

Dell Networking W-ClearPass Policy Manager



Getting Started Guide

Copyright Information

© 2015 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.

Powering Up and Configuring Policy Manager Hardware	5
Overviews	5
Server Port Overview	5
Initial Server Configuration	5
Before you Begin	5
Initial Setup Procedure	6
Powering Off the System	7
Resetting the Passwords to Factory Default	7
Generating a Support Key for Technical Support	8
A Subset of Useful CLI Commands	9
Accessing Policy Manager	11
Accessing Help	12
Checking Basic Services	13
Use Cases	15
802.1X Wireless Use Case	15
Configuring a Service	16
Creating a New Role Mapping Policy	17
Web Based Authentication Use Case	21
Configuring a Service	21
MAC Authentication Use Case	28
Configuring the Service	28
TACACS+ Use Case	31
Configuring the Service	31
Single Port Use Case	32

Overviews

This *Getting Started 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.

Server Port Overview

The back of the Policy Manager appliance contains three ports.

Figure 1: Policy Manager Backplane



The ports illustrated in the figure above are described in the following table:

Table 1: Device Ports

Key	Port	Description
A	Serial	Initially configures the W-ClearPass Policy Manager appliance using a hardwired terminal.
B - eth0	Management (Gigabit Ethernet)	Provides access for cluster administration and appliance maintenance using the WebUI, CLI, or internal cluster communication. This configuration is mandatory.
C - eth1	Data (Gigabit Ethernet)	Provides a point of contact for RADIUS, TACACS+, web authentication, and other dataplane requests. This configuration is optional. If this port is not configured, requests are redirected to the management port.

Initial Server Configuration

You can start the Initial Setup dialog when you connect a terminal, PC or workstation running a terminal emulation program to the serial port on the W-ClearPass appliance

Before you Begin

Before starting the installation, determine the following information for your network, write it in the table below, and keep it for your records:

Table 2: Required Information

Requirement	Value for Your Installation
Hostname (Policy Manager server)	
Management Port IP Address	
Management Port Subnet Mask	
Management Port Gateway	
Data Port IP Address (optional)	NOTE: The Data Port IP Address must not be in the same subnet as the Management Port IP Address.
Data Port Subnet Mask (optional)	
Data Port Gateway (optional)	
Primary DNS	
Secondary DNS	
NTP Server (optional)	

Initial Setup Procedure

Perform the following steps to set up the Policy Manager appliance:

1. Connect and power on

Connect the serial port on the appliance to a terminal using the null modem cable provided, and power on the appliance. The appliance is now 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. Log in

Use the following preconfigured credentials to log in to the appliance. (You can create a unique appliance/cluster administration password later.)

login: **appadmin**

password: **eTIPS123**

This initiates the Policy Manager Configuration Wizard.

3. Configure the Appliance

Follow the prompts, replacing the placeholder entries in the following illustration with the information you entered in [Table 2](#):

```
Enter hostname: <hostname>
Enter Management Port IP Address: <management port IP>
Enter Management Port Subnet Mask: <management port subnet>
Enter Management Port Gateway: <management port gateway>
Enter Data Port IP Address: <data port IP>
Enter Data Port Subnet Mask: <data port subnet>
Enter Data Port Gateway: <data port gateway>
Enter Primary DNS: <primary DNS>
Enter Secondary DNS: <secondary DNS>
```

4. Change your password

Enter any string with a minimum of six characters. You are prompted to confirm the password. Once this configuration is applied, you must use this new password for cluster administration and management of the appliance.

5. Change the date and time

Follow the prompts to configure the system date and time. To set the date and time by configuring and NTP server, use the primary and secondary NTP server information you entered in [Table 2](#)

6. Commit or restart the configuration

Follow the prompts to apply the configuration, restart the configuration procedure, or quit the setup process.

When the Policy Manager system is up and running, navigate to the **Administration > Agents and Software Updates > Software Updates** page to view and download any available software updates. Refer to in the *User Guide* for more information.

Powering Off the System

To power off the system gracefully without logging in, access the command-line interface through a serial connection to the front serial port, and enter the following commands.

```
login: poweroff
password: poweroff
```

This procedure gracefully shuts down the appliance.

Resetting the Passwords to Factory Default

To reset the administrator password in Policy Manager to factory defaults, you can login to the CLI as the *apprecovery* user. The password to log in as the *apprecovery* user is dynamically generated.

Perform the following steps to generate the recovery password:

1. Connect to the Policy Manager appliance using the front serial port (using any terminal program). See [Initial Server Configuration on page 5](#) for details.
2. Reboot the system using the `restart` command.
3. After the system reboots, the following prompt is displayed for ten seconds:

```
Generate support keys? [y/n]:
```

Enter **y** at the prompt. The system prompts you with the following choices:

```
Please select a support key generation option.
```

- 1) Generate password recovery key
- 2) Generate a support key
- 3) Generate password recovery and support keys

Enter the option or press any key to quit.

4. To generate a password recovery key, select option 1.
5. After the password recovery key is generated, email the key to Dell technical support. A unique password will be generated from the recovery key and emailed back to you.
6. Enter the following command at the command prompt:

```
[apprecovery] app reset-passwd
*****
* WARNING: This command will reset the system account *
*
* passwords to factory default values *
*****
Are you sure you want to continue? [y/n]: y
INFO - Password changed on local node
INFO - System account passwords have been reset to factory default values
```

7. Now you can login with the new administrator password emailed to you by Dell technical support.

Generating a Support Key for Technical Support

To troubleshoot certain critical system level errors, Dell technical support might need to log into a *support shell*. Perform the following steps to generate a dynamic support password:

1. Log into the CLI and enter the following command:

```
system gen-support-key
```

2. Connect to the Policy Manager appliance using the front serial port (using any terminal program). See [Initial Server Configuration on page 5](#) for details.
3. Reboot the system using the `restart` command.
4. When the system restarts, the following prompt appears for 10 seconds:

```
Generate support keys? [y/n]:
```

Enter **y** at the prompt. The system prompts with the following choices:

```
Please select a support key generation option.
1) Generate password recovery key
2) Generate a support key
3) Generate password recovery and support keys
```

Enter the option or press any key to quit.

5. To generate the support key, select option 2. If you want to generate a support key and a password recovery key, select option 3.
6. After the password recovery key is generated, email the key to Dell technical support. A unique password can now be generated by Dell technical support to log into the support shell.

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
* Software Version : 6.4.0.62080
*****
Logged in as group Local Administrator
[appadmin@company.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>	<ul style="list-style-type: none"> Network interface type: <i>mgmt</i> or <i>data</i> 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.

