Dell Networking W-ClearPass Policy Manager

Getting Started Guide

Copyright Information

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.

Chapter 1
Powering Up and Configuring Policy Manager Hardware

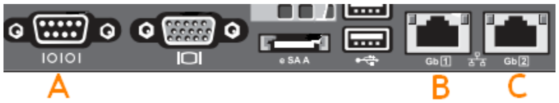
Overview

This *Getting Started Guide* for the Dell Networking W-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 W-ClearPass Policy Manager server requires initial port configuration. The backplane of the Policy Manager contains three ports.

Figure 1: *Policy Manager Backplane*



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

Table 1: *Device Ports*

Key	Port	Description
A	Serial	Configures the W-ClearPass Policy Manager appliance initially using hardwired terminal.
B - eth0	Management (gigabit Ethernet)	Provides access for cluster administration and appliance maintenance using Web access, CLI, or internal cluster communications. Configuration is mandatory.
C - eth1	Data (gigabit Ethernet)	Provides point of contact for RADIUS, TACACS+, Web Authentication, and other data-plane requests. Configuration is optional. If this port is not configured, requests are redirected to the management port.

Server Port Configuration

Before starting the installation, collect the following information that you need, 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	

Table 2: *Required Information (Continued)*

Requirement	Value for Your Installation
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 Gateway (optional)	
Data Port Subnet Mask (optional)	
Primary DNS	
Secondary DNS	
NTP Server (optional)	

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

1. **Connect and power on**

   Connect a serial port on the appliance to a terminal using the null modem cable provided and power on. The appliance is 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**

   You can create a unique appliance/cluster administration password later. For now, use the following preconfigured credentials:

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

   This initiates the Policy Manager Configuration Wizard.

3. **Configure the Appliance**

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

   ```
   Enter hostname: verne.xyzcompany.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 with a minimum of six characters:

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

   From now, you must use this password for cluster administration and management of the appliance.

5. **Change the 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
   ```

   After the timezone information is entered, you are prompted to confirm the selection.

6. **Commit or restart the configuration**

   Follow the prompts:

   ```
   Proceed with the configuration [y[Y]/n[N]/q[Q]
   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.
   ```

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

Perform the following steps to power off the system gracefully without logging in:

Connect to the CLI from the serial console using the front serial port and enter the following:

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

This procedure gracefully shuts down the appliance.

Resetting the Passwords to Factory Default

To reset Administrator passwords 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 "Resetting the Passwords to Factory Default" on page 8 for details.
2. Reboot the system and execute the `restart` command.
3. After the system restarts, 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 the recovery key, select option 1.
5. To generate a support key and a recovery key and support, select option 3.
6. 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.
7. 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
   ```

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 Command Line Interface (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 "Server Port 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. Select 3, if you want to generate a password recovery key as well.
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 : 6.3.0.62080                                                         *
******************************************************************************************
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>	● 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:

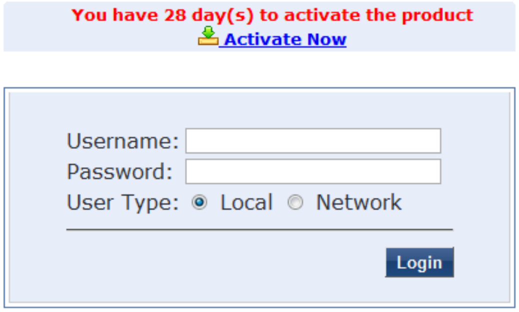
Flag/Parameter	Description
<domain-controller. domain-name>	Required. Host to be joined to the domain.
[domain NETBIOS name]	Optional.

Accessing Policy Manager

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.



You have 28 day(s) to activate the product

Username:

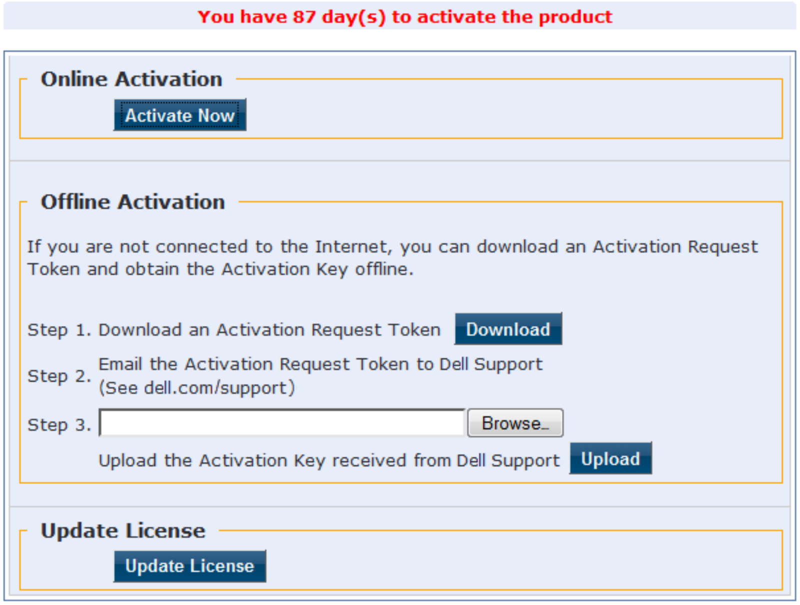
Password:

User Type: ● Local ○ Network

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.



You have 87 day(s) to activate the product

If you are not connected to the Internet, you can download an Activation Request Token and obtain the Activation Key offline.

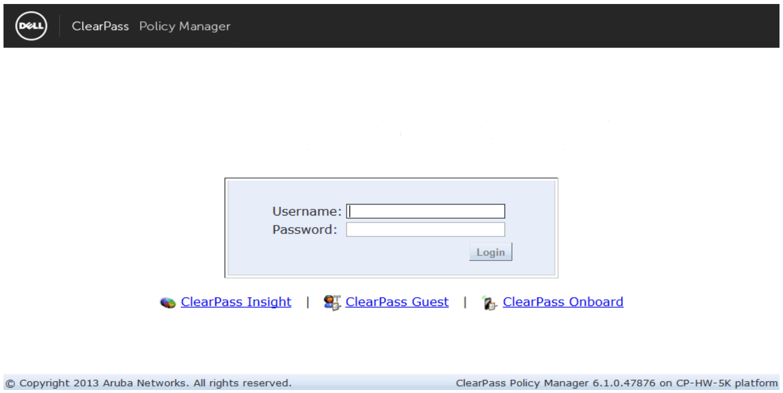
Step 1. Download an Activation Request Token

Step 2. Email the Activation Request Token to Dell Support (See dell.com/support)

Step 3.

Upload the Activation Key received from Dell Support

5. Login. Username: admin, Password: eTIPS123



ClearPass Policy Manager

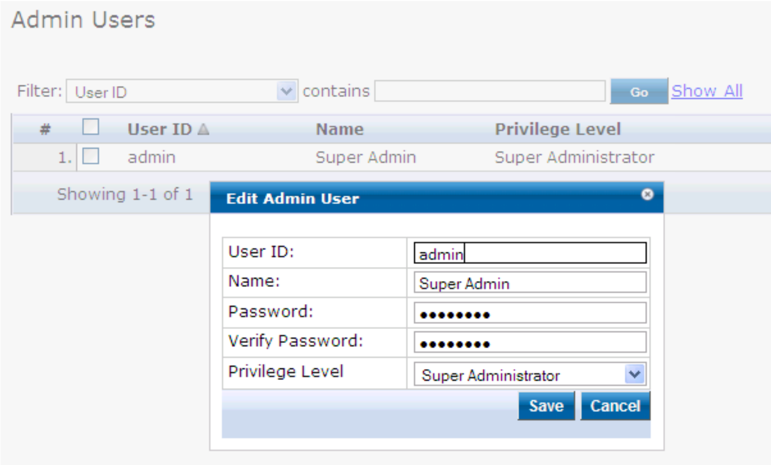
Username:
Password:
Login

ClearPass Insight | ClearPass Guest | ClearPass Onboard

© Copyright 2013 Aruba Networks. All rights reserved. ClearPass Policy Manager 6.1.0.47876 on CP-HW-5K platform

6. Change the password.

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



Admin Users

Filter: User ID contains Go Show All

#	□	User ID	Name	Privilege Level
1.	□	admin	Super Admin	Super Administrator

Showing 1-1 of 1

Edit Admin User

User ID:	admin
Name:	Super Admin
Password:	••••••••
Verify Password:	••••••••
Privilege Level	Super Administrator

Save Cancel

Accessing Help

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

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

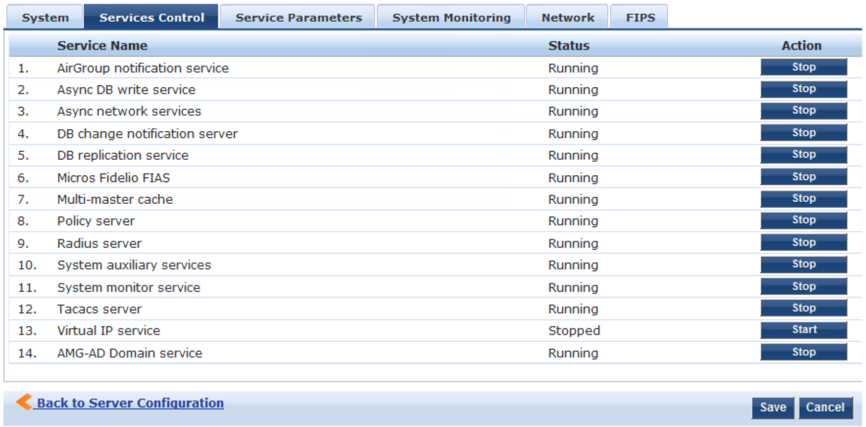
(where `<hostname>` is the hostname you configured during the initial configuration.)

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.



	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

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
```

