Dell Networking W-ClearPass Policy Manager 6.1

Quick Start Guide

Copyright Information

© 2013 Aruba Networks, Inc. Aruba Networks trademarks include the Aruba Networks logo, Aruba Networks®, Aruba Wireless Networks®, the registered Aruba the Mobile Edge Company logo, and Aruba Mobility Management System®. Dell™, the DELL™ logo, and PowerConnect™ are trademarks of Dell Inc.

All rights reserved. Specifications in this manual are subject to change without notice.

Originated in the USA. All other trademarks are the property of their respective owners.

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. Includes software from Litech Systems Design. The IF-MAP client library copyright 2011 Infoblox, Inc. All rights reserved.This product includes software developed by Lars Fenneberg, et al. 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.

Contents

Configuring Policy Manager 5
Installing Policy Manager 5
Server Port Overview 5
Server Port Configuration 5
A Subset of Useful CLI Commands 7
Accessing Policy Manager 9
Accessing Help 10
Checking Basic Services 11
802.1x Wireless Use Case 13
Configuring the Service 13
Web-Based Authentication Use Case 19
Configuring the Service 19
MAC Authentication Use Case 25
Configuring the Service 26

Chapter 1

Configuring Policy Manager

This Quick Start Guide for the Dell Networking W-ClearPass Policy Manager System (Policy Manager) describes the steps for installing the appliance using the *Command Line Interface* (CLI) and using the *User Interface* (UI) to ensure that the required services are running.

Installing Policy Manager

The Policy Manager server requires initial port configuration.

Server Port Overview

Policy Manager Backplane

P—Power Button; A—Serial port; B—Management port; C—Data port

as described in the following table:

Key	Port	Description
A	Serial	Configures the Policy Manager appliance initially, via hardwired terminal.
B - eth1	Management (gigabit Ethernet)	Provides access for cluster administration and appliance maintenance via web access, CLI, or internal cluster communications. Configuration required.
C - eth2	Data (gigabit Ethernet)	Provides point of contact for RADIUS, TACACS+, Web Authentication and other data-plane requests. Configuration optional. If not configured, requests redirected to the management port.

Server Port Configuration

Before starting the installation, gather the following required information:

Required Item	Item Information
Hostname (Policy Manager server)	
Management Port IP Address	
Management Port Subnet Mask	
Management Port Gateway	
Data Port IP Address (optional)	Data Port IP Address must not be in the same subnet as the Management Port IP Address
Data Port Gateway (optional)	
Data Port Subnet Mask (optional)	
Primary DNS	
Secondary DNS	
NTP Server (optional)	

To set up the Policy Manager appliance:

1. Connect and power on.

   Using the null modem cable provided, connect a serial port on the appliance to a terminal, then connect power and **switch on**. The appliance immediately becomes available for configuration.

   Use the following parameters for the serial port connection:

   - Bit Rate: 9600
   - Data Bits: 8
   - Parity: None
   - Stop Bits: 1
   - Flow Control: None

2. Login.

   Later, you will create a unique appliance/cluster administration password. For now, use the preconfigured credentials:

   ```
   login: appadmin
   password: eTIPS123
   ```

   This starts the Policy Manager Configuration Wizard.

3. Configure the appliance.

   Replace the bolded placeholder entries in the following illustration with your local information:

   ```
   Enter hostname: hyperion.us.arubanetworks.com
   Enter Management Port IP Address: 192.168.5.10
   Enter Management Port Subnet Mask: 255.255.255.0
   Enter Management Port Gateway: 192.168.5.1
   Enter Data Port IP Address: 192.168.7.55
   Enter Data Port Subnet Mask: 255.255.255.0
   Enter Data Port Gateway: 192.168.7.1
   Enter Primary DNS: 198.168.5.3
   ```

```
Enter Secondary DNS: 192.168.5.1
```

4. Change your password.

   Use any string of at least six characters:

   ```
   New Password:************
   Confirm Password:************
   ```

   Going forward, you will use this password for cluster administration and management of the appliance.

5. Change system date/time.

   ```
   Do you want to configure system date time information [y|n]: y
   Please select the date time configuration options.
   1) Set date time manually
   2) Set date time by configuring NTP servers
   Enter the option or press any key to quit: 2
   Enter Primary NTP Server: pool.ntp.org
   Enter Secondary NTP Server: time.nist.gov
   Do you want to configure the timezone? [y|n]: y
   ```

   Once the timezone information is entered, you are asked to confirm the selection.

6. Commit or restart the configuration.

   Follow the prompts:

   ```
   y[Y] to continue
   n[N] to start over again
   q[Q] to quit
   Enter the choice: Y
   Successfully configured Policy Manager appliance
   ************************************************************
   * Initial configuration is complete.
   * Use the new login password to login to the CLI.
   * Exiting the CLI session in 2 minutes. Press any key to exit now.
   ```

A Subset of Useful CLI Commands

The CLI provides a way to manage and configure Policy Manager information. Refer to *Appendix A: Command Line Interface* in the User Guide for more detailed information on the CLI.

The CLI can be accessed from the console using a serial port interface or remotely using SSH:

```
*********************************************************************************
*                                                                               *
* Dell W-ClearPass Policy Manager 6.1.0.50361                                   *
*                                                                               *
*********************************************************************************
Logged in as group Local Administrator
[appadmin@hyperion.us.arubanetworks.com]#
```

The following subset of CLI commands may be useful at this point:

- To view the Policy Manager data and management port IP address, and DNS configuration:

  ```
  [appadmin]# show ip
  ```

- To reconfigure DNS or add a new DNS:

  ```
  [appadmin]# configure dns <primary> [secondary] [tertiary]
  ```

- To reconfigure or add management and data ports:

  ```
  [appadmin]# configure ip <mgmt | data > <ipadd> netmask <netmask address> gateway <gateway address>
  ```

  where:

Flag/Parameter	Description
ip <mgmt|data> <ip address>	• Network interface type: *mgmt* or *data* • Server ip address.
netmask <netmask address>	Netmask address.
gateway <gateway address>	Gateway address.

- To configure the date (time and time zone optional):
  ```
  [appadmin]# configure date –d <date> [-t <time>] [-z <timezone>]
  ```
- To configure the hostname to the node:
  ```
  configure hostname <hostname>
  ```
- If you are using Active Directory to authenticate users, be sure to join the Policy Manager appliance to that domain as well.
  ```
  ad netjoin <domain-controller.domain-name> [domain NETBIOS name]
  ```
  where:

Flag/Parameter	Description
<domain-controller. domain-name>	Required. Host to be joined to the domain.
[domain NETBIOS name]	Optional.

