" in its sense of a physical connection on the NAS, not in the sense of a TCP or UDP port number.

- **Service-Type**: This attribute indicates the type of service the user has requested, or the type of service to be provided. It may be used in both Access-Request and Access-Accept packets.
- **Framed-Protocol**: This attribute indicates the framing to be used for framed access. It may be used in both Access-Request and Access-Accept packets.
- **Framed-IP-Address**: This attribute indicates the address to be configured for the user. In an Accounting-Request packet, it indicates the IP address of the user.
- **Framed-IP-Netmask**: This attribute indicates the IP netmask to be configured for the user when the user is a router to a network.
- **Framed-Routing:** This attribute indicates the routing method for the user, when the user is a router to a network. It is only used in Access-Accept packets.
- **Framed-MTU**: This attribute indicates the Maximum Transmission Unit to be configured for the user, when it is not negotiated by some other means (such as PPP). It is only used in Access-Accept packets.
- **Framed-Compression**: This attribute indicates a compression protocol to be used for the link.
- **Reply-Message**: This attribute indicates text which may be displayed to the user.
- **Callback-Number**: This attribute indicates a dialing string to be used for callback.
- **Callback-Id**: This attribute indicates the name of a place to be called, to be interpreted by the NAS.
- **Framed-Route:** This attribute provides routing information to be configured for the user on the NAS. It is used in the Access-Accept packet and can appear multiple times.
- **State**: This attribute is available to be sent by the server to the client in an Access-Challenge and MUST be sent unmodified from the client to the server in the new Access-Request reply to that challenge, if any.
- **Class**: This attribute is available to be sent by the server to the client in an Access-Accept and should be sent unmodified by the client to the accounting server as part of the Accounting-Request packet if accounting is supported.
- **Vendor-Specific**: This attribute is available to allow vendors to support their own extended Attributes not suitable for general usage.
- **Session-Timeout**: This attribute sets the maximum number of seconds of service to be provided to the user before termination of the session or prompt.
- **Idle-Timeout**: This attribute indicates how many octets have been received from the port over the course of this service being provided, and can only be present in Accounting-Request records where the Acct-Status-Type is set to Stop.
- **Acct-Output-Octets**: This attribute indicates how many octets have been sent to the port in the course of delivering this service, and can only be present in interim and stop Accounting-Request records.
- **Acct-Session-Id**: This attribute is a unique Accounting ID to make it easy to match start and stop records in a log file.
- **Acct-Authentic**: This attribute may be included in an Accounting-Request to indicate how the user was authenticated, whether by RADIUS, the NAS itself, or another remote authentication protocol. Users who are delivered service without being authenticated should not generate Accounting records.
- **Acct-Session-Time**: This attribute indicates how many seconds the user has received service for, and can only be present in Accounting-Request records where the Acct-Status-Type is set to Stop or Interim Update.
- **Acct-Input-Packets**: This attribute indicates how many packets have been received from the port over the course of this service being provided to a Framed User, and can only be present in Accounting-Request records where the Acct-Status-Type is set to Stop or Interim Update. This attribute indicates how many packets have been sent to the port in the course of delivering this service to a Framed User, and can only be present in Accounting-Request records where the Acct-Status-Type is set to Stop or Interim Update.

- **Acct-Terminate-Cause**: This attribute indicates how the session was terminated, and can only be present in Accounting-Request records where the Acct- Status-Type is set to Stop.

RADIUS Server Internal Attributes

The **Simultaneous-Use** attribute is used by the RADIUS server during the processing of a request. This internal attribute is never returned to a NAS. Simultaneous-Use specifies the maximum number of simultaneous logins a given user is permitted to have. When the user is logged in this number of times, any additional attempts to log in are rejected.

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.

- **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 See Table 65 can be used to perform pattern matching tasks using regular expressions.

Table 65 *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.

Chapter 13

Glossary

802.1X	IEEE standard for port-based network access control.
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-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.
accounting session time	Length of time the guest has been using the network.
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	Authorization controls the type of access that an authenticated user is permitted to have.
BYOD	Bring your own device. Refers to the trend of personal mobile devices being used with enterprise network infrastructure.
CA	See *Certificate Authority*.
captive portal	Implemented by NAS. Provides access to 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 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*.
common name (CN)	See *distinguished name*.
$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 pre-defined helper functions do not provide required flexibility.
CRL	Certificate revocation list. List of revoked certificates maintained by a certificate authority and regularly updated.
CSV	Comma-separated values.
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.
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.
distinguished name	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 (RFC 3748). An authentication framework that supports multiple authentication methods.
EAP-PEAP	Protected EAP. A widely-used protocol for securely transporting authentication data across a network.
EAP-TLS	Extensible Authentication Protocol – Transport LayerSecurity (RFC 5216). A certificate-based authentication method supporting mutual authentication, integrity-protected ciphersuite negotiation and key exchange between two endpoints.
form	Screen that collects data using fields.
field	Single item of information about a visitor account.
guest	See *Visitor*.
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.
landing page	See *Web login*.
LDAP	Lightweight Directory Access Protocol; communications protocol used to store and retrieve information about users and other objects in a directory.
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.
OCSP	Online certificate status protocol (RFC 2560). Protocol used to determine the current status of a digital certificate without requiring CRLs.
onboarding	See *device provisioning*.
onboard-capable device	Device supported by the QuickConnect application.
onboard provisioning	Process used to securely provision a device and configure it with network settings.

operator profile	Characteristics assigned to a class of operators, such as the permissions granted to those operators.
operator/operator login	Person who uses ClearPass Guest to create guest accounts or perform system administration.
OS X	Operating system from Apple, Inc. for desktop and laptop computers.
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.
PEAP	Protected EAP. See *EAP-PEAP*.
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	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*.
print template	Formatted template used to generate guest account receipts.
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).
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.
QuickConnect App	Application used to securely provision an Android, Windows, or OS X device and configure it with network settings.
RFC	Request For Comments; a commonly-used format for Internet standards documents.
role	Type of access being granted. You can 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 Guest. 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.
SCEP	Simple certificate enrollment protocol. Protocol for requesting and managing digital certificates.
self-signed certificate	See *root CA*.
session	Service provided by a NAS to an authorized user.
skin	Web site's external appearance, or "look and feel." It can be thought of as a container that holds the application, its style sheet (font size and color for example), its header and footer, and so forth.
SMS	Short Message System; a method for delivering short messages (up to 140 characters) to mobile phones.

sponsor	See *operator*.
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*.
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.
view	Table containing data. Used to interactively display data such as visitor accounts to operators.
visitor/guest	Someone who is permitted to access the Internet through your Network Access Server.
VPN	Virtual private network. Enables secure access to a corporate network when located remotely.
VSA	Vendor-specific attribute.
walled garden	Network resources that can be accessed by unauthorized users through the captive portal.
Web login	Login page displayed to a visitor.
X.509	Standard defining the format and contents of digital certificates.

Index

Numerics

A

B

C

D

E

F

G

H

N

O

P

Q

R

S

T

U

V

W

X