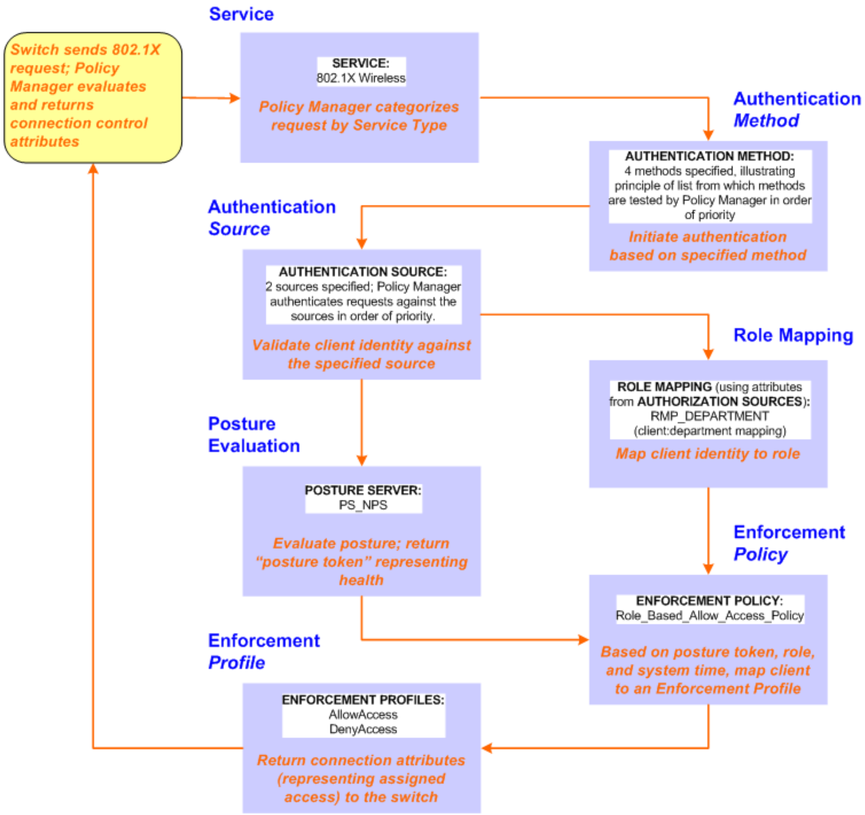
- The **Service Parameters** tab allows you to change system parameters for all services.
- The **System Monitoring** tab allows you to configure SNMP parameters, ensuring that external MIB browsers can browse the system-level MIB objects exposed by the Policy Manager appliance.
- The **Network** tab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

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*


Service
Switch sends 802.1X request; Policy Manager evaluates and returns connection control attributes
SERVICE:
802.1X Wireless
Policy Manager categorizes request by Service Type
Authentication Method
AUTHENTICATION METHOD:
4 methods specified, illustrating principle of list from which methods are tested by Policy Manager in order of priority
Initiate authentication based on specified method
Authentication Source
AUTHENTICATION SOURCE:
2 sources specified; Policy Manager authenticates requests against the sources in order of priority.
Validate client identity against the specified source
Role Mapping
ROLE MAPPING (using attributes from AUTHORIZATION SOURCES):
RMP_DEPARTMENT
(client:department mapping)
Map client identity to role
Posture Evaluation
POSTURE SERVER:
PS_NPS
Evaluate posture; return "posture token" representing health
Enforcement Policy
ENFORCEMENT POLICY:
Role_Based_Allow_Access_Policy
Based on posture token, role, and system time, map client to an Enforcement Profile
Enforcement Profile
ENFORCEMENT PROFILES:
AllowAccess
DenyAccess
Return connection attributes (representing assigned access) to the switch

Configuring the Service

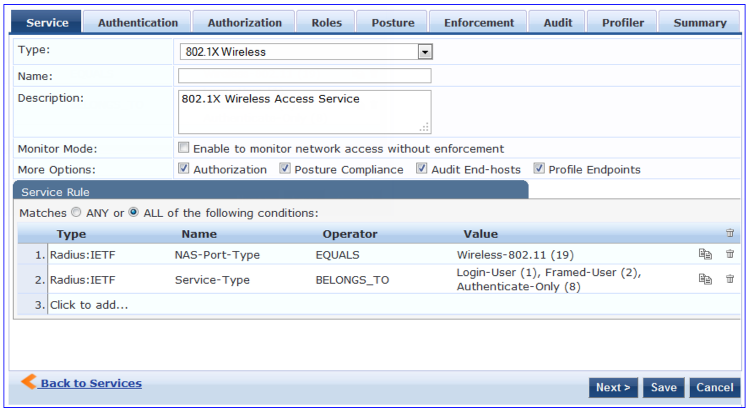
Follow the steps below to configure this basic 802.1X service:

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 3: *802.1X - Create Service Navigation and Settings*

Navigation	Settings
Create a new Service: • **Services** > • **Add Service** (link) >	 Configuration » Services Services Add Import Export All
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)	 Service | Authentication | Authorization | Roles | Posture | Enforcement | Audit | Profiler | Summary Type: 802.1X Wireless Name: Description: 802.1X Wireless Access Service Monitor Mode: □ Enable to monitor network access without enforcement More Options: ☑ Authorization ☑ Posture Compliance ☑ Audit End-hosts ☑ Profile Endpoints Service Rule Matches ○ ANY or ● ALL of the following conditions: Type | Name | Operator | Value 1. Radius:IETF | NAS-Port-Type | EQUALS | Wireless-802.11 (19) 2. Radius:IETF | Service-Type | BELONGS_TO | Login-User (1), Framed-User (2), Authenticate-Only (8) 3. Click to add... Back to Services Next > | Save | Cancel

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.

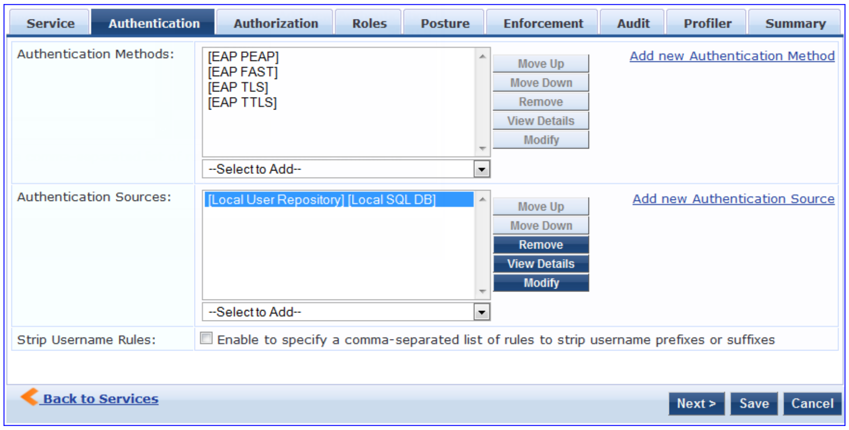
2. Configure Authentication.

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 4: *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] [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)	 Service Authentication Authorization Roles Posture Enforcement Audit Profiler Summary Move Up Move Down Remove View Details Modify Add new Authentication Method Add new Authentication Source Back to Services Next > Save Cancel Authentication Methods: [EAP PEAP] [EAP FAST] [EAP TLS] [EAP TTLS] --Select to Add-- Authentication Sources: [Local User Repository] [Local SQL DB] --Select to Add-- Strip Username Rules: ☐ Enable to specify a comma-separated list of rules to strip username prefixes or suffixes

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.

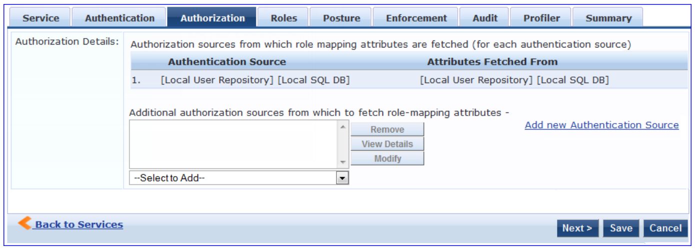
NOTE

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 5: *02.1X - 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).	 Authorization Details: Authorization sources from which role mapping attributes are fetched (for each authentication source) Authentication Source: 1. [Local User Repository] [Local SQL DB] — Attributes Fetched From: [Local User Repository] [Local SQL DB] Additional authorization sources from which to fetch role-mapping attributes - --Select to Add--

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 6: *Role Mapping Navigation and Settings*