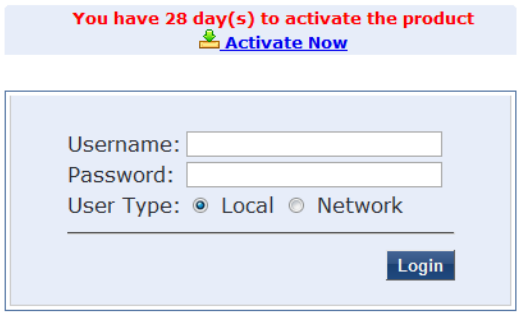
Chapter 2

Accessing Policy Manager

Use *Mozilla Firefox 3.0* (or higher) or *Internet Explorer 7.0.5* (or higher) to perform the following steps:

1. Open the administrative interface.

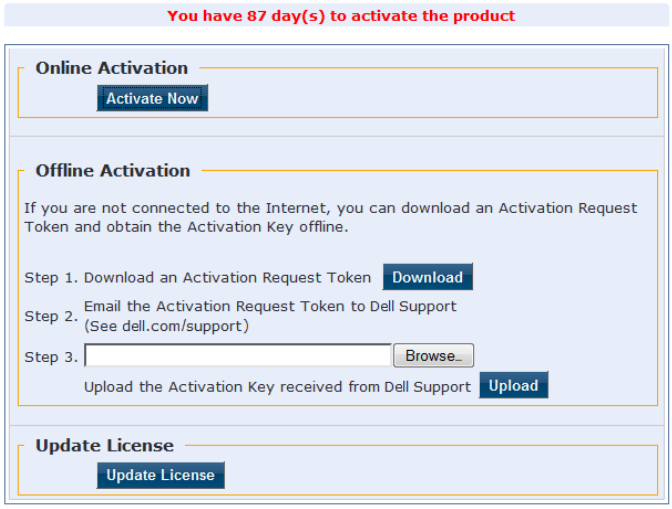
   Navigate to https://<hostname>/tips (where <hostname> is the hostname you configured during the initial configuration).
2. Enter License Key.
3. Click on the **Activate Now** link.



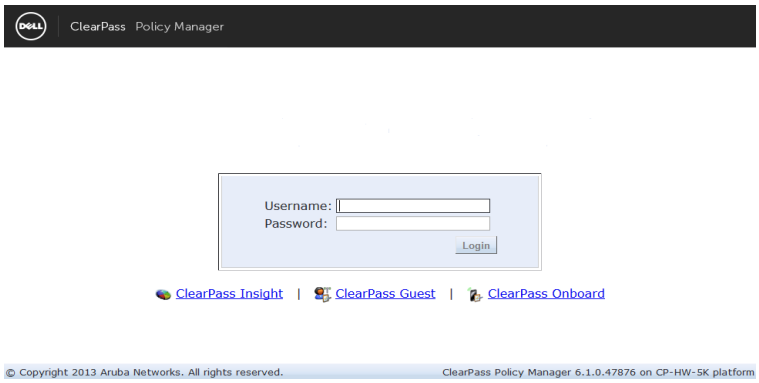
4. Activate the product.

   If the appliance is connected to the Internet, click on the **Activate Now** button. If not, click on the **Download** button to download the Activation Request Token. Contact Dell Support and provide your technician with the downloaded token in an email attachment. Once you receive the Activation Key from Dell Support, save it to a known location on your computer. Come back to this screen and click on the **Browse** button to select the Activation Key. Upload the key by clicking on the **Upload** button.

   The product is now activated.

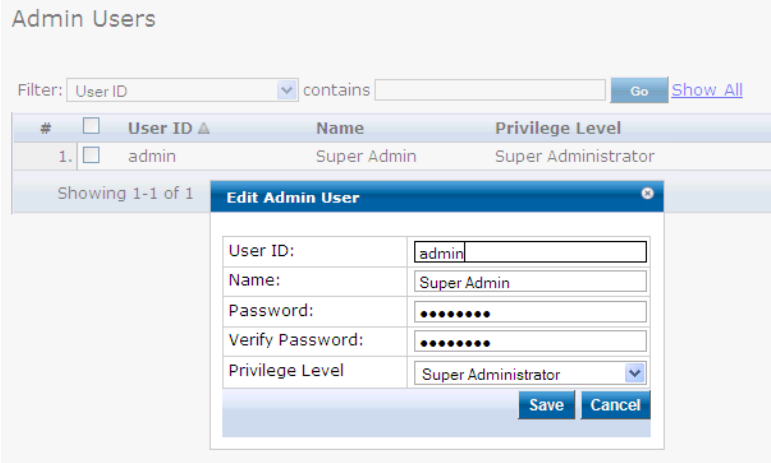


5. Login. Username: admin, Password: eTIPS123



6. Change the password.

   Navigate to **Administration > Admin Users**, then use the **Edit Admin User** popup to change the administration password.



Accessing Help

The Policy Manager User Guide (in PDF format) is built within the help system here:

`https://<hostname>/tipshelp/html/en/`

(where `<hostname>` is the hostname you configured during the initial configuration.)

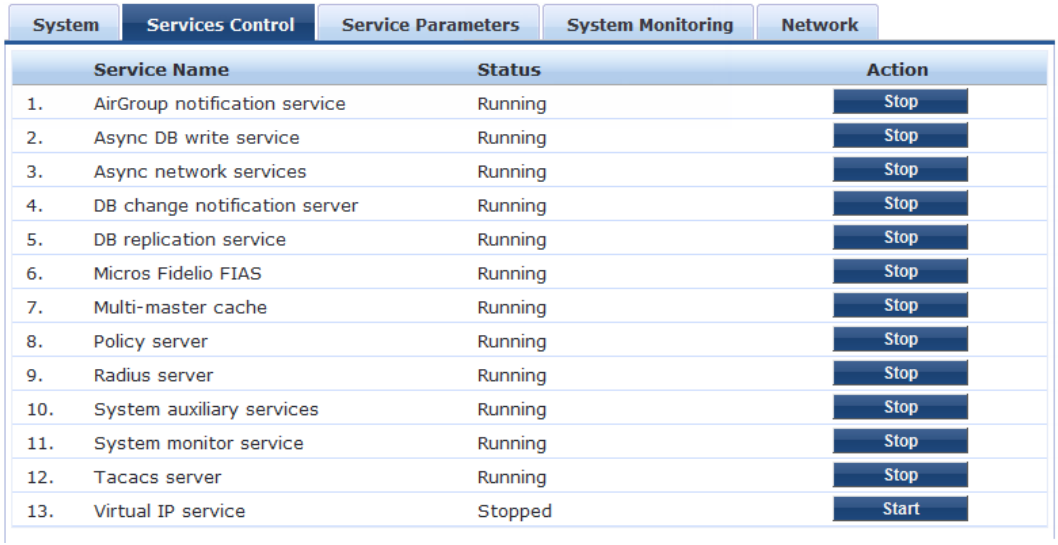
All Policy Manager user interface screens have context-sensitive help. To access context-sensitive help, click on the **Help** link at the top right hand corner of any screen.