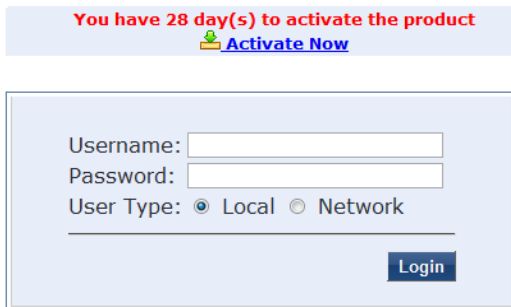
```
ad netjoin <domain-controller.domain-name> [domain NETBIOS name]
```

where:

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

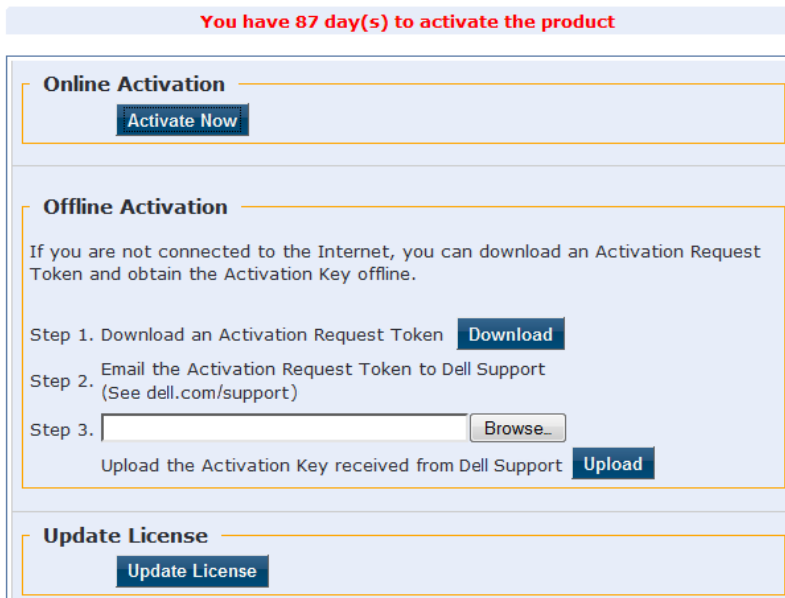
Use *Firefox 3.0* (or higher) or *Internet Explorer 7.0.5* (or higher) to perform the following steps:

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 the **Activate Now** link.



The screenshot shows a warning banner at the top: "You have 28 day(s) to activate the product" with a green person icon and a blue "Activate Now" link. Below this is a login form with fields for "Username:" and "Password:", a "User Type:" section with radio buttons for "Local" (selected) and "Network", and a blue "Login" button.

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.



The screenshot shows a warning banner: "You have 87 day(s) to activate the product". Below are three sections: "Online Activation" with an "Activate Now" button; "Offline Activation" with instructions and buttons for "Download", "Browse...", and "Upload"; and "Update License" with an "Update License" button.

5. Login. Username: admin, Password: eTIPS123

Username:
Password:

[ClearPass Insight](#) | [ClearPass Guest](#) | [ClearPass Onboard](#)

6. Change the password.

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

The screenshot shows the 'Admin Users' management interface. At the top, there is a filter section with 'User ID' selected and a 'contains' search box. Below this is a table with columns for '#', 'User ID', 'Name', and 'Privilege Level'. One user is listed: 'admin' with 'Super Admin' name and 'Super Administrator' privilege level. An 'Edit Admin User' popup is open over the 'admin' user, containing fields for 'User ID' (admin), 'Name' (Super Admin), 'Password' (masked with dots), 'Verify Password' (masked with dots), and 'Privilege Level' (Super Administrator). 'Save' and 'Cancel' buttons are at the bottom of the popup.

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.

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.

System	Services Control	Service Parameters	System Monitoring	Network	FIPS
Service Name	Status	Action			
1. AirGroup notification service	Running	Stop			
2. Async DB write service	Running	Stop			
3. Async network services	Running	Stop			
4. DB change notification server	Running	Stop			
5. DB replication service	Running	Stop			
6. Micros Fidelio FIAS	Running	Stop			
7. Multi-master cache	Running	Stop			
8. Policy server	Running	Stop			
9. Radius server	Running	Stop			
10. System auxiliary services	Running	Stop			
11. System monitor service	Running	Stop			
12. Tacacs server	Running	Stop			
13. Virtual IP service	Stopped	Start			
14. AMG-AD Domain service	Running	Stop			

[Back to Server Configuration](#)

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 **FIPS** tab is used to enable W-ClearPass in Federal Information Processing Standard mode. For most users, this tab should be ignored. Changing the mode to FIPS mode causes the database to be reset.

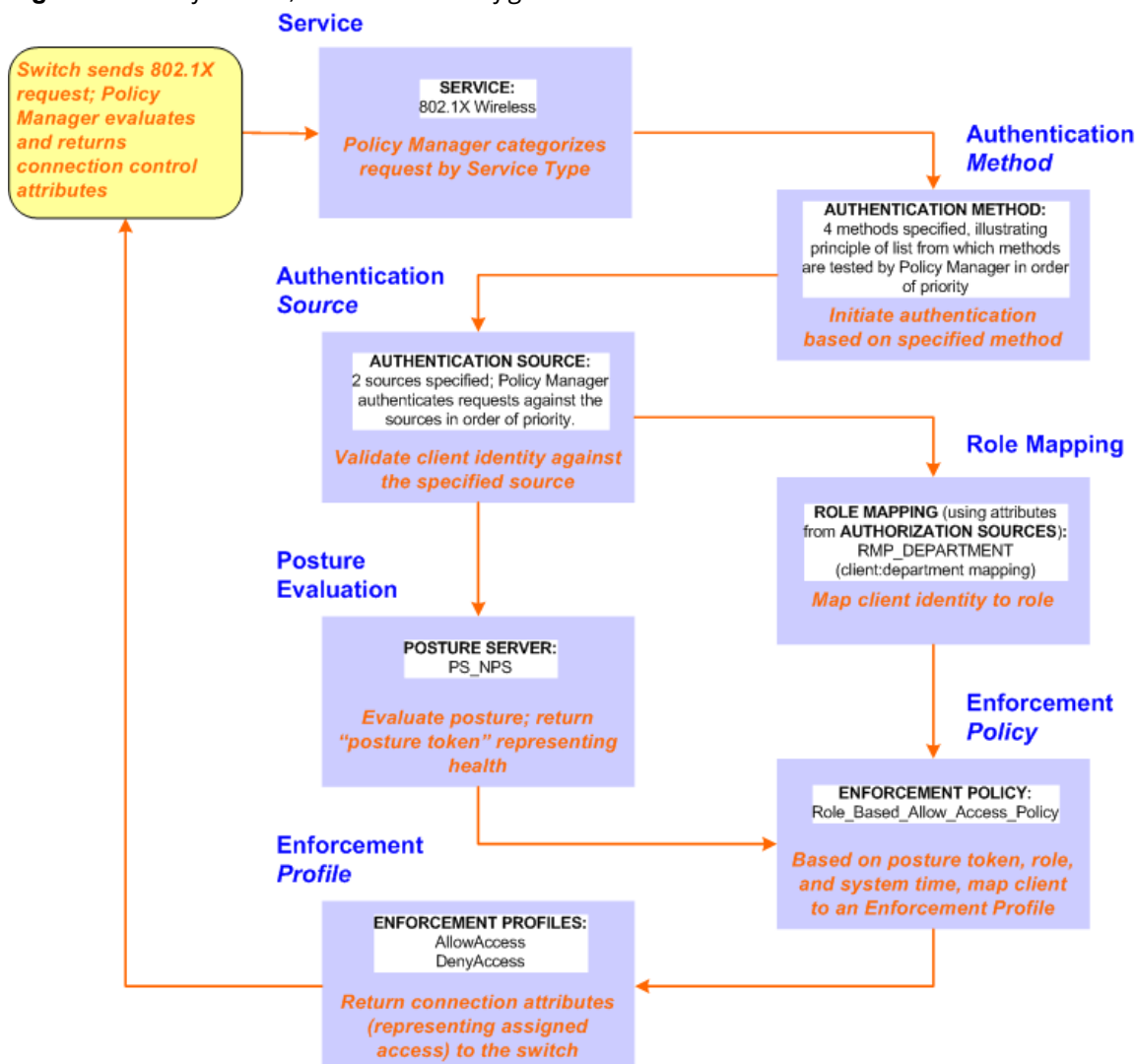
This appendix contains several specific W-ClearPass Policy Manager use cases. Each one explains what it is typically used for, and then describes how to configure Policy Manager for that use case.

