



ClearPass Policy Manager[®]

User Manual 5.0

Part No. DOC-CPASS-5-0-0-1

<http://www.arubanetworks.com>
email: info@arubanetworks.com
email: nasales@arubanetworks.com

Aruba Networks
1344 Crossman Ave.
Sunnyvale, CA 94089
Tel: +1 408.227.4500
Fax: +1 408.752.0626

Copyright © 2005–2012 Aruba Networks. All rights reserved. ClearPass Policy Manager and the Aruba Logo are registered trademarks of Aruba Networks. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

All specifications and information contained in this manual are subject to change without notice. All information and recommendations contained in this manual are believed to be accurate but are presented without warranty of any kind, either expressed or implied. Aruba Networks assumes no responsibility for any inaccuracies or omissions in this document. Aruba Networks reserves the right to change, modify, transfer, or otherwise revise this document without notice.

This document is an unpublished work protected by the United States copyright laws and is proprietary to Aruba Networks. No portion of this document may be disclosed, copied or reproduced without the prior written consent of Aruba Networks.

For all other copyright notices related to the software, see [“Software Copyright and License Statements”](#) (page 325).

Table of Contents

Chapter 1:	Powering Up, Configuring, and Updating the Policy Manager Hardware¹	
	Server Port Overview.....	1
	Server Port Configuration	1
	Updating the Policy Manager Software	3
	Powering Off the System.....	5
	Resetting Passwords to Factory Default	5
	Generating Support Key for Technical Support	6
Chapter 2:	Policy Manager Dashboard	9
Chapter 3:	Monitoring & Reporting	13
	Access Tracker	13
	Viewing Session Details	15
	Accounting	17
	OnGuard Activity	24
	Analysis & Trending	26
	System Monitor	28
	Activity Reports	30
	Add Report	31
	Import Reports.....	34
	Export Reports.....	34
	Exports	34
	Audit Viewer.....	35
	Event Viewer	37
	Data Filters.....	38
	Add Filter	40
Chapter 4:	Policy Manager Policy Model	43
	Services Paradigm	43
	Viewing Existing Services.....	46
	Adding and Removing Services	48
	Links to Use Cases and Configuration Instructions	48

	Policy Simulation	50
	Add Simulation Test.....	51
	Import Simulations	56
	Export Simulations	57
	Export.....	57
Chapter 5:	<i>802.1X Wireless Use Case</i>	59
	Configuring the Service	60
Chapter 6:	<i>Aruba Web-Based Authentication Use Case</i>	67
	Configuring the Service	68
Chapter 7:	<i>MAC Authentication Use Case</i>	73
	Configuring the Service	74
Chapter 8:	<i>TACACS+ Use Case</i>.....	77
	Configuring the Service	78
Chapter 9:	<i>Single Port Use Case</i>	81
Chapter 10:	Services	83
	Architecture and Flow.....	83
	Start Here Page	83
	Policy Manager Service Types	85
	Adding and Modifying Services.....	98
	Reordering Services	101
Chapter 11:	Authentication & Authorization	103
	Architecture and Flow.....	103
	Configuring Authentication Components	105
	Adding and Modifying Authentication Methods	107
	EAP-FAST	108
	EAP-PEAP	112
	EAP-TLS	114
	EAP-TTLS	115
	MAC-AUTH	117
	MSCHAP	118
	PAP	118
	CHAP & EAP-MD5.....	119

Adding and Modifying Authentication Sources	119
Generic LDAP or Active Directory	122
Kerberos	133
Generic SQL DB.....	134
Token Server	138
Static Host List	141

Chapter 12: Identity - Users, Endpoints, Roles & Role Mapping . 143

Architecture and Flow	143
Configuring a Role Mapping Policy	144
Adding and Modifying Role Mapping Policies	144
Adding and Modifying Roles	147
Local Users, Guest Users, Endpoints and Static Host List Configuration	149
Adding and Modifying Local Users.....	149
Adding and Modifying Guest Users	150
Adding and Modifying Endpoints	153
Adding and Modifying Static Host Lists	155

Chapter 13: Posture 159

Architecture and Flow	159
Configuring Posture	161
Adding and Modifying Posture Policies	162
Configuring Posture Policy Plugins.....	163
ClearPass Windows Universal System Health Validator - NAP Agent.....	167
ClearPass Windows Universal System Health Validator - OnGuard Agent.....	182
ClearPass Linux Universal System Health Validator - NAP Agent	182
ClearPass Linux Universal System Health Validator - OnGuard Agent.....	185
Windows System Health Validator - NAP Agent	185
Windows System Health Validator - OnGuard Agent	186
Windows Security Health Validator - NAP Agent.....	187
ClearPass Mac OS X Universal System Health Validator - OnGuard Agent	187
Adding and Modifying Posture Servers	189
Microsoft NPS.....	190

Chapter 14: Audit Servers 193

Architecture and Flow	193
Configuring Audit Servers.....	194
Built-In Audit Servers	194

	Adding Auditing to An Policy Manager Service.....	194
	Modifying Built-In Audit Servers	196
	Custom Audit Servers	197
	NESSUS Audit Server	197
	NMAP Audit Server	199
	Nessus Scan Profiles	200
	Post-Audit Rules	204
Chapter 15:	Enforcement.....	207
	Architecture and Flow	207
	Configuring Enforcement Profiles.....	208
	RADIUS Enforcement Profiles.....	212
	RADIUS CoA Enforcement Profiles.....	214
	SNMP Enforcement Profiles	214
	TACACS+ Enforcement Profiles	215
	Application Enforcement Profiles	218
	CLI Enforcement Profile	219
	Agent Enforcement Profile	219
	Configuring Enforcement Policies	220
Chapter 16:	Network Access Devices	223
	Adding and Modifying Devices	223
	Adding and Modifying Device Groups.....	227
	Adding and Modifying Proxy Targets	229
Chapter 17:	Administration	233
	Admin Users.....	233
	Add User.....	234
	Import Users	235
	Export Users	235
	Export.....	235
	Admin Privileges	236
	Import Admin Privileges.....	236
	Export Admin Privileges.....	236
	Export.....	237
	Server Configuration	237
	Set Date/Time	237
	Set Time Zone on Publisher	238

Change Cluster Password	239
Make Subscriber.....	239
Upload Nessus Plugins.....	240
Cluster-Wide Parameters	241
Collect Logs.....	242
Backup	243
Restore.....	244
Shutdown/Reboot.....	245
Drop Subscriber	245
Set Time Zone (Subscriber).....	245
Synchronize Cluster Password (Subscriber)	246
Promote To Publisher	246
System Tab	246
Services Control Tab	249
Service Parameters Tab.....	249
System Monitoring Tab.....	257
Log Configuration.....	258
Local Shared Folders.....	260
Snmp Trap Receivers	261
Add SNMP Trap Server	262
Import SNMP Trap Server.....	263
Export SNMP Trap Server.....	263
Export.....	263
Syslog Targets.....	264
Add Syslog Target	264
Import Syslog Target.....	265
Export Syslog Target	265
Export.....	266
Syslog Export Filters	266
Add Syslog Filter	267
Import Syslog Filter	269
Export Syslog Filter	269
Export.....	269
Messaging Setup	269
Certificates	271
Server Certificate	271
Create Self-Signed Certificate.....	272
Create Certificate Signing Request.....	274
Certificate Trust List.....	276

Add Certificate.....	277
Revocation Lists	277
Add Revocation List	278
Dictionaries	278
RADIUS Dictionaries	279
Posture Dictionaries.....	280
TACACS+ Services.....	281
Import Dictionary	282
Agent Settings	283
Guest Portal.....	284
Update Portal	288

Appendix A: Command Line Interface..... 291

Available Commands.....	291
Cluster Commands.....	293
drop-subscriber	294
list	294
make-publisher.....	294
make-subscriber	294
reset-database.....	295
set-cluster-passwd	295
set-local-passwd	295
Configure Commands	296
date	296
dns	296
hostname	297
ip.....	297
timezone	297
Network Commands	297
ip.....	298
nslookup	299
ping.....	299
reset	299
traceroute.....	300
Service commands	300
<action>	300
Show Commands.....	301
all-timezones	301

date	301
dns	302
domain.....	302
hostname	302
ip.....	302
license.....	303
timezone	303
version	303
System commands	303
boot-image	303
gen-support-key	304
install-license.....	304
restart.....	304
shutdown	305
update.....	305
upgrade	305
Miscellaneous Commands	306
ad auth.....	306
ad netjoin.....	306
ad netleave.....	307
ad testjoin	307
alias.....	307
backup	307
dump certchain	308
dump logs.....	308
dump servercert	309
exit	309
help.....	309
krb auth	309
krb list.....	310
ldapsearch	310
restore	310
quit	311
VM-Only Commands	311
configure vmhost.....	311
show vmhost.....	311

Appendix B: Rules Editing & Namepsaces 313

Namespaces	314
------------------	-----

Variables	321
Operators.....	322

Appendix C: Software Copyright and License Statements 325

Postgres Copyright.....	325
GNU LGPL	325
GNU GPL	333
Lighthttpd License.....	339
Apache License	340
OpenSSL License	343
OpenLDAP License	348
gSOAP Public License	349

Chapter 1:

Powering Up, Configuring,
and Updating the Policy
Manager Hardware

The Policy Manager server requires initial port configuration. Its backpanel contains three ports.

Server Port Overview

Figure 1-1 Policy Manager Backplane
A—Serial port; B—Management port; C—Data port



as described in the following table:

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

Server Port Configuration

Before starting the installation, gather the following information that will need:

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

To set up the Policy Manager appliance:

1. Connect and power on.

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

Use the following parameters for the serial port connection:

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

2. Login.

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

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

This starts the Policy Manager Configuration Wizard.

3. Configure the appliance.

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

```

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

```

4. Change your password.

Use any string of at least six characters:

```

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

```

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

5. Change system date/time.

```

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

```

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

6. Commit or restart the configuration.

Follow the prompts:

```

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.

```

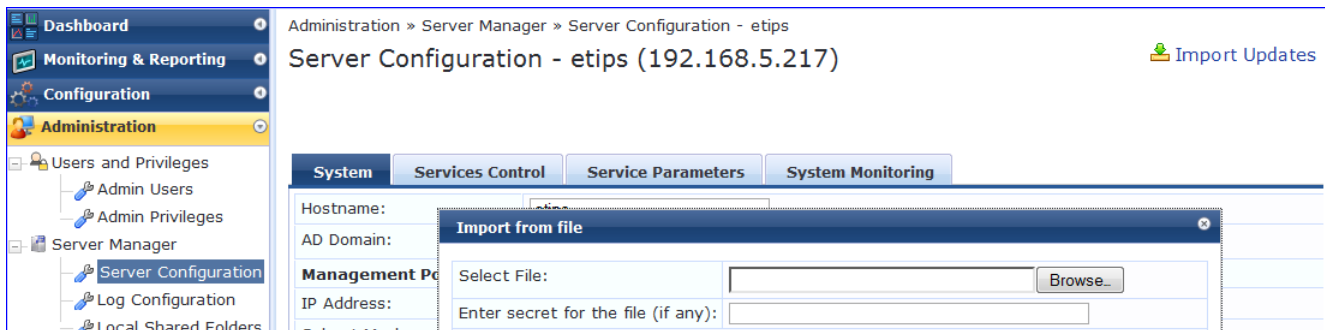
Updating the Policy Manager Software

By way of background, the Policy Manager *Publisher node* acts as master. Administration, configuration, and database write operations are allowed only on this master node. The Policy Manager appliance defaults to a Publisher node unless it is made a Subscriber node. An Policy Manager cluster can contain only one Publisher node. Cluster commands can be used to change the state of the node, hence the Publisher can be made a Subscriber.

To upgrade the image on a single Policy Manager appliance:

- From the Policy Manager UI, navigate to **Administration > Server Manager > Server Configuration**. From the listing page on the right, click on the server you want to upgrade. On top right corner of the server page, click on **Import Updates**. Select the upgrade file and click on **Import**. The upgrade file is now available to the `system upgrade` command on the CLI.

Figure 1-2 Importing Upgrade Image



Alternatively, transfer the image file to a Policy Manager external machine and make it available via http or SSH.

- Login to the Policy Manager appliance as *appadmin* user.
- Use the command `system upgrade`, which will upgrade your second partition, then reboot. Policy Manager boots into the upgraded image.

Note: If you access the appliance via serial console, you should also be able to boot into the previous image by choosing that image in the Grub boot screen.

- Verify that all configuration and session logs are restored and all services are running. Also verify that node-specific configuration such as the server certificate, log configuration and server parameters are also restored.

To upgrade the image on all appliances in an Policy Manager cluster:

- Upgrade publisher Policy Manager first, and reboot into the new image.

On the first boot after upgrade, all old configuration data is restored. Verify that all configuration and services are intact.

In the cluster servers screen, all subscriber node entries are present but marked as **Cluster Sync=false** (disabled for replication). Any configuration changes performed in this state do not replicate to subscribers until the sub-

scribers are also upgraded (effectively no configuration changes are possible on subscribers in this state).

Note: You can add a subscriber to the cluster from the User Interface:
Configuration > Administration > Server Configuration (page)
 > **Make Subscriber** (link).

- One node at a time, upgrade the subscriber nodes to the same Policy Manager version as the publisher, using the same steps as for a single Policy Manager server. On the first boot after upgrade, the node is added back to the cluster (the publisher node must be up and available for this to work).

Login to the UI and verify that the node is replicating and "Cluster Sync" is set to true.

Note: If the publisher is not available when the subscriber boots up after the upgrade, adding the node back to the cluster fails. In that case, the subscriber comes up with an empty database. Fix the problem by adding the subscriber back into the cluster from the CLI. All node configuration, including *certificates*, *log configuration* and *server parameters* are restored (as long as the node entry exists in the publisher with **Cluster Sync=false**).

Powering Off the System

To power off the system gracefully without logging in:

- Connect to the CLI from the serial console via the front serial port.

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

This procedure gracefully shuts down the appliance.

Resetting Passwords to Factory Default

Administrator passwords in Policy Manager can be reset to factory defaults by logging into the CLI as the *apprecovery* user. The password to log in as the *apprecovery* user is dynamically generated.

To generate the recovery password:

- Connect to the Policy Manager appliance via the front serial port (using any terminal program). See “[Server Port Overview](#)” (page 1) for details.
- Reboot the system. See “[restart](#)” (page 304) command.
- When the system restarts it waits at the following prompt for 10 seconds:
 - `Generate support keys? [y/n]:`

- Enter 'y' at the prompt. `Generate support keys? [y/n]:y`
- 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:
```

To generate the recovery key, select option 1 (or 3, if you want to generate a support key, as well).

- Once the password recovery key is generated:
 - Email the key to Aruba technical support.
 - A unique password is generated from the recovery key and emailed back to you.
 - Use this password to log in as the *apprecovery* user.
 - At the command prompt enter the following:

```
[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 Support Key for Technical Support

To troubleshoot certain critical system level errors Aruba technical support might need to log into a *support shell*. To generate a dynamic support password:

- Log into the Command Line Interface (CLI) and enter the command: *system gen-support-key*. See “[gen-support-key](#)” (page 304) for details.
- Connect to the Policy Manager appliance via the front serial port (using any terminal program). See “[Server Port Overview](#)” (page 1) for details.
- Reboot the system. See “[restart](#)” (page 304) command.
- When the system restarts it waits at the following prompt for 10 seconds:
 - `Generate support keys? [y/n]:`
- Enter 'y' at the prompt. `Generate support keys? [y/n]:y`