Chapter 3

Checking Basic Services

To check the status of service, navigate to **Administration > Server Manager > Server Configuration**, then click on a row to select a server:

- The **System** tab displays server identity and connection parameters.
- The **Service Control** tab displays all services and their current status. If a service is stopped, you can use its **Start/Stop** button (toggle) to restart it.



You can also start an individual service from the command line,

```
service start <service-name>
```

or all services from the command line,

```
service start all
```

- The **Service Parameters** tab allows you to change system parameters for all services.
- The **System Monitoring** tab allows you to configure SNMP parameters, ensuring that external MIB browsers can browse the system-level MIB objects exposed by the Policy Manager appliance.
- The **Network** tab allows you to view and create GRE tunnels and VLANs.

The following three use cases illustrate the process of configuring Policy Manager for basic 802.1x, WebAuth, and MAC Bypass Services:

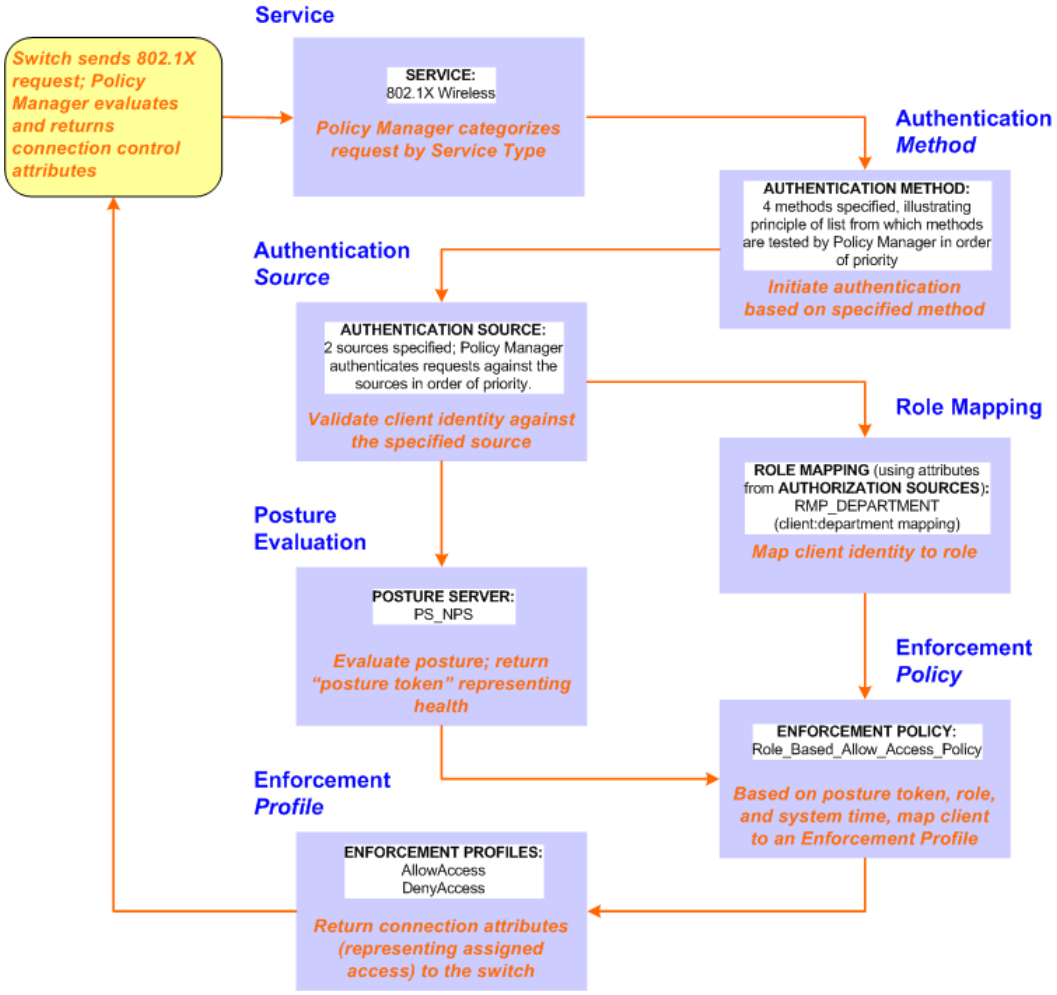
- 802.1x Wireless Use Case on page 13
- Web-Based Authentication Use Case on page 19
- MAC Authentication Use Case on page 25

Chapter 4

802.1x Wireless Use Case

The basic Policy Manager Use Case configures a Policy Manager Service to identify and evaluate an 802.1X request from a user logging into a Wireless Access Device. The following image illustrates the flow of control for this Service.

Figure 1: *Flow of Control, Basic 802.1X Configuration Use Case*



Configuring the Service

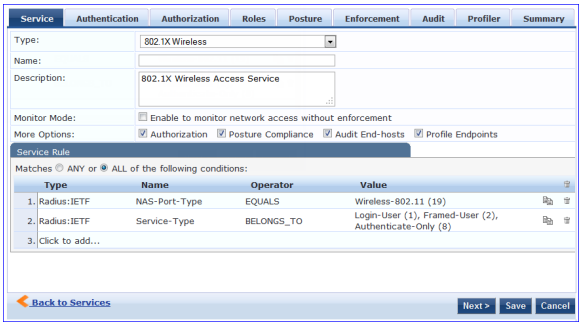
Follow the steps below to configure this basic 802.1X service:

1. Create the Service

   The following table provides the model for information presented in Use Cases, which assume the reader's ability to extrapolate from a sequence of navigational instructions (left column) and settings (in summary form in the right column) at each step. Below the table, we call attention to any fields or functions that may not have an immediately obvious meaning.

Policy Manager ships with fourteen preconfigured Services. In this Use Case, you select a Service that supports 802.1X wireless requests.

Table 1: *802.1X - Create Service Navigation and Settings*

Navigation	Settings
Create a new Service: • **Services** > • **Add Service** (link) >	
Name the Service and select a pre-configured Service Type: • **Service** (tab) > • **Type** (selector): **802.1X Wireless** > • **Name/Description** (freeform) > • Upon completion, click **Next** (to Authentication)	

The following fields deserve special mention:

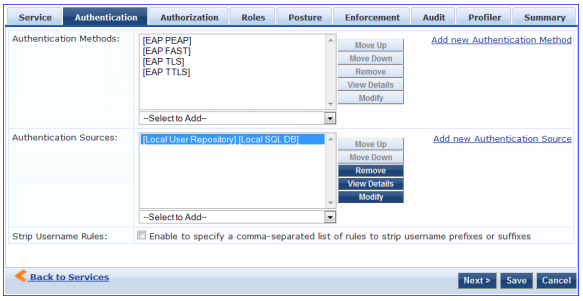
- **Monitor Mode:** Optionally, check here to allow handshakes to occur (for monitoring purposes), but without enforcement.
- **Service Categorization Rule:** For purposes of this Use Case, accept the preconfigured Service Categorization Rules for this Type.