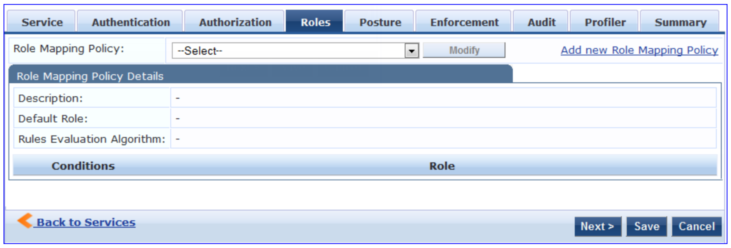
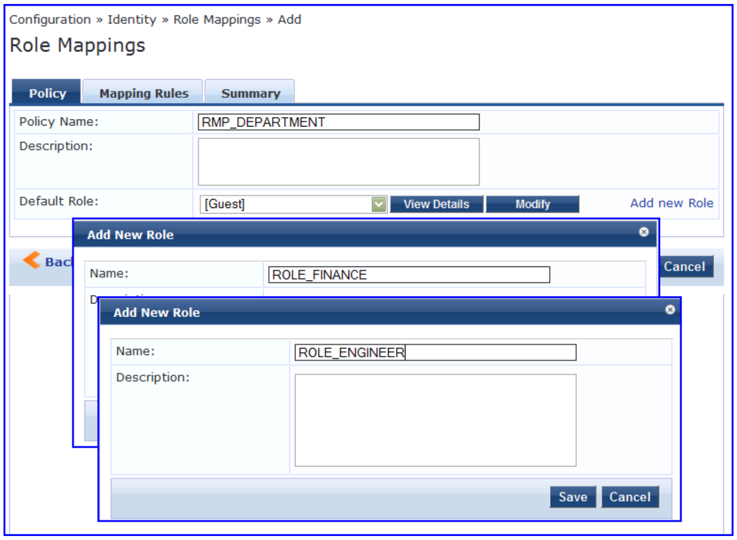
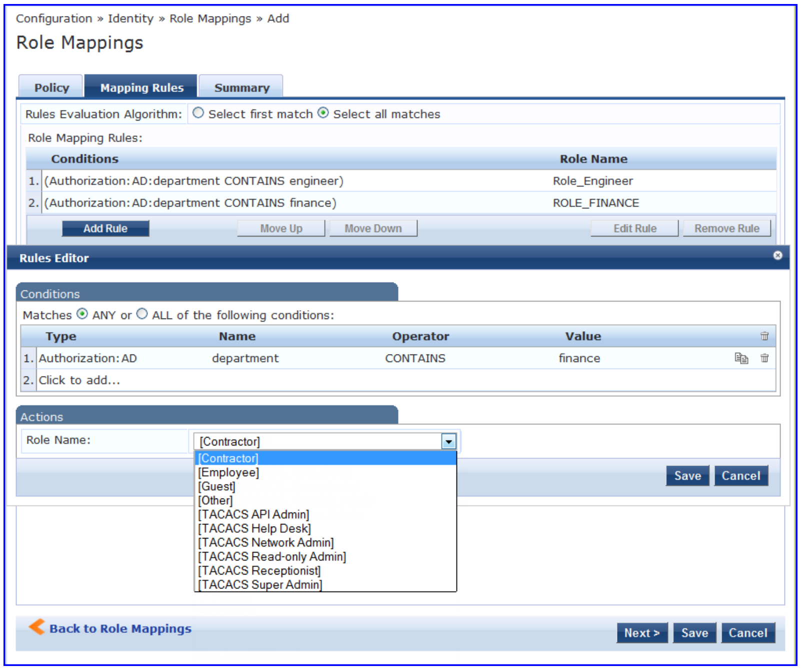
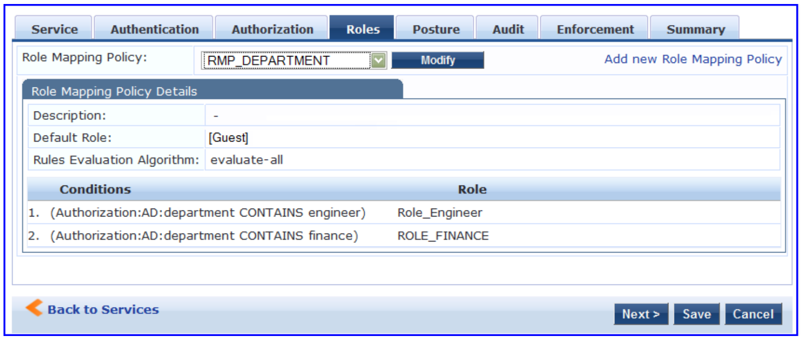
Navigation	Settings
Create the new Role Mapping Policy: - Roles (tab) > - Add New Role Mapping Policy (link) >	 Role Mapping Policy: --Select-- Role Mapping Policy Details Description: - Default Role: - Rules Evaluation Algorithm: -
Add new Roles (names only): - **Policy** (tab) > - **Policy Name** (freeform): 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)	 Configuration » Identity » Role Mappings » Add Role Mappings Policy Name: RMP_DEPARTMENT Description: Default Role: [Guest] Add New Role Name: ROLE_FINANCE Add New Role Name: ROLE_ENGINEER Description:

Table 6: *Role Mapping Navigation and Settings (Continued)*

Navigation	Settings
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)	 Configuration » Identity » Role Mappings » Add Role Mappings Policy Mapping Rules Summary Rules Evaluation Algorithm: ○ Select first match ● Select all matches Role Mapping Rules: Conditions — Role Name 1. (Authorization:AD:department CONTAINS engineer) — Role_Engineer 2. (Authorization:AD:department CONTAINS finance) — ROLE_FINANCE Add Rule Move Up Move Down Edit Rule Remove Rule Rules Editor Conditions Matches ● ANY or ○ ALL of the following conditions: Type — Name — Operator — Value 1. Authorization:AD — department — CONTAINS — finance 2. Click to add... Actions Role Name: [Contractor] [Contractor] [Employee] [Guest] [Other] [TACACS API Admin] [TACACS Help Desk] [TACACS Network Admin] [TACACS Read-only Admin] [TACACS Receptionist] [TACACS Super Admin] Save Cancel Back to Role Mappings Next > Save Cancel
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)	 Service Authentication Authorization Roles Posture Audit Enforcement Summary Role Mapping Policy: RMP_DEPARTMENT Modify Add new Role Mapping Policy Role Mapping Policy Details Description: - Default Role: [Guest] Rules Evaluation Algorithm: evaluate-all Conditions — Role 1. (Authorization:AD:department CONTAINS engineer) — Role_Engineer 2. (Authorization:AD:department CONTAINS finance) — ROLE_FINANCE Back to Services Next > Save Cancel

5. Configure a Posture Server.

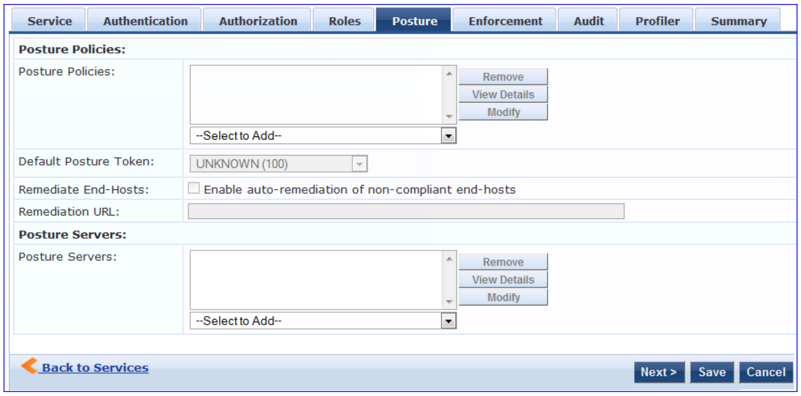
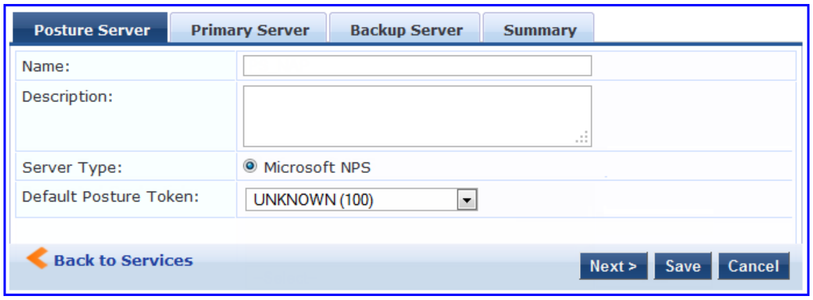
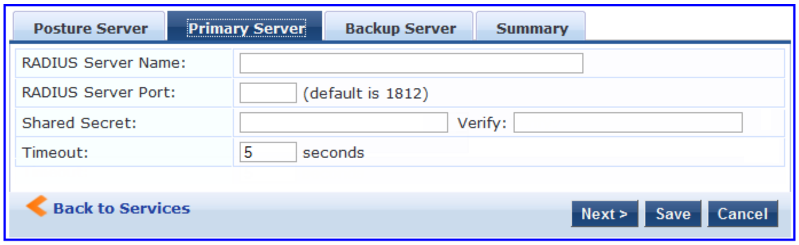
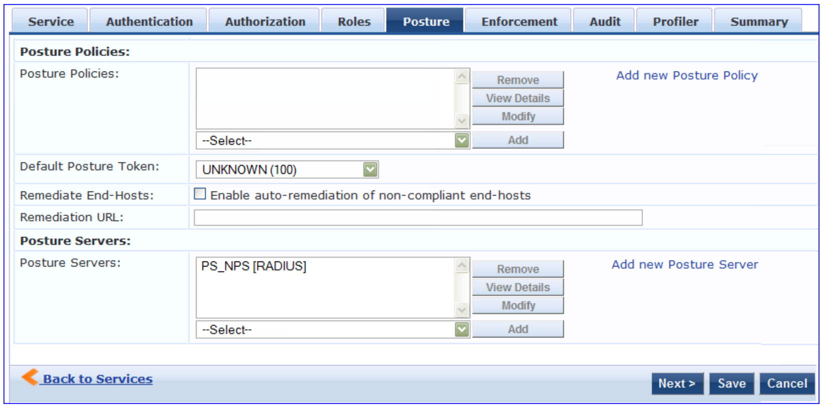
NOTE