- 802.1X Wireless Use Case on page 15
- Web Based Authentication Use Case on page 21
- MAC Authentication Use Case on page 28
- TACACS+ Use Case on page 31
- Single Port Use Case on page 32

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 2: Flow of Control, Basic 802.1X Configuration Use Case



Policy Manager ships with fourteen preconfigured services. In this use case, you select a service that supports 802.1X wireless requests. Follow the steps below to configure this basic 802.1X service that uses **[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.



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.

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. 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.

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)**.



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.

Configuring a Service

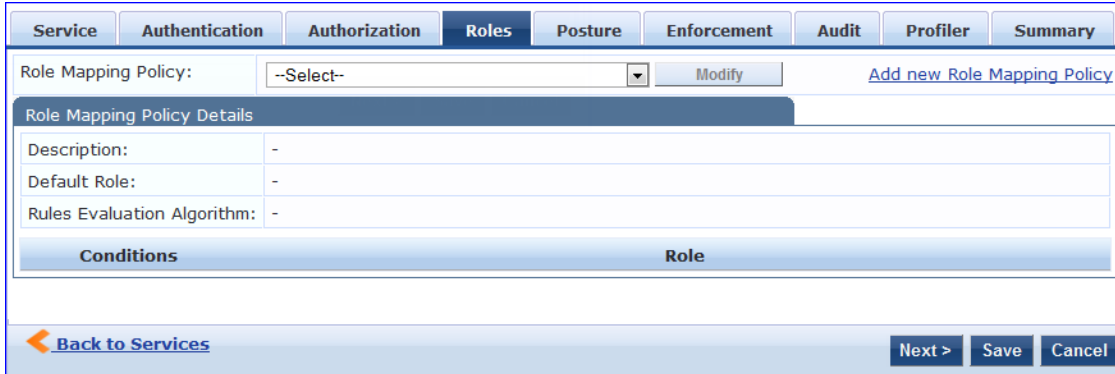
1. Navigate to **Configuration > Services**.
2. Click the **+ Add** icon to add a service. The **Configuration > Services > Add** window opens.
3. If it is not already selected, click the **Service** tab and define basic service information.
 - a. Enter a name for the service in the **Name** field.
 - b. Click the **Type** drop-down list and select **802.1X Wireless**.
 - c. (Optional) click the Monitor Mode checkbox to allow handshakes to occur (for monitoring purposes), but without enforcement.
 - d. Click **Next** to display the **Authentication** tab.
4. Configure authentication.
 - a. In the **Authentication Methods** field, select **[EAP Fast]**.
 - b. In the Authentication Sources field, click the Select to Add drop-down list and select the following sources.
 - [Local User Repository] [Local SQL DB]
 - [Guest User Repository] [Local SQL DB]
 - [Guest Device Repository] [Local SQL DB]
 - [Endpoints Repository] [Local SQL DB]
 - [Onboard Devices Repository] [Local SQL DB]
 - [Admin User Repository] [Local SQL DB]
 - [Active Directory]
 - c. (Optional) Select **Strip Username Rules** to pre-process the user name (to remove prefixes and suffixes) before sending it to the authentication source.

Creating a New Role Mapping Policy

To create a new Role Mapping policy:

1. Click the **Roles** tab.
2. Click **Add new Role Mapping Policy**. The **Role Mappings** page opens.

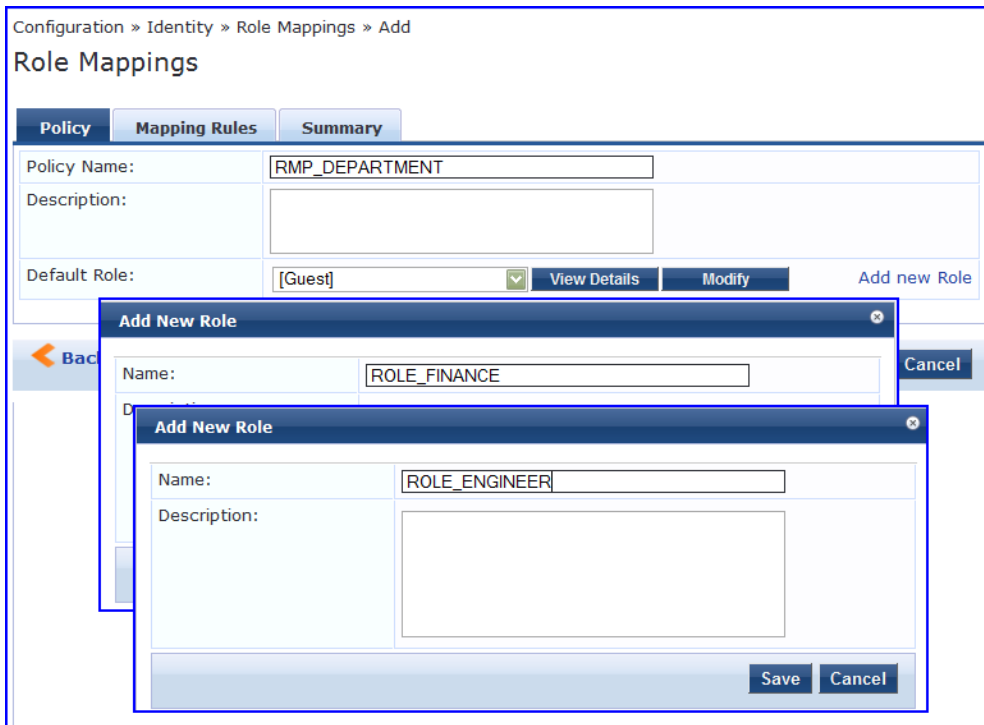
Figure 3: Role Mapping Navigation and Settings



The screenshot shows the 'Roles' tab in a configuration interface. At the top, there are navigation tabs: Service, Authentication, Authorization, Roles (selected), Posture, Enforcement, Audit, Profiler, and Summary. Below the tabs, there is a 'Role Mapping Policy:' dropdown menu set to '--Select--' with a 'Modify' button and a link 'Add new Role Mapping Policy'. A section titled 'Role Mapping Policy Details' contains three fields: 'Description:' with a value of '-', 'Default Role:' with a value of '-', and 'Rules Evaluation Algorithm:' with a value of '-'. Below these fields are two columns labeled 'Conditions' and 'Role'. At the bottom, there is a 'Back to Services' button on the left and 'Next >', 'Save', and 'Cancel' buttons on the right.