2. Configure Authentication.

   Follow the instructions to select **[EAP FAST]**, one of the pre-configured Policy Manager Authentication Methods, and **Active Directory Authentication Source (AD)**, an external Authentication Source within your existing enterprise.

NOTE: Policy Manager fetches attributes used for role mapping from the Authorization Sources (that are associated with the authentication source). In this example, the authentication and authorization source are one and the same.

Table 2: *Configure Authentication Navigation and Settings*

Navigation	Settings
Select an Authentication Method and an Active Directory server (that you have already configured in Policy Manager): • **Authentication** (tab) > • **Methods** (Select a method from the drop-down list) • **Add** > • **Sources** (**Select** drop-down list): [Local User Repository] [Local SQL DB] [Guest User Repository] [Local SQL DB]	

Navigation	Settings
[Guest Device Repository] [Local SQL DB] [Endpoints Repository] [Local SQL DB] [Onboard Devices Repository] [Local SQL DB] > [Admin User Repository] [Local SQL DB] > AmigoPod AD [Active Directory> • **Add** > • Upon completion, **Next** (to configure Authorization)	

The following field deserves special mention:

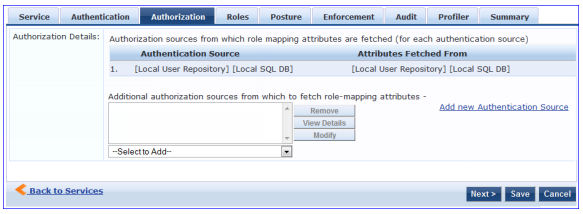
- **Strip Username Rules:** Optionally, check here to pre-process the user name (to remove prefixes and suffixes) before sending it to the authentication source.

NOTE: To view detailed setting information for any preconfigured policy component, select the item and click **View Details**.

3. Configure Authorization.

   Policy Manager fetches attributes for role mapping policy evaluation from the Authorization Sources. In this use case, the Authentication Source and Authorization Source are one and the same.

Table 3: *802.1X - Configure Authorization Navigation and Settings*

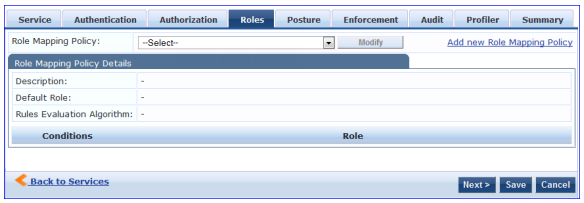
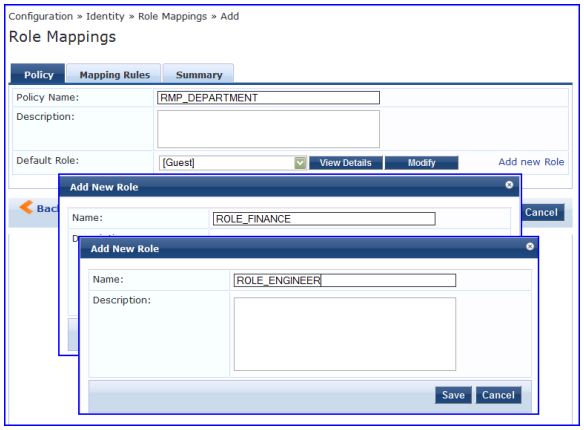
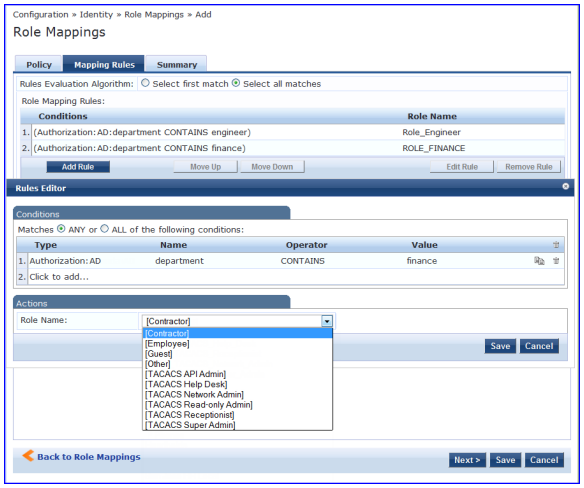
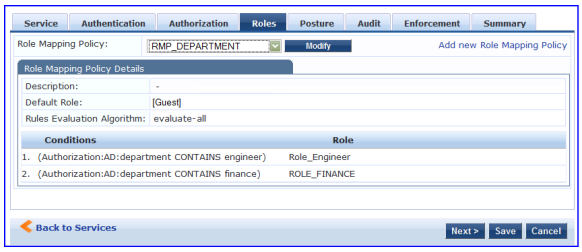
Navigation	Settings
• Configure Service level authorization source. In this use case there is nothing to configure. Click the **Next** button. • Upon completion, click **Next** (to Role Mapping).	

4. Apply a Role Mapping Policy

   Policy Manager tests client identity against role-mapping rules, appending any match (multiple roles acceptable) to the request for use by the Enforcement Policy. In the event of role-mapping failure, Policy Manager assigns a default role.

   In this Use Case, create the role mapping policy RMP_DEPARTMENT that distinguishes clients by department and the corresponding roles ROLE_ENGINEERING and ROLE_FINANCE, to which it maps:

Table 4: *Role Mapping Navigation and Settings*

Navigation	Settings
Create the new Role Mapping Policy: • Roles (tab) > • Add New Role Mapping Policy (link) >	
Add new Roles (names only): • **Policy** (tab) > • **Policy Name** (freeform): ROLE_ENGINEER > • **Save** (button) > • Repeat for ROLE_FINANCE > • When you are finished working in the **Policy** tab, click the **Next** button (in the Rules Editor)	
Create rules to map client identity to a Role: • **Mapping Rules** (tab) > • **Rules Evaluation Algorithm** (radio button): **Select all matches** > • **Add Rule** (button opens popup) > • **Add Rule** (button) > • **Rules Editor** (popup) > • **Conditions/ Actions:** match Conditions to Actions (drop-down list) > • Upon completion of each rule, click the **Save** button (in the Rules Editor) > • When you are finished working in the **Mapping Rules** tab, click the **Save** button (in the Mapping Rules tab)	
Add the new Role Mapping Policy to the Service: • Back in **Roles** (tab) > • **Role Mapping Policy** (selector): *RMP_DEPARTMENT* > • Upon completion, click **Next** (to Posture)	