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 **Micrsoft NPS** to the 802.1X service:

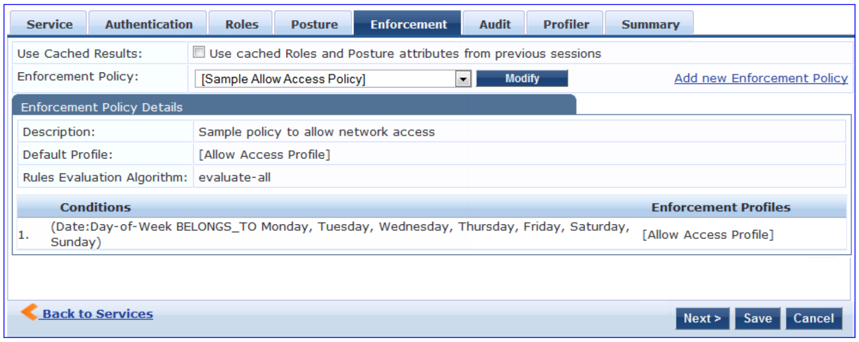
Table 7: *Posture Navigation and Settings*

Navigation	Setting
Add a new Posture Server: - **Posture** (tab) > - **Add new Posture Server** (button) >	 Service Authentication Authorization Roles Posture Enforcement Audit Profiler Summary Remove View Details Modify Back to Services Next > Save Cancel Posture Policies: Posture Policies: --Select to Add-- Default Posture Token: UNKNOWN (100) Remediate End-Hosts: □ Enable auto-remediation of non-compliant end-hosts Remediation URL: Posture Servers: Posture Servers: --Select to Add--
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)	 Posture Server Primary Server Backup Server Summary Back to Services Next > Save Cancel Name: Description: Server Type: ● Microsoft NPS Default Posture Token: UNKNOWN (100)
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.	 Posture Server Primary Server Backup Server Summary Back to Services Next > Save Cancel RADIUS Server Name: RADIUS Server Port: (default is 1812) Shared Secret: Verify: Timeout: 5 seconds
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.	 Service Authentication Authorization Roles Posture Enforcement Audit Profiler Summary Remove View Details Modify Add Add new Posture Policy Add new Posture Server Back to Services Next > Save Cancel Posture Policies: Posture Policies: --Select-- 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] --Select--

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 8: *Enforcement Policy Navigation and Settings*

Navigation	Setting
Configure the Enforcement Policy: - **Enforcement** (tab) > - **Enforcement Policy** (selector): **Role_Based_ Allow_Access_ Policy**	 Service · Authentication · Roles · Posture · Enforcement · 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 · Enforcement Profiles 1. (Date:Day-of-Week BELONGS_TO Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday) · [Allow Access Profile] Back to Services · Next > · Save · Cancel

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

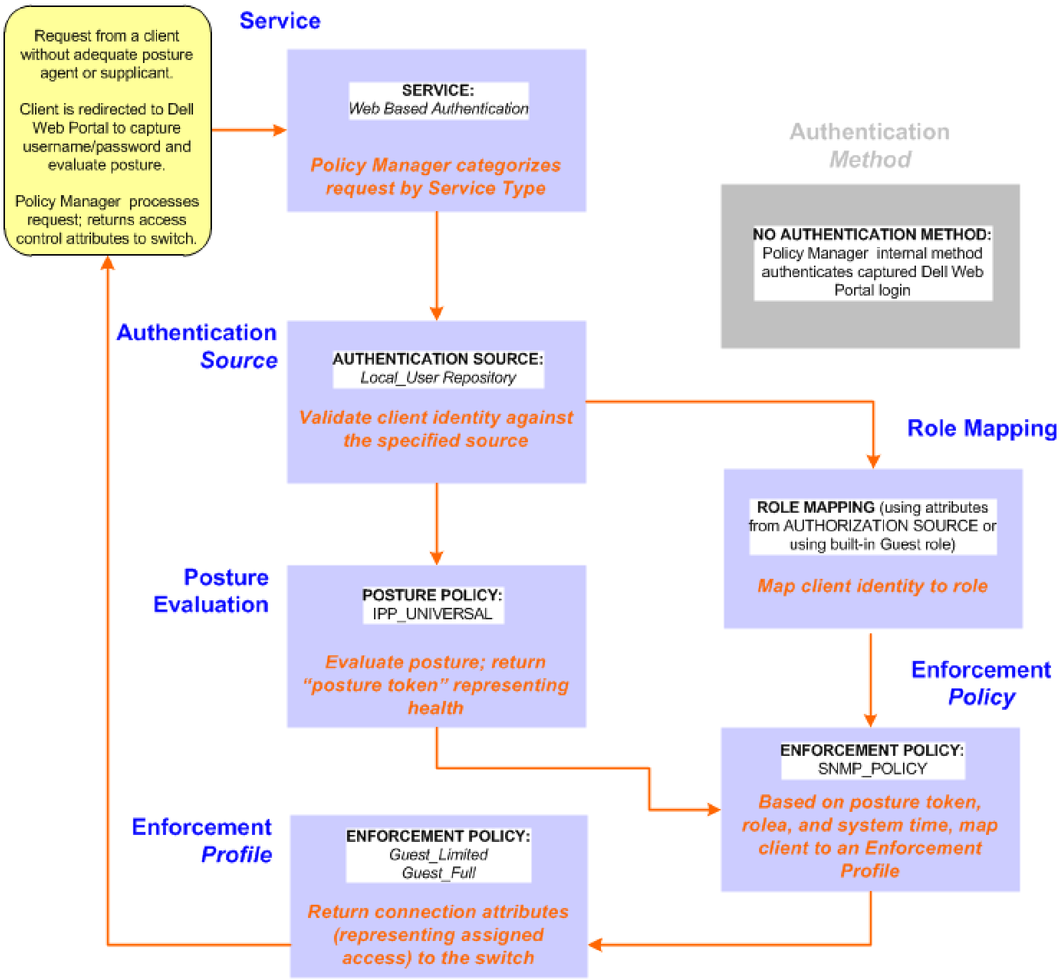
7. Save the Service.

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

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 3: *Flow-of-Control of Web-Based Authentication for Guests*


Request from a client without adequate posture agent or supplicant.
Client is redirected to Dell Web Portal to capture username/password and evaluate posture.
Policy Manager processes request; returns access control attributes to switch.
Service
SERVICE:
Web Based Authentication
Policy Manager categorizes request by Service Type
Authentication Method
NO AUTHENTICATION METHOD: Policy Manager internal method authenticates captured Dell Web Portal login
Authentication Source
AUTHENTICATION SOURCE:
Local_User Repository
Validate client identity against the specified source
Role Mapping
ROLE MAPPING (using attributes from AUTHORIZATION SOURCE or using built-in Guest role)
Map client identity to role
Posture Evaluation
POSTURE POLICY:
IPP_UNIVERSAL
Evaluate posture; return "posture token" representing health
Enforcement Policy
ENFORCEMENT POLICY:
SNMP_POLICY
Based on posture token, rolea, and system time, map client to an Enforcement Profile
Enforcement Profile
ENFORCEMENT POLICY:
Guest_Limited
Guest_Full
Return connection attributes (representing assigned access) to the switch

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.

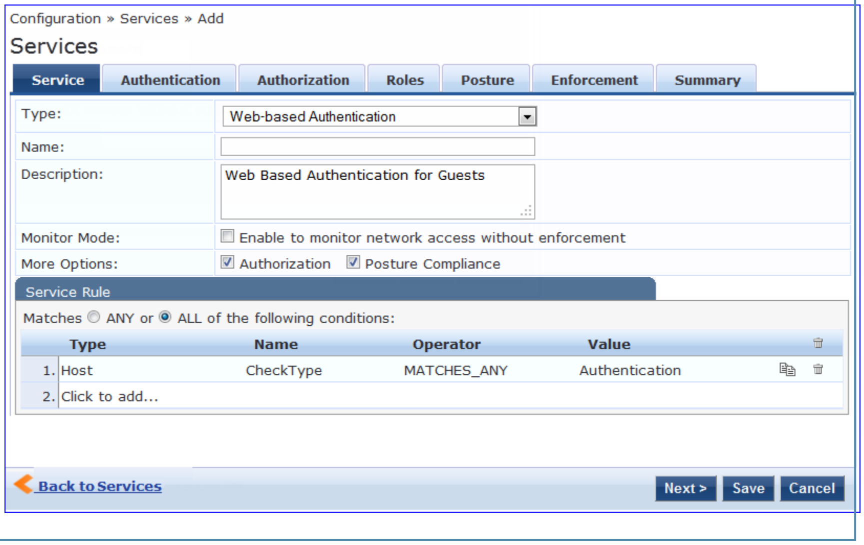
   Refer to your Network Access Device documentation to configure the switch such that it redirects HTTP requests to the *Dell Guest Portal*, which captures username and password and optionally launches an agent that returns posture data.

2. Create a WebAuth-based Service.

Table 9: *Service Navigation and Settings*

Navigation	Settings
Create a new Service: - **Services** > - **Add Service** >	Configuration » Services Services Add Import Export All

Table 9: *Service Navigation and Settings (Continued)*

Navigation	Settings
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**.	