- 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:
```






To generate the support key, select option 2 (or 3, if you want to generate a password recovery key, as well).

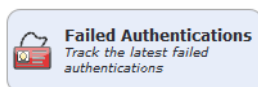
- Once the password recovery key is generated:
 - Email the key to Aruba technical support.
 - A unique password can now be generated by Aruba technical support to log into the support shell.

Chapter 2: Policy Manager Dashboard

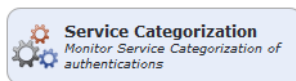
The Policy Manager Dashboard menu allows you to display system health and other request related statistics. Policy Manager comes pre-configured with different dashboard elements. The screen on the right of the dashboard menu is partitioned into five fixed slots. You can drag and drop any of the dashboard elements into the five slots. The dashboard elements are listed below:

Table 2-1 Policy Manager Dashboard Elements

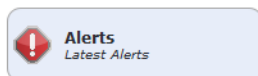
 All Requests <i>Trend all eTIPS requests</i>	This shows a graph of all requests processed by Policy Manager over the past week. This includes RADIUS, TACACS+ and WebAuth requests. The default data filter “All Requests” is used to plot this graph. Clicking on each bar in the graph drills down into the Access Tracker and shows the requests for that day.
 Health Status <i>Trend Healthy and Unhealthy requests</i>	This shows a graph of the “Healthy” vs. “Unhealthy” requests over the past week. Healthy requests are those requests where the health state was deemed to be healthy (based on the posture data sent from the client). Unhealthy requests are those requests whose health state was deemed to be quarantined (posture data received but health status is not compliant) or unknown (no posture data received). This includes RADIUS and WebAuth requests. The default data filters “Health Requests” and “Unhealthy Requests” are used to plot this graph. Clicking on each circle on the line graph drills down into the Access Tracker and shows the healthy or unhealthy requests for that day.
 Authentication Status <i>Trend Successful and Failed authentications</i>	This shows a graph of the “Failed” vs. “Successful” requests over the past week. This includes RADIUS, WebAuth and TACACS+ requests. The default data filters “Failed Requests” and “Successful Requests” are used to plot this graph. Clicking on each circle on the line graph drills down into the Access Tracker and shows the failed or successful requests for that day.
 Latest Authentications <i>Latest Authentications</i>	This shows a table of the last few authentications. Clicking on a row drills down into the Access Tracker and shows requests sorted by timestamp with the latest request showing first.
 Successful Authentications <i>Track the latest successful authentications</i>	This shows a table of the last few successful authentications. Clicking on a row drills down into the Access Tracker and shows successful requests sorted by timestamp with the latest request showing first.



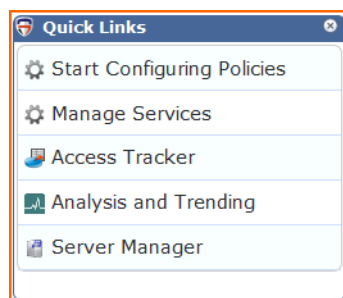
This shows a table of the last few failed authentications. Clicking on a row drills down into the Access Tracker and shows failed requests sorted by timestamp with the latest request showing first.



This shows a bar chart with each bar representing an Policy Manager service requests were categorized into. Clicking on a bar drills down into the Access Tracker and shows the requests that were categorized into that specific service.

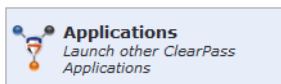


This shows a table of last few system level events. Clicking on a row drills down into the Event Viewer

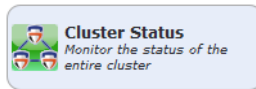


Quick Links shows links to common configuration tasks:

- **Start Configuring Policies** Link to the Start Here Page under Configuration menu. Start configuring Policy Manager Services from here.
- **Manage Services** Link to the Services page under Configuration menu. Shows a list of configured services.
- **Access Tracker** Link to Access Tracker screen under Reporting & Monitoring menu.
- **Analysis & Trending** Link to Analysis & Trending screen under Reporting & Monitoring menu.
- **Network Devices** Link to Network Devices screen under Configuration menu. Configure network devices from here.
- **Server Manager** Link to Server Configuration screen under Administration menu.



This shows links to the Aruba applications that are integrated with Policy Manager. E.g., GuestConnect, Insight.

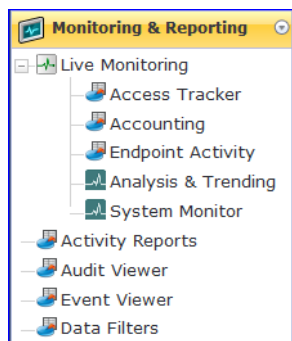


This shows the status of all nodes in the cluster. The following fields are shown for each node:

- **Status** This shows the overall health status of the system. Green indicates healthy and red indicates connectivity problems or high CPU or memory utilization. The status also shows red when a node is out-of-sync with the rest of the cluster.
 - **Host Name** Host name and IP address of the node
 - **CPU Util** Snapshot of the CPU utilization in percentage
 - **Mem Util** Snapshot of the memory utilization in percentage
 - **Server Role** Publisher or subscriber
-

Chapter 3: Monitoring & Reporting

The Policy Manager Monitoring & Reporting menu provides the following interfaces for monitoring and reporting:



- Live Monitoring
 - “Access Tracker” (page 13)
 - “Accounting” (page 17)
 - “OnGuard Activity” (page 24)
 - “Analysis & Trending” (page 26)
 - “System Monitor” (page 28)
- “Activity Reports” (page 30)
- “Audit Viewer” (page 35)
- “Event Viewer” (page 37)
- “Data Filters” (page 38)

Access Tracker

The Access Tracker provides a real-time display of system activity, with optional auto-refresh, at: **Monitoring & Reporting > Live Monitoring > Access Tracker**. Click on **Edit** to change the Access Tracker display parameters.

Figure 3-1 Access Tracker (Edit Mode)

Monitoring & Reporting » Live Monitoring » Access Tracker

Access Tracker

Jul 26, 2010 13:39:52 PDT Auto Refresh

Select Server: + Add

Select Filter: + Add



Select Date Range: Last before Show Latest Save Cancel

Filter: contains Go Clear Filter Show records

Server	Type	User	Service Name	Login	Date and Time ▼
192.168.5.217	RADIUS		Avenda Wireless Service	ACCEPT	2010/07/26 13:31:35
192.168.5.217	RADIUS			REJECT	2010/07/26 13:30:11
192.168.5.217	RADIUS		Avenda Wired Service	ACCEPT	2010/07/26 13:27:29
192.168.5.217	RADIUS		Avenda Wired Service	ACCEPT	2010/07/26 13:19:33
192.168.5.217	RADIUS		Avenda Wired Service	ACCEPT	2010/07/26 13:11:45
192.168.5.217	RADIUS		Handheld_a802.1X Wireless Service	REJECT	2010/07/26 13:04:05
192.168.5.217	RADIUS		Handheld_a802.1X Wireless Service	ACCEPT	2010/07/26 12:58:17
192.168.5.217	RADIUS		Handheld_a802.1X Wireless Service	REJECT	2010/07/26 12:58:08
192.168.5.217	RADIUS		Avenda Wired Service	ACCEPT	2010/07/26 12:57:28
192.168.5.217	RADIUS		Handheld_a802.1X Wireless Service	REJECT	2010/07/26 12:52:22
192.168.5.217	RADIUS		Avenda Wired Service	ACCEPT	2010/07/26 12:49:31
192.168.5.217	RADIUS		Avenda Wired Service	ACCEPT	2010/07/26 12:41:43
192.168.5.217	RADIUS		Avenda Wired Service	ACCEPT	2010/07/26 12:27:27
192.168.5.217	RADIUS		Avenda Wired Service	ACCEPT	2010/07/26 12:19:30
192.168.5.217	RADIUS		Avenda Wired Service	ACCEPT	2010/07/26 12:11:41
192.168.5.217	RADIUS		Avenda Wireless Service	ACCEPT	2010/07/26 12:00:34
192.168.5.217	RADIUS		Handheld_a802.1X Wireless Service	ACCEPT	2010/07/26 12:00:25
192.168.5.217	RADIUS		Avenda Wired Service	ACCEPT	2010/07/26 11:57:26
192.168.5.217	RADIUS		Avenda Wireless Service	REJECT	2010/07/26 11:55:54
192.168.5.217	RADIUS		Avenda Wired Service	ACCEPT	2010/07/26 11:49:29

Showing 1-20 of more than 20 records ▶

Table 3-1 Access Tracker Display Parameters

Container	Description
Select Server	Select server for which to display dashboard data. Select All to display transactions from all nodes in the Policy Manager cluster.
Auto Refresh	Click to toggle On/Off.
Select Filter	Select filter to constrain data display.
	Modify the currently displayed data filter
Add	Go to Data Filters page to create a new data filter.
	

Container	Description
Select Date Range	Select the number of days prior to the configured date for which Access Tracker data is to be displayed. Valid number of days is 1 day to a week.
Show Latest	Sets the date to Today in the previous step to Today.
Save/Cancel	Save or cancel edit operation

To display a specific set of records, use the simple filter controls. The filter controls enable you to filter by Protocol Type, User, Service Name, MAC Address, or Status. Note that this filter is applied on top of the display constraints configured previously (See table above).

Table 3-2 Access Tracker Simple Filter

Container	Description
Filter	Select a filter type from the dropdown list: Type, User, Service Name, MAC Address, Login
contains	Enter the string to search for.
Clear Filter	Clear the currently applied filter and show all entries.
Show n Records	Show 10, 20, 50 or 100 rows. Once selected, this setting is saved and available in subsequent logins.

Table 3-3 Access Tracker Session Types

Container	Description
RADIUS	All RADIUS transactions (802.1X, MAC-Auth, generic RADIUS)
TACACS+	All TACACS+ transactions
WebAuth	Web authentication transactions (Dissolvable Agent, OnGuard)
Application	All Aruba application authentications (Insight, GuestConnect, EdgeManager)

Viewing Session Details

To view details for a session, click on the row containing any entry. Policy Manager divides the view into multiple tabs. Depending on the type of authentication - RADIUS, WebAuth, TACACS, Application - the view displays different tabs.

- **Summary** - This tab shows a summary view of the transaction, including policies applied.

- **Input** - This tab shows protocol specific attributes that Policy Manager received in the transaction request; this includes authentication and posture details (if available). It also shows Compute Attributes, which are attributes that were derived from the request attributes. All of the attributes can be used in role mapping rules.
- **Output** - This tab shows the attributes that were sent to the network device and the (posture capable) endpoint.
- **Alerts** - This tab shows the reason for authentication or authorization failure.
- **Accounting** - This tab is only available for RADIUS sessions. This shows the RADIUS accounting details for the session, including reauthentication details.
- **Authorizations** - This tab is only available for TACACS+ sessions. This shows the commands entered at the network device, and the authorization status.
- **RADIUS CoA** - This tab is only available for RADIUS transactions for which a RADIUS Change of Authorization command was sent to the network device by Policy Manager. The view shows the RADIUS CoA actions sent to the network device in chronological order.

Table 3-4 Session Details Popup Actions

Container	Description
Change Status	<p>This button allows you to change the access control status of a session. This function is only available for RADIUS and WebAuth.</p> <ul style="list-style-type: none"> • Agent - This type of control is available for a session where the endpoint has the OnGuard Agent installed. Actions allowed are: Bounce, Send Message and tagging the status of the endpoint as Disabled or Known. • SNMP - This type of control is available for any session for which Policy Manager has the switch- and port-level information associated with the MAC address of the endpoint. Policy Manager bounces the switch port to which the endpoint is attached, via SNMP. Note that, for this type of control, SNMP read and write community strings have to be configured for the network device; furthermore, Policy Manager must be configured as an SNMP trap receiver to receive link up/down traps. • RADIUS CoA - This type of control is available for any session where access was previously controlled by a RADIUS transaction. Note that the network device must be RADIUS CoA capable, and RADIUS CoA must be enabled when you configure the network device in Policy Manager. The actions available depend on the type of device. The Disconnect (or Terminate Session) action is supported by all devices. Some devices support setting a session timeout, changing the VLAN for the session, applying an ACL, etc.
Export	Export this transaction and download as a compressed (.zip extension) file. The compressed file contains the session-specific logs, the policy XML for the transaction, and a text file containing the Access Tracker session details.
Show Logs	Show logs of this session. Error messages are color coded in red. Warning messages are color coded in orange.
Close	RADIUS response attributes sent to the device

Accounting


The Accounting display provides a dynamic report of accesses (as reported by the network access device by means of RADIUS/TACACS+ accounting records), at: **Monitoring & Reporting > Live Monitoring > Accounting**.


Figure 3-2 Accounting (Edit Mode)

Monitoring & Reporting » Live Monitoring » Accounting

Accounting

Select Server:

Select Filter:  Add

Select Date Range: Last before  Show Latest

Filter: contains Show records

Server	Protocol	User	Access Device	Start Time ▼
192.168.5.217	RADIUS	[redacted]	192.168.5.219:1	Jul 26, 2010 14:27:49 PDT
192.168.5.217	RADIUS	[redacted]	192.168.5.219:1	Jul 26, 2010 14:27:45 PDT
192.168.5.217	RADIUS	[redacted]	192.168.5.219:1	Jul 26, 2010 14:25:36 PDT
192.168.5.217	RADIUS	[redacted]	192.168.5.219:1	Jul 26, 2010 14:00:29 PDT
192.168.5.217	RADIUS	[redacted]	192.168.5.219:1	Jul 26, 2010 13:50:43 PDT
192.168.5.217	RADIUS	[redacted]	192.168.5.219:1	Jul 26, 2010 13:45:29 PDT
192.168.5.217	RADIUS	[redacted]	192.168.5.219:1	Jul 26, 2010 13:31:38 PDT
192.168.5.217	RADIUS	[redacted]	192.168.5.219:1	Jul 26, 2010 13:31:17 PDT
192.168.5.217	RADIUS	[redacted]	192.168.5.219:1	Jul 26, 2010 13:18:42 PDT
192.168.5.217	RADIUS	[redacted]	192.168.5.219:1	Jul 26, 2010 12:55:36 PDT




Showing 1-10 of more than 10 records 

Table 3-5 Accounting

Container	Description
Select Server	Select server for which to display dashboard data.
Select Filter	Select filter to constrain data display.
	Modify the currently displayed data filter
Add	Go to Data Filters page to create a new data filter.
	
Select Date Range	Select the number of days prior to the configured date for which Accounting data is to be displayed. Valid number of days is 1 day to a week.
Show Latest	Sets the date to Today in the previous step to Today.
Save/Cancel	Save or cancel edit operation
Show <n> records	Show 10, 20, 50 or 100 rows. Once selected, this setting is saved and available in subsequent logins.

Click on any row to display the corresponding Accounting Record Details.

Figure 3-3 RADIUS Accounting Record Details (Summary tab)

Accounting Record Details

Summary Auth Sessions Utilization Details

Session ID:	R0000003e-01-49b57348
Account Session ID:	192.168.5.214 <small>accountid</small> 11/14/93 08:48:26 01B20000
Start Timestamp:	Mar 09, 2009 10:51:30 PDT
End Timestamp:	Still Active
Status:	Active
Username:	<small>username</small>
Termination Cause:	-
Service Type:	Framed-User

Network Details -

NAS IP Address:	192.168.5.214:50101
NAS Port Type:	Ethernet
Calling Station ID:	00-14-38-1A-74-56
Called Station ID:	00-19-56-ED-43-01
Framed IP Address:	-
Account Auth:	RADIUS

Close

Figure 3-4 RADIUS Accounting Record Details (Auth Sessions tab)

Accounting Record Details

Summary **Auth Sessions** Utilization Details

Number of Authentication Sessions: 3

Authentication Sessions Details

SessionId	Type	Time Stamp
R00000033-01-49b5571f	initial	Mar 09, 2009 10:51:30 PDT
R00000037-01-49b56533	re-auth	Mar 09, 2009 11:51:35 PDT
R0000003e-01-49b57348	re-auth	Mar 09, 2009 12:51:38 PDT

Close

Figure 3-5 RADIUS Accounting Record Details (Utilization tab)

Accounting Record Details			
Summary	Auth Sessions	Utilization	Details
Active Time:	9027 Sec		
Account Delay Time:	-		
Account Input Octets :	2647001		
Account Output Octets :	11540248		
Account Input Packets :	14200		
Account Output Packets :	37866		

Close

Figure 3-6 RADIUS Accounting Record Details (Details tab)

Accounting Record Details			
Summary	Auth Sessions	Utilization	Details
Tunnel-Private-Group-Id5		Mar 06, 2009 14:26:49 PST	
For Session Id R0000000d-01-49b1b0a5 at Mar 06, 2009 15:24:21 PST			
NAS-Identifier	avenda-wapcontroller	Mar 06, 2009 15:24:21 PST	
Airespace-Wlan-Id	1	Mar 06, 2009 15:24:21 PST	
Tunnel-Type	VLAN	Mar 06, 2009 15:24:21 PST	
Tunnel-Medium-Type	IEEE-802	Mar 06, 2009 15:24:21 PST	
Tunnel-Private-Group-Id5		Mar 06, 2009 15:24:21 PST	
For Session Id R00000011-01-49b1be22 at Mar 06, 2009 16:21:54 PST			
NAS-Identifier	avenda-wapcontroller	Mar 06, 2009 16:21:54 PST	
Airespace-Wlan-Id	1	Mar 06, 2009 16:21:54 PST	
Tunnel-Type	VLAN	Mar 06, 2009 16:21:54 PST	
Tunnel-Medium-Type	IEEE-802	Mar 06, 2009 16:21:54 PST	
Tunnel-Private-Group-Id5		Mar 06, 2009 16:21:54 PST	
For Session Id R00000015-01-49b1cb9f at Mar 06, 2009 17:19:27 PST			
NAS-Identifier	avenda-wapcontroller	Mar 06, 2009 17:19:27 PST	

Close

Table 3-6 RADIUS Accounting Record Details

Tab	Container	Description
Summary	Session ID	Policy Manager session identifier (you can correlate this record with a record in Access Tracker)
	Account Session ID	A unique ID for this accounting record
	Start and End Timestamp	Start and end time of the session
	Status	Current connection status of the session
	Username	Username associated with this record
	Termination Cause	The reason for termination of this session
	Service Type	The value of the standard RADIUS attribute ServiceType
	NAS IP Address	IP address of the network device
	NAS Port Type	The access method - For example, Ethernet, 802.11 Wireless, etc.
	Calling Station ID	In most use cases supported by Policy Manager this is the MAC address of the client
	Called Station ID	MAC Address of the network device
	Framed IP Address	IP Address of the client (if available)
	Account Auth	Type of authentication - In this case, RADIUS.
Auth Sessions	Session ID	Policy Manager session ID
	Type	Initial authentication or a re-authentication
	Time Stamp	When the event occurred
Utilization	Active Time	How long the session was active
	Account Delay Time	How many seconds the network device has been trying to send this record for (subtract from record time stamp to arrive at the time this record was actually generated by the device)
	Account Input Octets	Octets sent and received from the device port over the course of the session
	Account Output Octets	
	Account Input Packets	Packets sent and received from the device port over the course of the session
	Account Output Packets	
Details	Shows details of RADIUS attributes sent and received from the network device during the initial authentication and subsequent reauthentications (each section in the details tab corresponds to a “session” in Policy Manager.	

Figure 3-7 TACACS+ Accounting Record Details (Request tab)

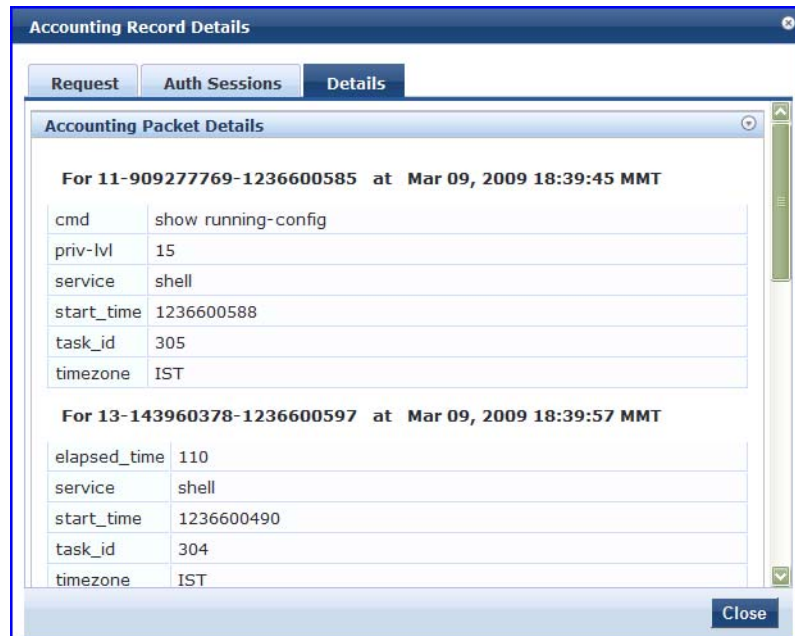
Accounting Record Details		
Request	Auth Sessions	Details
Session ID:	23-2590462887-1236600700	
User Session ID:	T00000002-04-49b506f1	
Start Timestamp:	Mar 09, 2009 18:39:45 MMT	
End Timestamp:	Mar 09, 2009 18:41:40 MMT	
User Name:	james	
Client IP :	192.168.12.27:tty2	
Remote IP:	192.168.12.101	
Flags:	4	
Privilege Level:	1	
Authentication Method:	AUTHEN_METH_TACACSPLUS	
Authentication Type:	AUTHEN_TYPE_ASCII	
Authentication Service:		

Close

Figure 3-8 TACACS+ Accounting Record Details (Auth Sessions tab)

Accounting Record Details		
Request	Auth Sessions	Details
Number of Authentication Sessions: 5		
Authentication Sessions Details		
SessionId	Type	Time Stamp
11-909277769-1236600585	initial	Mar 09, 2009 18:39:45 MMT
13-143960378-1236600597	authz	Mar 09, 2009 18:39:57 MMT
17-4035598695-1236600653	authz	Mar 09, 2009 18:40:53 MMT
21-2720020714-1236600682	authz	Mar 09, 2009 18:41:22 MMT
23-2590462887-1236600700	authz	Mar 09, 2009 18:41:40 MMT

Close

Figure 3-9 TACACS+ Accounting Record Details (Details tab)**Table 3-7 TACACS+ Accounting Record Details**

Tab	Container	Description
Request	Session ID	Unique ID associated with a request
	User Session ID	A session ID that correlates authentication, authorization and accounting records
	Start and End Timestamp	Start and end time of the session
	Username	Username associated with this record
	Client IP	The IP address and tty of the device interface
	Remote IP	IP address from which Admin is logged in
	Flags	Identifier corresponding to start, stop or update accounting record
	Privilege Level	Privilege level of administrator: 1 (lowest) to 15 (highest).
	Authentication Method	
	Authentication Type	
	Authentication Service	
Auth Sessions	Number of Authentication Sessions	Total number of authentications (always 1) and authorizations in this session
	Authentication Session Details	For each request ID, denotes whether it is an authentication or authorization request, and the time at which the request was sent

Tab	Container	Description
Details		For each authorization request, shows: cmd (command typed), priv-lvl (privilege level of the administrator executing the command), service (shell), etc.

OnGuard Activity

The OnGuard Activity screen shows the realtime status of all endpoints that have Aruba OnGuard persistent or dissolvable agent, at: **Monitoring & Reporting > Live Monitoring > OnGuard Activity**. This screen also presents configuration tools to bounce an endpoint and to send unicast or broadcast messages to all endpoints running the OnGuard agent. Note that bouncing of endpoints will only work with endpoints running the persistent agent.

Figure 3-10 OnGuard Activity

Monitoring & Reporting » Live Monitoring » Endpoint Activity

Endpoint Activity Nov 09, 2010 12:24:25 PST

Filter: User contains Go Clear Filter Show 10 records

#	<input type="checkbox"/>	User ▲	Host MAC	Host IP	Host OS	Status	Date and Time
1.	<input checked="" type="checkbox"/>		002312016c39	192.168.5.187	Mac OS X 10.6.4	●	2010/11/08 18:30:32
2.	<input type="checkbox"/>		001a927f8fcf	192.168.5.192	Windows 7 6.1	●	2010/11/08 21:48:26

Showing 1-2 of 2

Auto Refresh
Bounce Client (using SNMP)
Broadcast Message

Send Message Bounce

Table 3-8 OnGuard Activity

Container	Description
Auto Refresh	Toggle auto-refresh. If this is turned on, all endpoint activities are refreshed automatically.

Figure 3-11 Bounce Client (using SNMP)

Bounce Client (using SNMP)

Client IP or MAC Address: 002312016c39 Go

Host MAC:

Host IP:

Switch IP Address:

Switch Port:

Description:

Status:

Added by:

Bounce Cancel

Container	Description
Bounce Client (using SNMP)	<p>Given the MAC or IP address of the endpoint, perform a bounce operation (via SNMP) on the switch port to which the endpoint is connected. This feature only works with wired Ethernet switches.</p> <p>Note that, for this operation to work:</p> <ul style="list-style-type: none"> • The network device must be added to Policy Manager, and SNMP read and write parameters must be configured. • SNMP traps (link up and/or MAC notification) have to be enabled on the switch port. • In order to specify the IP address of the endpoint to bounce, the DHCP snooper service on Policy Manager must receive DHCP packets from the endpoint. Refer to your network device documentation to find out how to configure IP helper address.

Figure 3-12 Broadcast Message

Broadcast Message	Send a message to all active endpoints
Send Message	Send a message to the selected endpoints.

Figure 3-13 Bounce

Container	Description
Bounce	<p>Initiate a bounce on the managed interface on the endpoint.</p> <ul style="list-style-type: none"> • Display Message - An optional message to display on the endpoint (via the OnGuard interface). • Web link - An optional clickable URL that is displayed along with the Display Message. • Endpoint Status - <p>No change - No change is made to the status of the endpoint. The existing status of Known, Unknown or Disabled continues to be applied. Access control is granted or denied based on the endpoint's existing status.</p> <p>Allow network access - Always allow network access. Whitelist this endpoint. Note that this action just sets the status of the endpoint as "Known". You need to configure Enforcement Policy Rules to allow access to "Known" endpoints.</p> <p>Block network access - Always block network access. Blacklist this endpoint. Note that this action just sets the status of the endpoint as "Disabled". You need to configure Enforcement Policy Rules to allow access to "Disabled" endpoints.</p> <p>This action results in tags being created for the specified endpoint in the Endpoints table (Configuration > Identity > Endpoints). One or more of the following tags are created: Disabled by, Disabled Reason, Enabled by, Enabled Reason, Info URL.</p>