5. Configure a Posture Server

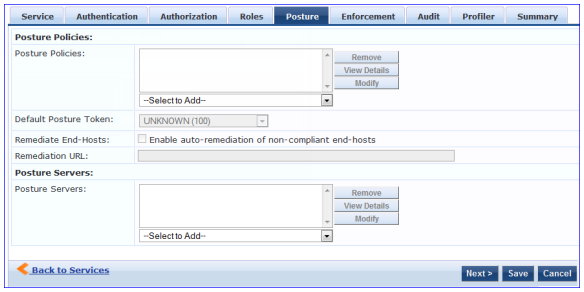
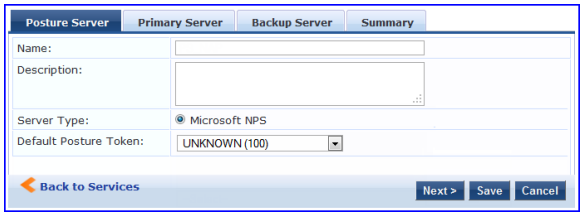
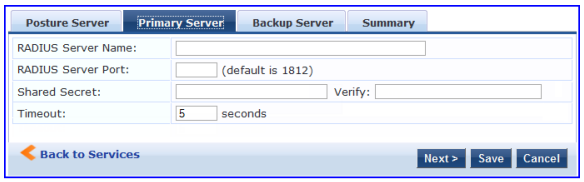
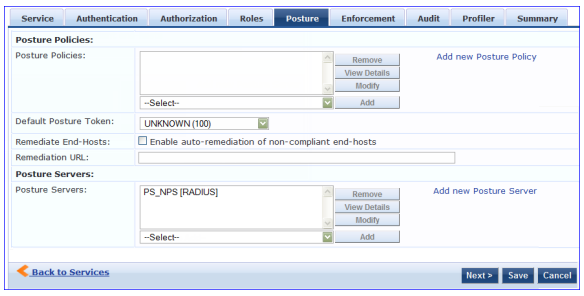
NOTE: For purposes of posture evaluation, you can configure a Posture Policy (internal to Policy Manager), a Posture Server

(external), or an Audit Server (internal or external). Each of the first three use cases demonstrates one of these options; here, the Posture Server

Policy Manager can be configured for a third-party posture server, to evaluate client health based on vendor-specific credentials, typically credentials that cannot be evaluated internally by Policy Manager (that is, not in the form of internal posture policies). Currently, Policy Manager supports the following posture server interface: **Microsoft NPS (RADIUS)**.

Refer to the following table to add the external posture server of type **Microsoft NPS** to the 802.1X service:

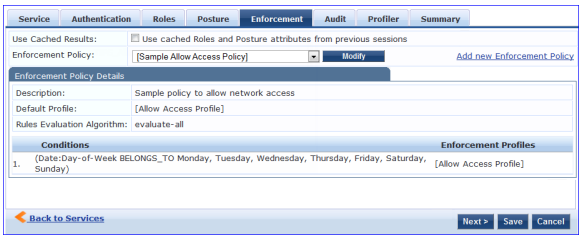
Table 5: *Posture Navigation and Settings*

Navigation	Setting
Add a new Posture Server: • **Posture** (tab) > • **Add new Posture Server** (button) >	
Configure Posture settings: • **Posture Server** (tab) > • **Name** (freeform): **PS_NPS** • **Server Type** (radio button): **Microsoft NPS** • **Default Posture Token** (selector): **UNKOWN** • **Next** (to Primary Server)	
Configure connection settings: • **Primary/ Backup Server** (tabs): Enter connection information for the RADIUS posture server. • **Next** (button): from Primary Server to Backup Server. • To complete your work in these tabs, click the **Save** button.	
Add the new Posture Server to the Service: • Back in the **Posture** (tab) > • **Posture Servers** (selector): **PS_NPS**, then click the **Add** button. • Click the **Next** button.	

6. Assign an Enforcement Policy

   Enforcement Policies contain dictionary-based rules for evaluation of Role, Posture Tokens, and System Time to Evaluation Profiles. Policy Manager applies all matching Enforcement Profiles to the Request. In the case of no match, Policy Manager assigns a default Enforcement Profile.

Table 6: *Enforcement Policy Navigation and Settings*

Navigation	Setting
Configure the Enforcement Policy: • **Enforcement** (tab) > • **Enforcement Policy** (selector): **Role_ Based_Allow_Access_ Policy**	

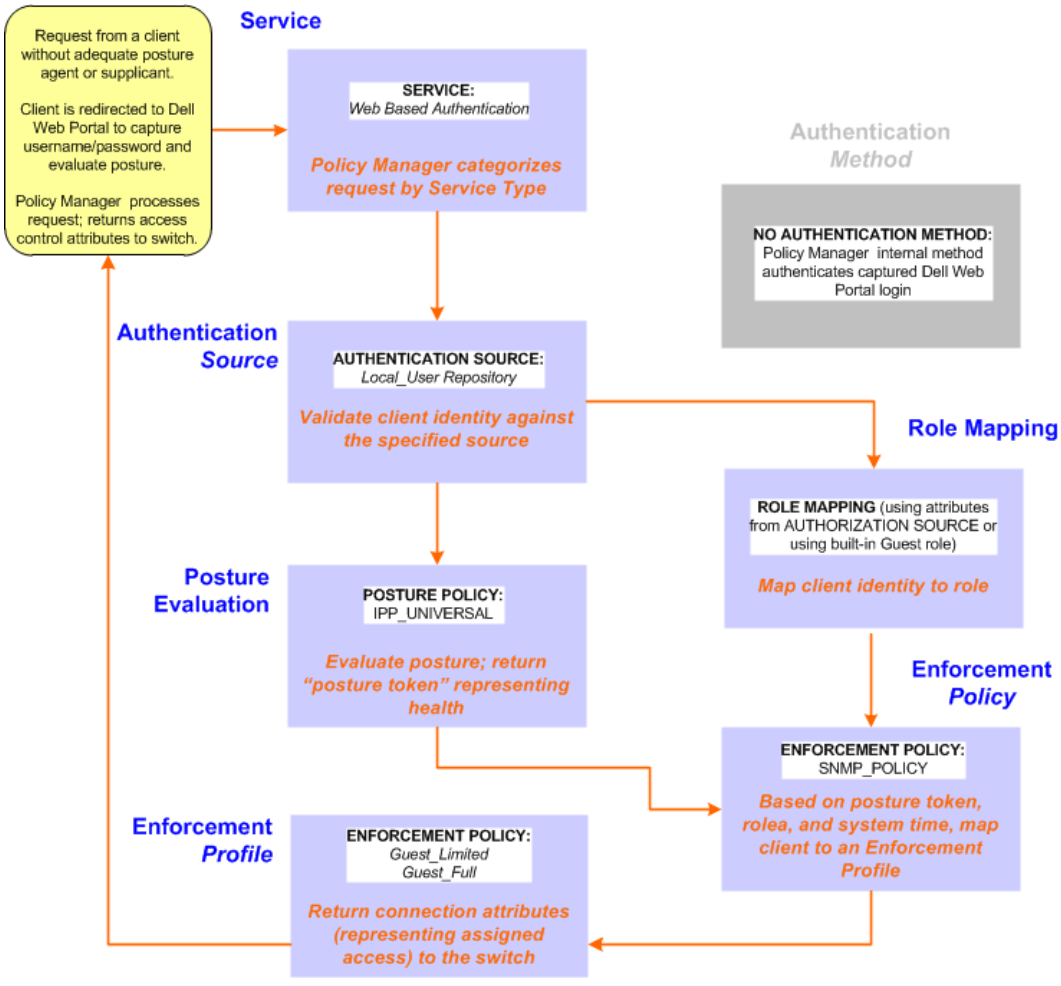
For instructions about how to build such an Enforcement Policy, refer to "Configuring Enforcement Policies" in the *Dell Networking W-ClearPass Policy Manager User Guide*.