Type: Web-based Authentication

Name:

Description: Web Based Authentication for Guests

Monitor Mode: □ Enable to monitor network access without enforcement

More Options: ☑ Authorization ☑ Posture Compliance

Service Rule

Matches ○ ANY or ● ALL of the following conditions:

	Type	Name	Operator	Value
1.	Host	CheckType	MATCHES_ANY	Authentication
2.	Click to add...			

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 10: *Local Policy Manager Database Navigation and Settings*

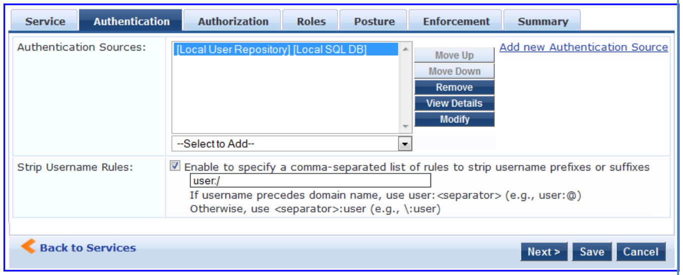
Navigation	Settings
Select the local Policy Manager database: - **Authentication** (tab) > - **Sources** (**Select** drop-down list): **[Local User Repository]** > - **Add** > - **Strip Username Rules** (check box) > - Enter an example of preceding or following separators (if any), with the phrase "user" 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).	 Service Authentication Authorization Roles Posture Enforcement Summary Move Up Move Down Remove View Details Modify Add new Authentication Source Back to Services Next > Save Cancel Authentication Sources: [Local User Repository] [Local SQL DB] --Select to Add-- Strip Username Rules: ☑ Enable to specify a comma-separated list of rules to strip username prefixes or suffixes user:/ If username precedes domain name, use user:<separator> (e.g., user:@) Otherwise, use <separator>:user (e.g., \:user)

Table 11: *Posture Policy Navigation and Settings*

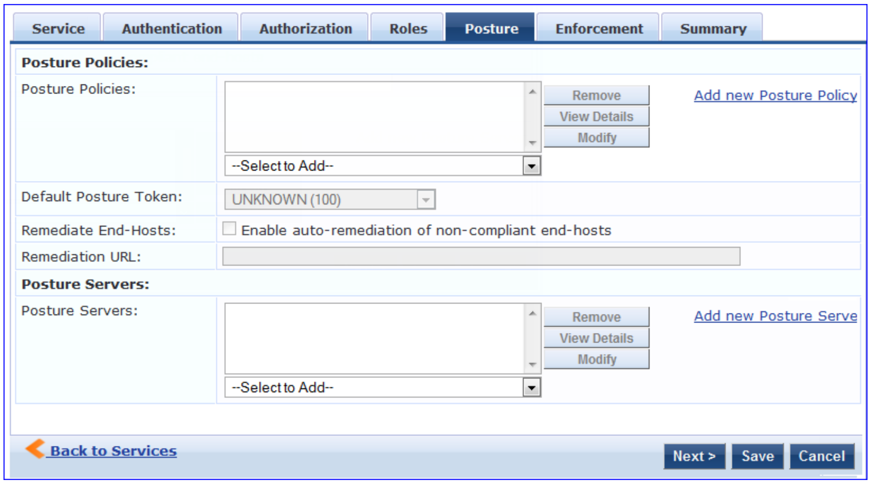
Navigation	Setting
Create a Posture Policy: - **Posture** (tab) > - Enable **Validation Check** (check box) > - **Add new Internal Policy** (link) >	 Service Authentication Authorization Roles Posture Enforcement Summary Remove View Details Modify Add new Posture Policy Remove View Details Modify Add new Posture Serve Back to Services Next > Save Cancel **Posture Policies:** Posture Policies: --Select to Add-- Default Posture Token: UNKNOWN (100) Remediate End-Hosts: □ Enable auto-remediation of non-compliant end-hosts Remediation URL: **Posture Servers:** Posture Servers: --Select to Add--

Table 11: *Posture Policy Navigation and Settings (Continued)*

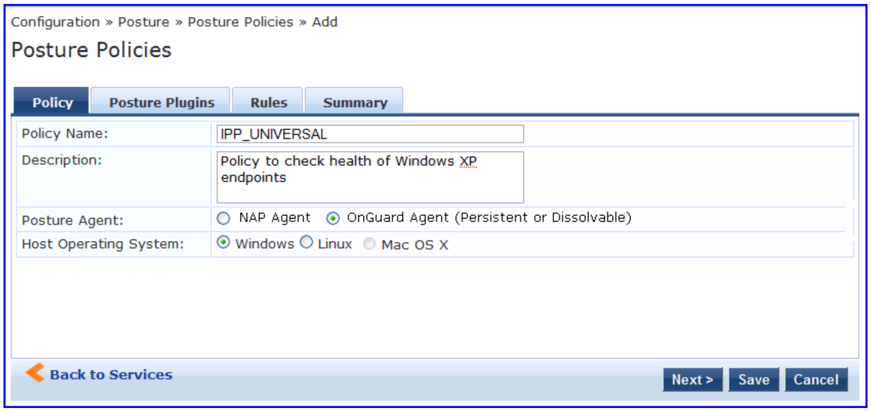
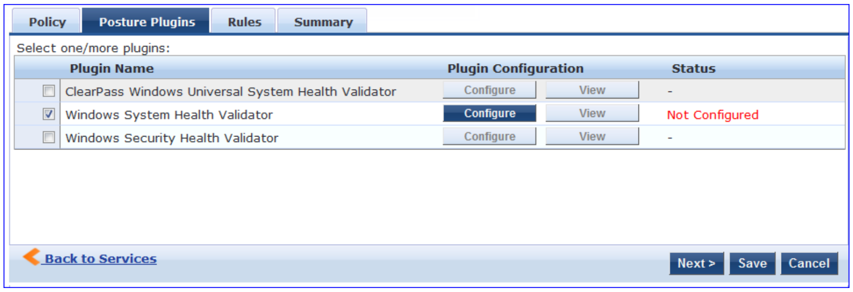
Navigation	Setting
Name the Posture Policy and specify a general class of operating system: - **Policy** (tab) > - **Policy Name** (freeform): *IPP_ UNIVERSAL* > - **Host Operating System** (radio buttons): **Windows** > - When finished working in the **Policy** tab, click **Next** to open the Posture Plugins tab	 Configuration » Posture » Posture Policies » Add Posture Policies Policy Posture Plugins Rules Summary Policy Name: IPP_UNIVERSAL Description: Policy to check health of Windows XP endpoints Posture Agent: ○ NAP Agent ● OnGuard Agent (Persistent or Dissolvable) Host Operating System: ● Windows ○ Linux ○ Mac OS X Back to Services Next > Save Cancel
Select a Validator: - **Posture Plugins** (tab) > - Enable **Windows Health System Validator** > - **Configure** (button) >	 Policy Posture Plugins Rules Summary Select one/more plugins: Plugin Name | Plugin Configuration | Status □ ClearPass Windows Universal System Health Validator | Configure View | - ☑ Windows System Health Validator | Configure View | Not Configured □ Windows Security Health Validator | Configure View | - Back to Services Next > Save Cancel