Analysis & Trending

Monitoring & Reporting > Live Monitoring > Analysis & Trending

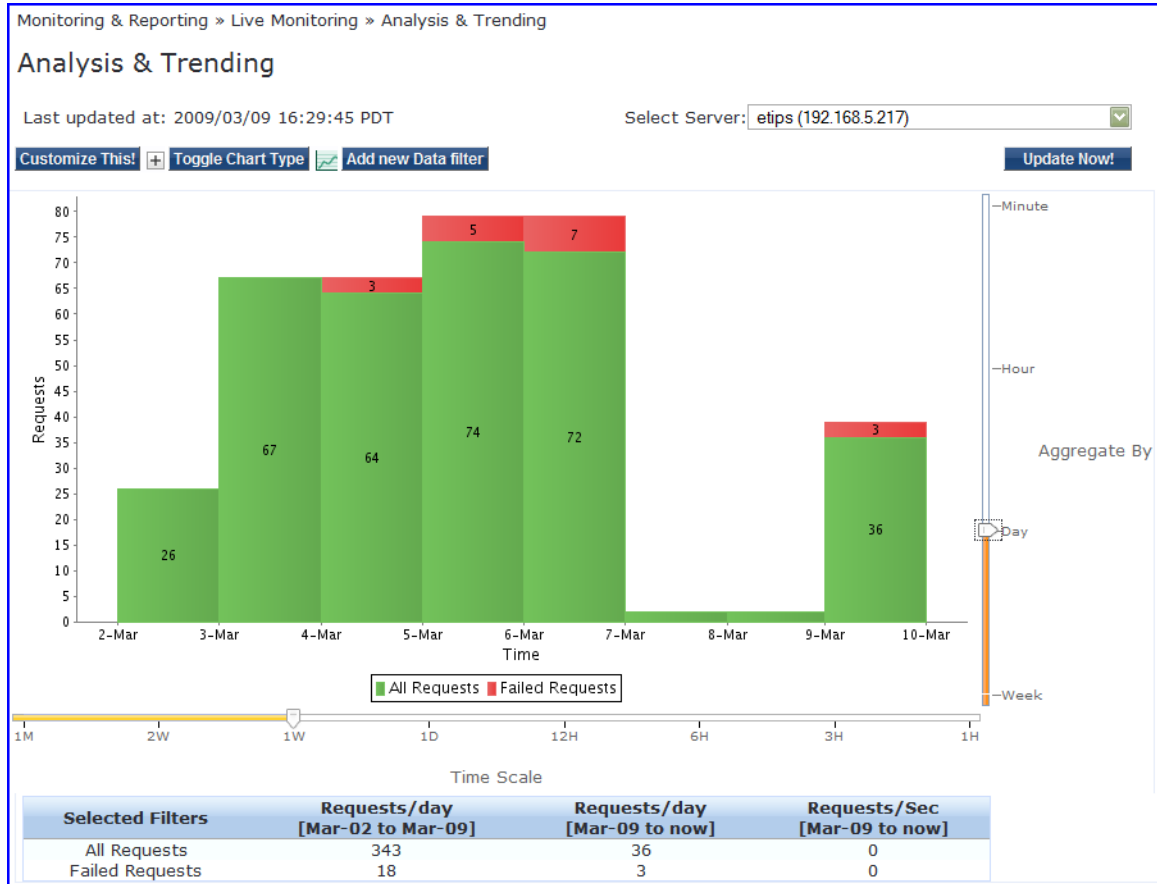
Analysis and Trending Page Displays monthly, bi-weekly, weekly, daily, or 12-hourly, 6-hourly, 3-hourly or hourly quantity of requests for the subset of components included in the selected filters. The data can be aggregated by minute, hour, day or week.

The summary table at the bottom shows the per-filter count for the aggregated data.

Each bar (corresponding to each filter) in the bar graph is clickable. Clicking on the bar drills down into the ["Access Tracker"](#) (page 13), showing session data for

that time slice (and for that many requests). Similarly, for a line graph, clicking on the circle (corresponding to each plotted point in the graph) drills down into Access Tracker.

Figure 3-14



- To add additional filters, refer to “Data Filters” (page 38).
- **Select Server** Select a node from the cluster for which data is to be displayed.
- **Update Now**- Click on this button to update the display with the latest available data.
- **Customize This**- Click on this link to customize the display by adding filters (up to a maximum of 4 filters)
- **Toggle Chart Type**- Click on this link to toggle chart display between line and bar type.
- **Add New Data Filter** - Click on this to add a new data filter in the global filter list.

System Monitor

Monitoring & Reporting > Live Monitoring > System Monitor

- **Select Server** Select a node from the cluster for which data is to be displayed.
- **Update Now**- Click on this button to update the display with the latest available data.

The **System Monitor Page** displays two tabs:

- **System Monitor.** For the selected server, provides load statistics, including CPU, memory, swap memory, physical disk space, and swap disk space:

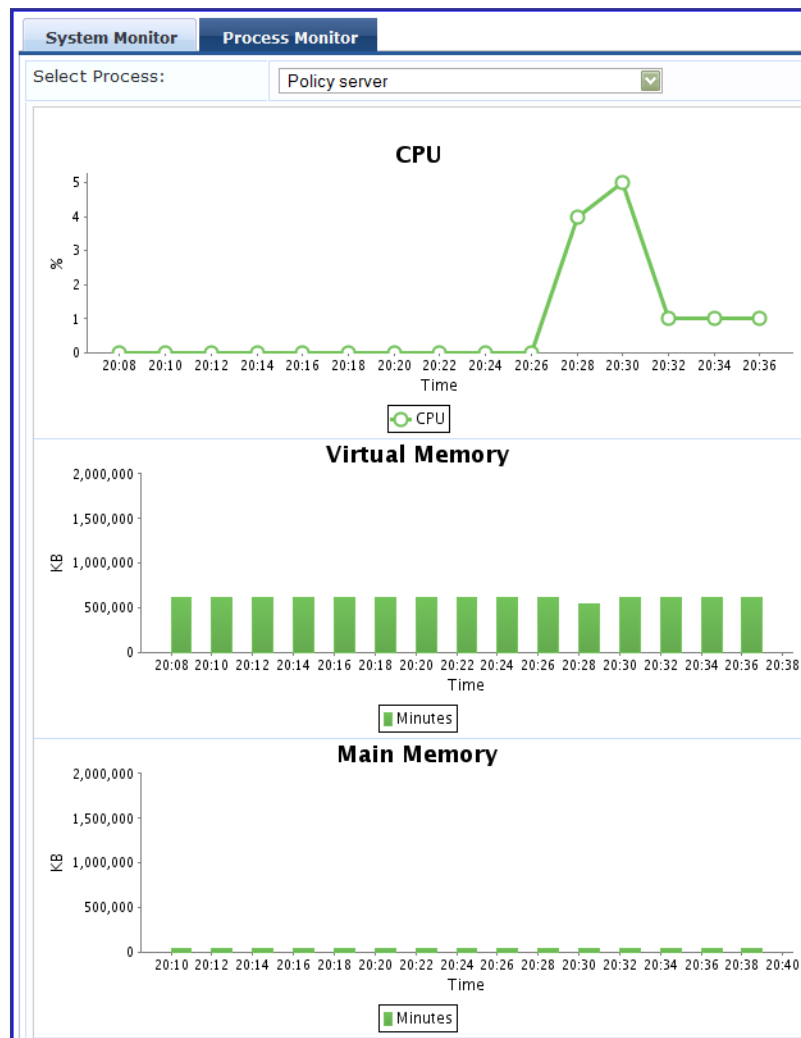
Figure 3-15 System Monitor Graphs



- **Process Monitor.** For the selected server and process, provides critical usage statistics, including CPU, Virtual Memory, and Main Memory. Use

Select **Process** to select the process for which you want to see the usage statistics.

Figure 3-16 Process Monitor Graphs



Activity Reports

The Activity Reports provide a periodic report of system activity, in PDF or HTML format, at: **Monitoring & Reporting > Activity Reports**. Policy Manager comes preconfigured with seven reports shown below:

Figure 3-17 Activity Reports

Monitoring & Reporting » Activity Reports

Activity Reports

Add Report

Import Reports

Export Reports

Download Store

Filter:

Name

 contains

Go

Clear Filter

Show

10

 records

#	<input type="checkbox"/>	Name ▲	Description	Report Time	View	Status
1.	<input type="checkbox"/>	Failed Authentications	Failed Authentications Report	Jun 25, 2009 21:51:19 UTC	<div><div></div> CSV</div>	Disabled
2.	<input type="checkbox"/>	Guest User Access	Guest User Access Report	Jun 25, 2009 21:51:33 UTC	<div><div></div> PDF <div></div> HTML</div>	Disabled
3.	<input type="checkbox"/>	Logged In Users	Logged in users report	Jun 25, 2009 21:51:40 UTC	<div><div></div> PDF <div></div> HTML</div>	Disabled
4.	<input type="checkbox"/>	Radius Accounting	Radius Accounting Report	Jun 25, 2009 21:51:39 UTC	<div><div></div> CSV</div>	Disabled
5.	<input type="checkbox"/>	Tacacs Access	TACACS Access Report	Jun 25, 2009 21:51:41 UTC	<div><div></div> PDF <div></div> HTML</div>	Disabled
6.	<input type="checkbox"/>	Tacacs Accounting	TACACS Accounting Report	Jun 25, 2009 21:51:44 UTC	<div><div></div> PDF <div></div> HTML</div>	Disabled
7.	<input type="checkbox"/>	Web Authentication	Web Authentication Report	Jun 25, 2009 21:51:48 UTC	<div><div></div> PDF <div></div> HTML</div>	Disabled

Showing 1-7 of 7

Run

Copy

Export

Delete

Table 3-9 Activity Reports

Container	Description
Add Report	Click to open the Add Report wizard
Import Reports	Click to open the Import Report popup
Export Reports	Click to open the Export Report popup
Download Store	Go to the “ Local Shared Folders ” (page 260) that contains the generated reports
Run	Run the selected report. Note: Once the report is run, the generated reports are placed in the “ Local Shared Folders ” (page 260).
Copy	Copy the selected report
Export	Click to open the Export popup to export selected reports
Delete	Click to delete the selected (checkbox on left) Activity Report(s).

Add Report

To add a report, configure its description and format in the **Report** tab and its content in the **Data** tab.

Figure 3-18 Report Tab

Monitoring & Reporting » Activity Reports » Edit - Logged In Users

Activity Reports - Logged In Users

Summary

Report

Data

Name:	Logged In Users
Description:	Logged in users report
Status:	Enabled
Schedule:	Daily <input type="button" value="v"/> At 1 AM <input type="button" value="v"/>
Report Customizations:	
Output Format:	<input checked="" type="radio"/> PDF <input type="radio"/> CSV
Title:	Report of Logged in Users
Footer:	Company Confidential

Back to Activity Reports

Disable
 Copy
 Save & Run
 Save
 Cancel

Table 3-10 Report Tab

Container	Description
Name	Name and description (freeform).
Description	
Status	Enabled or disabled
Schedule	How often and when the report generation is done.
Output Format	Output as a PDF for presentation, or as CSV for sorting and manipulation in a spreadsheet environment.
Title/Footer	Report title and footer (freeform)

Figure 3-19 Data Tab

Table 3-11 Data Tab

Container	Description
Data Filter	Specify the data filter. The data filter limits the type of records shown in the report
Data From Servers	Select the node in the cluster from which to collect reporting data
Select Report Fields	<p>This provides a way to limit the type of columns shown.</p> <p>There are Predfined Field Groups, which are column names grouped together for quick addition to the report.</p> <p>Additional Fields are available to add to the reports. You can select the type of attributes (which are the different table columns available in the session database). Policy Manager populates these column names by extracting the column names from existing sessions in the session database.</p> <p>For PDF output, you may select maximum of eight fields.</p>
Add/Remove/Up/Down	Use the Add button to add fields from Additional Fields to the Selected Fields table. Use the Remove button to remove fields from the Selected Fields table. Use the Up/Down buttons to move the fields up or down.

Container	Description
Enable Grouping	Enable to specify data grouping frequency: <i>daily</i> or <i>hourly</i> for reports scheduled to run daily; <i>daily</i> , <i>weekly</i> or <i>hourly</i> for reports scheduled to run weekly; <i>monthly</i> , <i>weekly</i> or <i>daily</i> for reports scheduled to run monthly
Disable	Disable this report. Report generation is performed on a periodic basis.
Copy	Make a copy of this report. The newly created report is saved with the name prefixed with “Copy_of_”.
Save and Run	Commit report parameters and generate the report immediately (without waiting for the scheduled time)
Save	Click Save to commit the report parameters.

Import Reports

Monitoring & Reporting > Activity Reports > Import Report (link).

Figure 3-20 Import Reports

Table 3-12 Import Reports

Container	Description
Select file	Browse to select name of the report file.
Enter secret for the file (if any)	If the report was exported using a secret password, enter that password here.
Import/Cancel	Commit or dismiss import.

Export Reports

Monitoring & Reporting > Activity Reports > Export Report (link).

To *export all reports*, click **Export Activity Report** (link). Your browser will display its normal **Save As** dialog, in which to enter the name of the XML file to contain the export.

Exports

Monitoring & Reporting > Activity Reports > Export (link).

To *export just one report*, select it (checkbox at left) and click **Export**. Your browser will display its normal **Save As** dialog, in which to enter the name of the XML file to contain the export.

Audit Viewer

The Audit Viewer display provides a dynamic report of Actions, filterable by Action, Name and Category (of policy component), and User, at: **Monitoring & Reporting > Audit Viewer**.

Figure 3-21 Audit Viewer

Monitoring & Reporting > Audit Viewer

Audit Viewer

Filter: Action contains Go Clear Filter Show 20 records

#	Action	Name	Category	User	Timestamp ▾
41.	ADD	Logged-in Users	Activity Report	Super Admin	Feb 05, 2009 15:05:39 PST
42.	MODIFY	Avenda Guest Portal	Guest Page Config	Super Admin	Feb 05, 2009 14:19:50 PST
43.	MODIFY	Avenda Guest Portal	Guest Page Config	Super Admin	Feb 05, 2009 14:19:49 PST
44.	MODIFY	Avenda Guest Portal	Guest Page Config	Super Admin	Feb 05, 2009 14:19:14 PST
45.	MODIFY	Avenda Guest Portal	Guest Page Config	Super Admin	Feb 05, 2009 14:19:06 PST
46.	ADD	Jonathan	Local User	joe	Feb 04, 2009 15:44:10 PST
47.	ADD	David D	Local User	Super Admin	Feb 04, 2009 14:52:03 PST
48.	REMOVE	David D	Local User	joe	Feb 04, 2009 14:49:36 PST
49.	ADD	Xirus Array	Network Device	Super Admin	Feb 03, 2009 17:41:27 PST
50.	MODIFY	Entertainment-Xirus ..	Service	Super Admin	Feb 03, 2009 17:40:52 PST
51.	MODIFY	Entertainment-Xirus ..	Service	Super Admin	Feb 03, 2009 17:37:59 PST
52.	MODIFY	Entertainment-Xirus ..	Enforcement Policy	Super Admin	Feb 03, 2009 17:35:18 PST
53.	ADD	Entertainment-Xirus ..	Radius Profile	Super Admin	Feb 03, 2009 17:34:42 PST
54.	ADD	Entertainment-Xirus ..	Service	Super Admin	Feb 03, 2009 17:33:49 PST
55.	ADD	Entertainment-Xirus ..	Enforcement Policy	Super Admin	Feb 03, 2009 17:33:42 PST
56.	ADD	David D	Local User	joe	Feb 03, 2009 17:23:49 PST
57.	MODIFY	joe	Admin User	Super Admin	Feb 03, 2009 17:22:57 PST
58.	MODIFY	192.168.5.217	Snmp Node Config	Super Admin	Jan 30, 2009 11:40:53 PST
59.	MODIFY	Handheld_a802.1X Wire..	Service	Super Admin	Jan 26, 2009 15:14:04 PST
60.	MODIFY	Handheld_Avenda_Wirel..	Enforcement Policy	Super Admin	Jan 26, 2009 15:13:00 PST

◀◀ Showing 41-60 of 446 ▶▶

Table 3-13 Audit Viewer

Container	Description
Select Filter	Select the filter by which to constrain the display of audit data.
Show <n> records	Show 10, 20, 50 or 100 rows. Once selected, this setting is saved and available in subsequent logins.

Click on any row to display the corresponding Audit Row Details:

- For **Add** Actions, a single popup displays, containing the new data.

Figure 3-22 Audit Row Details (Old Data tab)

Audit Row Details

Enforcement Policy - **Test_enf_Pol**

Enforcement Details

Name	Test_enf_Pol
Description	-
Type	RADIUS
Default Profile	-

Rules

Rules Evaluation Algorithm	evaluate-all
----------------------------	--------------

Conditions	Enforcement Profiles
1. (Tips:Role EQUALS Role_Engineer) AND (Tips:Posture EQUALS HEALTHY (0))	EMPLOYEE_VLAN
2. (Tips:Role EQUALS Senior_Mgmt) AND (Tips:Posture GREATER_THAN QUARANTINE (20))	EMPLOYEE_VLAN
3. (Tips:Role EQUALS eTIPS_Guest) AND (Date:Day-of-Week BELONGS_TO Monday, Tuesday, Wednesday,	WIRELESS_GUEST_NETWORK

Close

- For **Modify** Actions, a popup with three tabs displays, comparing the old data and the new.

Figure 3-23 Audit Row Details (Old Data tab)

Audit Row Details

Service Log Configuration - **Radius server**

Log Configuration

Node IP	192.168.5.96
Service	Radius server
Can override default log level	true
Syslog support	false

Modules

Module Name	Log Level
1. Radius Server	INFO

Close

Figure 3-24 Audit Row Details (New Data tab)

Audit Row Details

Old Data **New Data** Inline Difference

Service Log Configuration - Radius server

Log Configuration

Node IP	192.168.5.96
Service	Radius server
Can override default log level	true
Syslog support	false

Modules

Module Name	Log Level
1. Radius Server	DEBUG

Close

Figure 3-25 Audit Row Details (Inline Difference tab)

Audit Row Details

Old Data New Data **Inline Difference**

Modules

Module Name	Log Level
1. Radius Server	INFO DEBUG

Modified Added Deleted Moved up Moved down

Close

- For **Remove** Actions, a popup displays the removed data.

Event Viewer

The Event Viewer display provides a dynamic report of system level (not request-related) Events, filterable by Source, Level, Category, and Action, at: **Monitoring & Reporting > Event Viewer**.

Figure 3-26 Event Viewer

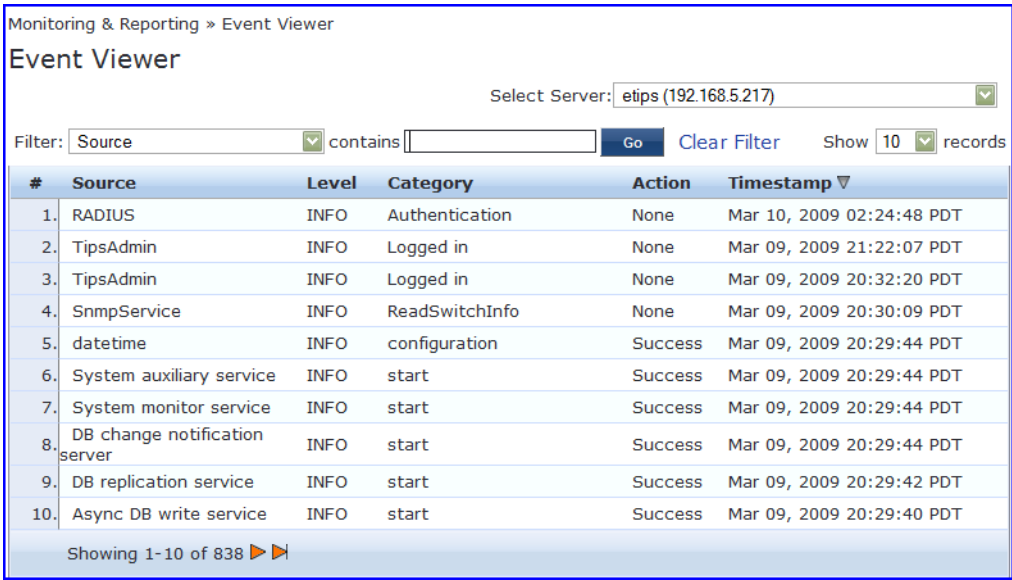
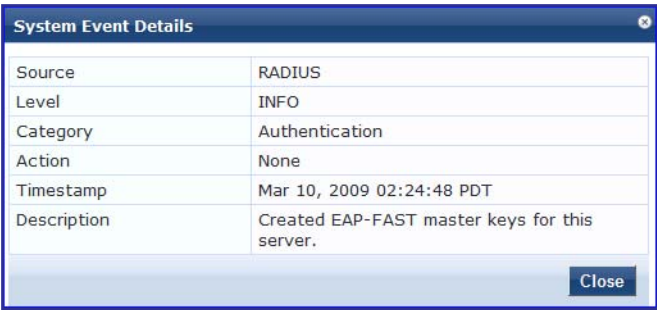


Table 3-14 Event Viewer

Container	Description
Select Server	Select the server for which to display accounting data.
Filter	Select the filter by which to constrain the display of accounting data.
Show <n> records	Show 10, 20, 50 or 100 rows. Once selected, this setting is saved and available in subsequent logins.

Click on any row to display the corresponding System Event Details.

Figure 3-27 System Event Details



Data Filters

The Data Filters provide a way to filter data (limit the number of rows of data shown by defining custom criteria or rules) that is shown in “Access Tracker”

(page 13), “Activity Reports” (page 30), “Syslog Export Filters” (page 266), “Analysis & Trending” (page 26) and “Accounting” (page 17) components in Policy Manager. It is available at: **Monitoring & Reporting> Data Filters**. Policy Manager comes preconfigured with nine data filters shown below:

Figure 3-28 Dashboard Filters

#	<input type="checkbox"/> Name ▲	Description
1.	<input type="checkbox"/> All Requests	All session log requests
2.	<input type="checkbox"/> Failed Requests	All Failed session log requests
3.	<input type="checkbox"/> Guest Access Requests	All Healthy session log requests
4.	<input type="checkbox"/> Healthy Requests	All Healthy session log requests
5.	<input type="checkbox"/> RADIUS Requests	All RADIUS requests
6.	<input type="checkbox"/> Successful Requests	All Successful session log requests
7.	<input type="checkbox"/> TACACS Requests	All TACACS requests
8.	<input type="checkbox"/> Unhealthy Requests	All Unhealthy session log requests
9.	<input type="checkbox"/> Webauth Requests	All Webauth Requests

Showing 1-9 of 9

Copy Export Delete

- All Requests - Shows all requests (without any rows filtered)
- Failed Requests - All authentication requests that were rejected or failed due to some reason; includes RADIUS, TACACS+ and Web Authentication results.
- Guest Access Requests - All requests - RADIUS or Web Authentication - where the user was assigned the built-in role called Guest.
- RADIUS Requests - All RADIUS requests
- Successful Requests - All authentication requests that were successful.
- TACACS Requests - All TACACS requests
- Unhealthy Requests - All requests that were not deemed healthy per policy.
- WebAuth Requests - All Web Authentication requests (requests originated from the Aruba Guest Portal).

Table 3-15 Data Filters

Container	Description
Add Filter	Click to open the Add Filter wizard.
Import Filters	Click to open the Import Filters popup.
Export Filters	Click to open the Export Filters popup. This exports all configured filters.
Copy	Copy the selected filters.
Export	Click to open the Export popup to export selected reports

Container	Description
Delete	Click to delete the selected filters.

Add Filter

To add a filter, configure its name and description in the **Filter** tab and its rules in the **Rules** tab.

Figure 3-29 Add Filter (Filter Tab)

Monitoring & Reporting » Data Filters » Add

Data Filters

Filter Rules Summary

Name: All RADIUS Request

Desc: Filter for all RADIUS requests

[Back to Data Filters](#) **Next >** **Save** **Cancel**

Table 3-16 Add Filter (Filter Tab)

Container	Description
Name	Name and description of the filter (freeform).
Description	

Figure 3-30 Add Filter (Rules Tab)

Monitoring & Reporting » Data Filters » Add

Data Filters

Filter Rules Summary

Rules Evaluation Algorithm: ☒ Select first match ☐ Select all matches

Data Filter Conditions:

Conditions

1. (Common Attributes:Protocol EQUALS RADIUS)

Add Rule **Move Up** **Move Down** **Edit Rule** **Remove Rule**

[Back to Data Filters](#) **Next >** **Save** **Cancel**

Table 3-17 Add Filter (Rules Tab)

Container	Description
Rule Evaluation Algorithm	Select first match is a logical OR operation of all the rules. Select all matches is a logical AND operation of all the rules.
Add Rule	Add a rule to the filter
Move Up/Down	Change the ordering of rules.
Edit/Remove Rule	Edit or remove a rule.
Save	Save this filter
Cancel	Cancel edit operation

When you click on **Add Rule** or **Edit Rule**, the **Data Filter Rules Editor** pops up.

Figure 3-31 Add Filter (Rules Tab) - Rules Editor
Table 3-18 Add Filter (Rules Tab) - Rules Editor

Container	Description
Matches	ANY matches one of the configured conditions. ALL matches all of the configured conditions.

Container	Description
Type	<p>This is the namespace for attributes.</p> <ul style="list-style-type: none"> • Common Attributes - These are attributes common to RADIUS, TACACS and WebAuth requests. • RADIUS Policy - Policy Manager policy objects assigned after evaluation of policies associated with RADIUS requests. Example: Auth Method, Auth Source, Enforcement Profiles • Web Authentication Policy - Policy Manager policy objects assigned after evaluation of policies associated with Web Authentication requests. Example: Auth Method, Auth Source, Enforcement Profiles • TACACS Policy - Policy Manager policy objects assigned after evaluation of policies associated with TACACS+ requests. Example: Command Privilege Level, Auth Source, Enforcement Profiles • RADIUS Accounting - RADIUS accounting attributes • TACACS Accounting - TACACS accounting attributes • Posture Request - Attributes related to posture request • RADIUS Request - Attributes that were sent in the RADIUS request • RADIUS Accounting Details - RADIUS accounting extended attributes • SNMP Response - Attributes sent in SNMP response • RADIUS Response - Attributes sent in RADIUS response • Posture Response - Attributes sent in posture response • Computed Attributes - Attributes computed by Policy Manager during policy evaluation.
Name	Name of the attributes corresponding to the selected namespace (Type).
Operator	A subset of string data type operators (EQUALS, NOT_EQUALS, CONTAINS, NOT_CONTAINS, EXISTS, BEGINS_WITH, ENDS_WITH, EQUALS_IGNORECASE, NOT_EXISTS).
Value	Value of the attribute.

Chapter 4: Policy Manager Policy Model

From the point of view of network device or other entities that need authentication and authorization services, Policy Manager appears as a RADIUS, TACACS+ or HTTP/S based Authentication server; however, its rich and extensible policy model allows it to broker security functions across a range of existing network infrastructure, identity stores, health/posture services and client technologies within the Enterprise.

Services Paradigm

Services are the highest level element in the Policy Manager policy model. They have two purposes:

- Unique **Categorization Rules** (per Service) enable Policy Manager to test Access Requests (“Requests”) against available Services to provide robust differentiation of requests by access method, location, or other network vendor-specific attributes.
Note: Policy Manager ships configured with a number of basic Service types. You can flesh out these Service types, copy them for use as templates, import other Service types from another implementation (from which you have previously exported them), or develop new Services from scratch.
- By wrapping a specific set of **Policy Components**, a Service can coordinate the flow of a request, from authentication, to role and health evaluation, to determination of enforcement parameters for network access.

Figure 4-1: Generic Policy Manager Service Flow of Control and Table 4-1: Policy Manager Service Components illustrate and describe the basic Policy Manager flow of control and its underlying architecture.

Figure 4-1 Generic Policy Manager Service Flow of Control

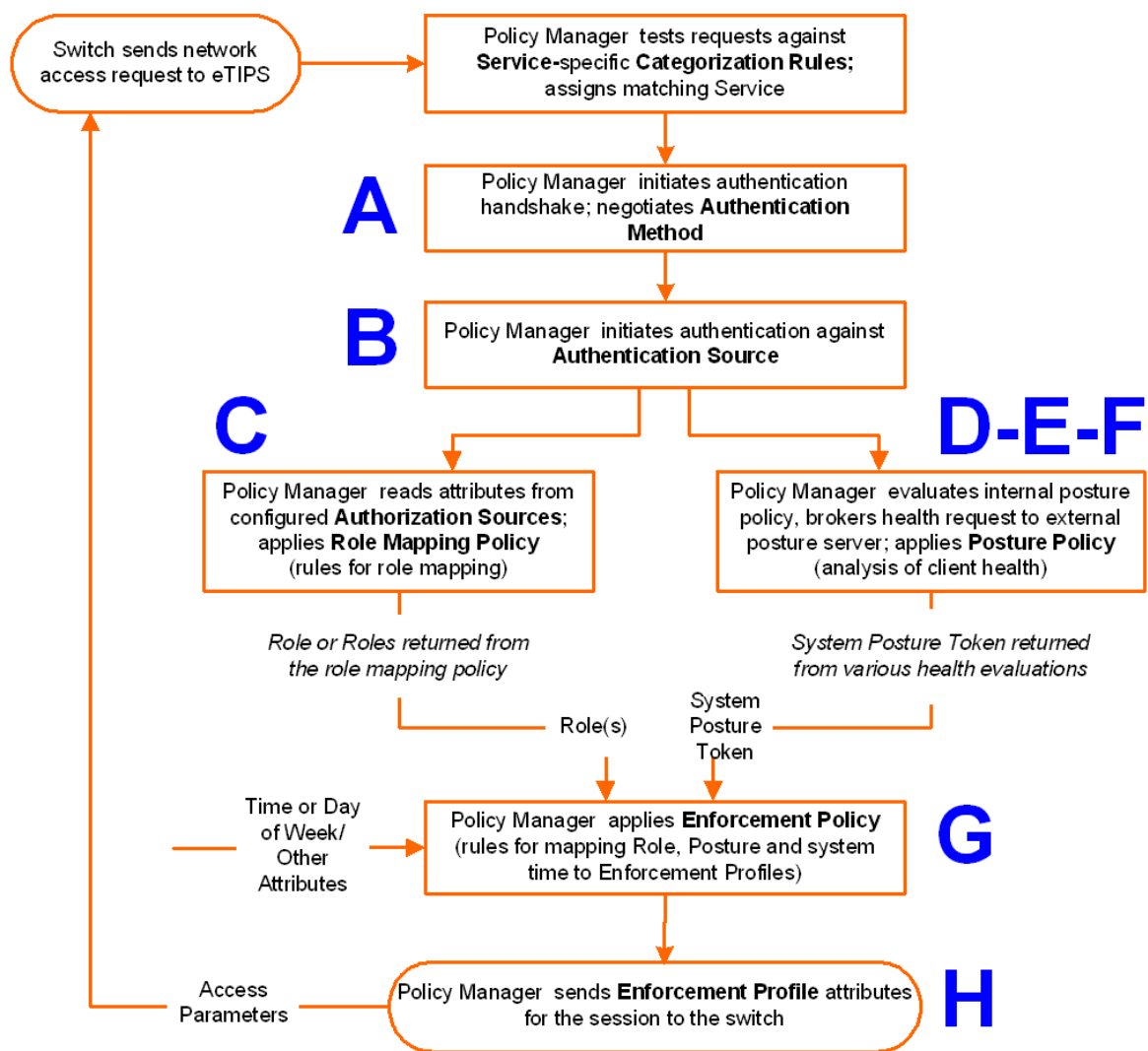


Table 4-1 Policy Manager Service Components

Component	Service: component ratio	Description
A - Authentication Method	Zero or more per service	<p>EAP or non-EAP method for client authentication. Policy Manager supports four broad classes of authentication methods:</p> <ul style="list-style-type: none"> • EAP, tunneled: PEAP, EAP-FAST, or EAP-TTLS. • EAP, non-tunneled: EAP-TLS or EAP-MD5. • Non-EAP, non-tunneled: CHAP, MS-CHAP, PAP, or [MAC AUTH]. <p>[MAC AUTH] must be used exclusively in a MAC-based Authentication Service. When the [MAC AUTH] method is selected, Policy Manager: (1) makes internal checks to verify that the request is indeed a <i>MAC Authentication</i> request (and not a spoofed request) and (2) makes sure that the MAC address of the device is present in the authentication source.</p> <p>Some Services (for example, <i>TACACS+</i>) contain internal authentication methods; in such cases, Policy Manager does not make this tab available.</p>
B - Authentication Source	Zero or more per service	<p>An Authentication Source is the identity repository against which Policy Manager verifies identity. It supports these Authentication Source types:</p> <ul style="list-style-type: none"> • Microsoft Active Directory • any LDAP compliant directory • RSA or other RADIUS-based token servers • SQL database, including the local user store. • Static Host Lists, in the case of MAC-based Authentication of managed devices.
C - Authorization Source	One or more per Authentication Source and zero or more per ser- vice	<p>An Authorization Source collects attributes for use in Role Mapping Rules. You specify the attributes you want to collect when you configure the authentication source. Policy Manager supports the following authorization source types:</p> <ul style="list-style-type: none"> • Microsoft Active Directory • any LDAP compliant directory • RSA or other RADIUS-based token servers • SQL database, including the local user store.

Component	Service: component ratio	Description
C - Role Mapping Policy	Zero or one per service	<p>Policy Manager evaluates Requests against Role Mapping Policy rules to match Clients to Role(s). All rules are evaluated and Policy Manager may return more than one Role. If no rules match, the request takes the configured Default Role.</p> <p>Some Services (for example, <i>MAC-based Authentication</i>) may handle role mapping differently:</p> <ul style="list-style-type: none"> For <i>MAC-based Authentication</i> Services, where role information is not available from an authentication source, an Audit Server can determine role by applying post-audit rules against the client attributes gathered during the audit.
D - Internal Posture Policies	Zero or more per service	An Internal Posture Policy tests Requests against internal Posture rules to assess health. Posture rule conditions can contain attributes present in vendor-specific posture dictionaries.
E - Posture Servers	Zero or more per service	<p>Posture servers evaluate client health based on specified vendor-specific posture credentials, typically posture credentials that cannot be evaluated internally by Policy Manager (that is, not by internal posture policies).</p> <p>Currently, Policy Manager supports two forms of posture server interfaces: , <i>RADIUS</i>, and <i>GAMEv2</i> posture servers.</p>
F - Audit Servers	Zero or more per service	<p>Audit servers evaluate the health of clients that do not have an installed agent, or which cannot respond to Policy Manager interactions. Audit servers typically operate in lieu of authentication methods, authentication sources, internal posture policies and posture server.</p> <p>In addition to returning posture tokens, Audit Servers can contain post-audit rules that map results from the audit into Roles.</p>
G - Enforcement Policy	One per service (mandatory)	Policy Manager tests Posture Tokens, Roles, system time and other contextual attributes against Enforcement Policy rules to return one or more matching Enforcement Policy Profiles (that define scope of access for the client).
H - Enforcement Profile	One or more per service	Enforcement Policy Profiles contain attributes that define a client's scope of access for the session. Policy Manager returns these Enforcement Profile attributes to the switch.

Viewing Existing Services

You can view all configured services in a list or drill down into individual services:

- **View and manipulate the list of current services.**

In the menu panel, click **Services** to view a list of services that you can filter by phrase or sort by order.

Figure 4-2 List of services with sorting tools

Filter by *Order* or *Name*, *Show All*, and/or *Reorder*

Summary	Service	Authentication	Roles	Posture	Audit	Enforcement