7. Save the Service.

   Click **Save**. The Service now appears at the bottom of the **Services** list.

This Service supports known Guests with inadequate 802.1X supplicants or posture agents. The following figure illustrates the overall flow of control for this Policy Manager Service.

Figure 2: *Flow-of-Control of Web-Based Authentication for Guests*



Configuring the Service

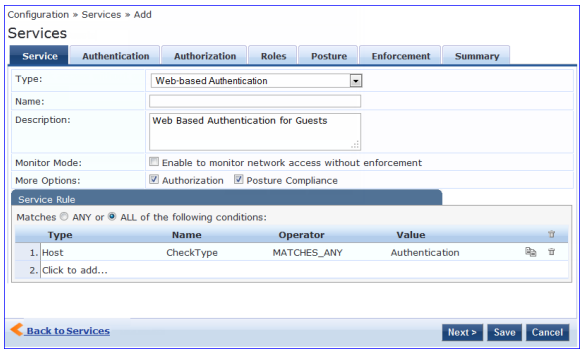
Perform the following steps to configure Policy Manager for WebAuth-based Guest access.

1. Prepare the switch to pre-process WebAuth requests for the Policy Manager *Dell WebAuth* service.

   Refer to your Network Access Device documentation to configure the switch such that it redirects HTTP requests to the *Dell Guest Portal* , which captures username and password and optionally launches an agent that returns posture data.

2. Create a WebAuth-based Service.

Table 7: *Service Navigation and Settings*

Navigation	Settings
Create a new Service: • **Services** > • **Add Service** >	
Name the Service and select a pre-configured Service Type: • **Service** (tab) > • **Type** (selector): Dell Web-Based Authentication > • **Name/Description** (freeform) > • Upon completion, click **Next**.	

3. Set up the Authentication.
   a. Method: The Policy Manager WebAuth service authenticates WebAuth clients internally.
   b. Source: Administrators typically configure Guest Users in the local Policy Manager database.
4. Configure a Posture Policy.

NOTE: For purposes of posture evaluation, you can configure a Posture Policy (internal to Policy Manager), a Posture Server (external), or an Audit Server (internal or external). Each of the first three use cases demonstrates one of these options. This use case demonstrates the Posture Policy.

As of the current version, Policy Manager ships with five pre-configured posture plugins that evaluate the health of the client and return a corresponding posture token.

To add the internal posture policy *IPP_UNIVERSAL_XP*, which (as you will configure it in this Use Case, checks any Windows XP clients to verify the most current Service Pack).

Table 8: *Local Policy Manager Database Navigation and Settings*

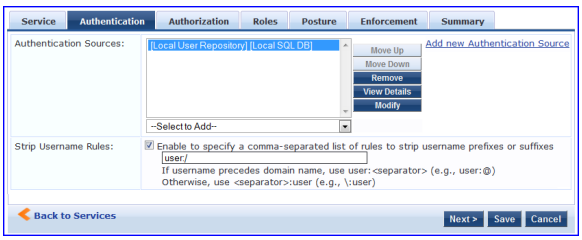
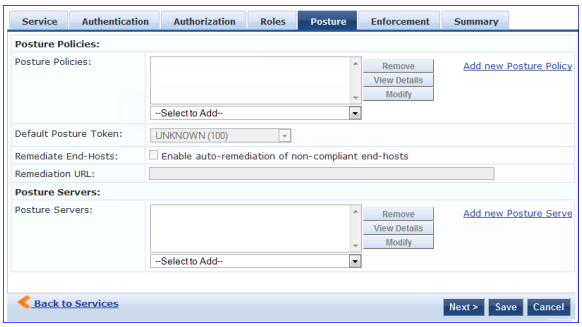
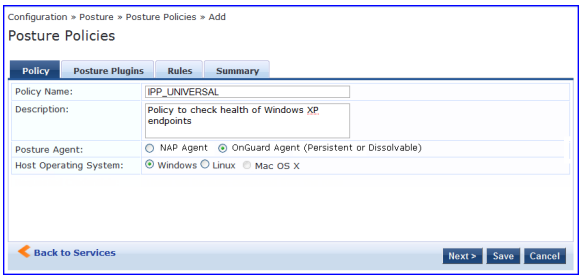
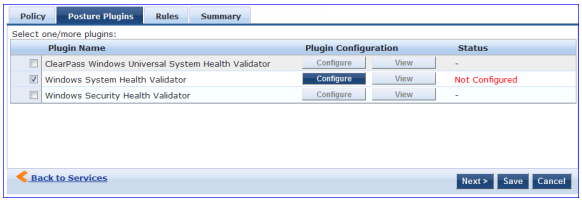
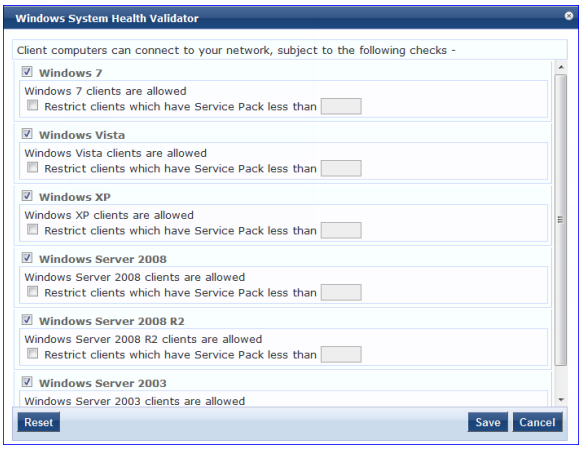
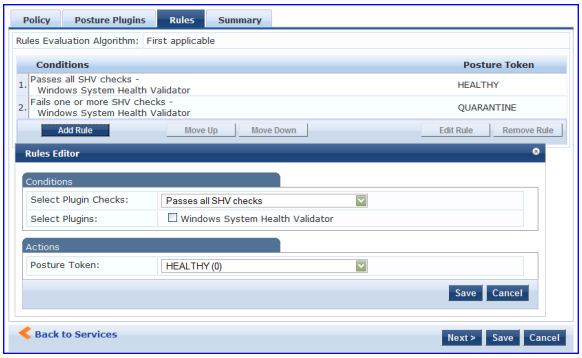
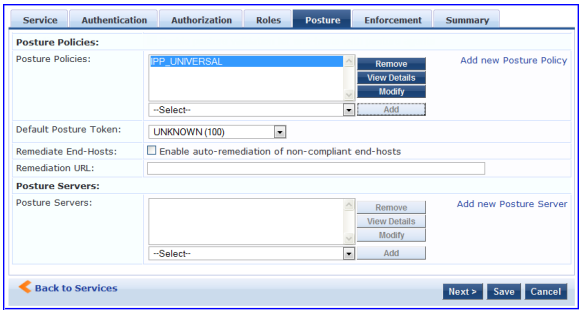
Navigation	Settings
Select the local Policy Manager database: • **Authentication** (tab) > • **Sources** (**Select** drop-down list): **[Local User Repository]** > • **Add** > • **Strip Username Rules** (check box) > • Enter an example of preceding or following separators (if any), with the phrase "user" representing the username to be returned. For authentication, Policy Manager strips the specified separators and any paths or domains beyond them. • Upon completion, click **Next** (until you reach Enforcement Policy).	