Table 11: *Posture Policy Navigation and Settings (Continued)*

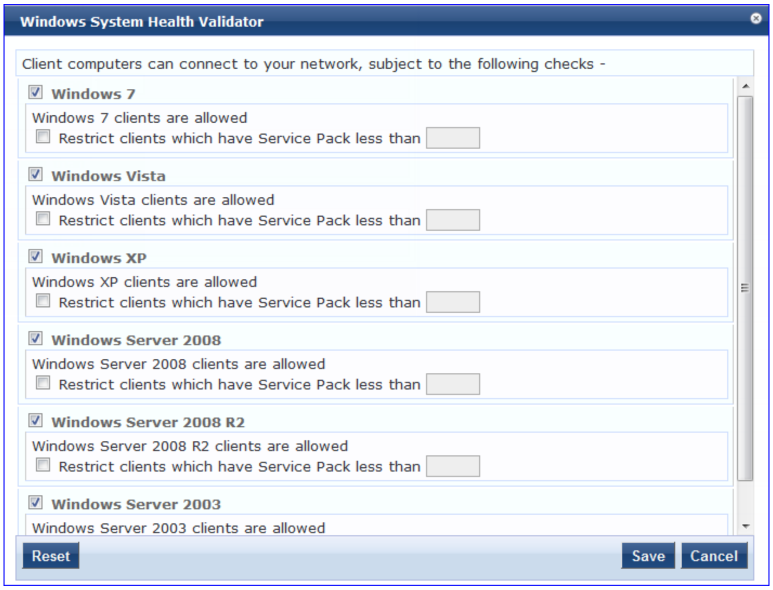
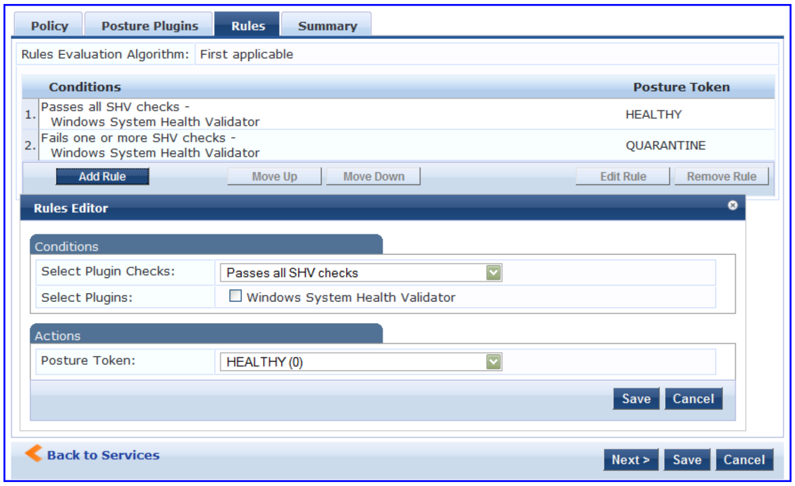
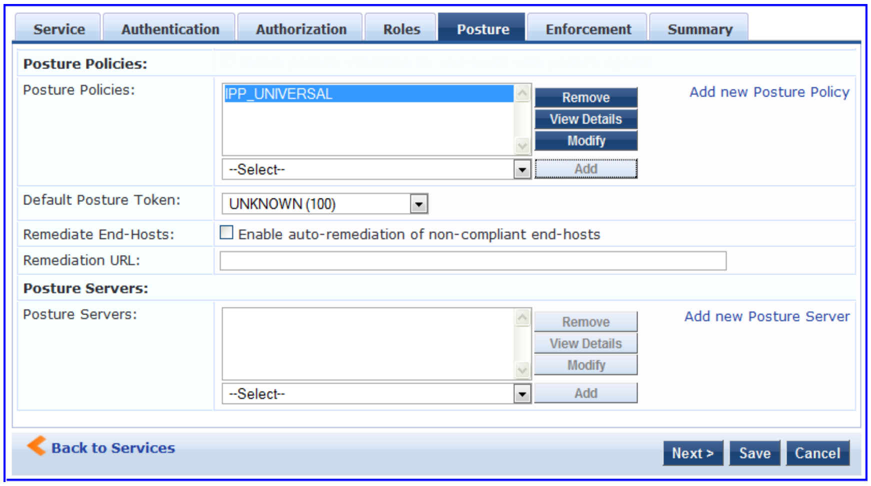
Navigation	Setting
Configure the Validator: - **Windows System Health Validator** (popup) > - **Enable all Windows operating systems** (check box) > - Enable Service Pack levels for Windows 7, Windows Vista®, Windows XP Windows Server® 2008, Windows Server 2008 R2, and Windows Server 2003 (check boxes) > - **Save** (button) > - When finished working in the **Posture Plugin** tab click **Next** to move to the Rules tab)	 Windows System Health Validator Client computers can connect to your network, subject to the following checks - ☑ Windows 7 Windows 7 clients are allowed □ Restrict clients which have Service Pack less than ☑ Windows Vista Windows Vista clients are allowed □ Restrict clients which have Service Pack less than ☑ Windows XP Windows XP clients are allowed □ Restrict clients which have Service Pack less than ☑ Windows Server 2008 Windows Server 2008 clients are allowed □ Restrict clients which have Service Pack less than ☑ Windows Server 2008 R2 Windows Server 2008 R2 clients are allowed □ Restrict clients which have Service Pack less than ☑ Windows Server 2003 Windows Server 2003 clients are allowed

Table 11: *Posture Policy Navigation and Settings (Continued)*

Navigation	Setting
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.	 Policy Posture Plugins Rules Summary Rules Evaluation Algorithm: First applicable 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 Add Rule Move Up Move Down Edit Rule Remove Rule Rules Editor Conditions Select Plugin Checks: Passes all SHV checks Select Plugins: □ Windows System Health Validator Actions Posture Token: HEALTHY (0) Save Cancel Back to Services Next > Save Cancel
Add the new Posture Policy to the Service: Back in **Posture** (tab) > **Internal Policies** (selector): **IPP_ UNIVERSAL_XP,** then click the **Add** button	 Service Authentication Authorization Roles Posture Enforcement Summary **Posture Policies:** Posture Policies: IPP_UNIVERSAL --Select-- Remove View Details Modify Add Add new Posture Policy Default Posture Token: UNKNOWN (100) Remediate End-Hosts: □ Enable auto-remediation of non-compliant end-hosts Remediation URL: **Posture Servers:** Posture Servers: --Select-- Remove View Details Modify Add Add new Posture Server Back to Services Next > Save Cancel

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.

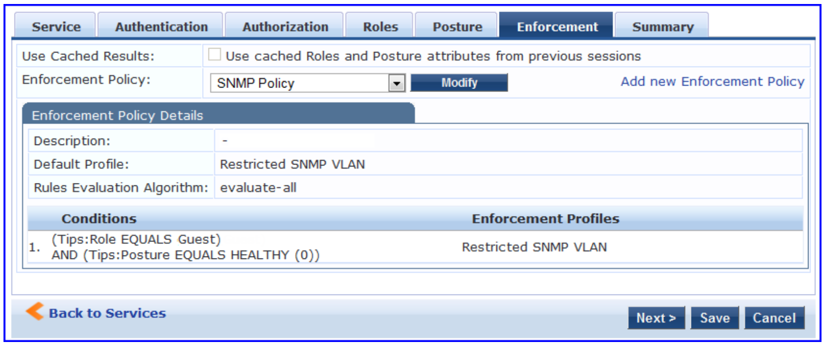
5. Create an Enforcement Policy.

   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 12: *Enforcement Policy Navigation and Settings*

Navigation	Setting
Add a new Enforcement Policy: ● **Enforcement** (tab) > ● Enforcement Policy (selector): **SNMP_ POLICY** ● Upon completion, click **Save**.	 Service | Authentication | Authorization | Roles | Posture | **Enforcement** | Summary Use Cached Results: □ Use cached Roles and Posture attributes from previous sessions Enforcement Policy: SNMP Policy ▾ Modify — Add new Enforcement Policy Enforcement Policy Details Description: - Default Profile: Restricted SNMP VLAN Rules Evaluation Algorithm: evaluate-all Conditions — Enforcement Profiles 1. (Tips:Role EQUALS Guest) AND (Tips:Posture EQUALS HEALTHY (0)) — Restricted SNMP VLAN Back to Services Next > Save Cancel

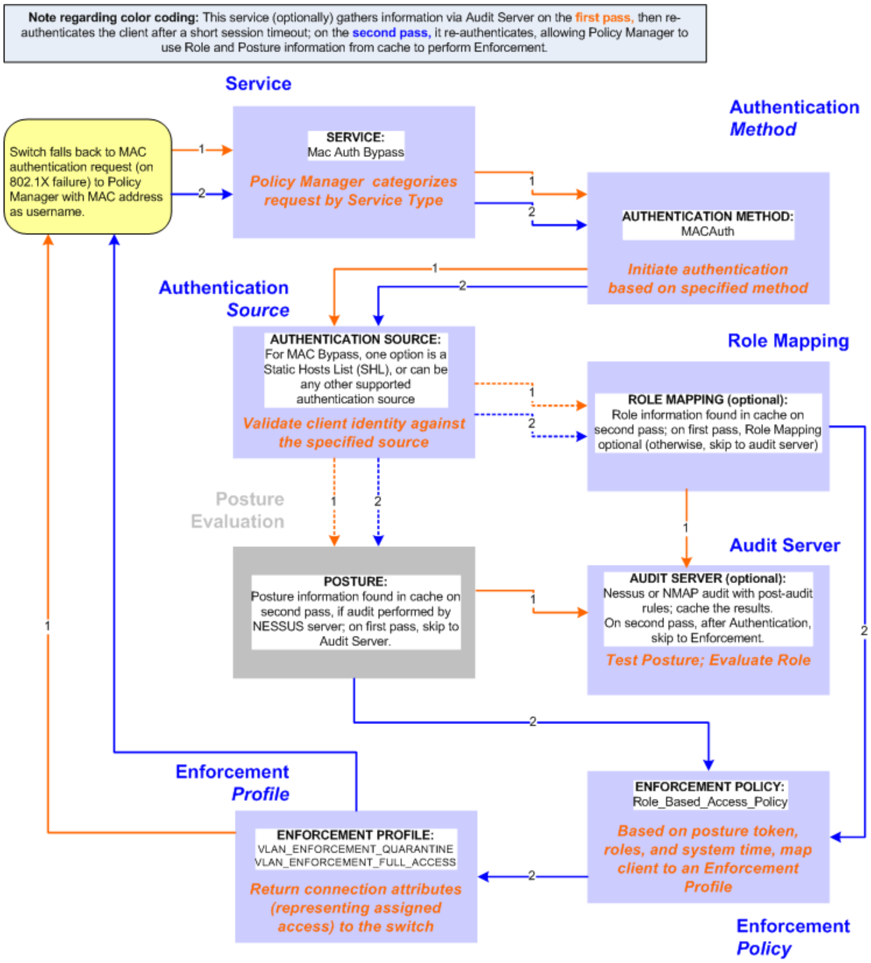
6. Save the Service.