Name:	WIRELESS_SERVICE					
Description:	802.1x Wireless service					
Monitor Mode:	<input type="checkbox"/> Enable to monitor network access control without enforcement					
Type:	802.1x Wireless					
Status:	Enabled					
Service Categorization Rule						
Matches <input type="radio"/> ANY or <input checked="" type="radio"/> 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...						

- **Drill down to view details for an individual service.**

In the **Services** page, click the name of a Service to display its details.

Figure 4-3 Details for an individual service

Policy Manager displays all policy components under corresponding headers; to display as *editable* parameters for a particular component, click the header or corresponding tab.

Summary	Service	Authentication	Roles	Posture	Audit	Enforcement
Service:						
Name:	DOT1X_WIRED_SERVICE					
Description:	802.1x Wired service					
Monitor Mode:	Disabled					
Type:	802.1x Wired					
Status:	Enabled					
Service Categorization Rule						
Match ALL of the following conditions:						
Type	Name	Operator	Value			
1. Radius:IETF	NAS-Port-Type	EQUALS	Ethernet (15)			
2. Radius:IETF	Service-Type	BELONGS_TO	Login-User (1), Framed-User (2), Authenticate-Only (8)			
Authentication:						
Methods:	eTIPS_MSCHAP[MSCHAP]					
Sources:	eTIPS_Local_User_Repository[Local]					
Strip Username Rules:	-					
Back to Services Disable Copy Save Cancel						

Adding and Removing Services

You can add to the list of services by working from a copy, importing from another configuration, or creating a service from scratch:

- **Create a template by copying an existing service.**

In the **Services** page, click a service's checkbox, then click **Copy**.

- **Clone a service by import (of a previously exported named file from this or another configuration).**

In the **Services** page, click a service's checkbox, then click the **Export a Service** link and provide the output filepath. Later, you can import this service by clicking **Import a Service** and providing the filepath.

- **Create a new service that you will configure from scratch.**

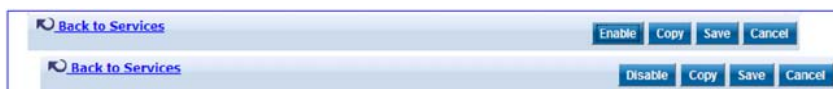
In the **Services** page, click **Add a Service**, then follow the configuration wizard from component to component by clicking **Next** as you complete each tab.

- **Remove a service.**

In the **Services** page, fill the checkbox for a service, then click the **Delete** button.

Note: You can also disable/enable a service from the service detail page by clicking **Disable/Enable** (lower right of page).

Figure 4-4 Disable/Enable toggle for a Policy Manager Service



Links to Use Cases and Configuration Instructions

For each of a Service's policy components that you can configure, the following table references an illustrative Use Case and detailed Configuration Instructions.

Table 4-2 Policy Component Use Cases and Configuration Instructions

Policy Component	Illustrative Use Cases	Configuration Instructions
Service	<ul style="list-style-type: none"> • "802.1X Wireless Use Case" (page 59). • "Aruba Web-Based Authentication Use Case" (page 67). • "MAC Authentication Use Case" (page 73). • "TACACS+ Use Case" (page 77). 	"Adding and Modifying Services" (page 98)

Policy Component	Illustrative Use Cases	Configuration Instructions
Authentication Method	<ul style="list-style-type: none"> • “802.1X Wireless Use Case” (page 59) demonstrates the principle of multiple authentication methods in a list. When Policy Manager initiates the authentication handshake, it tests the methods in priority order until one is accepted by the client. • “Aruba Web-Based Authentication Use Case” (page 67) has only a single authentication method, which is specifically designed for authentication of the request attributes received from the Aruba Web Portal. 	“Adding and Modifying Authentication Methods” (page 107)
Authentication Source	<ul style="list-style-type: none"> • “802.1X Wireless Use Case” (page 59) demonstrates the principle of multiple authentication sources in a list. Policy Manager tests the sources in priority order until the client can be authenticated. In this case Active Directory is listed first. • “Aruba Web-Based Authentication Use Case” (page 67) uses the local Policy Manager repository, as this is common practice among administrators configuring Guest Users. • “MAC Authentication Use Case” (page 73) uses a Static Host List for authentication of the MAC address sent by the switch as the device’s username. • “Single Port Use Case” (page 81) uses the local Policy Manager repository. Other authentication sources would also be fine. 	“Adding and Modifying Authentication Sources” (page 119)
Role Mapping	“802.1X Wireless Use Case” (page 59) has an explicit Role Mapping Policy that tests request attributes against a set of rules to assign a role.	<ul style="list-style-type: none"> • “Adding and Modifying Role Mapping Policies” (page 144) • “Adding and Modifying Roles” (page 147) • “Adding and Modifying Local Users” (page 149) • “Adding and Modifying Guest Users” (page 150) • “Adding and Modifying Static Host Lists” (page 155)

Policy Component	Illustrative Use Cases	Configuration Instructions
Posture Policy	“Aruba Web-Based Authentication Use Case” (page 67) uses an internal posture policy that evaluates the health of the originating client, based on attributes submitted with the request by the Aruba Web Portal, and returns a corresponding posture token.	“Adding and Modifying Posture Policies” (page 162)
Posture Server	“802.1X Wireless Use Case” (page 59) appends a third-party posture server to evaluate health policies based on vendor-specific posture credentials.	“Adding and Modifying Posture Servers” (page 189)
Audit Server	“MAC Authentication Use Case” (page 73), uses an Audit Server to provide port scanning for health.	“Configuring Audit Servers” (page 194)
Enforcement Policy and Profiles	All Use Cases have an assigned Enforcement Policy and corresponding Enforcement Rules.	<ul style="list-style-type: none"> • “Configuring Enforcement Profiles” (page 208) • “Configuring Enforcement Policies” (page 220)

Policy Simulation

Once the policies have been set up, the Policy Simulation utility can be used to evaluate these policies - before deployment. The Policy Simulation utility applies a set of request parameters as input against a given policy component and displays the outcome, at: **Configuration > Policy Simulation**.

The following types of simulations are supported:

- **Service Categorization** - A service categorization simulation allows you to specify a set of attributes in the RADIUS or Connection namespace and test which configured service the request will be categorized into. The request attributes that you specify represent the attributes sent in the simulated request.
- **Role Mapping** - Given the service name (and associated role mapping policy), the authentication source and the user name, the role mapping simulation maps the user into a role or set of roles. You can also use the role mapping simulation to test whether the specified authentication source is reachable.
- **Posture Validation** - A posture validation simulation allows you to specify a set of posture attributes in the posture namespace and test the posture status of the request. The posture attributes that you specify represent the attributes sent in the simulated request.

- **Audit** - An audit simulation allows you to specify an audit server (Nessus- or NMAP-based) and the IP address of the device you want to audit. An audit simulation triggers an audit on the specified device and displays the results.
- **Enforcement Policy** - Given the service name (and the associated enforcement policy), a role or a set of roles, the system posture status, and an optional date and time, the enforcement policy simulation evaluates the rules in the enforcement policy and displays the resulting enforcement profiles and their contents.
- **Chained Simulation** - Given the service name, authentication source, user name, and an optional date and time, the chained simulation combines the results of role mapping, posture validation and enforcement policy simulations and displays the corresponding results.

Figure 4-5 Policy Simulation

Table 4-3 Policy Simulation

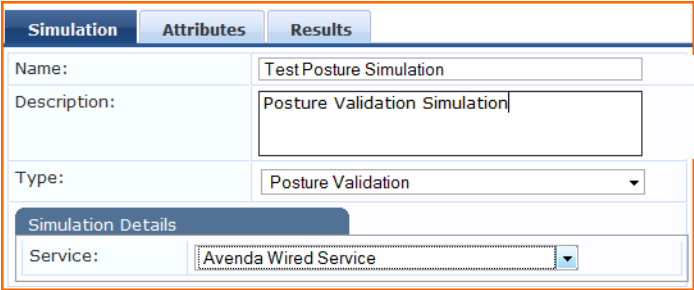
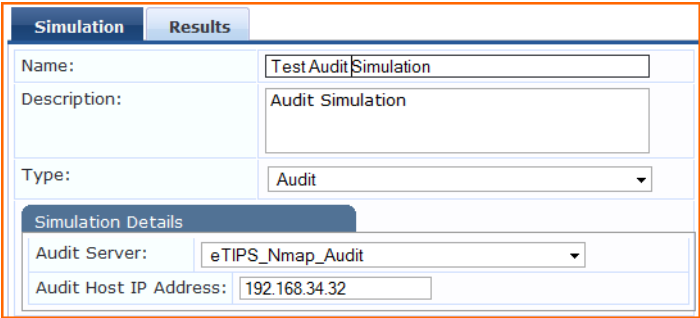
Container	Description
Add Simulation Test	Opens the Add Simulation Test page.
Import Simulations	Opens the Import Simulations popup.
Export Simulations	Opens the Export Simulations popup.
Filter	Select the filter by which to constrain the display of simulation data.
Copy	Make a copy the selected policy simulation. The copied simulation is renamed with a prefix of <i>Copy_Of_</i> .
Export	Opens the Export popup.
Delete	Click to delete a selected (checkbox on left) Policy Simulation.

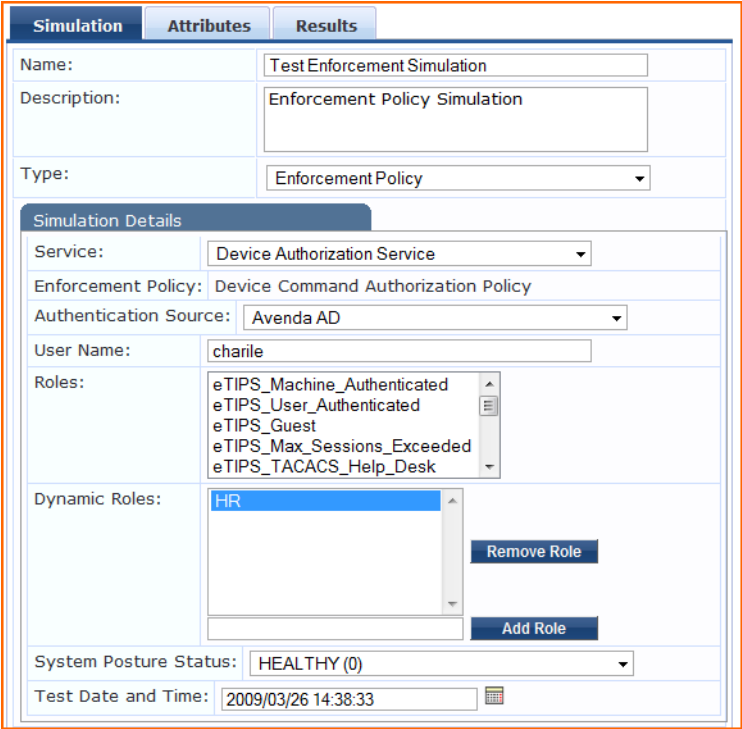
Add Simulation Test

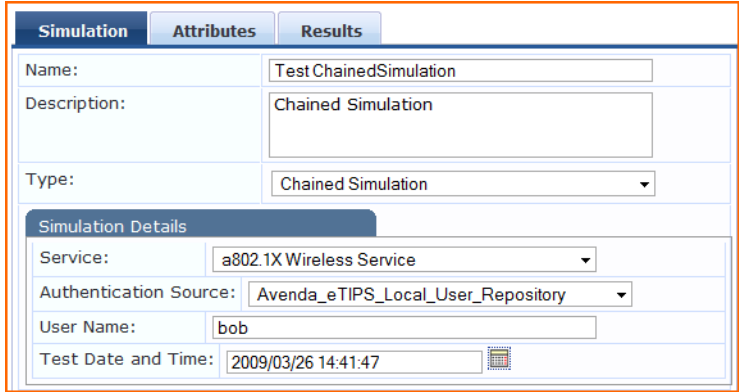
Configuration > Policy Simulation > Add Simulation (link). Depending on the simulation type selected the contents of the Simulation Tab changes.

Table 4-4 Add Policy Simulation (Simulation Tab)

Container	Description
Name/Description	Specify name and description (freeform).
Type	<ul style="list-style-type: none"> Input (Simulation tab): Select Date and Time. (optional - use if you have time based
Service Categorization.	<div data-bbox="600 371 1299 791" data-label="Form"> </div> <ul style="list-style-type: none"> service rules) Input (Attributes tab): Use the Rules Editor to create a request with the attributes you want to test. All namespaces relevant to service rules creation are loaded in the Attributes editor. Returns (Results tab): <i>Service Name (or status message in case of no match)</i>
Type	<ul style="list-style-type: none"> Input (Simulation tab): Select Service (Role Mapping policy is implicitly selected,
Role Mapping.	<div data-bbox="620 1037 1318 1457" data-label="Form"> </div> <p>because there is only one such policy associated with a service), Authentication Source, User Name, and Date/Time.</p> <ul style="list-style-type: none"> Input (Attributes tab): Use the Rules Editor to create a request with the attributes you want to test. All namespaces relevant for role mapping policies are loaded in the attributes editor. Returns (Results tab): <i>Role(s) - including authorization source attributes fetched as roles.</i>

Container	Description
Type Posture Validation.	<div><ul style="list-style-type: none">Input (Simulation tab): Select <i>Service</i> (Posture policies are implicitly selected by their association with the service).</div> <div></div> <div><ul style="list-style-type: none">Input (Attributes tab): Use the Rules Editor to create a request with the attributes you want to test. All namespaces relevant to posture evaluation (posture dictionaries) are loaded in the attributes editor.Returns (Results tab): <i>System Posture Status</i> and <i>Status Messages</i>.</div>
Type Audit.	<div><ul style="list-style-type: none">Input (Simulation tab): Select <i>Audit Server</i> and <i>host to be Audited</i> (IP address or hostname)</div> <div></div> <div><ul style="list-style-type: none">Returns (Results tab): <i>Summary Posture Status</i>, <i>Audit Attributes</i> and <i>Status</i></div> <div><p>Note: Audit simulations can take a while; an <i>AuditInProgress</i> status is shown until the audit completes.</p></div>

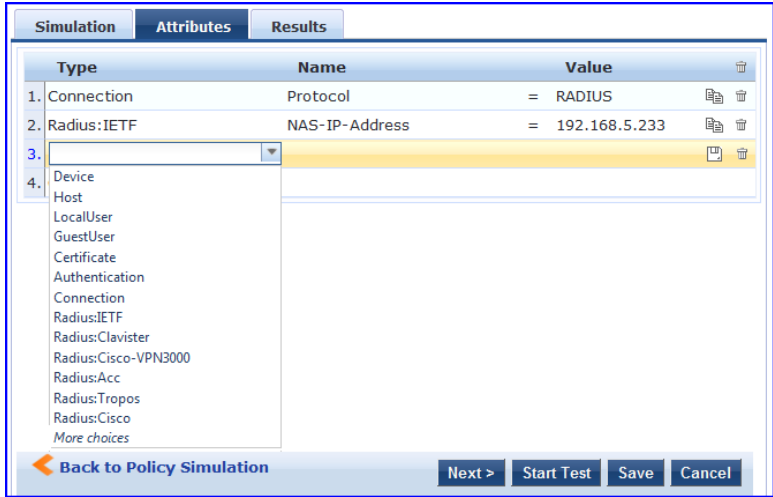
Container	Description
Type Enforcement Policy.	<ul style="list-style-type: none"> Input (Simulation tab): Select <i>Service</i> (<i>Enforcement Policy is implicit by its association with the Service</i>), <i>Authentication Source</i> (<i>optional</i>), <i>User Name</i> (<i>optional</i>), <i>Roles</i>, <i>Dynamic Roles</i> (<i>optional</i>), <i>System Posture Status</i>, and <i>Date/Time</i> (<i>optional</i>).  <ul style="list-style-type: none"> Input (Attributes tab): Use the Rules Editor to create a request with the attributes you want to test. Connection and RADIUS namespaces are loaded in the attributes editor. Returns (Results tab): <i>Enforcement Profile(s)</i> and <i>the attributes sent to the device..</i> <p>Note: <i>Authentication Source</i> and <i>User Name</i> inputs are used to derive dynamic values in the enforcement profile that are fetched from authorization source. These inputs are optional.</p> <p>Note: Dynamic Roles are attributes (that are enabled as a role) fetched from the authorization source. For an example of enabling attributes as a role, refer to “Generic LDAP or Active Directory” (page 122).</p>

Container	Description
Type Chained Simulations.	<ul style="list-style-type: none"> Input (Simulation tab): Select <i>Service</i>, <i>Authentication Source</i>, <i>User Name</i> and <i>Date/Time</i>.
	
	<ul style="list-style-type: none"> Input (Attributes tab): Use the Rules Editor to create a request with the attributes you want to test. All namespaces that are relevant in the Role Mapping Policy context are loaded in the attributes editor. Returns (Results tab): <i>Role(s)</i>, <i>Post Status</i>, <i>Enforcement Profiles</i> and <i>Status Messages</i>.
Test Date/Time	Use the calendar widget to specify date and time for simulation test.
Next	Upon completion of your work in this tab, click Next to open the Attributes tab.
Start Test	Run test. Outcome is displayed in the Results tab.
Save/Cancel	Click Save to commit or Cancel to dismiss the popup.

In the **Attributes** tab, enter the attributes of the policy component to be tested. The namespaces loaded in the Type column depend on the type of simulation (See above).

Note: If you select the *Audit* policy component in the **Simulation** tab, no Attributes tab appears.

Figure 4-6 Add Simulation (Attributes Tab)



In the **Results** tab, Policy Manager displays the outcome of applying the test request parameters against the specified policy component(s). What is shown in the results tab again depends on the type of simulation.

Figure 4-7 Add Simulation (Results Tab)

Simulation	
Summary -	
Audit Status	AuditComplete
System Posture Status	HEALTHY (0)
Audit Timeout	600 seconds
Audit Attributes -	
Avenda:Audit:Audit-Status	AUDIT_SUCCESS
Avenda:Audit:Device-Type	print server
Avenda:Audit:Mac-Vendor	Hewlett-packard
Avenda:Audit:Network-Apps	ftp, http, http-mgmt, printer, ipp,
Avenda:Audit:OS-Info	HP JetDirect J3110A print server
Avenda:Audit:Open-Ports	21, 80, 280, 515, 631,
Avenda:Audit:Output-Msgs	

Back to Policy Simulation Start Test Copy Save Cancel

Import Simulations

Configuration > Policy Simulation > Import Simulations ([link](#)).

Figure 4-8 Import Simulations

Import from file

Select File: Browse...

Enter secret for the file (if any):

Import Cancel

Table 4-5 Import Simulations

Container	Description
Select file	Browse to select name of simulations import file.
Import/Cancel	Import to commit or Cancel to dismiss popup.

Export Simulations

Configuration > Policy Simulation > Export Simulations (link).

To export all simulations, click **Export Simulations** (link). Your browser will display its normal **Save As** dialog, in which to enter the name of the XML file to contain the export.

Export

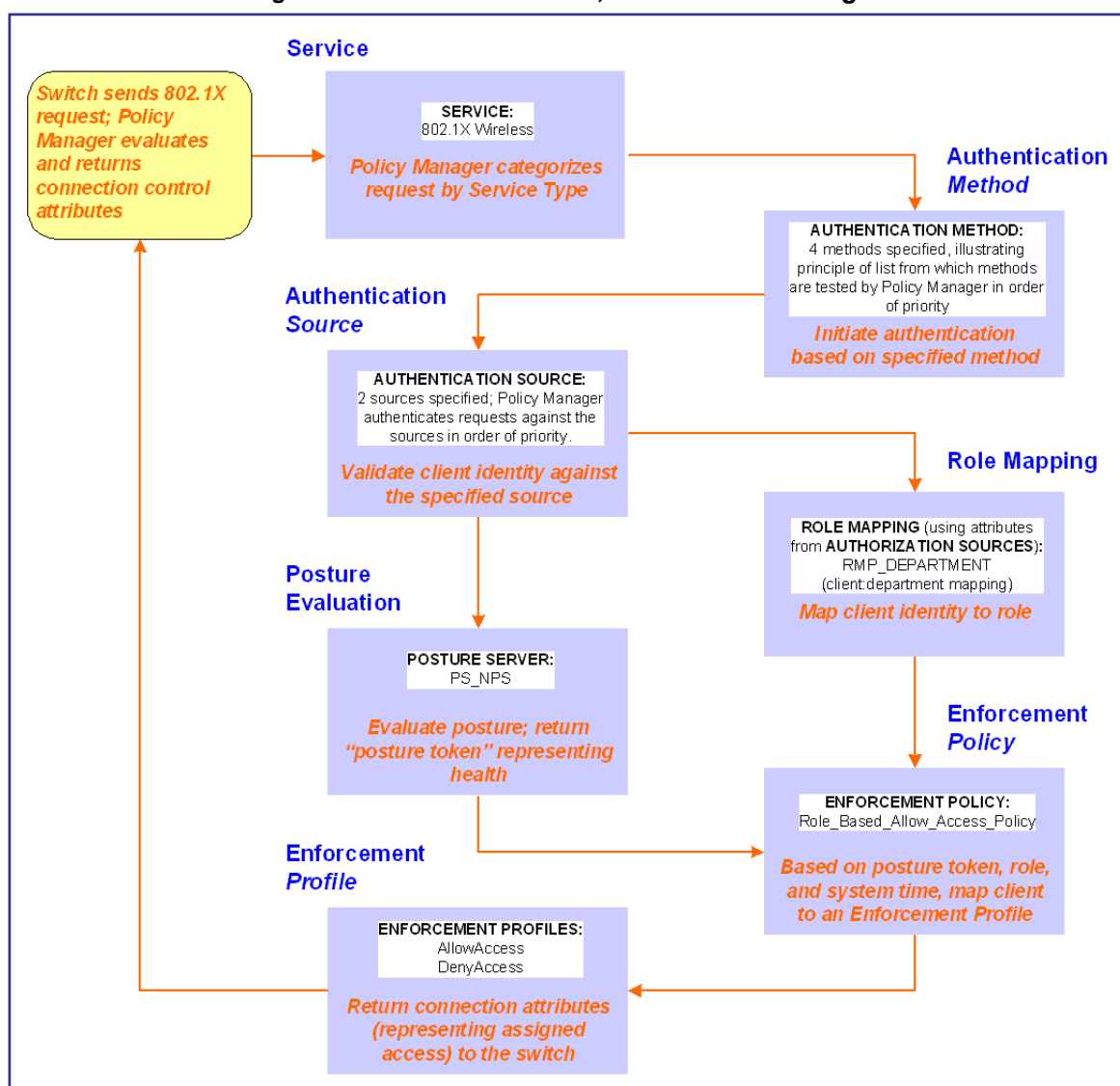
Configuration > Policy Simulation > Export (button).

To export just one simulation, select it (checkbox at left) and click **Export**. Your browser will display its normal **Save As** dialog, in which to enter the name of the XML file to contain the export.

Chapter 5: 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. Figure 5-1: Flow of Control, Basic 802.1X Configuration Use Case illustrates the flow of control for this Service.

Figure 5-1 Flow of Control, Basic 802.1X Configuration Use Case




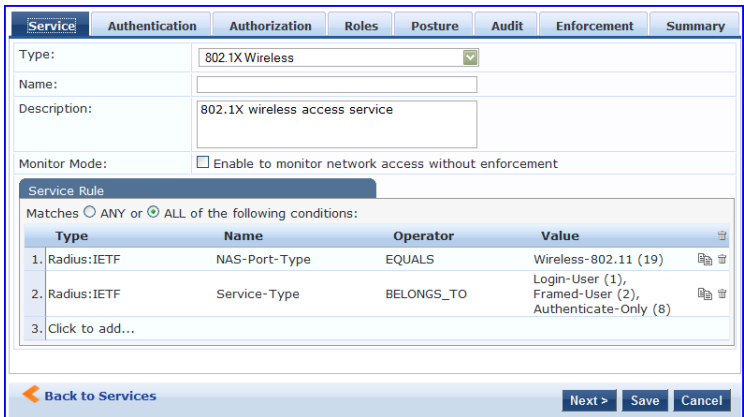
Configuring the Service

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 fifteen preconfigured Services. In this Use Case, you select a Service that supports 802.1X wireless requests.

Navigation	Settings
Create a new Service: <ul style="list-style-type: none"> • Services > • Add Service (link) > 	
Name the Service and select a pre-configured Service Type: <ul style="list-style-type: none"> • Service (tab) > • Type (selector): <i>802.1X Wireless</i> > • Name/Description (freeform) > • Upon completion, click Next (to Authentication) 	

The following fields deserve special mention:

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

2. Configure Authentication.

Follow the instructions to select *[EAP FAST]*, one of the pre-configured Policy Manager Authentication Methods, and *Active Directory Authentication*

Source (AD), an external Authentication Source within your existing enterprise.

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

Navigation

Select an Authentication Method and an Active Directory server (that you have already configured in Policy Manager):

- **Authentication** (tab) >
- **Methods** (Select from the drop-down list): *[EAP PEAP]*, *[EAP FAST]*, *[EAP TLS]*, and *[EAP TTLS]* >
- **Add** >
- **Sources** (Select drop-down list): *Avenda AD [Active Directory]* and *[Local User Repository]* >
- **Add** >
- Upon completion, **Next** (to Authorization)

Settings

Service	Authentication	Authorization	Roles	Posture	Audit	Enforcement	Summary
<p>Authentication Methods:</p> <div> eTIPS_EAP_PEAP [EAP-PEAP] eTIPS_EAP_FAST [EAP-FAST] eTIPS_EAP_TLS [EAP-TLS] eTIPS_EAP_TTLS [EAP-TTLS] </div> <div> Move Up Move Down Remove View Details Modify </div>							
<p>Authentication Sources:</p> <div> Avenda AD [Active Directory] eTIPS_Local_User_Repository [Local SQL DE] </div> <div> Move Up Move Down Remove View Details Modify </div>							
<p>Strip Username Rules:</p> <input type="checkbox"/> Enable to specify a comma-separated list of rules to strip username prefixes or suffixes							
<div> Back to Services Next > Save Cancel </div>							

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.

- Configure Service level authorization source. In this use case there is nothing to configure. Click the Next Button
- Upon completion, **Next** (to Role Mapping)

Authentication Source	Attributes Fetched From
1. Avenda AD [Active Directory]	Avenda AD [Active Directory]
2. eTIPS_Local_User_Repository [Local SQL DB]	eTIPS_Local_User_Repository [Local SQL DB]

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:

Navigation

Create the new Role Mapping Policy:

- **Roles** (tab) >
- **Add New Role Mapping Policy** (link) >

Settings

Navigation

Add new Roles (names only):

- **Policy** (tab) >
- **Policy Name** (freeform):
ROLE_ENGINEER >
- **Save** (button) >
- Repeat for
ROLE_FINANCE >
- When finished working in the **Policy** tab, click **Next** (button in the Rules Editor)

Settings

Configuration » Identity » Role Mappings » Add

Role Mappings

Policy | Mapping Rules | Summary

Policy Name:

Description:

Default Role: [View Details](#) [Modify](#) [Add new Role](#)

Add New Role

Name:

[Cancel](#)

Add New Role

Name:

Description:

[Save](#) [Cancel](#)

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 **Save** (button in the Rules Editor) >
- When finished working in the **Mapping Rules** tab, click **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:Avenda AD:department CONTAINS engineer)	Role_Engineer
2. (Authorization:Avenda AD:department CONTAINS finance)	ROLE_FINANCE

[Add Rule](#) [Move Up](#) [Move Down](#) [Edit Rule](#) [Remove Rule](#)

Rules Editor

Matches ☒ ANY or ☐ ALL of the following conditions:

Type	Name	Operator	Value	
1.	Authorization:Avenda AD	department	CONTAINS	finance
2.	Click to add...			

Actions

Role Name:

[Save](#) [Cancel](#)

[Back to Role Mappings](#) [Next >](#) [Save](#) [Cancel](#)

Navigation

Add the new Role Mapping Policy to the Service:

- Back in **Roles** (tab) >
- **Role Mapping Policy** (selector):
RMP_DEPARTMENT >
- Upon completion, **Next** (to Posture)

Settings

Conditions	Role
1. (Authorization:Avenda AD:department CONTAINS engineer)	Role_Engineer
2. (Authorization:Avenda AD:department CONTAINS finance)	ROLE_FINANCE

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)*.

To add the external posture server of type *Microsoft NPS* to the 802.1X service:

Navigation

Add a new Posture Server:

- **Posture** (tab) >
- **Add new Posture Server** (button) >

Setting

Navigation

Setting

Configure *posture* settings:

- **Posture Server** (tab) >
- **Name** (freeform): *PS_NPS*
- **Server Type** (radio button):
Microsoft NPS
- **Default Posture Token**
(selector): *UNKNOWN*
- **Next** (to Primary Server)

Configure connection settings:

- **Primary/ Backup Server** (tabs): Enter connection information for the RADIUS posture server.
- **Next** (button): from **Primary Server** to **Backup Server**.
To complete your work in these tabs, click **Save** (button).

Add the new Posture Server to the Service:

- Back in **Posture** (tab) >
- **Posture Servers** (selector): *PS_NPS*, then **Add** (button)
- **Next** (button)

6. Assign an Enforcement Policy.

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

Navigation

Configure the Enforcement Policy:

- **Enforcement** (tab) >
- **Enforcement Policy** (selector):
Role_Based_Allow_Access_Policy

Setting

The screenshot shows the 'Enforcement' tab in the ClearPass Policy Manager interface. The 'Enforcement Policy' dropdown is set to 'Sample_Allow_Access_Policy'. Below this, the 'Enforcement Policy Details' section shows the following configuration:

Enforcement Policy Details	
Description:	Sample policy to allow network access
Default Profile:	eTIPS_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) AND (Tips:Role MATCHES_ANY Role_Engineer ROLE_FINANCE)	eTIPS_Allow_Access_Profile

At the bottom of the form, there are buttons for 'Back to Services', 'Next >', 'Save', and 'Cancel'.

Note: For instructions about how to build such an Enforcement Policy, refer to “Configuring Enforcement Policies” (page 220).

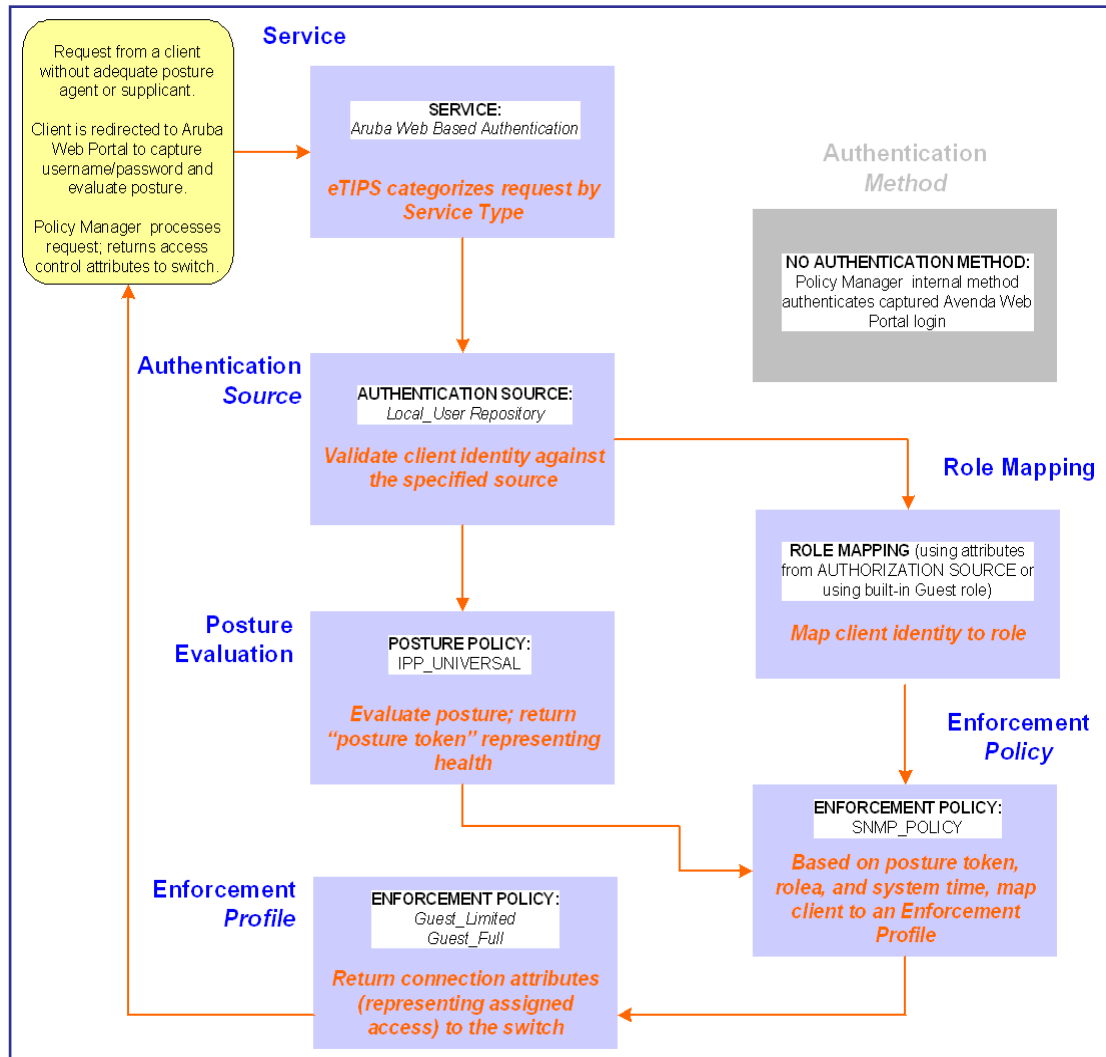
7. Save the Service.

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

Chapter 6: *Aruba Web-Based Authentication Use Case*

This Service supports known Guests with inadequate 802.1X supplicants or posture agents. Figure 6-1: Flow-of-Control of Web-Based Authentication for Guests illustrates the overall flow of control for this Policy Manager Service.

Figure 6-1 Flow-of-Control of Web-Based Authentication for Guests



Configuring the Service

To configure Policy Manager for WebAuth-based Guest access:

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

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

2. Create a WebAuth-based Service.

Navigation

Create a new Service:

- **Services** >
- **Add Service** >

Settings



Name the Service and select a pre-configured Service Type:

- **Service** (tab) >
- **Type** (selector): *Aruba Web-Based Authentication* >
- **Name/Description** (freeform) >
- Upon completion, click **Next**

The screenshot shows the 'Configuration > Services > Add' page. The title is 'Services'. There are tabs for 'Service', 'Authentication', 'Authorization', 'Roles', 'Posture', 'Enforcement', and 'Summary'. The 'Service' tab is active. The form contains the following fields:

- Type:** A dropdown menu with 'Aruba Web-based Authentication' selected.
- Name:** An empty text field.
- Description:** A text field containing 'Web Based Authentication for Guests'.
- Monitor Mode:** A checkbox labeled 'Enable to monitor network access without enforcement' which is currently unchecked.
- Service Rule:** A section with a 'Matches' radio button set to 'ANY' (with 'ALL' also available). Below it is a table with columns 'Type', 'Name', 'Operator', and 'Value'. The first row contains '1. Click to add...'.

 At the bottom, there are buttons for 'Back to Services', 'Next >', 'Save', and 'Cancel'.

3. Set up 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:

Navigation

Select the local Policy Manager database:

- **Authentication** (tab) >
- **Sources** (Select drop-down list):
[Local User Repository] >
- **Add** >
- **Strip Username Rules**
(checkbox) >
- 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)

Settings

The screenshot shows the 'Authentication' tab in the Aruba Web-Based Authentication settings. The 'Authentication Sources' section has a dropdown menu with 'eTIPS_Local_User_Repository' and 'Local SQL DE' selected. To the right of the dropdown are buttons: 'Move Up', 'Move Down', 'Remove', 'View Details', 'Modify', and 'Add'. Below the dropdown is a '-Select-' button. The 'Strip Username Rules' section has a checkbox labeled 'Enable to specify a comma-separated list of rules to strip username prefixes or suffixes', which is checked. Below the checkbox is a text input field containing 'user,'. To the right of the input field is a button labeled 'Add'. At the bottom of the form are buttons: 'Back to Services', 'Next >', 'Save', and 'Cancel'.