Table 9: *Posture Policy Navigation and Settings*

Navigation	Setting
Create a Posture Policy: • **Posture** (tab) > • Enable **Validation Check** (check box) > • **Add new Internal Policy** (link) >	
Name the Posture Policy and specify a general class of operating system: • **Policy** (tab) > • **Policy Name** (freeform): *IPP_UNIVERSAL* > • **Host Operating System** (radio buttons): **Windows** > • When finished working in the **Policy** tab, click **Next** to open the Posture Plugins tab	
Select a Validator: • **Posture Plugins** (tab) > • Enable **Windows Health System Validator** > • **Configure** (button) >	
Configure the Validator: • **Windows System Health Validator** (popup) > • **Enable all Windows operating systems** (check box) > • Enable Service Pack levels for Windows 7, Vista, XP Server 2008, Server 2008 R2, and Server 2003 (check boxes) > • **Save** (button) >	

Navigation	Setting
• When finished working in the **Posture Plugin** tab click **Next** to move to the Rules tab)	
Set rules to correlate validation results with posture tokens: • **Rules** (tab) > • **Add Rule** (button opens popup) > • **Rules Editor** (popup) > • **Conditions/ Actions:** match Conditions (Select Plugin/ Select Plugin checks) to Actions (Posture Token)> • In the **Rules Editor,** upon completion of each rule, click the **Save** button > • When finished working in the **Rules** tab, click the **Next** button.	
Add the new Posture Policy to the Service: Back in **Posture** (tab) > **Internal Policies** (selector): **IPP_ UNIVERSAL_XP**, then click the **Add** button	

The following fields deserve special mention:

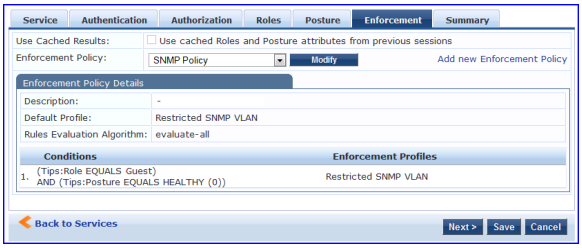
- **Default Posture Token.** Value of the posture token to use if health status is not available.
- **Remediate End-Hosts.** When a client does not pass posture evaluation, redirect to the indicated server for remediation.
- **Remediation URL.** URL of remediation server.

5. Create an Enforcement Policy.

   Because this Use Case assumes the *Guest* role, and the *Dell Web Portal* agent has returned a posture token, it does not require configuration of Role Mapping or Posture Evaluation.

NOTE: The SNMP_POLICY selected in this step provides full guest access to a Role of [Guest] with a Posture of Healthy, and limited guest access.

Table 10: *Enforcement Policy Navigation and Settings*

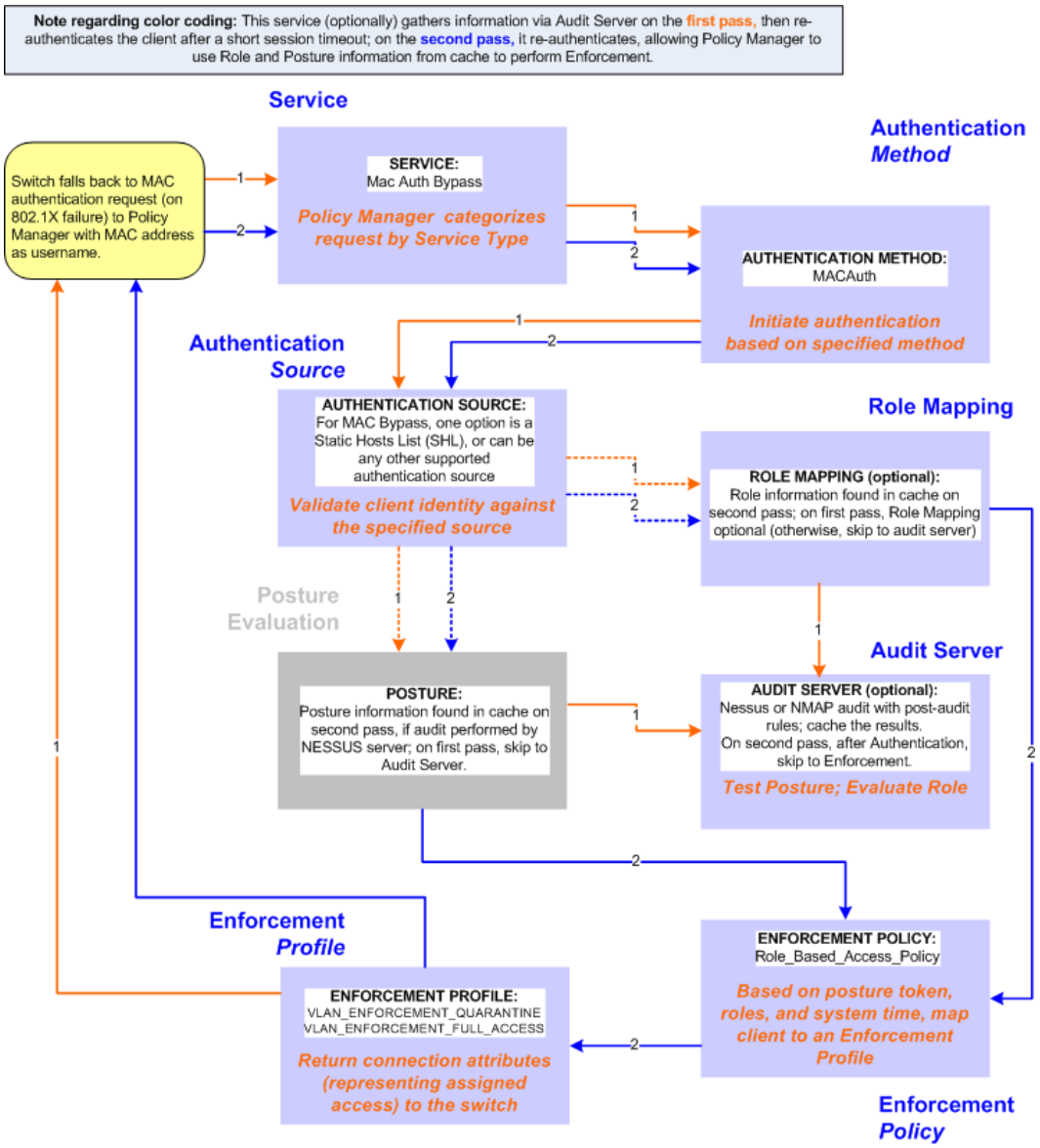
Navigation	Setting
Add a new Enforcement Policy: • **Enforcement** (tab) > • Enforcement Policy (selector): **SNMP_POLICY** • Upon completion, click **Save**.	