3. Add a new role, navigate to the **Policy** tab. Enter the **Policy Name**, For example, ROLE_ENGINEER and click **Save**. Repeat the same step for ROLE_FINANCE. The following figure displays the **Policy** tab:

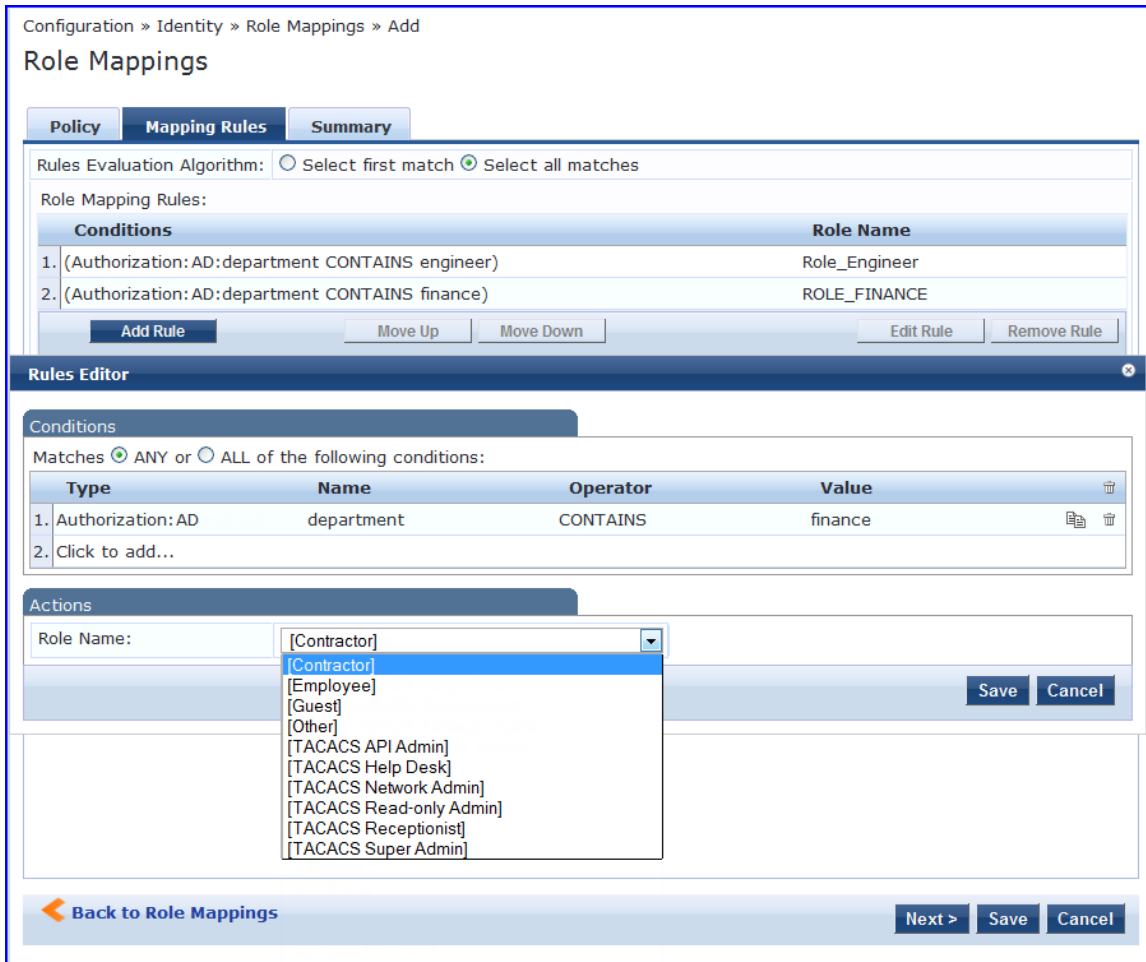
Figure 4: Policy Tab



The screenshot shows the 'Role Mappings' page with the 'Policy' tab selected. The main form has 'Policy Name:' set to 'RMP_DEPARTMENT', 'Description:' (empty), and 'Default Role:' set to '[Guest]'. There are 'View Details' and 'Modify' buttons, and a link 'Add new Role'. Two 'Add New Role' dialog boxes are overlaid on the page. The first dialog has 'Name:' set to 'ROLE_FINANCE' and 'Description:' (empty). The second dialog has 'Name:' set to 'ROLE_ENGINEER' and 'Description:' (empty). Both dialogs have 'Save' and 'Cancel' buttons. The background page also shows a 'Back' button on the left.

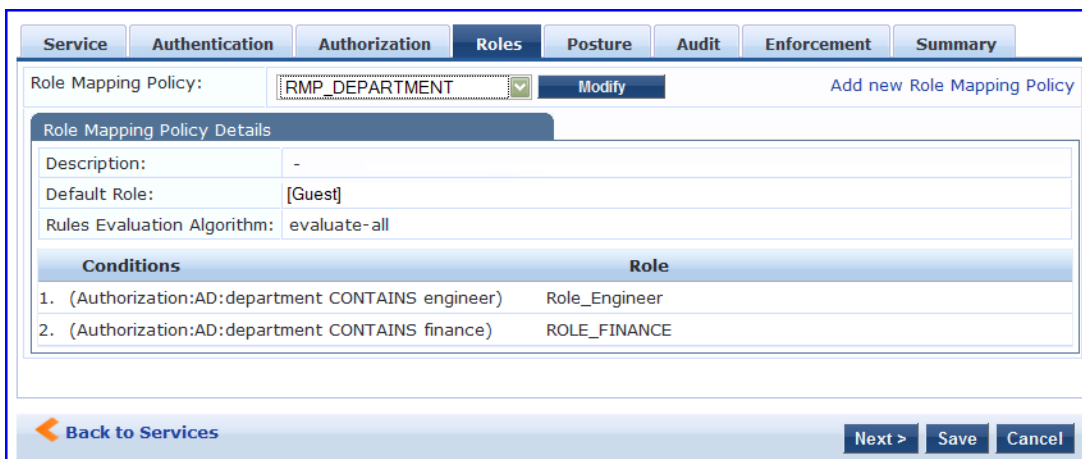
4. Click the **Next** button in the **Rules Editor**.
5. Create rules to map client identity to a role. From the **Mapping Rules** tab, select the **Rules Evaluation Algorithm** radio button. The following figure displays the **Mapping Rules** tab:

Figure 5: Mapping Rules Tab



6. Select the **Select all matches** radio button.
7. Match the conditions with the role name. Click the **Add Rule** button. The **Rules Editor** pop-up opens. Upon completion of each rule, click the **Save** button in the **Rules Editor**.
8. Click the **Save** button.
9. Add the new role mapping policy to the service from the **Roles** tab. The following figure displays the **Roles** tab:

Figure 6: Roles Tab



10. Select **Role Mapping Policy**, for example, RMP_DEPARTMENT. Click **Next**.
11. Add an **Microsoft NPS** external posture server to the 802.1X service. Click the **Posture** tab. The following figure displays the **Posture** tab:

Figure 7: Posture Tab

12. Click **Add new Posture Server** to add a new posture server.
13. Configure the following posture settings examples:
 - **Name** (freeform): **PS_NPS**
 - **Server Type** radio button: **Microsoft NPS**
 - **Default Posture Token** (selector): **UNKOWN**

The following figure displays the **Posture Server** tab:

Figure 8: Posture Server Tab

14. Click **Next**.
15. Configure connection settings in the **Primary/ Backup Server** tabs by entering the connection information for the RADIUS posture server. The following figure displays the **Primary Server** tab:

Figure 9: Primary Server Tab

The screenshot shows the 'Primary Server' configuration tab. It includes the following fields and controls:

- Posture Server** (selected tab), Backup Server, Summary
- RADIUS Server Name:
- RADIUS Server Port: (default is 1812)
- Shared Secret: Verify:
- Timeout: 5 seconds
- Buttons: Back to Services, Next >, Save, Cancel

16. Click **Next** from primary server to backup server. Click **Save**.

17. Add the new posture server to the service. From the **Posture** tab, enter the **Posture Servers**, for example, **PS_NPS**, then click the **Add** button. The following figure displays the **Posture** tab:

Figure 10: Posture Tab

The screenshot shows the 'Posture' configuration tab. It includes the following sections and controls:

- Service, Authentication, Authorization, Roles, **Posture** (selected tab), Enforcement, Audit, Profiler, Summary
- Posture Policies:**
 - Posture Policies: Remove, View Details, Modify, Add
 - Default Posture Token: UNKNOWN (100)
 - Remediate End-Hosts: Enable auto-remediation of non-compliant end-hosts
 - Remediation URL:
- Posture Servers:**
 - Posture Servers: PS_NPS [RADIUS] Remove, View Details, Modify, Add
- Buttons: Back to Services, Next >, Save, Cancel

18. Click the **Next** button. Assign an enforcement policy.

19. 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. The following figure displays the **Enforcement** tab:

Table 3: Enforcement Policy Navigation and Settings

The screenshot shows the 'Enforcement' configuration tab. It includes the following sections and controls:

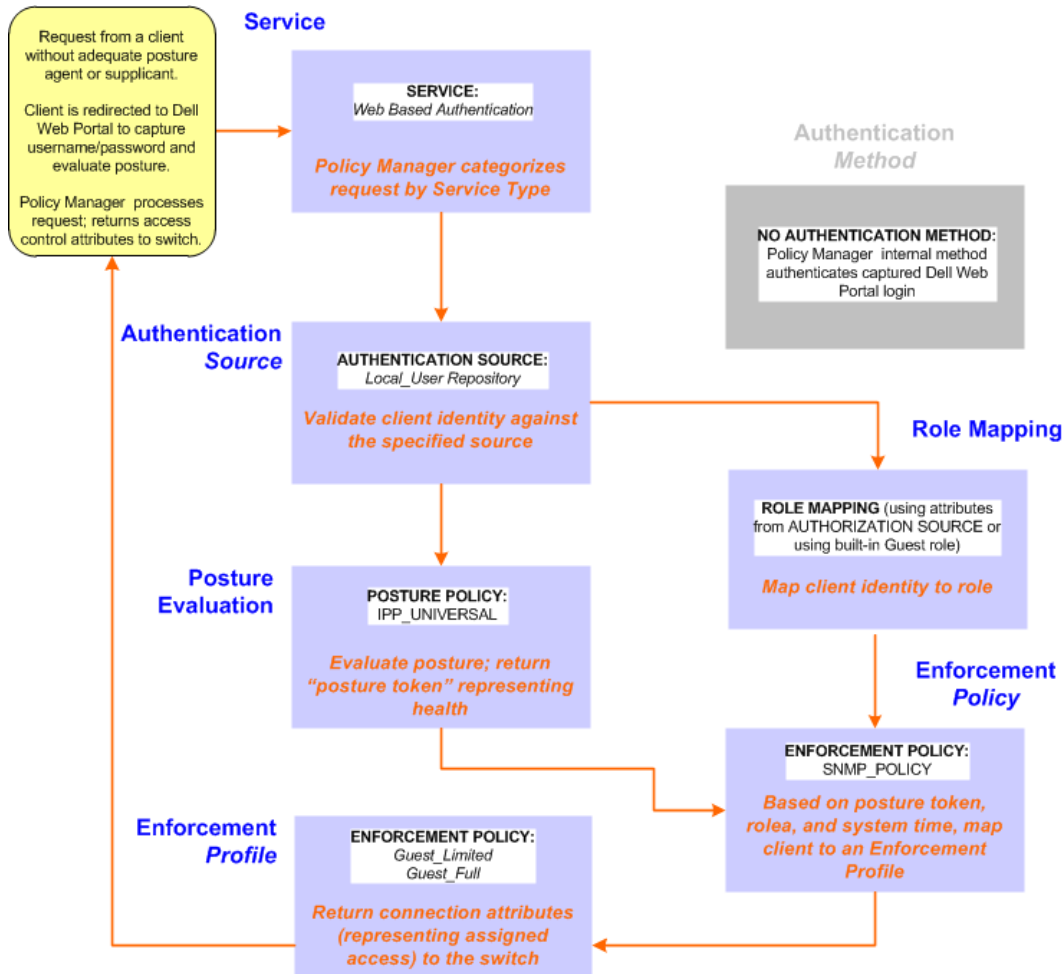
- Service, Authentication, Roles, Posture, **Enforcement** (selected tab), Audit, Profiler, Summary
- Use Cached Results: Use cached Roles and Posture attributes from previous sessions
- Enforcement Policy: [Sample Allow Access Policy] Modify Add new Enforcement Policy
- Enforcement Policy Details**
 - Description: Sample policy to allow network access
 - Default Profile: [Allow Access Profile]
 - Rules Evaluation Algorithm: evaluate-all
- Conditions**
 - 1. (Date:Day-of-Week BELONGS_TO Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday)
- Enforcement Profiles**
 - [Allow Access Profile]
- Buttons: Back to Services, Next >, Save, Cancel

20. From the **Enforcement** tab, select the **Enforcement Policy**, for example, **Role_Based_Allow_Access_Policy**. For instructions about how to build such an enforcement policy, refer to "Configuring Enforcement Policies" in the *W-ClearPass Policy Manager User Guide*.
21. Save the service.

Web Based Authentication Use Case

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 11: Flow-of-Control of Web-Based Authentication for Guests





Configuring a 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 4: Service Navigation and Settings

Navigation	Settings
<p>Create a new Service:</p> <ul style="list-style-type: none"> • Services > • Add Service > 	
<p>Name the Service and select a pre-configured Service Type:</p> <ul style="list-style-type: none"> • 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.



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 5: Local Policy Manager Database Navigation and Settings

Navigation	Settings
<p>Select the local Policy Manager database:</p> <ul style="list-style-type: none"> ● 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 6: Posture Policy Navigation and Settings

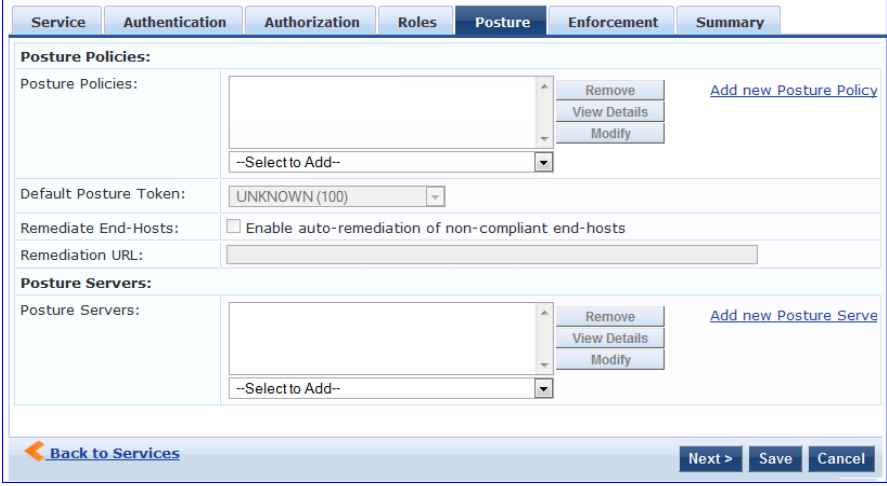
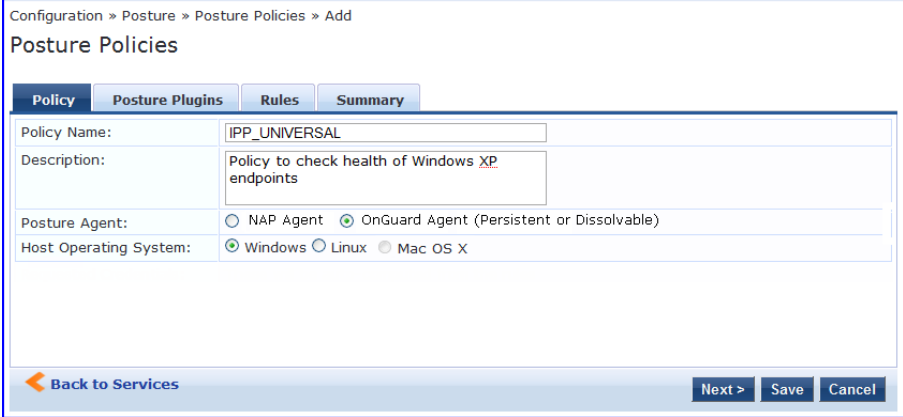
Navigation	Setting
<p>Create a Posture Policy:</p> <ul style="list-style-type: none"> ● Posture (tab) > ● Enable Validation Check (check box) > ● Add new Internal Policy (link) > 	
<p>Name the Posture Policy and specify a general class of operating system:</p> <ul style="list-style-type: none"> ● Policy (tab) > ● Policy Name (freeform): <i>IPP_UNIVERSAL</i> > ● Host Operating System (radio buttons): Windows > ● When finished working in the Policy tab, click Next to open the Posture Plugins tab 	