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; here, 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).

Navigation

Setting

Create a Posture Policy:

- **Posture** (tab) >
- Enable **Validation Check** (checkbox) >
- **Add new Internal Policy** (link) >

Name the Posture Policy and specify a general class of operating system:

- **Policy** (tab) >
- **Policy Name** (freeform): *IPP_UNIVERSAL* >
- **Host Operating System** (radio buttons): *Windows* >
- When finished working in the **Policy** tab, **Next** (to Posture Plugins tab)

Select a Validator:

- **Posture Plugins** (tab) >
- Enable *Windows Health System Validator* >
- **Configure** (button) >

Plugin Name	Plugin Configuration	Status
<input type="checkbox"/> Avenda Windows Universal System Health Validator	Configure View	-
<input checked="" type="checkbox"/> Windows System Health Validator	Configure View	Not Configured

Navigation

Setting

Configure the Validator:

- **Windows System Health Validator** (popup) >
- **Enable all Windows operating systems** (checkbox) >
- **Enable Service Pack levels for Windows 7, Vista, XP and Server 2008** (checkbox) >
- **Save** (button) >
- When finished working in the **Posture Plugin** tab, **Next** (to Rules tab)

The screenshot shows the 'Windows System Health Validator' configuration window. It contains a list of operating systems with checkboxes to enable them and input fields for service pack levels. The 'Windows Vista' section is expanded, showing 'Restrict clients which have Service Pack less than' with a value of 1. The 'Windows XP' section is also expanded, showing a value of 3. The 'Windows Server 2008' section is expanded, showing a value of 1. The 'Windows 2000' and 'Windows Server 2003' sections are collapsed. At the bottom, there are 'Reset', 'Save', and 'Cancel' buttons.

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 **Save** (button) >
- When finished working in the **Rules** tab, **Next** (button)

The screenshot shows the 'Rules Editor' configuration window. It has tabs for 'Policy', 'Posture Plugins', 'Rules', and 'Summary'. The 'Rules' tab is active, showing a table of rules. The table has two columns: 'Conditions' and 'Posture Token'. The first rule is 'Passes all SHV checks - Windows System Health Validator' with a 'HEALTHY' posture token. The second rule is 'Fails one or more SHV checks - Windows System Health Validator' with a 'QUARANTINE' posture token. Below the table, there are 'Add Rule', 'Move Up', 'Move Down', 'Edit Rule', and 'Remove Rule' buttons. The 'Rules Editor' popup is also visible, showing the 'Conditions' and 'Actions' sections. The 'Conditions' section has 'Select Plugin Checks' set to 'Passes all SHV checks' and 'Select Plugins' set to 'Windows System Health Validator'. The 'Actions' section has 'Posture Token' set to 'HEALTHY (0)'. At the bottom, there are 'Save' and 'Cancel' buttons.

Add the new Posture Policy to the Service:

- Back in **Posture** (tab) >
- **Internal Policies** (selector): *IPP_UNIVERSAL_XP*, then **Add** (button)

The screenshot shows the 'Posture' configuration window. It has tabs for 'Service', 'Authentication', 'Authorization', 'Roles', 'Posture', 'Enforcement', and 'Summary'. The 'Posture' tab is active, showing a 'Validation Check' section with a checkbox 'Enable posture validation for end-hosts with posture agents'. Below this is a 'Posture Policies' section with a list of policies. The 'IPP_UNIVERSAL' policy is selected. To the right of the list are 'Remove', 'View Details', 'Modify', and 'Add' buttons. Below the list is a 'Default Posture Token' dropdown set to 'UNKNOWN (100)'. There is also a 'Remediate End-Hosts' checkbox and a 'Remediation URL' field. At the bottom, there are 'Back to Services', 'Next >', 'Save', and 'Cancel' buttons.

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 *Aruba 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 otherwise.

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

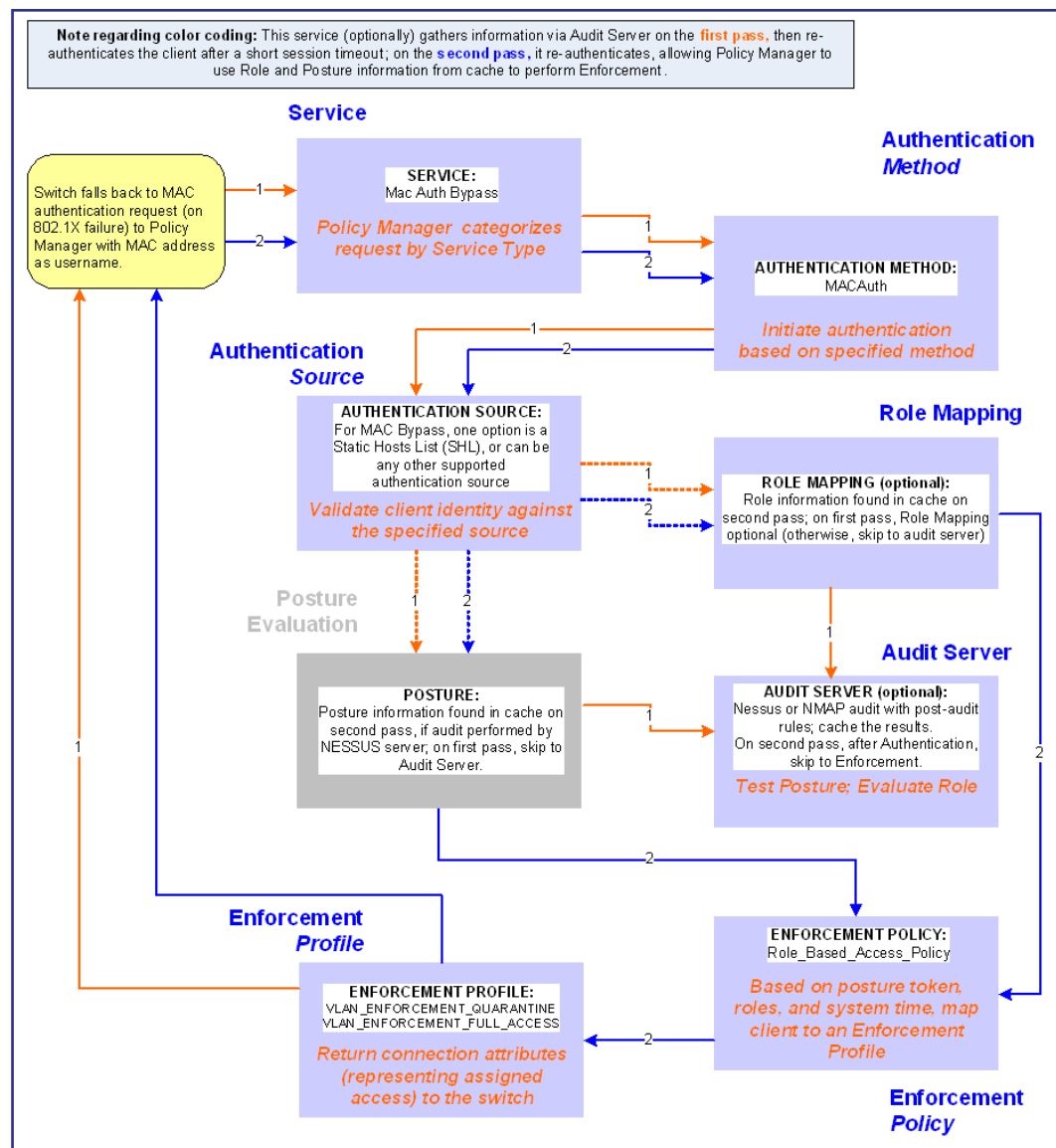
6. Save the Service.

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

Chapter 7: *MAC Authentication Use Case*

This Service supports *Network Devices*, such as printers or handhelds. [Figure 7-1: Flow-of-Control of MAC Authentication for Network Devices](#) 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


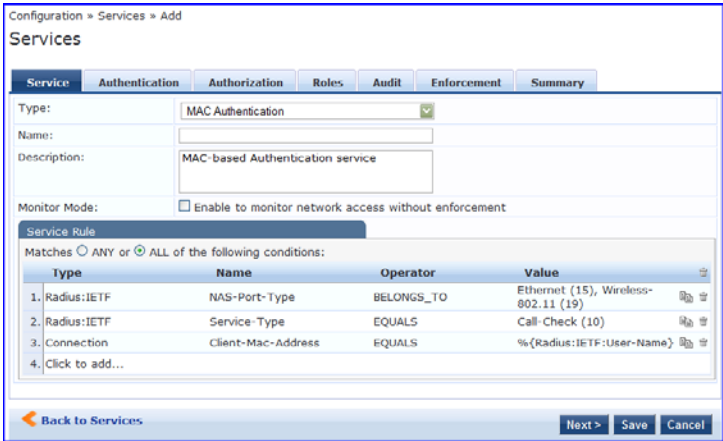
Figure 7-1 Flow-of-Control of MAC Authentication for Network Devices



Configuring the Service

To configure Policy Manager for MAC-based Network Device access:

1. Create a MAC Authentication Service.

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

2. Set up Authentication.

Note that you can select any type of authentication/authorization source for a MAC Authentication service. Only a [Static Host List](#) of type MAC Address List or MAC Address Regular Expression shows up in the list of authentication sources (of type Static Host List). You can also select any other supported type of authentication source.

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 LDA*
- **Add** >
- Upon completion, **Next** (to Audit)

3. Configure an Audit Server.

Optional, if no Role Mapping Policy is provided, or if you wish 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:

Navigation

Settings

Configure the Audit Server:

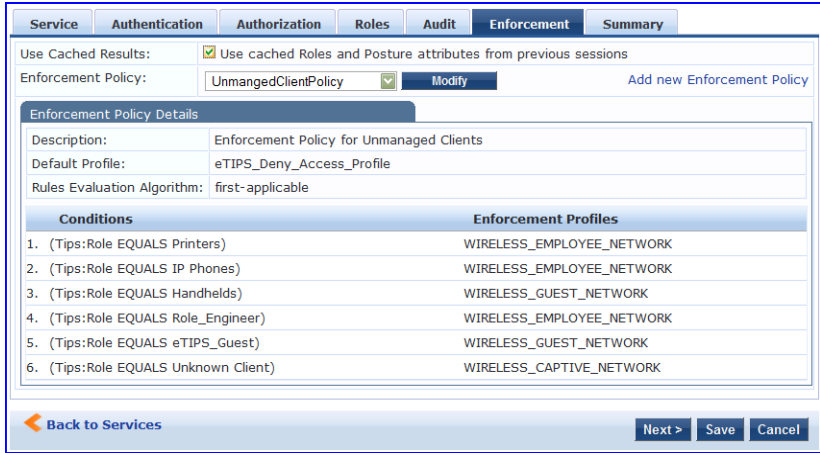
- **Audit** (tab) >
- **Audit End Hosts** (enable) >
- **Audit Server** (selector): *NMAP*
- **Trigger Conditions** (radio button): *For MAC authentication requests*
- **Reauthenticate client** (checkbox): *Enable*

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.

4. Select an Enforcement Policy.

Select the Enforcement Policy *Sample_Allow_Access_Policy*:

Navigation	Setting														
<p>Select the Enforcement Policy:</p> <ul style="list-style-type: none"> • Enforcement (tab) > • Use Cached Results (checkbox): <i>Use cached Roles and Posture attributes from previous sessions</i> > • Enforcement Policy (selector): <i>UnmanagedClientPolicy</i> • When you are finished with your work in this tab, click Save. 	 <p>The screenshot shows the 'Enforcement' tab in the ClearPass configuration interface. At the top, there are tabs for Service, Authentication, Authorization, Roles, Audit, Enforcement, and Summary. The 'Enforcement' tab is active. Below the tabs, there is a section for 'Use Cached Results' with a checked checkbox and the text 'Use cached Roles and Posture attributes from previous sessions'. Below this is the 'Enforcement Policy' dropdown menu, which is set to 'UnmanagedClientPolicy'. To the right of the dropdown is a 'Modify' button and a link to 'Add new Enforcement Policy'. Below this is the 'Enforcement Policy Details' section, which contains a table with the following data:</p> <table border="1"> <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> <p>At the bottom of the interface, there is a 'Back to Services' button on the left and 'Next >', 'Save', and 'Cancel' buttons on the right.</p>	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).

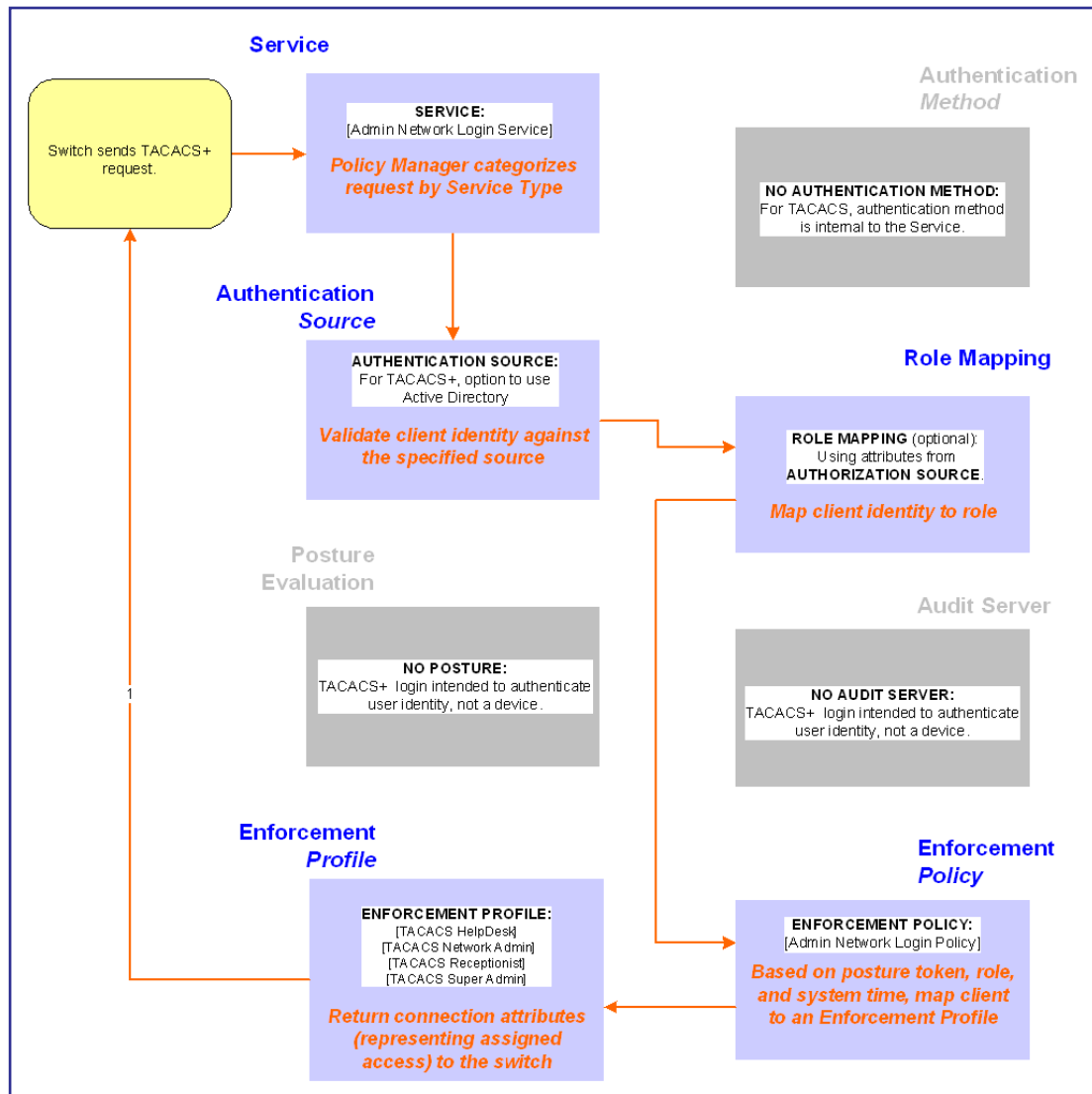
5. Save the Service.

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

Chapter 8: TACACS+ Use Case

This Service supports Administrator connections to Network Access Devices via TACACS+. Figure 8-1: Administrator connections to Network Access Devices via TACACS+ illustrates the overall flow of control for this Policy Manager Service.


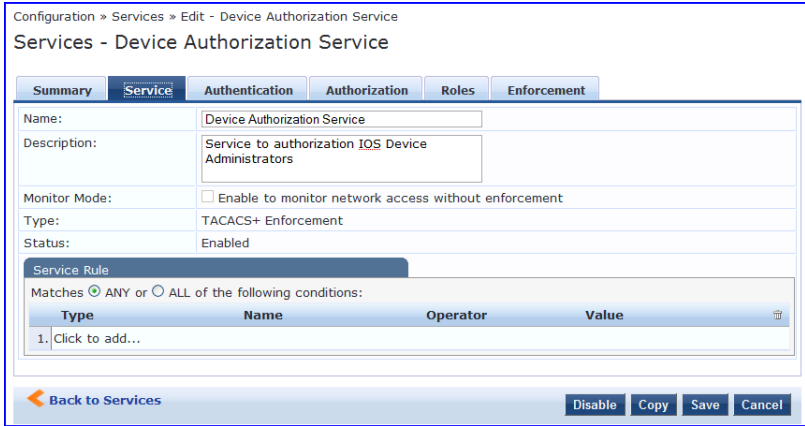
Figure 8-1 Administrator connections to Network Access Devices via TACACS+



Configuring the Service

To configure Policy Manager for TACACS+-based access:

1. Create a TACACS+ Service.

Navigation	Settings
Create a new Service: <ul style="list-style-type: none"> • Services > • Add Service (link) > 	
Name the Service and select a pre-configured Service Type: <ul style="list-style-type: none"> • Service (tab) > • Type (selector): <i>[Policy Manager Admin Network Login Service]</i> > • Name/Description (freeform) > • Upon completion, click Next (to Authentication) 	

2. Set up 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:

Navigation**Settings**

Select an Active Directory server (that you have already configured in Policy Manager):

- **Authentication** (tab) >
- **Add** >
- **Sources** (Select drop-down list): *Avenda AD (Active Directory)* >
- **Add** >
- Upon completion, **Next** (to Authentication)

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*).

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**.

4. Save the Service.

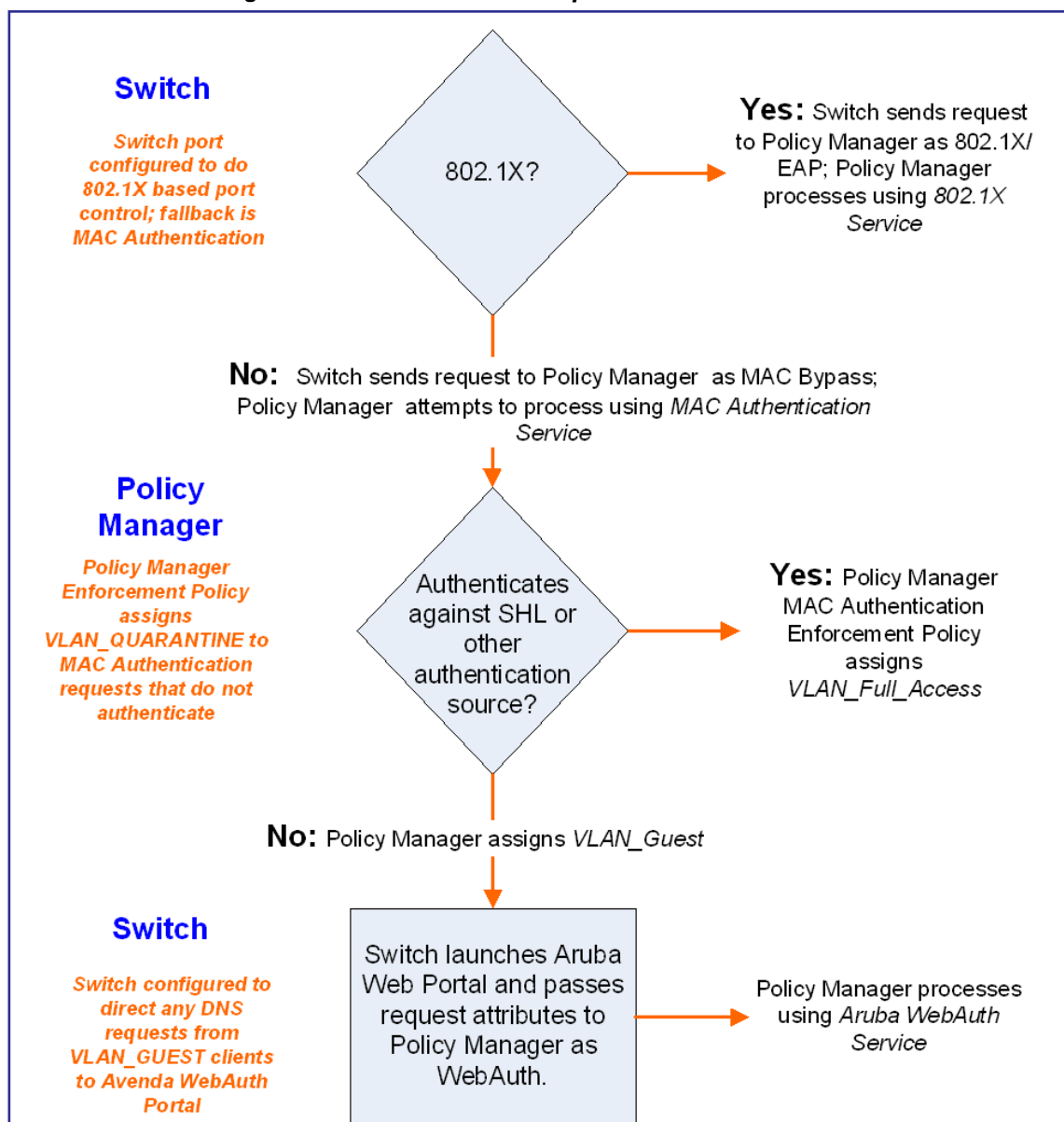
Click **Save**. The Service now appears at the bottom of the **Services** list.

Chapter 9: *Single Port Use Case*

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

Figure 9-1: Flow of the *Multiple Protocol Per Port Case* 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 9-1 Flow of the *Multiple Protocol Per Port Case*



Chapter 10: Services

The Policy Manager policy model groups policy components that serve a particular type of request into *Services*, which sit at the top of the policy hierarchy.

Architecture and Flow

Architecturally, Policy Manager Services are:

- **Parents** of their policy components, which they wrap (hierarchically) and coordinate in processing requests.
- **Siblings** of other Policy Manager Services, within an ordered priority that determines the sequence in which they are tested against requests.
- **Children** of Policy Manager, which tests requests against their Rules, to find a matching Service for each request.

The flow-of-control for requests parallels this hierarchy:

- *Policy Manager* tests for the first Request-to-Service-Rule match
- The matching *Service* coordinates execution of its policy components
- Those *policy components* process the request to return Enforcement Profiles to the network access device, and, optionally, posture results to the client.

There are two approaches to creating a new Service in Policy Manager:

- Bottom-Up Approach - Create all policy components (Authentication Method, Authentication Source, Role Mapping Policy, Posture Policy, Posture Servers, Audit Servers, Enforcement Profiles, Enforcement Policy) first, as needed, and then create the Service from using Service creation Wizard.
- Top-Down Approach - Start with the Service creation wizard, and create the associated policy components as and when you need them, all in the same flow.

To help you get started, Policy Manager comes preconfigured with 15 different Service types or templates. If these service types do not suit your needs, you may roll your own service, with custom service rules.

Start Here Page


From the **Start Here** page (**Configuration > Start Here**), you can create a new service by clicking on any of the pre-configured “[Policy Manager Service Types](#)” ([page 85](#))

Each of the service types is listed in a graphical list, with a description of each type:


Figure 10-1 Start Here Page

Configuration » Start Here


Choose a deployment type to start configuring network policy




802.1X Wireless
For wireless end-hosts connecting through an 802.11 wireless access device or controller, with authentication via IEEE 802.1X. Allows configuring both identity and posture based policies.




802.1X Wired
For end-hosts connecting through an Ethernet LAN, with authentication via IEEE 802.1X. Allows configuring both identity and posture based policies.



MAC Authentication
MAC-based authentication bypass service, for end-hosts without an 802.1X supplicant or a posture agent (printers, other embedded devices, and computers owned by guests or contractors). Authentication is based on the MAC-address of the end-host being present in a white list or black list.



Web-based Authentication
Web-based authentication service for guests or agentless hosts, via the SecureConnect Portal. The user is redirected to the SecureConnect captive portal by the network device, or by a DNS server that is set up to redirect traffic on a subnet to a specific URL. The web page collects username and password, and also optionally collects health information.



Web-based Health Check Only
Web-based authentication service for guests or agentless hosts, via the SecureConnect Portal. Health-Check only.

Once you select a service type, the associated service wizard is displayed with a clickable diagram that shows on top of the wizard:

Figure 10-2 Service Wizard with Clickable Flow

Configuration » Services » Add

Services

Service → Authentication → Authorization → Roles → Posture → Audit → Enforcement

Service	Authentication	Authorization	Roles	Posture	Audit	Enforcement	Summary
Type:	802.1X Wireless						
Name:							
Description:	802.1X wireless access service						
Monitor Mode:	<input type="checkbox"/> Enable to monitor network access without enforcement						
Service Rule							
Matches <input type="radio"/> ANY or <input checked="" type="radio"/> 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 Start Here Next > Save Cancel							

The rest of the service configuration flow is as described in “Policy Manager Service Types” (page 85)

Policy Manager Service Types

The following service types come preconfigured on Policy Manager:

Table 10-1 Policy Manager Service Types

Service Type	Description/ Available Policy Components (in tabs)/ Service Rule (in Rules Editor)/ Service-specific policy components (called out with legend below)
--------------	-------------------------------------------------------------------------------------------------------------------------------------------------------

**802.1X Wireless**

For wireless clients connecting through an 802.11 wireless access device or controller, with authentication via IEEE 802.1X.

To configure authentication methods and authentication source, click on the **Authentication** tab.

The *Authentication methods* used for this service depend on the 802.1X supplicants and the type of authentication methods you choose to deploy. The common types are PEAP, EAP-TLS, EAP-FAST or EAP-TTLS (These methods are automatically selected). Non-tunneled EAP methods such as EAP-MD5 can also be used as authentication methods.

The *Authentication sources* used for this type of service can be one or more instances of the following: Active Directory, LDAP Directory, SQL DB, Token Server or the Policy Manager local DB. For more information on configuring authentication sources, refer to “Adding and Modifying Authentication Sources” (page 119)

You can enable **Strip Username Rules** to, optionally, pre-process the user name (to remove prefixes and suffixes) before authenticating and authorizing against the authentication source.

Service Type	Description/ Available Policy Components (in tabs)/ Service Rule (in Rules Editor)/ Service-specific policy components (called out with legend below)
--------------	-------------------------------------------------------------------------------------------------------------------------------------------------------

802.1X Wireless
Contd.

To create authorization source for this service click on the **Authorization** tab. Policy Manager fetches role mapping attributes from the authorization sources associated with service, regardless of which authentication source was used to authenticate the user. For a given service, role mapping attributes are fetched from the following authorization sources:

- The authorization sources associated with the authentication source
- The authorization sources associated with the service. For more information on configuring authorization sources, refer to “Adding and Modifying Authentication Sources” (page 119)

To associate a role mapping policy with this service click on the **Roles** tab. For information on configuring role mapping policies, refer to “Configuring a Role Mapping Policy” (page 144)

Service Type	Description/ Available Policy Components (in tabs)/ Service Rule (in Rules Editor)/ Service-specific policy components (called out with legend below)
--------------	-------------------------------------------------------------------------------------------------------------------------------------------------------

802.1X Wireless
Contd.

By default, this type of service does not have *Posture* checking enabled. To enable posture checking for this service select **Enable posture validation for end-hosts with posture agents**. You can enable posture checking for this kind of service if you are deploying Policy Manager in a Microsoft NAP or Cisco NAC framework environment, or if you are deploying an Aruba hosted captive portal that does posture checks through a dissolvable agent. You can also choose to **Enable auto-remediation of non-compliant end-hosts** and enter the **Remediation URL** of a server resource that can perform remediation action (when a client is quarantined).

For more information on configuring *Posture Policies* and *Posture Servers* refer to topics: “Configuring Posture” (page 161) and “Adding and Modifying Posture Servers” (page 189)

Summary	Service	Authentication	Authorization	Roles	Posture	Audit	Enforcement
Validation Check: <input checked="" type="checkbox"/> Enable posture validation for end-hosts with posture agents							
Posture Policies: Posture Policies: <div> <div>Basic Linux Health Check</div> <div>Basic Windows Health Check</div> <div>--Select--</div> <div>Remove</div> <div>View Details</div> <div>Modify</div> <div>Add</div> </div> Add new Posture Policy							
Default Posture Token: UNKNOWN (100)							
Remediate End-Hosts: <input checked="" type="checkbox"/> Enable auto-remediation of non-compliant end-hosts							
Remediation URL: remediation.us.avendasys.com							
Posture Servers: Posture Servers: <div> <div></div> <div>PS_NPS [RADIUS]</div> <div>Remove</div> <div>View Details</div> <div>Modify</div> <div>Add</div> </div> Add new Posture Server							
<div> Back to Services <div>Disable Copy Save Cancel</div> </div>							

By default, this type of service does not have *Audit* checking enabled. To enable posture checking for this service select **Enable auditing of end hosts**.

Summary	Service	Authentication	Authorization	Roles	Posture	Audit	Enforcement
Audit End-Hosts: <input checked="" type="checkbox"/> Enable auditing of end-hosts							
Audit Server: eTIPS_Nmap_Audit <div>View Details Modify</div> Add new Audit Server							
Audit Trigger Conditions: <div> <input type="radio"/> Always <input checked="" type="radio"/> When posture is not available <input type="radio"/> For MAC authentication request </div>							
Re-Authenticate End-Host: <input checked="" type="checkbox"/> Force re-authentication of the end-host after audit							

Service Type	Description/ Available Policy Components (in tabs)/ Service Rule (in Rules Editor)/ Service-specific policy components (called out with legend below)
802.1X Wireless Contd.	<p>Select an Audit Server - either built-in or customized. Refer to “Configuring Audit Servers” (page 194) for audit server configuration steps. For this type of service you can perform audit Always or only When posture is not available. Performing audit on a client is an asynchronous task, which means the audit can be performed only after the 802.1X request has been completed and the client has acquired an IP address through DHCP. Once the audit results are available, there needs to be a way for Policy Manager to re-apply policies on the network device. This can be accomplished in two ways:</p> <ul style="list-style-type: none"> By setting a short session-timeout for the 802.1X, so the audit results can be applied in a subsequent 802.1X request. Send this short session timeout only if an audit is triggered, and not otherwise. This session timeout must be set to a value that would give Policy Manager enough time to finish auditing the client. By enabling Force re-authentication of the client after audit. When this checkbox is enabled, Policy Manager resets the connection associated with the client after the audit is done, so another request is triggered by the network device. When Policy Manager gets the next 802.1X request it uses the cached audit results to send the right enforcement profile to the network device. See “Configuring Enforcement Profiles” (page 208) <p>You must select an enforcement policy (See “Configuring Enforcement Policies” (page 220)) for a service.</p>

Summary	Service	Authentication	Authorization	Roles	Posture	Audit	Enforcement				
Use Cached Results: <input checked="" type="checkbox"/> Use cached Roles and Posture attributes from previous sessions Enforcement Policy: Employee Enforcement Policy Modify Add new Enforcement Policy											
Enforcement Policy Details											
Description: Enforcement policies for corporate employees Default Profile: INTERNET_VLAN Rules Evaluation Algorithm: evaluate-all											
<table border="1"> <thead> <tr> <th>Conditions</th> <th>Enforcement Profiles</th> </tr> </thead> <tbody> <tr> <td> 1. (Tips:Posture EQUALS HEALTHY (0)) AND (Tips:Role MATCHES_ANY eTIPS_User_Authenticated role_engineer senior_mgmt) </td> <td>EMPLOYEE_VLAN</td> </tr> </tbody> </table>								Conditions	Enforcement Profiles	1. (Tips:Posture EQUALS HEALTHY (0)) AND (Tips:Role MATCHES_ANY eTIPS_User_Authenticated role_engineer senior_mgmt)	EMPLOYEE_VLAN
Conditions	Enforcement Profiles										
1. (Tips:Posture EQUALS HEALTHY (0)) AND (Tips:Role MATCHES_ANY eTIPS_User_Authenticated role_engineer senior_mgmt)	EMPLOYEE_VLAN										

Enable **Use cached Roles and Posture attributes from previous sessions** if posture and/or role information is not available through this service (because the 802.1X supplicant that is deployed on your clients cannot send health and/or identity credentials), but you have configured other types of services (such as WebAuth or Audit services) to collect this information. When this checkbox is enabled, Policy Manager triggers a re-authentication after the posture is collected (through a captive portal, for example), so another 802.1X request is triggered by the network device. When Policy Manager gets the next 802.1X request it uses the cached posture and roles to send the right enforcement profile to the network device.

Service Type	Description/ Available Policy Components (in tabs)/ Service Rule (in Rules Editor)/ Service-specific policy components (called out with legend below)
--------------	-------------------------------------------------------------------------------------------------------------------------------------------------------



802.1X Wired

For clients connecting through an Ethernet LAN, with authentication via IEEE 802.1X.

Configuration » Services » Add

Services

Service Authentication Authorization Roles Posture Audit Enforcement Summary

Type: 802.1X Wireless

Name:

Description: 802.1X wireless access service

Monitor Mode: ☐ Enable to monitor network access without enforcement

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

Except for the service rules shown above, configuration for the rest of the tabs is similar to the 802.1X Wireless Service.

Note: If you want to administer the same set of policies for wired and wireless access, you can combine the service rule to define one single service. The other option is to keep two services for wired and wireless access, but re-use the policy components (authentication methods, authentication source, authorization source, role mapping policies, posture policies, and enforcement policies) in both services.

Refer to [802.1X Wireless](#) service type for description of the different tabs.

Service Type	Description/ Available Policy Components (in tabs)/ Service Rule (in Rules Editor)/ Service-specific policy components (called out with legend below)
--------------	-------------------------------------------------------------------------------------------------------------------------------------------------------



MAC Authentication

MAC-based authentication service, for clients without an 802.1X supplicant or a posture agent (printers, other embedded devices, and computers owned by guests or contractors). The network access device sends a MAC authentication request to Policy Manager. Policy Manager can look up the client in a white list or a black list, authenticate and authorize the client against an external authentication/authorization source, and optionally perform an audit on the client.