   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 4: *Flow-of-Control of MAC Authentication for Network Devices*



Note regarding color coding: This service (optionally) gathers information via Audit Server on the first pass, then re-authenticates the client after a short session timeout; on the second pass, it re-authenticates, allowing Policy Manager to use Role and Posture information from cache to perform Enforcement.
Service
Switch falls back to MAC authentication request (on 802.1X failure) to Policy Manager with MAC address as username.
1
2
SERVICE:
Mac Auth Bypass
Policy Manager categorizes request by Service Type
Authentication Method
AUTHENTICATION METHOD:
MACAuth
Initiate authentication based on specified method
Authentication Source
AUTHENTICATION SOURCE:
For MAC Bypass, one option is a Static Hosts List (SHL), or can be any other supported authentication source
Validate client identity against the specified source
Role Mapping
ROLE MAPPING (optional):
Role information found in cache on second pass; on first pass, Role Mapping optional (otherwise, skip to audit server)
Posture Evaluation
POSTURE:
Posture information found in cache on second pass, if audit performed by NESSUS server; on first pass, skip to Audit Server.
Audit Server
AUDIT SERVER (optional):
Nessus or NMAP audit with post-audit rules; cache the results.
On second pass, after Authentication, skip to Enforcement.
Test Posture; Evaluate Role
Enforcement Profile
ENFORCEMENT PROFILE:
VLAN_ENFORCEMENT_QUARANTINE
VLAN_ENFORCEMENT_FULL_ACCESS
Return connection attributes (representing assigned access) to the switch
ENFORCEMENT POLICY:
Role_Based_Access_Policy
Based on posture token, roles, and system time, map client to an Enforcement Profile
Enforcement Policy

Configuring the Service

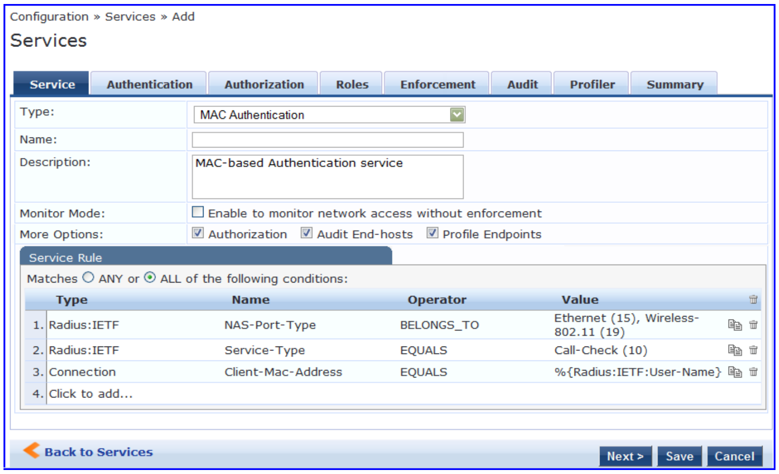
Follow these steps to configure Policy Manager for MAC-based Network Device access.

1. Create a MAC Authentication Service.

Table 13: *MAC Authentication Service Navigation and Settings*

Navigation	Settings
Create a new Service: ● **Services** > ● **Add Service** (link) >	 Configuration » Services Services Add Import Export All

Table 13: *MAC Authentication Service Navigation and Settings (Continued)*

Navigation	Settings
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	

Configuration » Services » Add

Services

Type: MAC Authentication

Name:

Description: MAC-based Authentication service

Monitor Mode: □ Enable to monitor network access without enforcement

More Options: ☑ Authorization ☑ Audit End-hosts ☑ Profile Endpoints

Service Rule

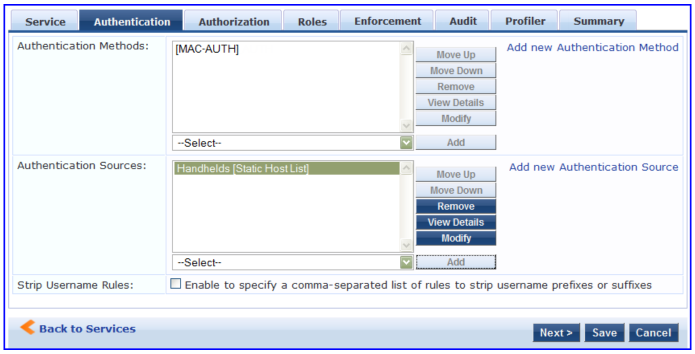
Matches ○ ANY or ● ALL of the following conditions:

	Type	Name	Operator	Value
1.	Radius:IETF	NAS-Port-Type	BELONGS_TO	Ethernet (15), Wireless-802.11 (19)
2.	Radius:IETF	Service-Type	EQUALS	Call-Check (10)
3.	Connection	Client-Mac-Address	EQUALS	%{Radius:IETF:User-Name}
4.	Click to add...			

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). Refer to "Adding and Modifying Static Host Lists" in the *ClearPass Policy Manager User Guide* for more information. You can also select any other supported type of authentication source.

Table 14: *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)	

Authentication Methods: [MAC-AUTH]

--Select--

Authentication Sources: Handhelds [Static Host List]

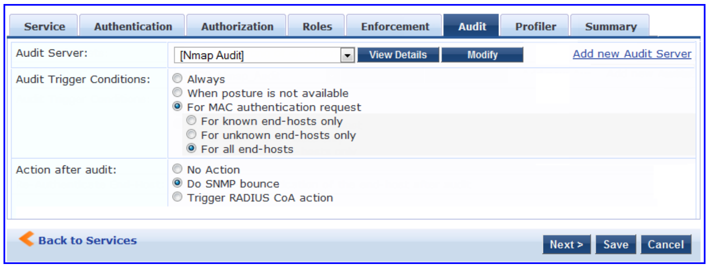
--Select--

Strip Username Rules: □ Enable to specify a comma-separated list of rules to strip username prefixes or suffixes

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.

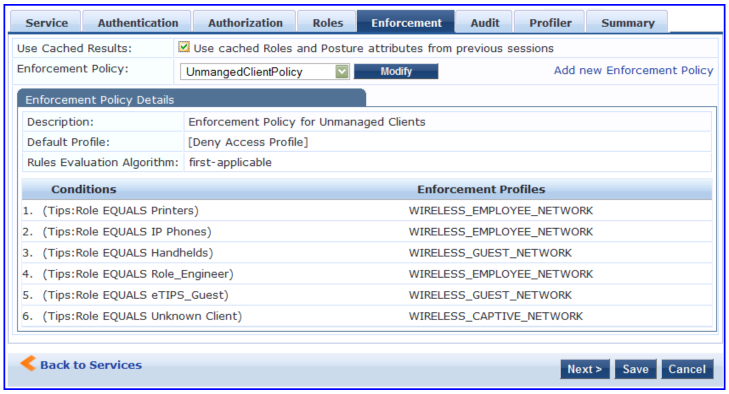
Table 15: *Audit Server Navigation and Settings*

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**	 Service Authentication Authorization Roles Enforcement Audit Profiler Summary View Details Modify Add new Audit Server Back to Services Next > Save Cancel Audit Server: [Nmap Audit] Audit Trigger Conditions: ○ Always ○ When posture is not available ● For MAC authentication request ○ For known end-hosts only ○ For unknown end-hosts only ● For all end-hosts Action after audit: ○ No Action ● Do SNMP bounce ○ Trigger RADIUS CoA action

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 16: *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**.	 Service Authentication Authorization Roles Enforcement Audit Profiler Summary Modify Add new Enforcement Policy Back to Services Next > Save Cancel Use Cached Results: ☑ Use cached Roles and Posture attributes from previous sessions Enforcement Policy: UnmangedClientPolicy Enforcement Policy Details Description: Enforcement Policy for Unmanaged Clients Default Profile: [Deny Access Profile] Rules Evaluation Algorithm: first-applicable 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).

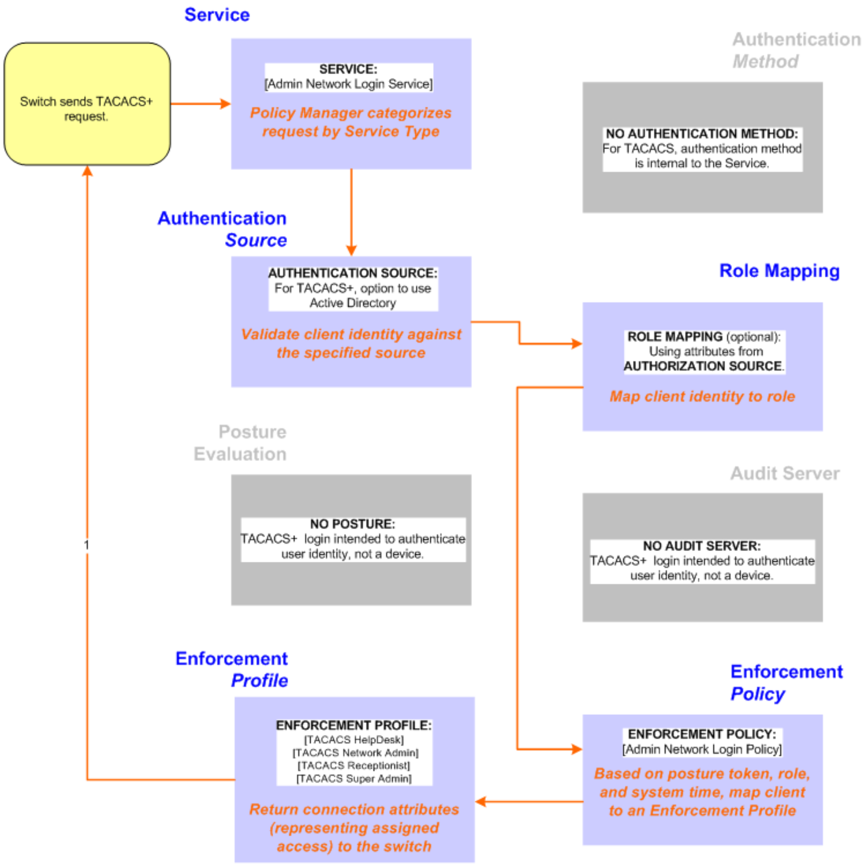
5. Save the Service.