6. Save the Service.

   Click **Save**. The Service now appears at the bottom of the **Services** list.

This Service supports *Network Devices*, such as printers or handhelds. The following image illustrates the overall flow of control for this Policy Manager Service. In this service, an audit is initiated on receiving the first MAC Authentication request. A subsequent MAC Authentication request (forcefully triggered after the audit, or triggered after a short session timeout) uses the cached results from the audit to determine posture and role(s) for the device

Figure 3: *Flow-of-Control of MAC Authentication for Network Devices*

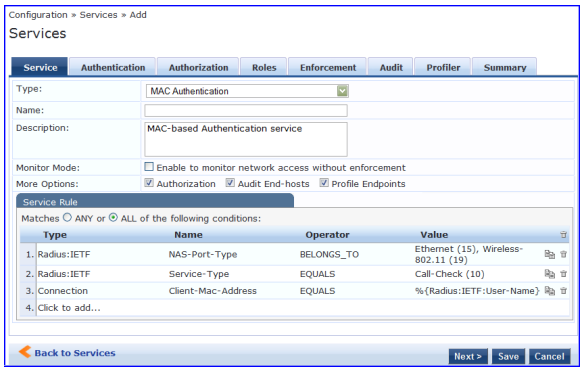


Configuring the Service

Follow these steps to configure Policy Manager for MAC-based Network Device access.

1. Create a MAC Authentication Service.

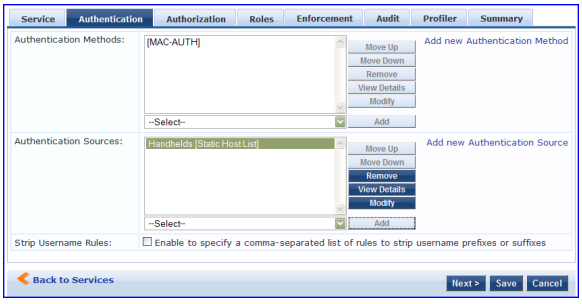
Table 11: *MAC Authentication Service Navigation and Settings*

Navigation	Settings
Create a new Service: • **Services** > • **Add Service** (link) >	
Name the Service and select a pre-configured Service Type: • **Service** (tab) > • **Type** (selector): **MAC Authentication** > • **Name/Description** (freeform) > • Upon completion, click **Next** to configure Authentication	

2. Set up Authentication

   Note that you can select any type of authentication/authorization source for a MAC Authentication service. Only a Static Host list of type MAC Address List or MAC Address Regular Expression shows up in the list of authentication sources (of type Static Host List). Refer to "Adding and Modifying Static Host Lists" in the *Dell Networking W-ClearPass Policy Manager User Guide* for more information. You can also select any other supported type of authentication source.

Table 12: *Authentication Method Navigation and Settings*

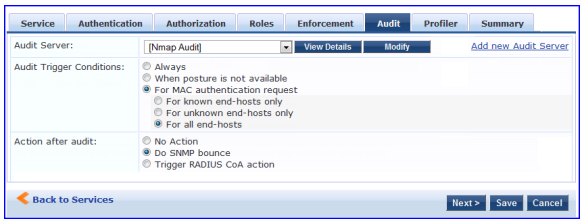
Navigation	Settings
Select an Authentication Method and two authentication sources - one of type Static Host List and the other of type Generic LDAP server (that you have already configured in Policy Manager): • **Authentication** (tab) > • **Methods** (This method is automatically selected for this type of service): **[MAC AUTH]** > • **Add** > • **Sources** (**Select** drop-down list): **Handhelds [Static Host List]** and Policy Manager Clients White List [Generic LDAP] > • **Add** > • Upon completion, **Next** (to Audit)	

3. Configure an Audit Server.

   This step is optional if no Role Mapping Policy is provided, or if you want to establish health or roles using an audit. An audit server determines health by performing a detailed system and health vulnerability analysis

(NESSUS). You can also configure the audit server (NMAP or NESSUS) with post-audit rules that enable Policy Manager to determine client identity.

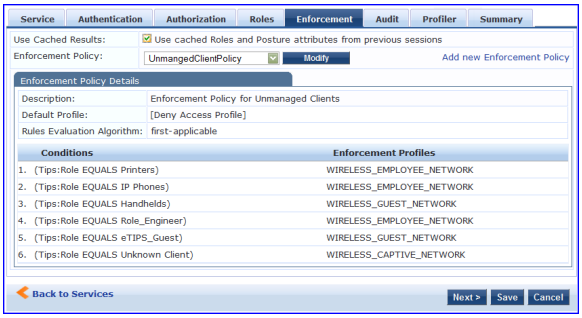
Table 13: *Audit Server Navigation and Settings*

Navigation	Settings
Configure the Audit Server: • **Audit** (tab) > • **Audit End Hosts** (enable) > • **Audit Server** (selector): **NMAP** • **Trigger Conditions** (radio button): **For MAC authentication requests** • **Reauthenticate client** (check box): **Enable**	

Upon completion of the audit, Policy Manager caches Role (NMAP and NESSUS) and Posture (NESSUS), then resets the connection (or the switch reauthenticates after a short session timeout), triggering a new request, which follows the same path until it reaches Role Mapping/Posture/Audit; this appends cached information for this client to the request for passing to Enforcement. Select an Enforcement Policy.

4. Select the Enforcement Policy *Sample_Allow_Access_Policy*:

Table 14: *Enforcement Policy Navigation and Settings*

Navigation	Setting
Select the Enforcement Policy: • **Enforcement** (tab) > • **Use Cached Results** (check box): Select **Use cached Roles and Posture attributes from previous sessions** > • **Enforcement Policy** (selector): UnmanagedClientPolicy • When you are finished with your work in this tab, click **Save**.	

Unlike the 802.1X Service, which uses the same Enforcement Policy (but uses an explicit Role Mapping Policy to assess Role), in this use case Policy Manager applies post-audit rules against attributes captured by the Audit Server to infer Role(s).

5. Save the Service.

   Click **Save.** The Service now appears at the bottom of the **Services** list.