Service	Authentication	Authorization	Roles	Audit	Enforcement	Summary																				
Type: <input type="text" value="MAC Authentication"/> Name: <input type="text"/> Description: <input type="text" value="MAC-based Authentication service"/> Monitor Mode: <input type="checkbox"/> Enable to monitor network access without enforcement Service Rule Matches <input type="radio"/> ANY or <input checked="" type="radio"/> ALL of the following conditions: <table border="1"> <thead> <tr> <th>Type</th> <th>Name</th> <th>Operator</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>1. Radius:IETF</td> <td>NAS-Port-Type</td> <td>BELONGS_TO</td> <td>Ethernet (15), Wireless-802.11 (19)</td> </tr> <tr> <td>2. Radius:IETF</td> <td>Service-Type</td> <td>EQUALS</td> <td>Call-Check (10)</td> </tr> <tr> <td>3. Connection</td> <td>Client-Mac-Address</td> <td>EQUALS</td> <td>%{Radius:IETF:User-Name}</td> </tr> <tr> <td>4.</td> <td colspan="3">Click to add...</td> </tr> </tbody> </table>							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...		
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...																									
<input type="button" value="Back to Services"/> <input type="button" value="Next >"/> <input type="button" value="Save"/> <input type="button" value="Cancel"/>																										

The default Authentication method used for this type of service is [MAC AUTH], which is a special type of method called MAC-AUTH. When this authentication method is selected, Policy Manager does stricter checking of the MAC Address of the client. This type of service can use either a built-in static host list (refer to [“Adding and Modifying Static Host Lists”](#) (page 155)), or any other authentication source for the purpose of white-listing or black-listing the client. You can also specify the role mapping policy, based on categorization of the MAC addresses in the authorization sources.

Service	Authentication	Authorization	Roles	Audit	Enforcement	Summary
Authentication Methods: <div> <input type="text" value="eTIPS_MAC_AUTH [MAC-AUTH]"/> <div> <input type="button" value="Move Up"/> <input type="button" value="Move Down"/> <input type="button" value="Remove"/> <input type="button" value="View Details"/> <input type="button" value="Modify"/> </div> </div> <div> <input type="text" value="--Select--"/> <input type="button" value="Add"/> </div>						
Authentication Sources: <div> <input type="text" value="Handhelds [Static Host List]"/> <div> <input type="button" value="Move Up"/> <input type="button" value="Move Down"/> <input type="button" value="Remove"/> <input type="button" value="View Details"/> <input type="button" value="Modify"/> </div> </div> <div> <input type="text" value="eTIPS_Clients_White_List_LDAP [Generic LDAP]"/> <div> <input type="button" value="Move Up"/> <input type="button" value="Move Down"/> <input type="button" value="Remove"/> <input type="button" value="View Details"/> <input type="button" value="Modify"/> </div> </div> <div> <input type="text" value="--Select--"/> <input type="button" value="Add"/> </div>						
Strip Username Rules: <input checked="" type="checkbox"/> Enable to specify a comma-separated list of rules to strip username prefixes or suffixes						

You cannot configure Posture for this type of service.

Service Type	Description/ Available Policy Components (in tabs)/ Service Rule (in Rules Editor)/ Service-specific policy components (called out with legend below)
MAC Authentication Contd.	Audit can optionally be enabled for this type of service by checking Enable auditing of end-hosts .

Service	Authentication	Authorization	Roles	Audit	Enforcement	Summary
Audit End-Hosts:	<input checked="" type="checkbox"/> Enable auditing of end-hosts					
Audit Server:	eTIPS_Nmap_Audit View Details Modify Add new Audit Server					
Audit Trigger Conditions:	<input type="radio"/> Always <input type="radio"/> When posture is not available <input checked="" type="radio"/> For MAC authentication request <input type="radio"/> For known end-hosts only <input checked="" type="radio"/> For unknown end-hosts only <input type="radio"/> For all end-hosts					
Re-Authenticate End-Host:	<input type="checkbox"/> Force re-authentication of the end-host after audit					

You can perform audit **For known clients only** or **For unknown clients only** or **For all clients**. Known clients are defined as those clients that are found in the authentication source(s) associated with this service. Performing audit on a client is an asynchronous task, which means the audit can be performed only after the MAC authentication request has been completed and the client has acquired an IP address through DHCP. Once the audit results are available, there needs to be a way for Policy Manager to re-apply policies on the network device. This can be accomplished in two ways:

- By setting a short session-timeout for the MAC authentication session, so the audit results can be applied in a subsequent MAC Authentication request. Send this short session timeout only if an audit is triggered, and not otherwise. This session timeout must be set to a value that would give Policy Manager enough time to finish auditing the client.
- By enabling **Force re-authentication of the client after audit**. When this checkbox is enabled, Policy Manager resets the connection associated with the client after the audit is done, so another request is triggered by the network device. When Policy Manager gets the next MAC Authentication request it uses the cached audit results to send the right enforcement profile to the network device. See [“Configuring Enforcement Profiles”](#) (page 208)

Refer to 802.1X Wireless Service for description of the other tabs.

Service Type	Description/ Available Policy Components (in tabs)/ Service Rule (in Rules Editor)/ Service-specific policy components (called out with legend below)
--------------	-------------------------------------------------------------------------------------------------------------------------------------------------------



Web-based Authentication

Web-based authentication service for guests or agentless hosts, via the Aruba built-in Portal. The user is redirected to the Aruba captive portal by the network device, or by a DNS server that is set up to redirect traffic on a subnet to a specific URL. The web page collects username and password, and also optionally collects health information (on Windows Windows 7, Vista, Windows XP, Windows Server 2008, Windows 2000, Windows Server 2003, popular Linux systems). There is an internal service rule (*Connection:Protocol EQUALS WebAuth*) that categorizes request into this type of service. You can add other rules, if needed.

Service	Authentication	Authorization	Roles	Posture	Enforcement	Summary								
Type:	Avenda Web-based Authentication													
Name:	Web Auth Service													
Description:	Captive portal service that collects health													
Monitor Mode:	<input type="checkbox"/> Enable to monitor network access without enforcement													
Service Rule Matches <input type="radio"/> ANY or <input checked="" type="radio"/> ALL of the following conditions: <table border="1"> <thead> <tr> <th>Type</th> <th>Name</th> <th>Operator</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>1.</td> <td colspan="3">Click to add...</td> </tr> </tbody> </table>							Type	Name	Operator	Value	1.	Click to add...		
Type	Name	Operator	Value											
1.	Click to add...													

There is no authentication method associated with this type of service (Authentication methods are only relevant for RADIUS requests). You can select any type of authentication source with this type of service.





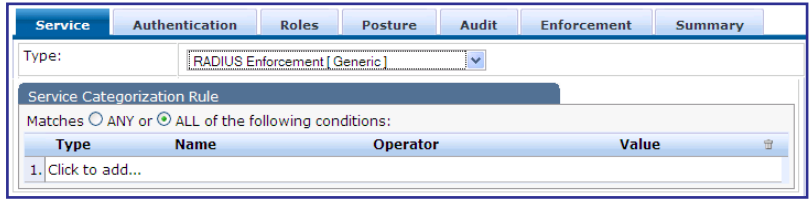
Service	Authentication	Authorization	Roles	Posture	Enforcement	Summary										
Authentication Sources: <table border="1"> <tr> <td>Avenda AD [Active Directory]</td> <td rowspan="4"> Move Up Move Down Remove View Details Modify </td> <td rowspan="4">Add new Authentication Source</td> </tr> <tr> <td>Sagano AD [Active Directory]</td> </tr> <tr> <td>eTIPS_Local_User_Repository [Local SQL DE</td> </tr> <tr> <td>--Select--</td> </tr> <tr> <td colspan="2"></td> <td>Add</td> <td></td> </tr> </table>							Avenda AD [Active Directory]	Move Up Move Down Remove View Details Modify	Add new Authentication Source	Sagano AD [Active Directory]	eTIPS_Local_User_Repository [Local SQL DE	--Select--			Add	
Avenda AD [Active Directory]	Move Up Move Down Remove View Details Modify	Add new Authentication Source														
Sagano AD [Active Directory]																
eTIPS_Local_User_Repository [Local SQL DE																
--Select--																
		Add														
Strip Username Rules: <input type="checkbox"/> Enable to specify a comma-separated list of rules to strip username prefixes or suffixes																

Note that when you configure posture policies, only those that are configured for the OnGuard Agent are shown in list of posture policies. Refer to 802.1X Wireless Service for description of the other tabs.



Web-based Health Check Only

This type of service is the same as the Web-based Authentication service, except that there is no authentication performed; only health checking is done. There is an internal service rule (*Connection:Protocol EQUALS WebAuth*) that categorizes request into this type of service. There is also an external service rule that is automatically added when you select this type of service: *Host:CheckType EQUALS Health*.

Service Type	Description/ Available Policy Components (in tabs)/ Service Rule (in Rules Editor)/ Service-specific policy components (called out with legend below)
 <p>Web-based Open Network Access</p>	<p>This type of service is similar to other Web-based services, except that authentication and health checking are not performed on the endpoint. A Terms of Service page (as configured on the Guest Portal page) is presented to the user. Network access is granted when the user click on the submit action on the page.</p>
 <p>802.1X Wireless - Identity Only</p>	<p>This type of service is the same as regular 802.1X Wireless Service, except that posture and audit policies are not configurable when you use this template.</p>
 <p>802.1X Wired - Identity Only</p>	<p>This type of service is the same as regular 802.1X Wired Service, except that posture and audit policies are not configurable when you use this template.</p>
 <p>RADIUS Enforcement [Generic]</p>	<p>Template for any kind of RADIUS request. Rules can be added to handle RADIUS requests that sends any type of standard or vendor-specific attributes.</p>  <p>Note: No default rule associated with this service type. Rules can be added to handle any type of standard or vendor-specific RADIUS attributes (any attribute that is loaded through the pre-packaged vendor-specific or standard RADIUS dictionaries, or through other dictionaries imported into Policy Manager).</p> <p>Refer to 802.1X Wireless Service for description of the other tabs.</p>

Service Type	Description/ Available Policy Components (in tabs)/ Service Rule (in Rules Editor)/ Service-specific policy components (called out with legend below)
--------------	-------------------------------------------------------------------------------------------------------------------------------------------------------



RADIUS Proxy

Template for any kind of RADIUS request that needs to be proxied to another RADIUS server (a Proxy Target).

- No default rule associated with this service type. Rules can be added to handle any type of standard or vendor-specific RADIUS attributes. Typically, proxying is based on a realm or domain of the user trying to access the network.

Authentication, Posture and Audit tabs are not shown for this service type.




Role mapping rules can be created based on the RADIUS attributes that are returned by the proxy target (using standard or vendor-specific RADIUS attributes).

The servers to which requests are proxied are called **Proxy Targets**. Requests can be dispatched to the proxy targets randomly; over time these requests are **Load Balanced**. Instead, in the **Failover** mode, requests can be dispatched to the first proxy target in the ordered list of targets, and then subsequently to the other proxy targets, sequentially, if the prior requests failed. When you **Enable proxy for accounting requests** accounting requests are also sent to the proxy targets.



Cisco 802.1X Wireless

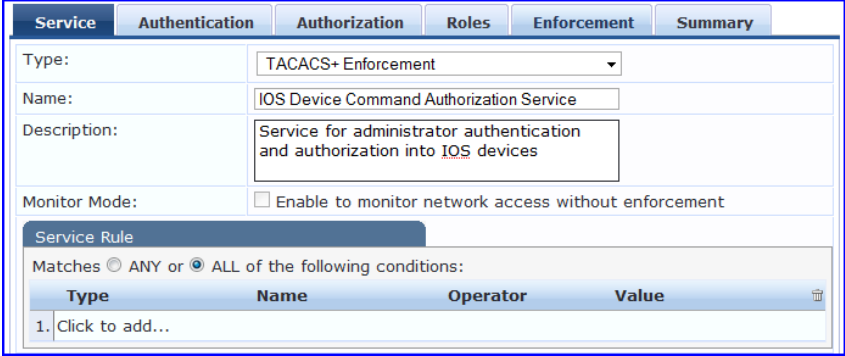
Template for wireless hosts connecting through Cisco 802.11 wireless access device or controller, with authentication via IEEE 802.1X. Service rules are customized for a typical Cisco WLAN Controller deployment.

Service Type	Description/ Available Policy Components (in tabs)/ Service Rule (in Rules Editor)/ Service-specific policy components (called out with legend below)
 Aruba 802.1X Wireless	Template for wireless hosts connecting through an Aruba 802.11 wireless access device or controller, with authentication via IEEE 802.1X. Service rules are customized for a typical Aruba WLAN Mobility Controller deployment.
 Xirrus 802.1X Wireless	Template for wireless hosts connecting through an Aruba 802.11 wireless array, with authentication via IEEE 802.1X. Service rules are customized for a typical Xirrus WLAN Array deployment.
 Meru 802.1X Wireless	Template for wireless hosts connecting through a Meru 802.11 wireless access device or controller, with authentication via IEEE 802.1X. Service rules are customized for a typical Meru WLAN Controller deployment.

Service Type	Description/ Available Policy Components (in tabs)/ Service Rule (in Rules Editor)/ Service-specific policy components (called out with legend below)
--------------	-------------------------------------------------------------------------------------------------------------------------------------------------------

Template for any kind of TACACS+ request.


TACACS+ Enforcement



Type	Name	Operator	Value
1. Click to add...			

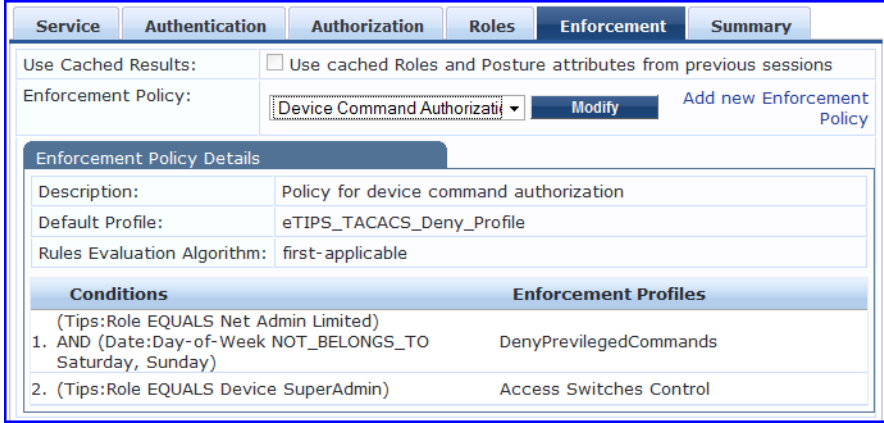
Note: No default rule associated with this service type. Rules can be added to filter the request based on the Date and Connection namespaces .

See “Rules Editing & Namespaces” (page 313).

TACACS+ users can be authenticated against any of the supported authentication source types: Local DB, SQL DB, Active Directory, LDAP Directory or Token Servers with a RADIUS interface. Similarly, service level authorization sources can be specified from the **Authorization** tab.

A role mapping policy can be associated with this service from the **Roles** tab.

The result of evaluating a TACACS+ enforcement policy is one or more TACACS+ enforcement profiles. For more information on TACACS+ enforcement profiles, see



Conditions	Enforcement Profiles
(Tips:Role EQUALS Net Admin Limited)	
1. AND (Date:Day-of-Week NOT_BELONGS_TO Saturday, Sunday)	DenyPrivilegedCommands
2. (Tips:Role EQUALS Device SuperAdmin)	Access Switches Control

“TACACS+ Enforcement Profiles” (page 215).

Service Type

Description/ Available Policy Components (in tabs)/ Service Rule (in Rules Editor)/ Service-specific policy components (called out with legend below)



Cisco Web-Authentication Proxy

Web-based authentication service for guests or agentless hosts. The Cisco switch hosts a captive portal; the portal web page collects username and password. The switch then sends a RADIUS request in the form of a PAP authentication request to Policy Manager.

Service	Authentication	Authorization	Roles	Audit	Enforcement	Summary
Type:	Cisco Web Authentication Proxy					
Name:						
Description:						
Monitor Mode:	<input type="checkbox"/> Enable to monitor network access without enforcement					
Service Rule						
Matches <input type="radio"/> ANY or <input checked="" type="radio"/> ALL of the following conditions:						
Type	Name	Operator	Value			
1. Radius:IETF	NAS-Port-Type	BELONGS_TO	Async (0), Wireless-802.11 (19)			
2. Radius:IETF	Service-Type	EQUALS	Outbound-User (5)			
3. Click to add...						

By default, this service uses:

- The Authentication Method *[PAP]* *[PAP]*

Refer to 802.1X Wireless Service for description of the tabs.



Aruba Application Authentication

This type of service provides authentication and authorization to users of Aruba applications: GuestConnect and Insight. “Application Enforcement Profiles” (page 218) can be sent to these or other generic applications for authorizing the users.

Service	Authentication	Roles	Enforcement	Summary
Type:	Aruba Application Authentication			
Name:				
Description:	Authentication service for applications			
Monitor Mode:	<input type="checkbox"/> Enable to monitor network access without enforcement			
Service Rule				
Matches <input type="radio"/> ANY or <input checked="" type="radio"/> ALL of the following conditions:				
Type	Name	Operator	Value	
1. Application	Name	EQUALS	Enter App Name	
2. Click to add...				

Adding and Modifying Services

You can use these service types as configured, or you can edit their settings.

From the **Services** page (**Configuration > Services**) or from the **Start Here** page (**Configuration > Start Here**), you can create a new service (**Add Service**). You can modify an existing service (by clicking on its name) in the **Configuration > Services** page.

Figure 10-3 Service Listing Page

Configuration » Services

Services

[Add Service](#)
[Import Services](#)
[Export Services](#)

Filter: contains [Go](#) [Clear Filter](#) Show records

#	<input type="checkbox"/>	Order ▲	Name	Type	Template	Status
1.	<input type="checkbox"/>	1	TG Wired Service	RADIUS	802.1X Wired	
2.	<input type="checkbox"/>	2	Avenda Employee Portal Service	RADIUS	RADIUS Enforcement (Generic)	
3.	<input type="checkbox"/>	3	Avenda Guest Portal Service	RADIUS	RADIUS Enforcement (Generic)	
4.	<input type="checkbox"/>	4	Avenda Unmanaged Hosts	RADIUS	MAC Authentication	
5.	<input type="checkbox"/>	5	Avenda Guest Access [No Health Check]	WEBAUTH	Avenda Web-based Authentication	
6.	<input type="checkbox"/>	6	Avenda Guest Service - WebAuth	RADIUS	RADIUS Enforcement (Generic)	[m]
7.	<input type="checkbox"/>	7	Handheld_a802.1X Wireless Service	RADIUS	802.1X Wireless	
8.	<input type="checkbox"/>	8	Avenda Wireless Service	RADIUS	802.1X Wireless	
9.	<input type="checkbox"/>	9	Avenda Wired Service	RADIUS	802.1X Wired	
10.	<input type="checkbox"/>	10	[eTIPS Admin Network Login Service]	TACACS	TACACS+ Enforcement	
11.	<input type="checkbox"/>	11	Wireless Admin Access	RADIUS	RADIUS Enforcement (Generic)	
12.	<input type="checkbox"/>	12	LegacyDot1X with CCA	RADIUS	802.1X Wired	
13.	<input type="checkbox"/>	13	North America Wireless Access	RADIUS	802.1X Wireless	
14.	<input type="checkbox"/>	14	Avenda RSA Token Server Service	RADIUS	RADIUS Enforcement (Generic)	
15.	<input type="checkbox"/>	15	Entertainment-Xirus Guest Service	RADIUS	Cisco Web Authentication Proxy	
16.	<input type="checkbox"/>	16	Device Authorization Service	TACACS	TACACS+ Enforcement	
17.	<input type="checkbox"/>	17	GuestConnect Application Service	Application	Avenda Application Authentication	
18.	<input type="checkbox"/>	18	Insight Application Service	Application	Avenda Application Authentication	
19.	<input type="checkbox"/>	19	Switch Keep-Alive Service	RADIUS	RADIUS Enforcement (Generic)	

Showing 1-19 of 19

[Reorder](#)
[Copy](#)
[Export](#)
[Delete](#)

Table 10-2 Service Listing Page Configuration

Label	Description
Add Service	Add a service
Import Services	Import previously exported services
Export Service	Export all currently defined services, including all associated policies
Filter	Filter the service listing by specifying values for different listing fields (Order, Name, Type, Template, Status)
Status	The green/red icon indicate enabled/disabled state. Clicking on the icon allows you to toggle the status of a Service between Enabled and Disabled. Note that when a service is in Monitor Mode, an <i>[m]</i> indicator is displayed next to the status icon.
Reorder	Reorder services (Refer to “ Reordering Services ” (page 101))
Copy	Create a copy of the service. An instance of the name prefixed with <i>Copy_of_</i> is created
Export	Export the selected services
Delete	Delete the selected services

Figure 10-4 Service Configuration

Service Rule				
Matches <input type="radio"/> ANY or <input checked="" type="radio"/> 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.	Radius:Airespace	Airespace-Wlan-Id	EQUALS	1
4.	Click to add...			

Table 10-3 Service Page (General Parameters)

Label	Description
Name	Label for a Service.
Description	Description for a Service (optional).
Monitor Mode	<p>Monitor Mode: Optionally, check here to allow authentication and health validation exchanges to take place between endpoint and Policy Manager, but without enforcement. In monitor mode, no enforcement profiles (and associated attributes) are sent to the network device.</p> <p>Policy Manager also allows <i>Policy Simulation</i> (Monitoring > Policy Simulation) where the administrator can test for the results of a particular configuration of policy components.</p>
Type	During Service creation, select from available types of Services. To create new Services, you can copy or import other Services for use <i>as is</i> or as templates, or you can create a new Service from scratch.
Status	The Enable/Disable button allows you to toggle the status of a Service between Enabled and Disabled.

Table 10-4 Service Page (Rules Editor)

Label	Description
Service Rule	<p>The rules editor appears throughout the Policy Manager interface. It exposes different namespace dictionaries depending on context. When working with service rules, you can select from the following namespace dictionaries:</p> <ul style="list-style-type: none"> • Date: Time-of-Day, Day-of-Week, or Date-of-Year • Connection: Originator address (Src-IP-Address, Src-Port), Destination address (Dest-IP-Address, Dest-Port), and Protocol • RADIUS: Policy Manager ships with a number of vendor-specific namespace dictionaries and distinguishes vendor-specific RADIUS namespaces with the notation <i>RADIUS:vendor</i> (sometimes with an additional suffix for a particular device). To add a dictionary for a vendor-specific RADIUS namespace, navigate to Administration > Dictionaries > Radius > Import Dictionary (link). The notation <i>RADIUS:IETF</i> refers to the RADIUS attributes defined in RFC 2865 and associated RFCs. As the name suggests, RADIUS namespace is only available when the request type is RADIUS. • Any other supported namespace. See “Namespaces” (page 314) for an exhaustive list of namespaces and their descriptions.
Name of attribute	Drop-down list of attributes present in the selected namespace.
Operator	Drop-down list of context-appropriate (with respect to the attribute) operators. See “Operators” (page 322) for an exhaustive list of operators and their descriptions.
Value of attribute	Depending on attribute data type, may be a free-form (one or many lines) edit box, a drop-down list, or a time/date widget.

Reordering Services

Policy Manager evaluates requests against the service rules of each service that is configured, in the order in which these services are defined. The service associated with the first matching service rule is then associated with this request. To change the order in which service rules are processed, you can change the order of services.

From the **Services** page (**Configuration > Services**), you can reorder services by clicking on the **(Reorder)** button.

Figure 10-5 Service Reorder Button

Configuration » Services

Services

Filter: Order equals Go Clear Filter Show 20 records

#	Order	Name	Type	Template	Status
14.	14	Entertainment-Xirrus Guest Service	RADIUS	Cisco Web Authentication Proxy	Disable
15.	15	Device Authorization Service	TACACS	TACACS+ Enforcement	Disable

Showing 1-15 of 15

Reorder Copy Export Delete

Figure 10-6 Reordering Services

Configuration » Services » Reorder

Reorder Services

Order	Name
1	TG Wired Service
2	Avenda Unmanaged Hosts
3	Avenda Guest Access [No Health Check]
4	Avenda Guest Service - WebAuth
5	Handheld_a802.1X Wireless Service
6	a802.1X Wireless Service
7	1_Enterprise Wireless Service
8	Avenda Wired Service
9	eTIPS_Admin_TACACS_Service
10	Wireless Admin Access
11	LegacyDot1X with CCA
12	North America Wireless Access
13	Avenda RSA Token Server Service

Move Up Move Down

Service Details:

Name: a802.1X Wireless Service

Template: 802.1X Wireless

Type: RADIUS

Description: Avenda Production 802.1x Wireless service

Status: Enabled

Service Rule