Table 6: Posture Policy Navigation and Settings (Continued)

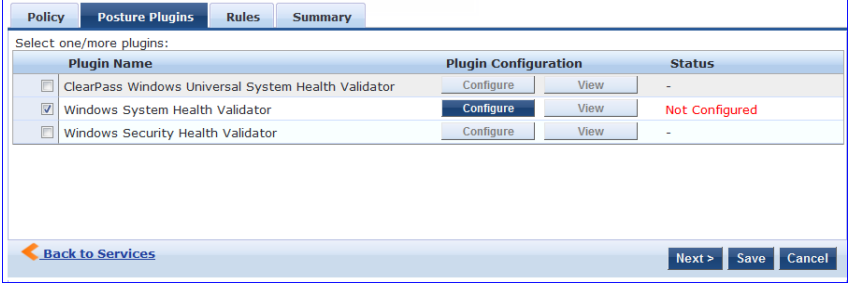
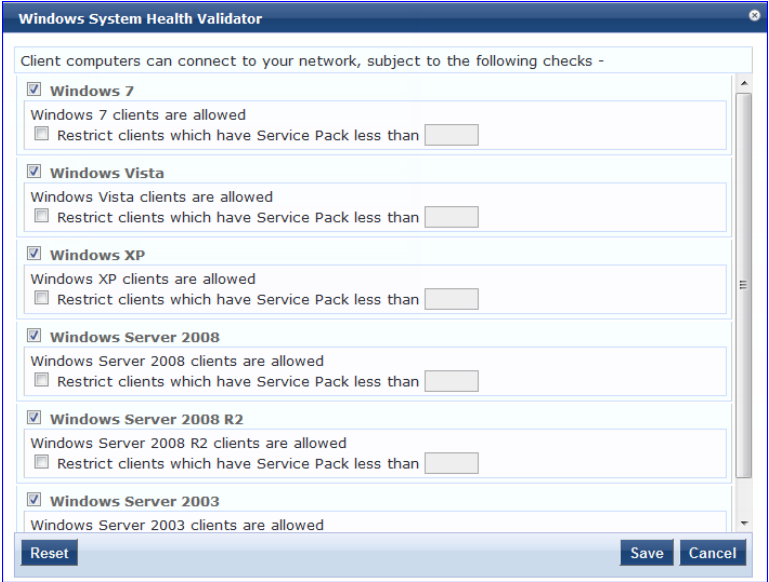
Navigation	Setting
<p>Select a Validator:</p> <ul style="list-style-type: none"> ● Posture Plugins (tab) > ● Enable Windows Health System Validator > ● Configure (button) > 	
<p>Configure the Validator:</p> <ul style="list-style-type: none"> ● Windows System Health Validator (popup) > ● Enable all Windows operating systems (check box) > ● Enable Service Pack levels for Windows 7, Windows Vista®, Windows XP, Windows Server®, 2008, Windows Server 2008 R2, and Windows Server 2003 (check boxes) > ● Save (button) > 	

Table 6: Posture Policy Navigation and Settings (Continued)

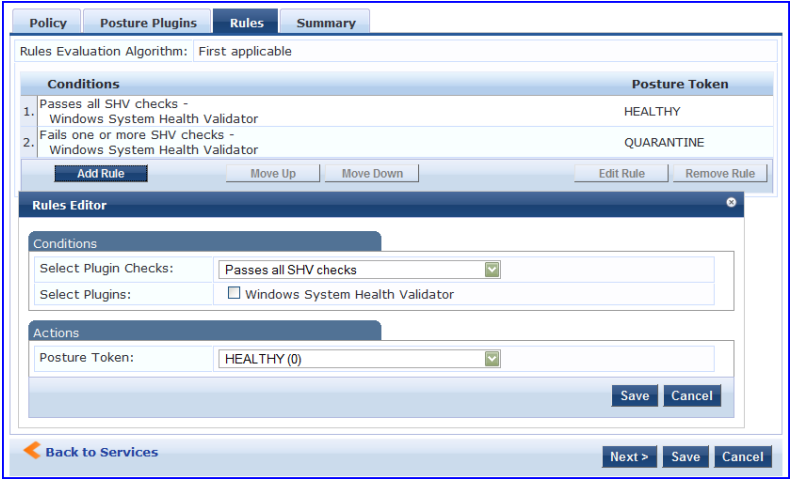
Navigation	Setting						
<ul style="list-style-type: none"> When finished working in the Posture Plugin tab click Next to move to the Rules tab) 							
<p>Set rules to correlate validation results with posture tokens:</p> <ul style="list-style-type: none"> Rules (tab) > Add Rule (button opens popup) > 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. 	 <p>The screenshot displays the 'Rules' tab in the Posture Policy Manager. At the top, there are tabs for 'Policy', 'Posture Plugins', 'Rules', and 'Summary'. Below the tabs, the 'Rules Evaluation Algorithm' is set to 'First applicable'. A table lists two conditions:</p> <table border="1"> <thead> <tr> <th>Conditions</th> <th>Posture Token</th> </tr> </thead> <tbody> <tr> <td>1. Passes all SHV checks - Windows System Health Validator</td> <td>HEALTHY</td> </tr> <tr> <td>2. Fails one or more SHV checks - Windows System Health Validator</td> <td>QUARANTINE</td> </tr> </tbody> </table> <p>Below the table are buttons for 'Add Rule', 'Move Up', 'Move Down', 'Edit Rule', and 'Remove Rule'. A 'Rules Editor' popup is open, showing the configuration for a rule. It has two sections: 'Conditions' and 'Actions'. In the 'Conditions' section, 'Select Plugin Checks' is set to 'Passes all SHV checks' and 'Select Plugins' has a checkbox for 'Windows System Health Validator'. In the 'Actions' section, 'Posture Token' is set to 'HEALTHY (0)'. There are 'Save' and 'Cancel' buttons at the bottom of the popup. At the bottom of the main interface, there are buttons for 'Back to Services', 'Next >', 'Save', and 'Cancel'.</p>	Conditions	Posture Token	1. Passes all SHV checks - Windows System Health Validator	HEALTHY	2. Fails one or more SHV checks - Windows System Health Validator	QUARANTINE
Conditions	Posture Token						
1. Passes all SHV checks - Windows System Health Validator	HEALTHY						
2. Fails one or more SHV checks - Windows System Health Validator	QUARANTINE						

Table 6: Posture Policy Navigation and Settings (Continued)

Navigation	Setting
<p>Add the new Posture Policy to the Service: Back in Posture (tab) > Internal Policies (selector): IPP_UNIVERSAL_XP, then click the Add button</p>	

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.