   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 5: *Administrator connections to Network Access Devices via TACACS+*

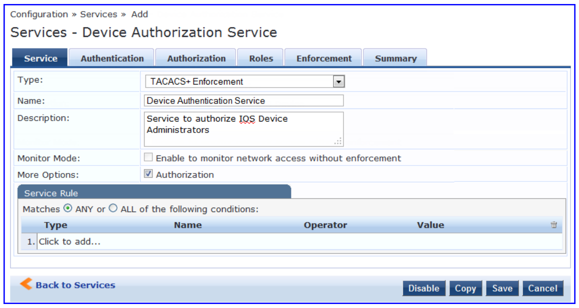

Service
Switch sends TACACS+ request.
SERVICE: [Admin Network Login Service]
Policy Manager categorizes request by Service Type
Authentication Method
NO AUTHENTICATION METHOD: For TACACS, authentication method is internal to the Service.
Authentication Source
AUTHENTICATION SOURCE: For TACACS+, option to use Active Directory
Validate client identity against the specified source
Role Mapping
ROLE MAPPING (optional): Using attributes from AUTHORIZATION SOURCE.
Map client identity to role
Posture Evaluation
NO POSTURE: TACACS+ login intended to authenticate user identity, not a device.
Audit Server
NO AUDIT SERVER: TACACS+ login intended to authenticate user identity, not a device.
1
Enforcement Profile
ENFORCEMENT PROFILE: [TACACS HelpDesk] [TACACS Network Admin] [TACACS Receptionist] [TACACS Super Admin]
Return connection attributes (representing assigned access) to the switch
Enforcement Policy
ENFORCEMENT POLICY: [Admin Network Login Policy]
Based on posture token, role, and system time, map client to an Enforcement Profile

Configuring the Service

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

1. Create a TACACS+ Service.

Table 17: *TACACS+ Navigation and Settings*

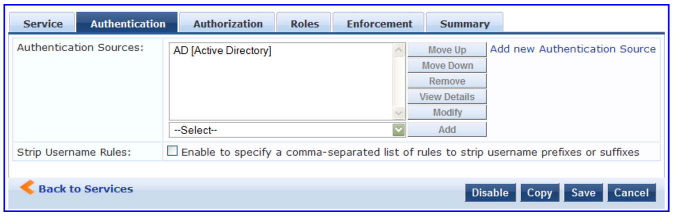
Navigation	Settings
Create a new Service: - **Services** > - **Add Service** (link) >	 Configuration » Services Services Add Import Export All
Name the Service and select a pre-configured Service Type: - **Service** (tab) > - **Type** (selector): **[Policy Manager Admin Network Login Service]** > - **Name/Description** (freeform) > - Upon completion, click **Next** (to Authentication)	 Configuration » Services » Add Services - Device Authorization Service Service | Authentication | Authorization | Roles | Enforcement | Summary Type: TACACS+ Enforcement Name: Device Authentication Service Description: Service to authorize IOS Device Administrators Monitor Mode: □ Enable to monitor network access without enforcement More Options: ☑ Authorization Service Rule Matches ● ANY or ○ ALL of the following conditions: Type | Name | Operator | Value 1. Click to add... Back to Services Disable | Copy | Save | Cancel

2. Set up the Authentication.

   a. Method: The Policy Manager TACACS+ service authenticates TACACS+ requests internally.

b. Source: For purposes of this use case, Network Access Devices authentication data will be stored in the Active Directory.

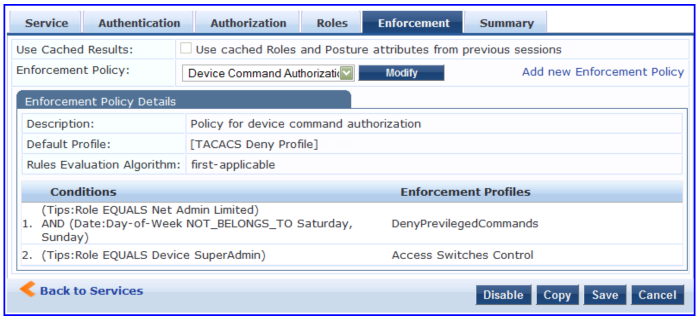
Table 18: *Active Directory Navigation and Settings*

Navigation	Settings
Select an Active Directory server (that you have already configured in Policy Manager): • **Authentication** (tab) > • **Add** > • **Sources** (**Select** drop-down list): AD (Active Directory) > • **Add** > • Upon completion, click **Next** (to Enforcement Policy)	 Authentication Sources: AD [Active Directory] --Select-- Strip Username Rules: □ Enable to specify a comma-separated list of rules to strip username prefixes or suffixes Service Authentication Authorization Roles Enforcement Summary Move Up Move Down Remove View Details Modify Add Add new Authentication Source Back to Services Disable Copy Save Cancel

3. Select an Enforcement Policy.

   Select the Enforcement Policy **[Admin Network Login Policy]** that distinguishes the two allowed roles (**Net Admin Limited** and **Device SuperAdmin**.

Table 19: *Enforcement Policy Navigation and Settings*

Navigation	Setting
Select the Enforcement Policy: • **Enforcement** (tab) > • **Enforcement Policy** (selector): **Device Command Authorization Policy** • When you are finished with your work in this tab, click **Save**.	 Use Cached Results: □ Use cached Roles and Posture attributes from previous sessions Enforcement Policy: Device Command Authorizati Enforcement Policy Details Description: Policy for device command authorization Default Profile: [TACACS Deny Profile] Rules Evaluation Algorithm: first-applicable Conditions / Enforcement Profiles 1. (Tips:Role EQUALS Net Admin Limited) AND (Date:Day-of-Week NOT_BELONGS_TO Saturday, Sunday) — DenyPrevilegedCommands 2. (Tips:Role EQUALS Device SuperAdmin) — Access Switches Control Service Authentication Authorization Roles Enforcement Summary Modify Add new Enforcement Policy Back to Services Disable Copy Save Cancel

4. Save the Service.

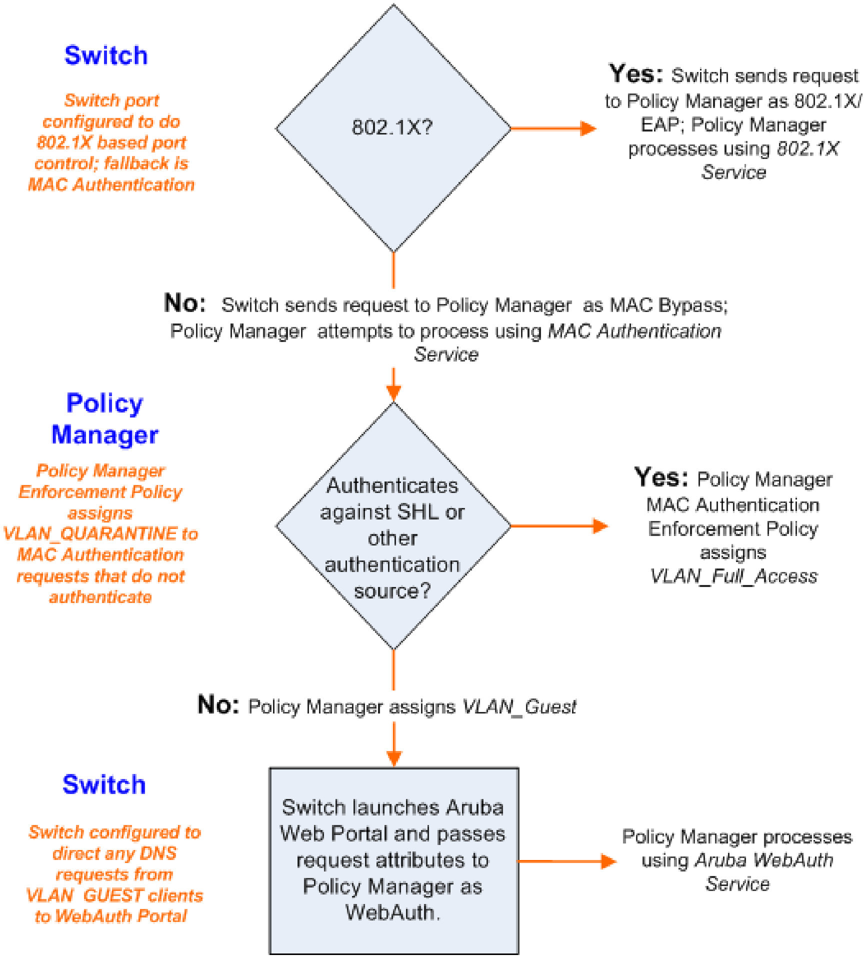
   Click **Save.** The Service now appears at the bottom of the **Services** list.

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 6: *Flow of the Multiple Protocol Per Port Case*


Switch
Switch port configured to do 802.1X based port control; fallback is MAC Authentication
802.1X?
Yes: Switch sends request to Policy Manager as 802.1X/ EAP; Policy Manager processes using 802.1X Service
No: Switch sends request to Policy Manager as MAC Bypass; Policy Manager attempts to process using MAC Authentication Service
Policy Manager
Policy Manager Enforcement Policy assigns VLAN_QUARANTINE to MAC Authentication requests that do not authenticate
Authenticates against SHL or other authentication source?
Yes: Policy Manager MAC Authentication Enforcement Policy assigns VLAN_Full_Access
No: Policy Manager assigns VLAN_Guest
Switch
Switch configured to direct any DNS requests from VLAN GUEST clients to WebAuth Portal
Switch launches Aruba Web Portal and passes request attributes to Policy Manager as WebAuth.
Policy Manager processes using Aruba WebAuth Service