```
( (Radius:IETF:NAS-Port-Type EQUALS Wireless-802.11 (19))
AND (Radius:IETF:Service-Type BELONGS_TO Login-User (1), Framed-User (2),
Authenticate-Only (8))
AND (Radius:Airespace:Airespace-Wlan-Id EQUALS 1 ) )
AND (Connection:Protocol EQUALS RADIUS)
```

Back to Services Save Cancel

Table 10-5 Reordering Services

Label	Description
Move Up	Select a service from the list and move it up or down
MoveDown	
Save	Save the reorder operation
Cancel	Cancel the reorder operation

Chapter 11: Authentication & Authorization

As the first step in Service-based processing, Policy Manager uses an *Authentication Method* to authenticate the user or device against an *Authentication Source*. Once the user or device is authenticated, Policy Manager fetches attributes for role mapping policies from the *Authorization Sources* associated with this Authentication Source.

Architecture and Flow

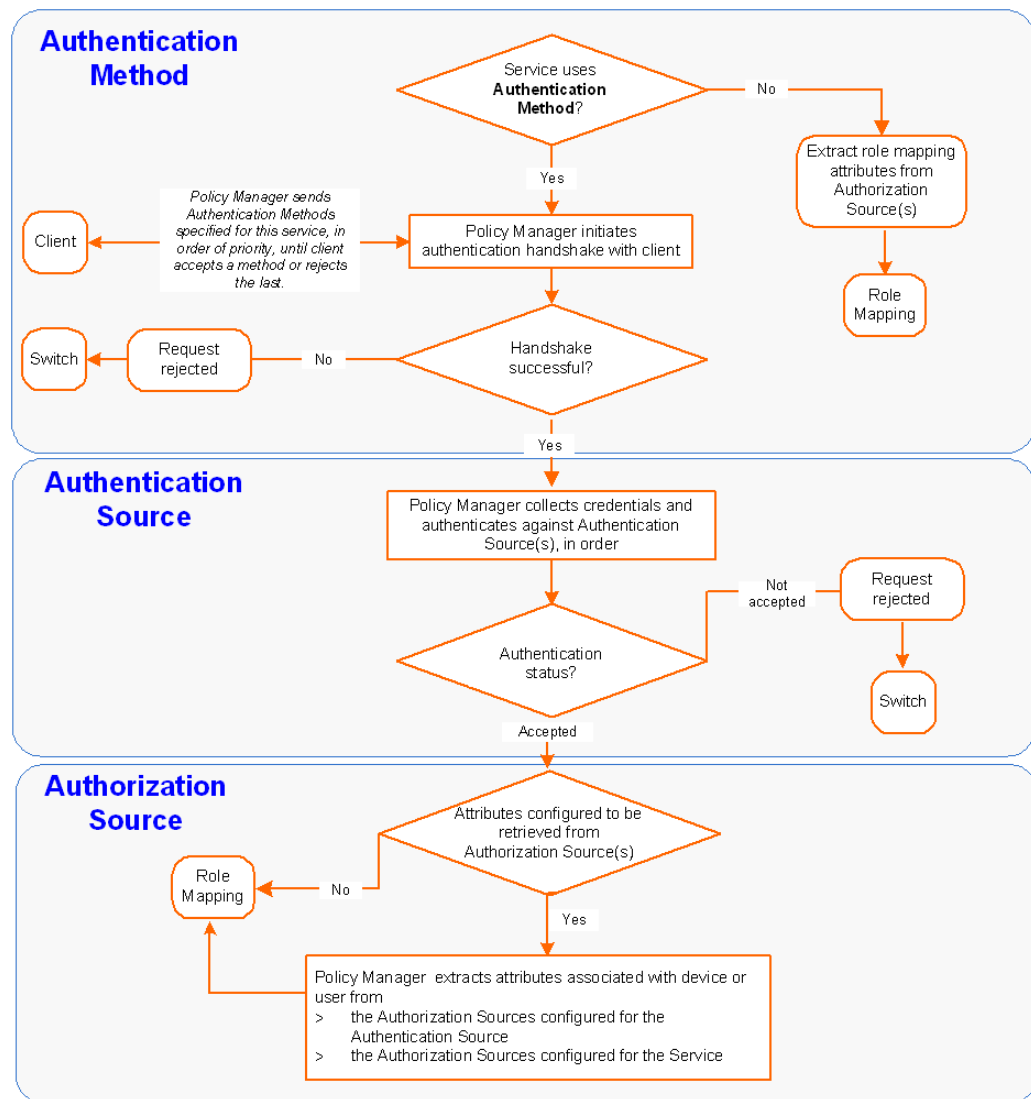
Policy Manager divides the architecture of authentication and authorization into three components:

- **Authentication Method.** Policy Manager initiates the authentication handshake by sending available methods, in priority order, until the client accepts a method or until it NAKs the last method, with the following possible outcomes:
 - Successful negotiation returns a method, for use in authenticating the client against the Authentication Source.
 - Where no method is specified (for example, for unmanageable devices), Policy Manager passes the request to the next configured policy component for this Service.
 - Policy Manager rejects the connection.
- **Note:** Note that an Authentication Method is only configurable for some service types (Refer to “[Policy Manager Service Types](#)” (page 85)). All 802.1X services (wired and wireless) have an associated Authentication Method. An authentication method (of type *MAC_AUTH*) can be associated with MAC authentication service type.
- **Authentication Source.** In Policy Manager, an authentication source is the identity store (Active Directory, LDAP directory, SQL DB, token server) against which users and devices are authenticated. Policy Manager first tests whether the connecting entity - device or user - is present in the ordered list of configured Authentication Sources. Policy Manager looks for the device or user by executing the first *Filter* associated with the authentication source. Once the device or user is found, Policy Manager then authenticates this entity against this authentication source. The flow is outlined below:
 - On successful authentication, Policy Manager moves on to the next stage of policy evaluation, which is to collect role mapping attributes from the authorization sources.

- Where no authentication source is specified (for example, for unmanageable devices), Policy Manager passes the request to the next configured policy component for this Service.
- If Policy Manager does not find the connecting entity in any of the configured authentication sources, it rejects the request.
- **Authorization Source.** In Policy Manager, an authorization source is the identity store (Active Directory, LDAP directory, SQL DB, token server) from which role mapping attributes are fetched. Authentication and authorization source definition is interchangeable in most use cases, because Policy Manager uses the same identity store to fetch role mapping attributes as it does for authenticating the user or device. Once the connecting entity is successfully authenticated, Policy Manager retrieves role mapping attributes from the authorization sources. In most use cases, Authentication and Authorization source refers to the same identity store. The flow is outlined below:
 - Once Policy Manager successfully authenticates the user or device against an authentication source, it retrieves role mapping attributes from each of the authorization sources configured for that authentication source. It also, optionally, can retrieve attributes from authorization sources configured for the Service.

The flow of control for authentication takes these components in sequence:

Figure 11-1 Authentication & Authorization Flow of Control



Configuring Authentication Components

To configure authentication, you can:

- For an existing Service, you can add or modify authentication method or source, by opening the Service (**Configuration > Services**, then select), then opening the **Authentication** tab.
- For a new Service, the Policy Manager wizard automatically opens the **Authentication** tab for configuration.
- Outside of the context of a particular Service, you can open an authentication method or source by itself: **Configuration >**

Authentication > Methods or Configuration > Authentication > Sources.

Figure 11-2 Authentication Components

Configuration » Services » Edit - a802.1X Wireless Service

Services - a802.1X Wireless Service

Authentication

Authentication Methods:

- eTIPS_EAP_PEAP [EAP-PEAP]
- eTIPS_EAP_FAST [EAP-FAST]
- Select--

Authentication Sources:

- Avenda_eTIPS_Local_User_Repository [Local User Repository]
- Avenda AD [Active Directory]
- Select--

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

[Back to Services](#) [Disable](#) [Copy](#) [Save](#) [Cancel](#)

From the **Authentication** tab of a service, you can configure three features of authentication:

Table 11-1 Authentication Features at the Service Level

Configurable Component	How to Configure
Sequence of Authentication Methods	<p>Select a Method, then Move Up, Move Down, or Remove. Select View Details to view the details of the selected method. Select Modify to modify the selected authentication method (This brings up a popup with the edit widgets for the select authentication method).</p> <p>To add a previously configured Authentication Method, select from the Select drop-down list, then click Add.</p> <p>To configure a new Method, click Add New Authentication Method (link) and refer to “Adding and Modifying Authentication Methods” (page 107).</p> <p>Note: Note that an Authentication Method is only configurable for some service types (Refer to “Policy Manager Service Types” (page 85)).</p>
Sequence of Authentication Sources	<p>Select an Source, then Move Up, Move Down, or Remove. Select View Details to view the details of the selected authentication source. Select Modify to modify the selected authentication source (This brings up authentication source configuration wizard for the selected authentication source).</p> <p>To add a previously configured Authentication Source, select from the Select drop-down list, then click Add.</p> <p>To configure a new Authentication Source, click Add New Authentication Source (link) and refer to “Adding and Modifying Authentication Sources” (page 119).</p>

Configurable Component	How to Configure
Whether to standardize the form in which usernames are presented.	Select <i>Enable to specify a comma-separated list of rules to strip usernames</i> (checkbox) to pre-process the user name (to remove prefixes and suffixes) before authenticating it to the authentication source.

Adding and Modifying Authentication Methods

Policy Manager supports specific EAP and non-EAP, tunneled and non-tunneled, methods.

Table 11-2 Policy Manager Supported Authentication Methods

	EAP	Non-EAP
Tunneled	<ul style="list-style-type: none"> EAP Protected EAP (EAP-PEAP) EAP Flexible Authentication Secure Tunnel (EAP-FAST) EAP Transport Layer Security (EAP-TLS) EAP Tunneled TLS (EAP-TTLS) 	
Non-Tunneled	<ul style="list-style-type: none"> EAP Message Digest 5 (EAP-MD5) EAP Microsoft Challenge Handshake Authentication Protocol version 2 (EAP-MSCHAPv2) EAP Generic Token Card (EAP-GTC) 	<ul style="list-style-type: none"> Challenge Handshake Authentication Protocol (CHAP) Password Authentication Protocol (PAP) Microsoft CHAP version 1 and version 2 MAC Authentication Method (MAC-AUTH) MAC-AUTH must be used exclusively in a MAC-based Authentication Service. When the MAC_AUTH method is selected, Policy Manager makes internal checks to verify that the request is indeed a <i>MAC_Authentication</i> request (and not a spoofed request).

Note: In tunneled EAP methods, authentication and posture credential exchanges happen inside of a protected outer tunnel.

From the **Services** page (**Configuration > Service**), you can configure authentication for a new service (as part of the flow of the **Add Service** wizard), or modify an existing authentication method directly (**Configuration > Authentication > Methods**, then click on its name in the Authentication Methods listing).

When you click **Add New Authentication Method** from any of these locations, Policy Manager displays the **Add Authentication Method** popup.

Figure 11-3 Add Authentication Method (popup)

Configuration » Authentication » Methods

Add Authentication Method

General

Name:

Description:

Type:

PAP

CHAP

MSCHAP

EAP-MD5

EAP-MSCHAPv2

EAP-GTC

EAP-TLS

EAP-TTLS

EAP-PEAP

EAP-FAST

MAC-AUTH

Save Cancel

Filter: Show 20 records

1.	s for EAP-FAST
2.	s for EAP-TTLS
3.	s for CHAP
4.	s for EAP-FAST
5.	s for EAP-GTC
6.	s for EAP-MD5
7.	s for EAP-MSCHAPv2
8.	s for EAP-PEAP
9.	s for EAP-PEAP used for EAPoUDP
10.	s for EAP-TLS
11.	s for EAP-TTLS
12.	s for MAC-AUTH
13.	s for MSCHAP

Depending on the **Type** selected, different tabs and fields appear. Refer to:

- “EAP-FAST” (page 108)
- “EAP-PEAP” (page 112)
- “EAP-TLS” (page 114)
- “EAP-TTLS” (page 115)
- “MAC-AUTH” (page 117)
- “MSCHAP” (page 118)
- “PAP” (page 118)
- “CHAP & EAP-MD5” (page 119)

EAP-FAST

The EAP-FAST method contains four tabs:

- The **General** Tab labels the method and defines session details.

Figure 11-4 EAP-FAST (General Tab)

Add Authentication Method

General Inner Methods PACs PAC Provisioning

Name:

Description:

Type:

Method Details

Session Resumption: ☒ Enable

Session Timeout: hours

Client Authentication:

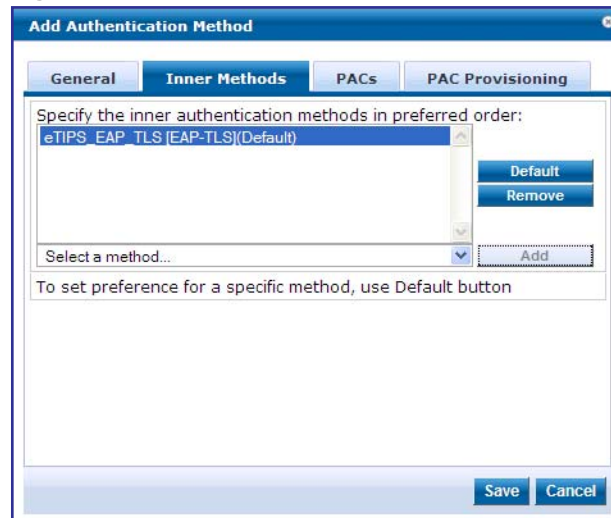
Certificate Comparison:

Save Cancel

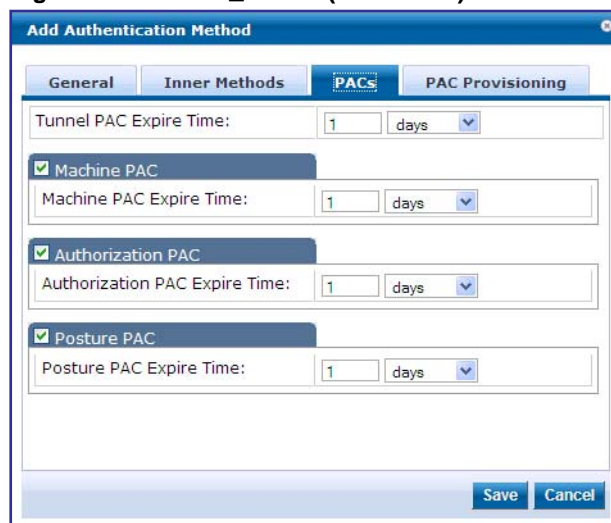
Table 11-3 EAP_FAST (General Tab)

Parameter	Description
Name/Description	Freeform label and description.
Type	In this context, always <i>EAP_FAST</i> .
Session Resumption.	Caches EAP-FAST sessions on Policy Manager for reuse if the user/end-host reconnects to Policy Manager within the session timeout interval.
Session Timeout	Caches EAP-FAST sessions on Policy Manager for reuse if the user/end-host reconnects to Policy Manager within the session timeout interval. If session timeout value is set to 0, the cached sessions are not purged.
Fast Reconnect	Enable to allow fast reconnect. When enabled, the inner method of the server-authenticated outer tunnel is also bypassed. This makes the process of re-authentication faster. For fast reconnect to work, <i>session resumption</i> must be enabled.
End-Host Authentication	Refers to establishing the EAP-Fast Phase 1 Outer tunnel: <ul style="list-style-type: none"> Choose <i>Using PACs</i> to use a strong shared secret. Choose <i>Using Client Certificate</i> to use a certificate.
Certificate Comparison.	Type of certificate comparison (identity matching) upon presenting Policy Manager with a client certificate: <ul style="list-style-type: none"> To skip the certificate comparison, choose <i>Do not compare</i>. To compare specific attributes, choose <i>Compare Common Name (CN)</i>, <i>Compare Subject Alternate Name (SAN)</i>, or <i>Compare CN or SAN</i>. To perform a binary comparison of the <i>stored</i> (in the end-host record in Active Directory or another LDAP-compliant directory) and <i>presented</i> certificates, choose <i>Compare Binary</i>.

- The **Inner Methods** Tab controls the inner methods for the EAP-FAST method:

Figure 11-5 Inner Methods Tab

- To *append* an inner method to the displayed list, select it from the drop-down list, then click **Add**. The list can contain multiple inner methods, which Policy Manager will send, in priority order, until negotiation succeeds.
- To *remove* an inner method from the displayed list, select the method and click **Remove**.
- To *set* an inner method as the default (the method tried first), select it and click **Default**.
- The **PACs** Tab enables/disables PAC types:

Figure 11-6 EAP_FAST (PACs Tab)

- To *provision a Tunnel PAC* on the end-host after initial successful machine authentication, enable the **Tunnel PAC** check box. During authentication, Policy Manager can use the *Tunnel PAC* shared secret to create the outer EAP-FAST tunnel. Specify **Tunnel PAC Expire Time**

(until the PAC expires and must be replaced, by automatic or manual provisioning) in hours, days, weeks, months, or years.

- To *provision a Machine PAC* on the end-host after initial successful machine authentication, enable the **Machine PAC** check box. During authentication, Policy Manager can use the *Machine PAC* shared secret to create the outer EAP-FAST tunnel. Specify **Machine PAC Expire Time** (until the PAC expires and must be replaced, by automatic or manual provisioning) in hours, days, weeks, months, or years. This can be a long-lived PAC (specified in months and years).
- To *provision an authorization PAC* upon successful user authentication, enable the **Authorization PAC** check box. Authorization PAC results from a prior user authentication and authorization. When presented with a valid Authorization PAC, Policy Manager skips the inner user authentication handshake within EAP-FAST. Specify **Authorization PAC Expire Time** (until the PAC expires and must be replaced, by automatic or manual provisioning) in hours, days, weeks, months, or years. This is typically a short-lived PAC (specified in hours, rather than months and years).
- To *provision a posture PAC* upon successful posture validation, enable the **Posture PAC** check box. Posture PACs result from prior posture evaluation. When presented with a valid Posture PAC, Policy Manager skips the posture validation handshake within the EAP-FAST protected tunnel; the prior result is used to ascertain end-host health. Specify **Authorization PAC Expire Time** (until the PAC expires and must be replaced, by automatic or manual provisioning) in hours, days, weeks, months, or years. This is typically a short-lived PAC (specified in hours, rather than months and years).
- The **PAC Provisioning** Tab controls anonymous and authenticated modes:

Figure 11-7 EAP_FAST (PAC Provisioning Tab)

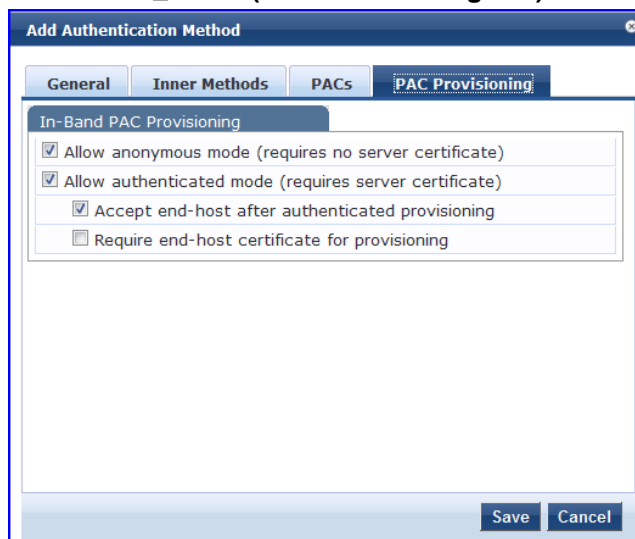


Table 11-4 EAP_FAST (PAC Provisioning Tab)

Parameter	Description	Considerations
Allow Anonymous Mode	<p>When in anonymous mode, <i>phase 0</i> of EAP_FAST provisioning establishes an outer tunnel without end-host/Policy Manager authentication (not as secure as the authenticated mode).</p> <p>Once the tunnel is established, end-host and Policy Manager perform mutual authentication using MSCHAPv2, then Policy Manager provisions the end-host with an appropriate PAC (tunnel or machine).</p>	<p><i>Authenticated mode</i> is more secure than <i>anonymous provisioning mode</i>. Once the server is authenticated, the phase 0 tunnel is established, the end-host and Policy Manager perform mutual authentication, and Policy Manager provisions the end-host with an appropriate PAC (tunnel or machine):</p> <ul style="list-style-type: none"> • If both anonymous and authenticated provisioning modes are enabled, and the end-host sends a cipher suite that supports server authentication, Policy Manager picks the authenticated provisioning mode. • Otherwise, if the appropriate cipher suite is supported by the end-host, Policy Manager performs anonymous provisioning.
Allow Authenticated Mode	<p>Enable to allow authenticated mode provisioning. When in Allow Authenticated Mode <i>phase 0</i>, Policy Manager establishes the outer tunnel inside of a server-authenticated tunnel. The end-host authenticates the server by validating the Policy Manager certificate.</p>	
Accept end-host after authenticated provisioning	<p>Once the authenticated provisioning mode is complete and the end-host is provisioned with a PAC, Policy Manager rejects end-host authentication; the end-host subsequently reauthenticates using the newly provisioned PAC. When enabled, Policy Manager accepts the end-host authentication in the provisioning mode itself; the end-host does not have to re-authenticate.</p>	
Required end-host certificate for provisioning	<p>In authenticated provisioning mode, the end-host authenticates the server by validating the server certificate, resulting in a protected outer tunnel; the end-host is authenticated by the server inside this tunnel. When enabled, the server can require the end-host to send a certificate inside the tunnel for the purpose of authenticating the end-host.</p>	

EAP-PEAP

The EAP-PEAP method contains two tabs:

- The **General** Tab labels the method and defines session details.

Figure 11-8 EAP-PEAP (General Tab)

Add Authentication Method

General | Inner Methods

Name:

Description:

Type: EAP-PEAP

Method Details

Session Resumption: ☒ Enable

Session Timeout: hours

Fast Reconnect: ☒ Enable

EAPoUDP Support: ☐ Enable

Microsoft NAP Support: ☒ Enable

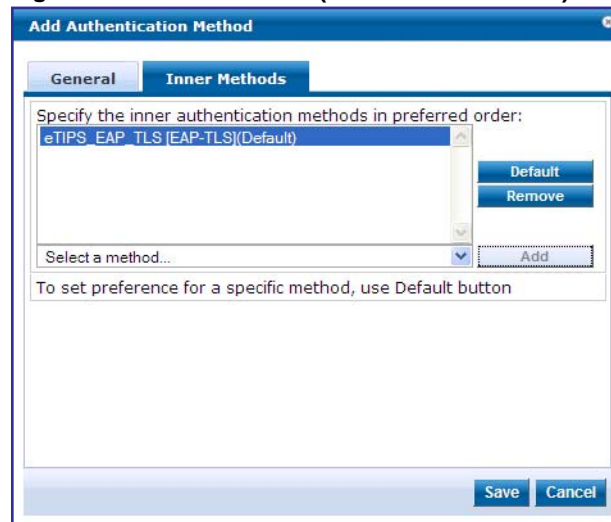
Enforce Cryptobinding: ☐ Enable

Save **Cancel**

Table 11-5 EAP-PEAP (General Tab)

Parameter	Description
Name/Description	Freeform label and description.
Type	In this context, always <i>EAP-PEAP</i> .
Session Resumption.	Caches EAP-PEAP sessions on Policy Manager for reuse if the user/client reconnects to Policy Manager within the session timeout interval.
Session Timeout	Caches EAP-PEAP sessions on Policy Manager for reuse if the user/client reconnects to Policy Manager within the session timeout interval. If session timeout value is set to 0, the cached sessions are not purged.
Fast Reconnect	Enable this checkbox to allow fast reconnect; when fast reconnect is enabled, the inner method that happens inside the server authenticated outer tunnel is also bypassed. This makes the process of re-authentication faster. For fast reconnect to work, session resumption must be enabled.
EAPoUDP Support	Enable EAPoUDP support. When EAPoUDP support is enabled Policy Manager does not expect user authentication to happen within the protected tunnel.
Microsoft NAP Support	Enable while Policy Manager establishes the protected PEAP tunnel with a Microsoft NAP-enabled client. When enabled, Policy Manager prompts the client for Microsoft Statement of Health (SoH) credentials.
Enforce Cryptobinding	Enabling the cryptobinding setting ensures an extra level of protection for PEAPv0 exchanges. It ensures that the PEAP client and PEAP server (Policy Manager) participated in both the outer and inner handshakes. This is currently valid only for the client PEAP implementations in Windows 7, Windows Vista and Windows XP SP3.

- The **Inner Methods** Tab controls the inner methods for the EAP-PEAP method:

Figure 11-9 EAP-PEAP (Inner Methods Tab)

Select any method available in the current context from the drop-down list. Functions available in this tab include:

- To *append* an inner method to the displayed list, select it from the drop-down list, then click **Add**. The list can contain multiple inner methods, which Policy Manager will send, in priority order, until negotiation succeeds.
- To *remove* an inner method from the displayed list, select the method and click **Remove**.
- To *set* an inner method as the default (the method tried first), select it and click **Default**.

EAP-TLS

The EAP-TLS method contains one tab that labels the method and defines session details.

Figure 11-10 EAP_TLS (General Tab)

The screenshot shows a Windows-style dialog box titled "Add Authentication Method". It has a "General" tab selected. The "General" tab contains three input fields: "Name:", "Description:", and "Type:". The "Type:" dropdown is set to "EAP-TLS". Below these is a "Method Details" section. It contains three settings: "Session Resumption:" with a checked checkbox and the text "Enable"; "Session Timeout:" with a text box containing "6" and the label "hours"; and "Certificate Comparison:" with a dropdown menu set to "Do not compare". At the bottom right of the dialog are "Save" and "Cancel" buttons.

Table 11-6 EAP_TLS (General Tab)

Parameter	Description
Name/Description	Freeform label and description.
Type	In this context, always <i>EAP_TLS</i> .
Session Resumption.	Caches EAP-TLS sessions on Policy Manager for reuse if the user/client reconnects to Policy Manager within the session timeout interval.
Session Timeout.	How long (in hours) to retain cached EAP-TLS sessions.
Certificate Comparison.	Type of certificate comparison (identity matching) upon presenting Policy Manager with a client certificate: <ul style="list-style-type: none"> • To skip the certificate comparison, choose <i>Do not compare</i>. • To compare specific attributes, choose <i>Compare Common Name (CN)</i>, <i>Compare Subject Alternate Name (SAN)</i>, or <i>Compare CN or SAN</i>. • To perform a binary comparison of the <i>stored</i> (in the client record in Active Directory or another LDAP-compliant directory) and <i>presented</i> certificates, choose <i>Compare Binary</i>.

EAP-TTLS

The EAP-TTLS method contains two tabs:

- The **General** Tab labels the method and defines session details.

Figure 11-11 EAP_TTLS (General Tab)

The screenshot shows the 'Add Authentication Method' dialog box with the 'General' tab selected. The 'Type' dropdown is set to 'EAP-TTLS'. Under the 'Method Details' section, 'Session Resumption' is checked and 'Session Timeout' is set to 6 hours. The 'Save' and 'Cancel' buttons are located at the bottom right of the dialog.

Table 11-7 EAP_TTLS (General Tab)

Parameter	Description
Name/Description	Freeform label and description.
Type	In this context, always <i>EAP_TTLS</i> .
Session Resumption.	Caches EAP-TTLS sessions on Policy Manager for reuse if the user/client reconnects to Policy Manager within the session timeout interval.
Session Timeout.	How long (in hours) to retain cached EAP-TTLS sessions.

- The **Inner Methods** Tab controls the inner methods for the EAP-TTLS method:

Figure 11-12 EAP_TTLS (Inner Methods Tab)

The screenshot shows the 'Add Authentication Method' dialog box with the 'Inner Methods' tab selected. The 'Type' dropdown is still set to 'EAP-TTLS'. Under the 'Method Details' section, 'Session Resumption' is checked and 'Session Timeout' is set to 6 hours. The 'Save' and 'Cancel' buttons are located at the bottom right of the dialog.

Select any method available in the current context from the drop-down list. Functions available in this tab include:

- To *append* an inner method to the displayed list, select it from the drop-down list, then click **Add**. The list can contain multiple inner methods, which Policy Manager will send, in priority order, until negotiation succeeds.
- To *remove* an inner method from the displayed list, select the method and click **Remove**.
- To *set* an inner method as the default (the method tried first), select it and click **Default**.

MAC-AUTH

The MAC-AUTH method contains one tab that labels the method and defines session details.

Figure 11-13 MAC-AUTH (General Tab)

Table 11-8 MAC-AUTH (General Tab)

Parameter	Description
Name/Description	Freeform label and description.
Type	In this context, always <i>MAC_AUTH</i> .
Allow Unknown End-Hosts	<p>Enables further policy processing of MAC authentication requests of unknown clients.</p> <p><i>If not enabled</i>, Policy Manager automatically rejects a request whose MAC address is not in a configured authentication source. This setting is enabled, for example, when you want Policy Manager to trigger an audit for an unknown client. By turning on this checkbox and enabling audit (See “Built-In Audit Servers” (page 194)), you can trigger an audit of an unknown client.</p>

MSCHAP

The MS_CHAP method contains one tab that labels the method and defines session details.

Figure 11-14 MSCHAP (General Tab)

The screenshot shows a window titled "Add Authentication Method". Inside, the "General" tab is active. There are three input fields: "Name:" with a text box, "Description:" with a larger text box, and "Type:" with a dropdown menu currently showing "MSCHAP". At the bottom right, there are "Save" and "Cancel" buttons.

Table 11-9 MSCHAP (General Tab)

Tab	Parameter	Description
General	Name/Description	Freeform label and description.
	Type	In this context, always <i>MS_CHAP</i> .

PAP

The PAP method contains one tab:

- The **General** Tab labels the method and defines session details.

Figure 11-15 PAP (General Tab)

The screenshot shows a window titled "Add Authentication Method". Inside, the "General" tab is active. There are three input fields: "Name:" with a text box, "Description:" with a larger text box, and "Type:" with a dropdown menu currently showing "PAP". Below these fields is a section titled "Method Details" which contains an "Encryption Scheme:" dropdown menu. This menu is open, showing a list of options: "Clear", "Crypt", "MD5", and "SHA1". At the bottom right, there are "Save" and "Cancel" buttons.

Table 11-10 PAP (General Tab)

Tab	Parameter	Description
General	Name/Description	Freeform label and description.
	Type	In this context, always <i>PAP</i> .
	Encryption Scheme	Select the PAP authentication encryption scheme. Supported schemes are: Clear, Crypt, MD5 and SHA1.

CHAP & EAP-MD5

Besides the methods listed above, Policy Manager also comes packaged with CHAP and EAP-MD5 methods. These are named [CHAP] and [EAP MD5], respectively. You can add methods of this type with a custom name. These methods can also be associated to a *Service* as authentication methods.

Adding and Modifying Authentication Sources

Policy Manager supports five specific Authentication Sources:

Table 11-11 Policy Manager Supported Authentication Sources

Source	Description	Special Considerations
Active Directory	Policy Manager can perform NTLM/MSCHAPv2, PAP/GTC and certificate-based authentications against Microsoft Active Directory.	Retrieve role mapping attributes by using filters. See “Adding and Modifying Role Mapping Policies” (page 144)
LDAP compliant directory service	Policy Manager can perform MSCHAPv2 and PAP/GTC authentication against any LDAP-compliant directory (for example, Novell eDirectory, OpenLDAP, or Sun Directory Server).	Retrieve role mapping attributes by using filters..
Kerberos service	Policy Manager can perform standard PAP/GTC or tunneled PAP/GTC (for example, EAP-PEAP[EAP-GTC]) authentication against any Kerberos 5 compliant server such as the Microsoft Active Directory server.	It is mandatory to pair this Source type with an authorization source (identity store) containing user records.
Open Data Base Connectivity (ODBC) compliant SQL databases	Policy Manager can perform MSCHAPv2 and PAP/GTC authentication against any ODBC-compliant database (for example, Microsoft SQL Server, Oracle, MySQL, or PostgreSQL).	Specify a stored procedure to query the relevant tables. Retrieve role mapping attributes by using filters.

Source	Description	Special Considerations