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 7: Enforcement Policy Navigation and Settings

Navigation	Setting
<p>Add a new Enforcement Policy:</p> <ul style="list-style-type: none"> ● Enforcement (tab) > ● Enforcement Policy (selector): SNMP_POLICY ● Upon completion, click Save. 	

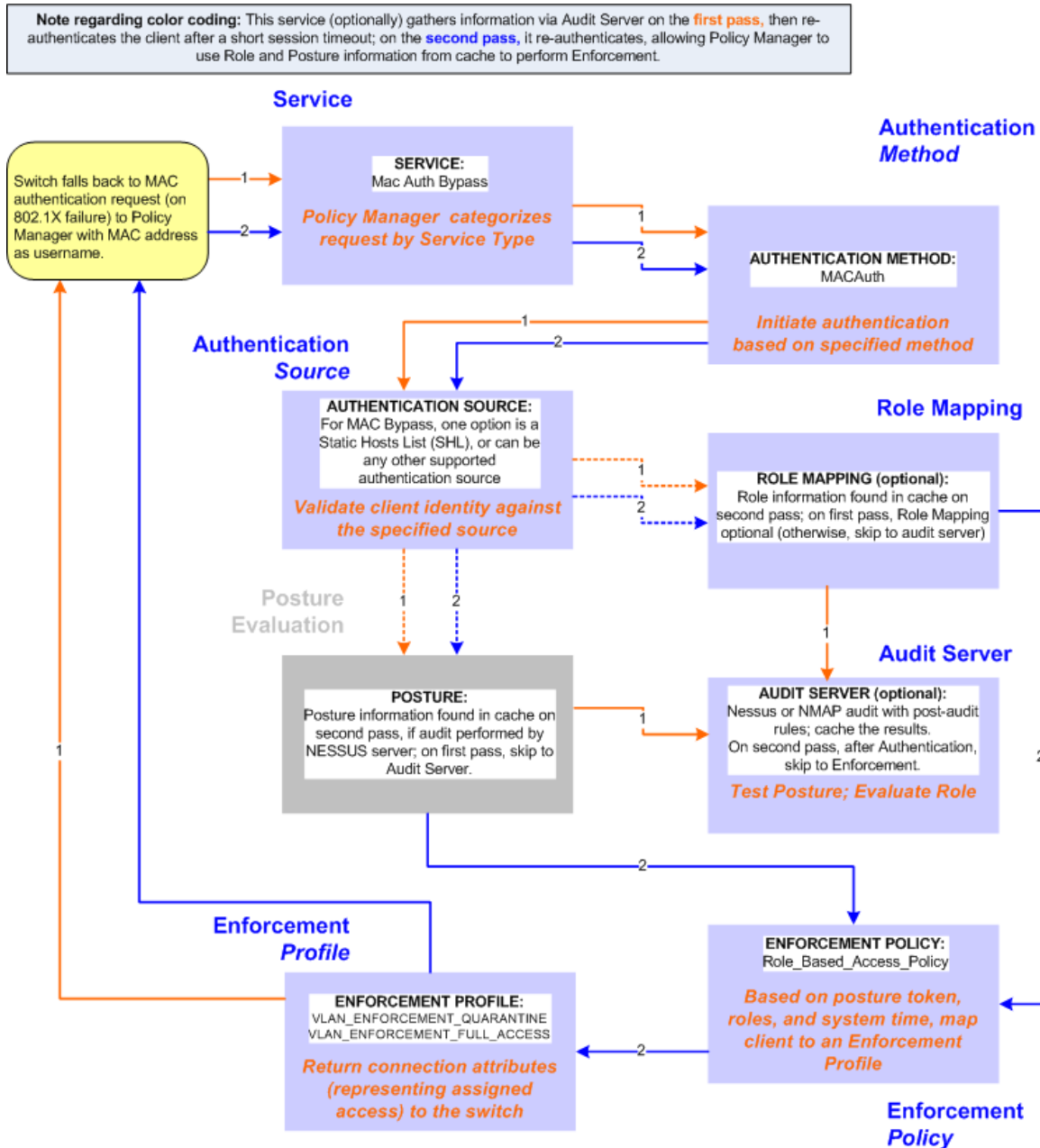
6. Save the Service.

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

MAC Authentication Use Case

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 12: 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 8: MAC Authentication Service Navigation and Settings

Navigation	Settings
<p>Create a new Service:</p> <ul style="list-style-type: none"> • Services > • Add Service (link) > 	
<p>Name the Service and select a pre-configured Service Type:</p> <ul style="list-style-type: none"> • Service (tab) > • Type (selector): MAC Authentication > • Name/Description (freeform) > • Upon completion, click Next to configure Authentication 	

2. Set up Authentication.

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). For more information on static host list, see "Adding and Modifying Static Host Lists" in the *W-ClearPass Policy Manager User Guide*. You can also select any other supported type of authentication source.

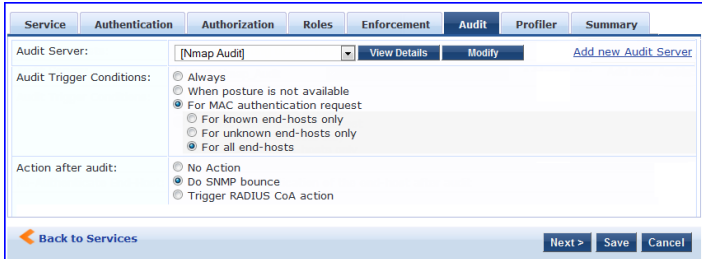
Table 9: Authentication Method Navigation and Settings

Navigation	Settings
<p>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):</p> <ul style="list-style-type: none"> • 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.

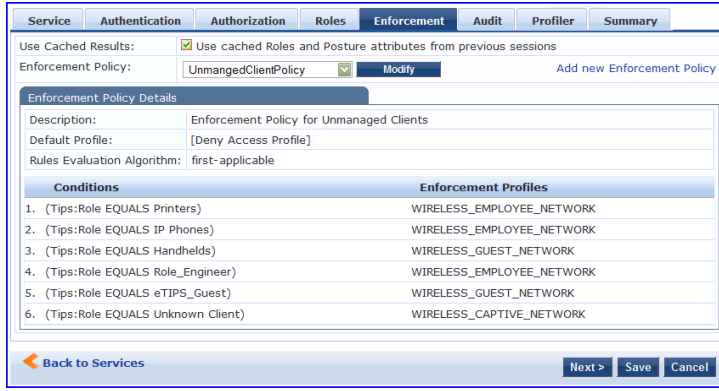
Table 10: Audit Server Navigation and Settings

Navigation	Settings
<p>Configure the Audit Server:</p> <ul style="list-style-type: none"> ● 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 11: Enforcement Policy Navigation and Settings

Navigation	Setting														
<p>Select the Enforcement Policy:</p> <ul style="list-style-type: none"> ● 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. 	 <table border="1" style="margin-top: 10px;"> <thead> <tr> <th>Conditions</th> <th>Enforcement Profiles</th> </tr> </thead> <tbody> <tr> <td>1. (Tips:Role EQUALS Printers)</td> <td>WIRELESS_EMPLOYEE_NETWORK</td> </tr> <tr> <td>2. (Tips:Role EQUALS IP Phones)</td> <td>WIRELESS_EMPLOYEE_NETWORK</td> </tr> <tr> <td>3. (Tips:Role EQUALS Handhelds)</td> <td>WIRELESS_GUEST_NETWORK</td> </tr> <tr> <td>4. (Tips:Role EQUALS Role_Engineer)</td> <td>WIRELESS_EMPLOYEE_NETWORK</td> </tr> <tr> <td>5. (Tips:Role EQUALS eTIPS_Guest)</td> <td>WIRELESS_GUEST_NETWORK</td> </tr> <tr> <td>6. (Tips:Role EQUALS Unknown Client)</td> <td>WIRELESS_CAPTIVE_NETWORK</td> </tr> </tbody> </table>	Conditions	Enforcement Profiles	1. (Tips:Role EQUALS Printers)	WIRELESS_EMPLOYEE_NETWORK	2. (Tips:Role EQUALS IP Phones)	WIRELESS_EMPLOYEE_NETWORK	3. (Tips:Role EQUALS Handhelds)	WIRELESS_GUEST_NETWORK	4. (Tips:Role EQUALS Role_Engineer)	WIRELESS_EMPLOYEE_NETWORK	5. (Tips:Role EQUALS eTIPS_Guest)	WIRELESS_GUEST_NETWORK	6. (Tips:Role EQUALS Unknown Client)	WIRELESS_CAPTIVE_NETWORK
Conditions	Enforcement Profiles														
1. (Tips:Role EQUALS Printers)	WIRELESS_EMPLOYEE_NETWORK														
2. (Tips:Role EQUALS IP Phones)	WIRELESS_EMPLOYEE_NETWORK														
3. (Tips:Role EQUALS Handhelds)	WIRELESS_GUEST_NETWORK														
4. (Tips:Role EQUALS Role_Engineer)	WIRELESS_EMPLOYEE_NETWORK														
5. (Tips:Role EQUALS eTIPS_Guest)	WIRELESS_GUEST_NETWORK														
6. (Tips:Role EQUALS Unknown Client)	WIRELESS_CAPTIVE_NETWORK														

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).

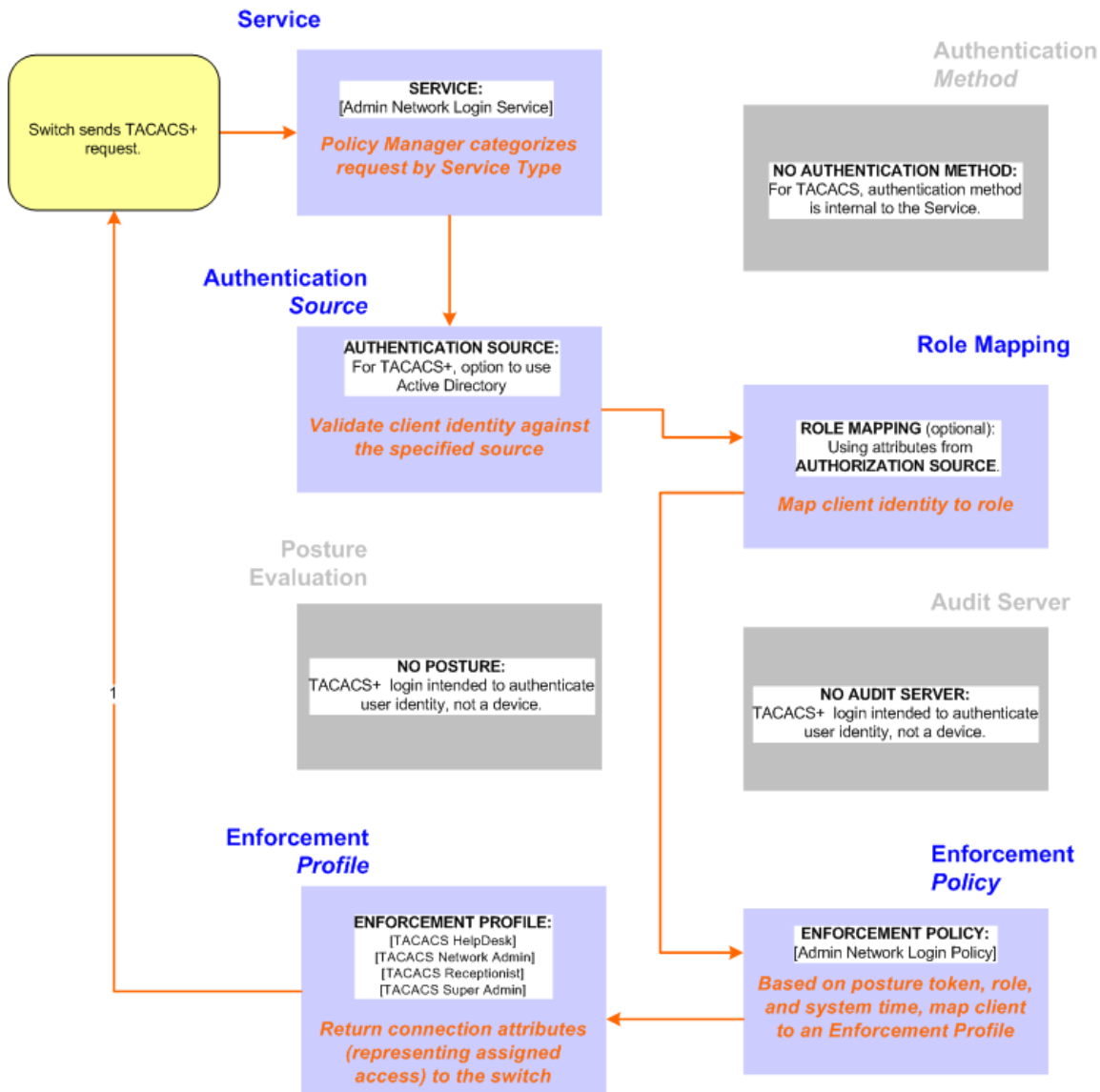
5. Save the Service.

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

TACACS+ Use Case

This Service supports Administrator connections to Network Access Devices via TACACS+. The following image illustrates the overall flow of control for this Policy Manager Service.

Figure 13: Administrator connections to Network Access Devices via TACACS+



Configuring the Service

Perform the following steps to configure Policy Manager for TACACS+-based access:

1. Navigate to **Configuration > Services**.
2. Click the **Add** icon to add a service. The **Configuration > Services > Add** window opens.
3. If it is not already selected, click the **Service** tab and define basic service information.
 - a. Enter a name for the service in the **Name** field.
 - b. Click the **Type** drop-down list and select the preconfigured service type that matches your Policy Manager Admin Network Login Service.
 - c. Click **Next** to display the **Authentication** tab.

4. Define the Authentication settings for the service. Authentication methods can be left to their default values, as the Policy Manager TACACS+ service authenticates TACACS+ requests internally.
 - a. In the **Authentication Sources** section, click the **Select to Add** drop-down list.
 - b. Select **AD (Active Directory)**. For this use case example, Network Access Device authentication data will be stored in the Active Directory.
5. Click the **Enforcement** tab and select an Enforcement Policy.
 - a. Click the Enforcement Policy drop-down list and select the Enforcement Policy **[Admin Network Login Policy]** that distinguishes the two allowed roles (**Net Admin Limited** and **Device SuperAdmin**).
6. Click **Save**. The Service now appears at the bottom of the **Services** list.

Single Port Use Case

This Service supports all three types of connections on a single port.

The following figure illustrates both the overall flow of control for this hybrid service, in which complementary switch and Policy Manager configurations allow all three types of connections on a single port:

Figure 14: Flow of the Multiple Protocol Per Port Case