Token Servers (for example, RSA SecurID)	<p>Policy Manager can perform GTC authentication against any token server than can authenticate users by acting as a RADIUS server (e.g., RSA SecurID Token Server).</p> <p>Policy Manager can authenticate users against a token server and fetch role mapping attributes from any other configured Authorization Source.</p>	<p>Pair this Source type with an authorization source (identity store) containing user records.</p> <p>When using a token server as an authentication source, use the administrative interface to optionally configure a separate authorization server.</p> <p>Note: Policy Manager can also use the RADIUS attributes returned from a token server to create role mapping policies. See “Namespaces” (page 314).</p>
Internal User Database	<p>An internal relational database stores Policy Manager configuration data and locally configured user and device accounts.</p> <p>Three pre-defined authentication sources, <i>[Local User Repository]</i>, <i>[Guest User Repository]</i>, and <i>[Guest Device Repository]</i>, represent the three databases used to store local users, guest users and registered devices, respectively.</p> <p>While regular users typically reside in an authentication source such as Active Directory (or in other LDAP-compliant stores), temporary users, including guest users can be configured in the Policy Manager local repositories.</p> <p>For a user account created in the local database, the role is statically assigned to that account, which means a role mapping policy need not be specified for user accounts in the local database. However, if new custom attributes are assigned to a user (local or guest) account in the local database, these can be used in role mapping policies.</p>	<p>The local user database is pre-configured with a filter to retrieve the password and the expiry time for the account.</p> <p>Policy Manager can perform MSCHAPv2 and PAP/GTC authentication against the local database.</p>

From the **Services** page (**Configuration > Service**), you can configure authentication source for a new service (as part of the flow of the **Add Service** wizard), or modify an existing authentication source directly (**Configuration > Authentication > Sources**, then click on its name in the listing page).

Figure 11-16 Authentication Sources Listing Page

Configuration » Authentication » Sources

Authentication Sources

[Add Authentication Source](#)
[Import Authentication Sources](#)
[Export Authentication Sources](#)

Filter: Name contains Go Clear Filter Show 10 records

#	<input type="checkbox"/>	Name ▲	Type	Description
1.	<input type="checkbox"/>	Active_Directory(Traffic Generator)	Active Directory	Authenticate users against Active Directory
2.	<input type="checkbox"/>	Avenda AD	Active Directory	Avenda AD
3.	<input type="checkbox"/>	Avenda_eTIPS_Local_User_Repository	Local SQL DB	Authenticate users against eTIPS local user database
4.	<input type="checkbox"/>	eTIPS_Clients_White_List_LDAP	Generic LDAP	
5.	<input type="checkbox"/>	eTIPS_Local_User_Repository	Local SQL DB	Authenticate users against eTIPS local user database
6.	<input type="checkbox"/>	Handhelds	Static Host List	Auth source for handhelds. Right now, we use a statically configured host list in eTIPS
7.	<input type="checkbox"/>	Sagano AD	Active Directory	Active Directory Domain Controller for Sagano
8.	<input type="checkbox"/>	Test RSA Token Server	Token Server	Test server for RSA OTP authentication

Showing 1-8 of 8

Copy Export Delete

When you click **Add New Authentication Source** from any of these locations, Policy Manager displays the **Add** page.

Figure 11-17 Add Authentication Source Page

Configuration » Authentication » Sources » Add

Authentication Sources

General

Name:

Description:

Type: Kerberos

Use for Authorization: ☐ Enable to use this authentication source to also fetch role mapping attributes

Authorization Sources:

Remove View Details

Back to Authentication Sources Next > Save Cancel

Depending on the **Authentication Source** selected, different tabs and fields appear. Refer to:

- “Generic LDAP or Active Directory” (page 122)
- “Kerberos” (page 133)
- “Generic SQL DB” (page 134)
- “Token Server” (page 138)
- “Static Host List” (page 141)

Generic LDAP or Active Directory

Both LDAP and Active Directory based server configurations are similar. At the top level, there are buttons to:

- **Clear Cache:** Clears the attributes cached by Policy Manager for all entities that authorize against this server.
- **Copy:** Creates a copy of this authentication/authorization source.

The Generic LDAP and Active Directory authentication sources contain three tabs:

- The **General** Tab labels the authentication source and defines session details.

Figure 11-18 Generic LDAP or Active Directory (General Tab)

Configuration » Authentication » Sources » Add

Authentication Sources

General Primary Attributes Summary

Name:

Description:

Type:

Use for Authorization: ☒ Enable to use this authentication source to also fetch role mapping attributes

Authorization Sources:

Backup Servers -

Server Timeout: seconds

Server Priority:

[Back to Authentication Sources](#)

Table 11-12 Generic LDAP or Active Directory (General Tab)

Parameter	Description
Name/Description	Freeform label and description.
Type	In this context, <i>Generic LDAP</i> or <i>Active Directory</i> .
Use for Authorization	<p>This checkbox instructs Policy Manager to fetch role mapping attributes (or authorization attributes) from this authentication source. If a user or device successfully authenticates against this authentication source, then Policy Manager also fetches role mapping attributes from the same source (if this setting is enabled).</p> <p>This box is checked (enabled) by default</p>

Parameter	Description
Authorization Sources	<p>You can specify additional sources from which to fetch role mapping attributes. Select a previously configured authentication source from the drop down list, and click Add to add it to the list of authorization sources. Click Remove to remove it from the list.</p> <p>If Policy Manager authenticates the user or device from this authentication source, then it also fetches role mapping attributes from these additional authorization sources.</p> <p>Note: As described in the “Services” (page 83) chapter, additional authorization sources can be specified at the Service level. Policy Manager fetches role mapping attributes regardless of which authentication source the user or device was authenticated against.</p>
Backup Servers	<p>To add a backup server, click Add Backup. When the Backup 1 tab appears, you can specify connection details for a backup server (same fields as for primary server, specified below).</p> <p>To remove a backup server, select the server name and click Remove. Move Up or Move Down to change the server priority of the backup servers. This is the order in which Policy Manager attempts to connect to the backup servers. Server Timeout is the time in seconds that Policy Manager waits before attempting to fail over from primary to the backup servers (in the order in which they are configured)</p>
Server Timeout	The time period that Policy Manager waits before considering this server unreachable.
Cache Timeout	Policy Manager caches attributes fetched for an authenticating entity. This parameter controls the time period for which the attributes are cached.

- The **Primary** Tab defines the settings for the primary server.

Figure 11-19 Generic LDAP or Active Directory (Primary Tab)

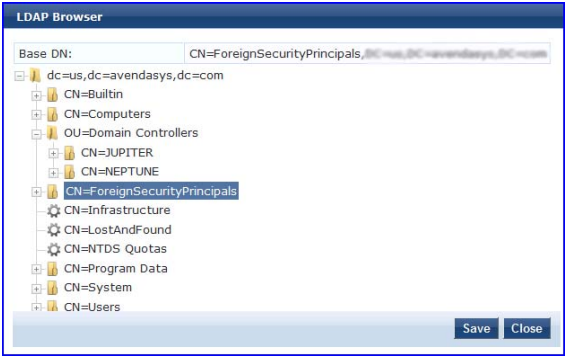
The screenshot shows the 'Primary' tab of the configuration window. The 'Connection Details' section includes the following fields and values:

- Host Name: sense.sagano.com
- Connection Security: StartTLS
- Port: 389 (For secure connection, use 636)
- Bind DN: cn=admin, ou=sense, dc=sagano, dc=com (e.g. administrator@example.com OR cn=admin, ou=sense, dc=sagano, dc=com)
- Bind Password: [Masked]
- Base DN: ou=employees, ou=sense, dc=sagano, dc=com
- Search Scope: SubTree Search
- LDAP Referrals: ☒ Follow referrals
- Bind User: ☐ Allow bind using user password
- User Certificate : userCertificate

At the bottom of the window, there is a 'Back to Authentication Sources' button and 'Copy', 'Save', and 'Cancel' buttons.

Table 11-13 Generic LDAP or Active Directory (Primary Tab)

Parameter	Description
Host Name/Port	<ul style="list-style-type: none"> • Hostname or IP address of the LDAP or Active Directory server. • TCP port at which the LDAP or Active Directory Server is listening for connections. (The default TCP port for LDAP connections is 389. The default port for LDAP over SSL is 636).
Connection Security	<ul style="list-style-type: none"> • Select <i>None</i> for default non-secure connection (usually port 389) • Select <i>StartTLS</i> for secure connection that is negotiated over the standard LDAP port. This is the preferred way to connect to an LDAP directory securely. • Select <i>LDAP over SSL</i> or <i>AD over SSL</i> to choose the legacy way of securely connecting to an LDAP directory. Port 636 must be used for this type of connection.
Bind DN/Password	<p>Distinguished Name (DN) of the administrator account. Policy Manager uses this account to access all other records in the directory.</p> <p>Note that, for Active Directory, the bind DN can also be in the administrator@domain format (e.g., administrator@acme.com).</p> <p>Password for the administrator DN entered in the Bind DN field.</p>
NetBIOS Domain Name	<p>The AD domain name for this server. Policy Manager prepends this name to the user ID to authenticate users found in this Active Directory.</p> <p>Note: This setting is only available for Active Directory.</p>

Parameter	Description
Base DN	<p>Enter DN of the node in your directory tree from which to start searching for records.</p> <p>Once you have entered values for the fields described above, click on Search Base DN to browse the directory hierarchy. The LDAP Browser is popped up. You can navigate to the DN that you want to use as the Base DN.</p> 
	<p>Click on any node in the tree structure that is displayed to select it as a Base DN. Note that the Base DN is displayed at the top of the LDAP Browser.</p> <p>Note: This is also one way to test the connectivity to your LDAP or AD directory. If the values entered for the primary server attributes are correct, you should be able to browse the directory hierarchy by clicking on Search Base DN</p>
Search Scope	<p>Scope of the search you want to perform, starting at the Base DN.</p> <ul style="list-style-type: none">• Subtree Search allows you to search the entire subtree under the base DN (including at the base DN level).• One Level Search allows you to search up to one level below (immediate children of) the base DN.• Base Object Search allows you to search at the level specified by the base DN.
LDAP Referral	<p>Enable this checkbox to automatically follow referrals returned by your directory server in search results. Refer to your directory documentation for more information on referrals.</p>

Parameter	Description
Bind User	<p>Enable to authenticate users by performing a bind operation on the directory using the credentials (user name and password) obtained during authentication.</p> <p>For clients to be authenticated by using the LDAP bind method, Policy Manager must receive the password in cleartext.</p>
Password Attribute (Present only for Generic LDAP directory)	Enter the name of the attribute in the user record from which user password can be retrieved. This is not available for Active Directory.
User Certificate	Enter the name of the attribute in the user record from which user certificate can be retrieved.

- The **Attributes** Tab defines the LDAP or Active Directory query filters and the attributes to be fetched by using those filters.

Figure 11-20 Active Directory Attributes Tab (With Default Data)

Filter Name	Attribute Name	Alias Name	Enable as role
1. Authentication	dn	UserDN	false
	department	department	false
	title	title	false
	company	company	false
	memberOf	memberOf	false
2. Group	cn	groupName	false
3. Machine	dNSHostName	hostDnsName	false
	operatingSystem	hostOperatingSystem	false
	operatingSystemServicePack	hostServicePack	false

Figure 11-21 Generic LDAP Directory Attributes Tab (With Default Data)

Filter Name	Attribute Name	Alias Name	Enable as role
1. Authentication	dn	UserDN	false
2. Group	cn	groupName	false

When you add a new authentication source of type Active Directory or LDAP, a few default filters and attributes are pre-populated. You can add other filters and attributes, or you can modify the pre-defined filters.

Note: Note that at least one filter must be specified for the LDAP and Active Directory authentication source. This filter is used by Policy Manager to search for the user or device record. If not specified, authentication requests will be rejected.

Note: The attributes that are defined for the authentication source show up as attributes in role mapping policy rules editor (under the authentication source instance namespace).

Table 11-14 AD/LDAP Attributes Tab (Filter Listing Screen)

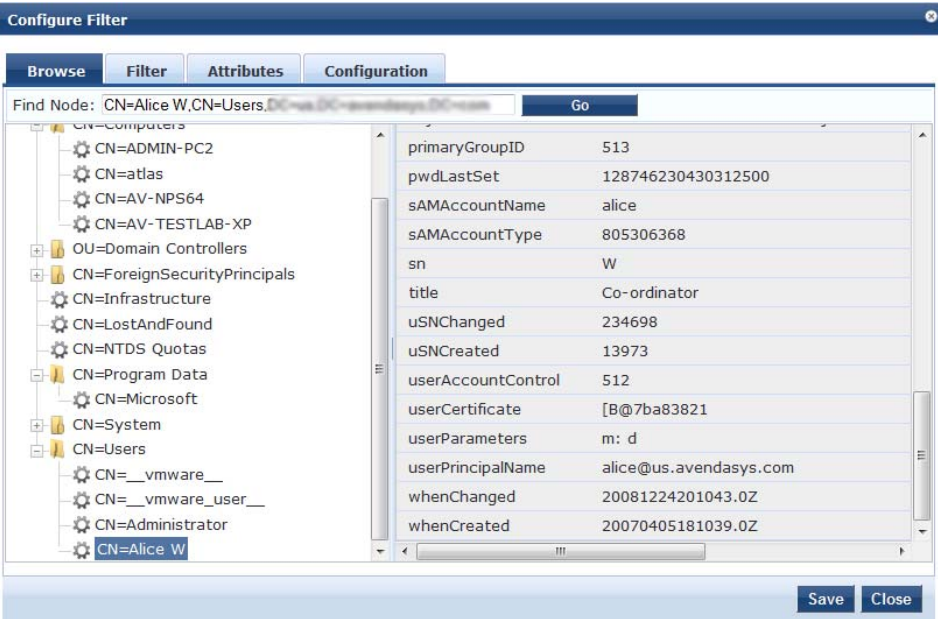
Tab	Parameter/Description
Filter Name / Attribute Name / Alias Name / Enable as Role	<p>Listing column descriptions:</p> <ul style="list-style-type: none"> • <i>Filter Name:</i> Name of the filter. • <i>Attribute Name:</i> Name of the LDAP/AD attributes defined for this filter. • <i>Alias Name:</i> For each attribute name selected for the filter, you can specify an alias name. • <i>Enable as Role:</i> Indicates whether an attribute has been enabled as a role.
Add More Filters	Brings up the filter creation popup.

Table 11-15 AD/LDAP Default Filters Explained

Directory	Default Filters
Active Directory	<ul style="list-style-type: none"> Authentication - This is the filter used for authentication. The query searches in objectClass of type <i>user</i>. This query finds both user and machine accounts in Active Directory: <code>(&(objectClass=user)(sAMAccountName=%{Authentication:Username}))</code> When a request arrives, Policy Manager populates %{Authentication:Username} with the authenticating user or machine. This filter is also set up to fetch the following attributes based on this filter query: <ul style="list-style-type: none"> <i>dn</i> (aliased to UserDN): This is an internal attribute that is populated with the user or machine record's Distinguished Name (DN) <i>department</i>, <i>title</i> and <i>company</i> <i>memberOf</i>: In Active Directory, this attribute is populated with the groups that the user or machine belongs to. This is a multi-valued attribute. Group - This is filter used for retrieving the name of the groups a user or machine belongs to. <code>(distinguishedName=%{memberOf})</code> This query fetches all group records, where the distinguished name is the value returned by the <i>memberOf</i> variable. The values for the <i>memberOf</i> attribute are fetched by the first filter (Authentication) described above. The attribute fetched with this filter query is <i>cn</i>, which is the name of the group Machine - This query fetches the machine record in Active Directory. <code>(&(objectClass=computer)(sAMAccountName=%{Host:Name}))</code> %{Host:Name} is populated by Policy Manager with name of the connecting host (if available). <i>dnsHostName</i>, <i>operatingSystem</i> and <i>operatingSystemServicePack</i> attributes are fetched with this filter query.
Generic LDAP Directory	<ul style="list-style-type: none"> Authentication - This is the filter used for authentication. <code>(&(objectClass=*)(uid=%{Authentication:Username}))</code> When a request arrives, Policy Manager populates %{Authentication:Username} with the authenticating user or machine. This filter is also set up to fetch the following attributes based on this filter query: <ul style="list-style-type: none"> <i>dn</i> (aliased to UserDN): This is an internal attribute that is populated with the user record's Distinguished Name (DN) Group - This is filter used for retrieving the name of the groups a user belongs to. <code>(&(objectClass=groupOfNames)(member=%{UserDn}))</code> This query fetches all group records (of objectClass groupOfNames), where member field contains the DN of the user record (<i>UserDN</i>, which is populated after the Authentication filter query is executed. The attribute fetched with this filter query is <i>cn</i>, which is the name of the group (this is aliased to a more readable name: <i>groupName</i>)

The Filter Creation Popup defines a filter query and the related attributes to be fetched.

Figure 11-22 AD/LDAP Filter Creation Popup (Browse Tab)

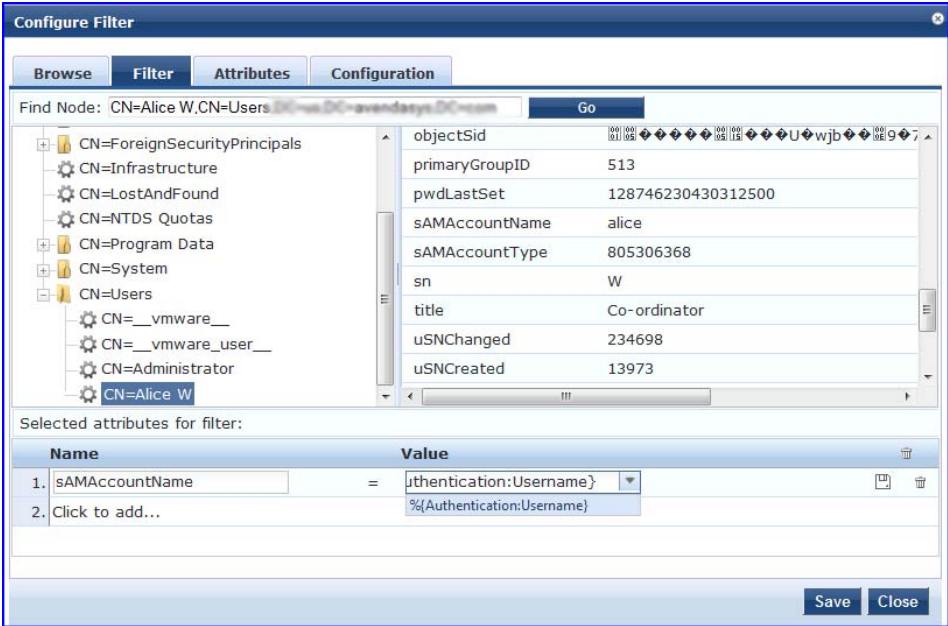


The **Browse** Tab shows an LDAP Browser from which you can browse the nodes in the LDAP or AD directory, starting at the base DN. This is presented in read-only mode. Selecting a leaf node - a node that has no children - brings up the attributes associated with that node.

Table 11-16 AD/LDAP Filter Creation Popup (Browse Tab)

Find Node / Go	Go directly to a given node by entering its Distinguished Name (DN) and clicking on the Go button.
----------------	-----------------------------------------------------------------------------------------------------------

Figure 11-23 AD/LDAP Filter Creation Popup (Filter Tab)



The **Filter** Tab provides an LDAP browser interface to define the filter search query. Through this interface you can define the attributes used in the filter query.

Note: Policy Manager comes prepopulated with filters and selected attributes for Active Directory and generic LDAP directory. New filters need to be created only if you need Policy Manager to fetch role mapping attributes from a new type of record.

Note: Records of different types can be fetched by specifying multiple filters that use different dynamic session attributes. For example, for a given request Policy Manager can fetch the user record associated with `%{Authentication:Username}`, and a machine record associated with `%{RADIUS:IETF:Calling-Station-ID}`.

Table 11-17 Filter Creation Popup (Filter Tab)

Parameter	Description
Find Node / Go	Go directly to a given node by entering its Distinguished Name (DN) and clicking on the Go button.
Select the attributes for filter	<p>This table has a name and value column. There are two ways to enter the attribute name</p> <ul style="list-style-type: none"> By going to a node of interest, inspecting the attributes, and then manually entering the attribute name by clicking on Click to add... in the table row. By clicking on an attribute on the right hand side of the LDAP browser. The attribute name and value are automatically populated in the table. <p>The attribute value field can be a value that has been automatically populated by selecting an attribute from the browser, or it can be manually populated. To aid in populating the value with dynamic session attribute values, a drop down with the commonly used namespace and attribute names is presented (See image below).</p>

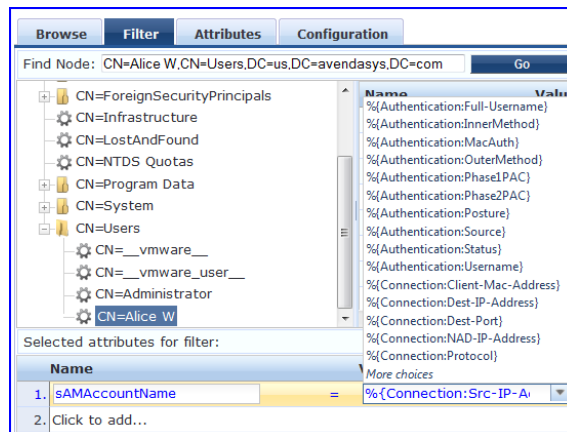


Table 11-18 Filter Creation Steps

Step	Description
Step 1 Select filter node	The goal of filter creation is to help Policy Manager understand how to find a user or device connecting to the network in LDAP or Active Directory. From the Filter tab, click on a node that you want to extract user or device information from. For example, browse to the Users container in Active Directory and select the node for a user (Alice, for example). On the right hand side, you see attributes associated with that user.
Step 2 Select attribute	Click on attributes that will help Policy Manager to uniquely identify the user or device. For example, in Active Directory, an attribute called sAMAccountName stores the user ID. The attributes that you select are automatically populated in the filter table displayed below the browser section (along with their values). In this example, if you select sAMAccountName, the row in the filter table will show this attribute with a value of alice (assuming you picked Alice's record as a sample user node).
Step 3 Enter value (optional)	After Step 3 , you have values for a specific record (Alice's record, in this case). Change the value to a dynamic session attribute that will help Policy Manager to associate a session with a specific record in LDAP/AD. For example, if you selected the sAMAccountName attribute in AD, click on the value field and select <code>%{Authentication:Username}</code> . When Policy Manager processes an authentication request <code>%{Authentication:Username}</code> is populated with the user ID of the user connecting to the network.
Step 4 Add more attributes from the node of interest and continue with Step 2 .	

Figure 11-24 AD/LDAP Filter Creation Popup (Attributes Tab)

Configure Filter

Execute filter query to select attributes for role mapping:

Filter Query: `(&(sAMAccountName=%{Authentication:Username}))(objectClass=user)`

Please enter the values for the parameters before executing the query:

`%{Authentication:Username}` =

Attributes

Name	Alias Name	Enable As Role
1. countryCode	countryCode	= false
2. msNPAllowDialin	msNPAllowDialin	= false
3. userPrincipalName	userPrincipalName	= false
4. Click to add		

Save **Close**

The **Attributes** Tab defines the attributes to be fetched from Active Directory or LDAP directory. Each attribute can also be “Enabled as Role,” which

means the value fetched for this attribute can be used directly in Enforcement Policies (See [Configuring Enforcement Policies](#)).

Table 11-19 AD/LDAP Filter Creation Popup (Attributes Tab)

Parameter	Description
Enter values for parameters	Policy Manager parses the filter query (created in the Filter tab and shown at the top of the Attributes tab) and prompts to enter the values for all dynamic session parameters in the query. For example, if you have <code>%{Authentication:Username}</code> in the filter query, you are prompted to enter the value for it. You can enter wildcard character (*) here to match all entries. Note: If there are thousands of entries in the directory, entering the wildcard character (*) can take a while to fetch all matching entries.
Execute	Once you have entered the values for all dynamic parameters, click on Execute to execute the filter query. You see all entries that match the filter query. Click on one of the entries (nodes) and you see the list of attributes for that node. You can now click on the attribute names that you want to use as role mapping attributes.
Name / Alias Name / Enable as Role	<p><i>Name:</i> This is the name of the attribute</p> <p><i>Alias Name:</i> A friendly name for the attribute. By default, this is the same as the attribute name.</p> <p><i>Enable as Role:</i> Click here to enable this attribute value to be used directly as a role in an Enforcement Policy. This bypasses the step of having to assign a role in Policy Manager through a Role Mapping Policy.</p>

Figure 11-25 Filter Creation Popup (Configuration Tab)

Configure Filter

Browse Filter Attributes **Configuration**

Filter Name:

Filter Query: `(& (sAMAccountName=%{Authentication:Username})) (objectClass=user)`

Name	Alias Name	Enable As Role	
1. countryCode	countryCode	= false	🗑
2. msNPAllowDialin	msNPAllowDialin	= false	🗑
3. userPrincipalName	userPrincipalName	= false	🗑
4. Click to add...			

Save Close

The **Configuration** Tab shows the filter and attributes configured in the **Filter** and **Attributes** tabs, respectively. From this tab, you can also manually edit the filter query and attributes to be fetched.

Kerberos

The Kerberos authentication source contains two tabs:

- The **General** Tab labels the authentication source and defines session details, authorization sources, and backup server details.

Figure 11-26 Kerberos (General Tab)

Configuration » Authentication » Sources » Add

Authentication Sources

General Primary Summary

Name:

Description:

Type:

Use for Authorization: ☐ Enable to use this authentication source to also fetch role mapping attributes

Authorization Sources:

-
-
-
- Select --

Backup Servers -

Server Priority:

-
-
-
-
-

Table 11-20 Kerberos (General Tab)

Parameter	Description
Name/Description	Freeform label and description.
Type	In this context, <i>Kerberos</i>
Use for Authorization	Disabled in this context.
Authorization Sources	<p>You must specify one or more authorization sources from which to fetch role mapping attributes. Select a previously configured authentication source from the drop down list, and click Add to add it to the list of authorization sources. Click Remove to remove it from the list.</p> <p>Note: As described in the “Services” (page 83) chapter, additional authorization sources can be specified at the Service level. Policy Manager fetches role mapping attributes regardless of which authentication source the user or device was authenticated against.</p>

Parameter	Description
Backup Servers	<p>To add a backup kerberos server, click Add Backup. When the Backup 1 tab appears, you can specify connection details for a backup server (same fields as for primary server, specified below).</p> <p>To remove a backup server, select the server name and click Remove. Move Up or Move Down to change the server priority of the backup servers. This is the order in which Policy Manager attempts to connect to the backup servers.</p>

- The **Primary** Tab defines the settings for the primary server.

Figure 11-27 Kerberos (Primary Tab)

Table 11-21 Token Server (Primary Tab)

Parameter	Description
Host Name/Port	Host name or IP address of the kerberos server, and the port at which the token server listens for kerberos connections. The default port is 88.
Realm	The domain of authentication. In the case of Active Directory, this is the AD domain.
Service Principal Name	The identity of the service principal as configured in the Kerberos server.
Service Principal Password	Password for the service principal.

Generic SQL DB

The Generic SQL authentication source contains three tabs to configure primary and backup servers, session details, and the filter query and role mapping attributes to fetch.

At the top level, there are buttons to:

- **Clear Cache:** Clears the attributes cached by Policy Manager for all entities that authorize against this server.
- **Copy:** Creates a copy of this authentication/authorization source.

Figure 11-28 Generic SQL DB (General Tab)

Table 11-22 Generic SQL DB (General Tab)

Parameter	Description
Name/Description	Freeform label and description.
Type	In this context, <i>Generic SQL DB</i> .
Use for Authorization	<p>This checkbox instructs Policy Manager to fetch role mapping attributes (or authorization attributes) from this authentication source. If a user or device successfully authenticates against this authentication source, then Policy Manager also fetches role mapping attributes from the same source (if this setting is enabled).</p> <p>This box is checked (enabled) by default</p>

Parameter	Description
Authorization Sources	<p>You can specify additional sources from which to fetch role mapping attributes. Select a previously configured authentication source from the drop down list, and click Add to add it to the list of authorization sources. Click Remove to remove it from the list.</p> <p>If Policy Manager authenticates the user or device from this authentication source, then it also fetches role mapping attributes from these additional authorization sources.</p> <p>Note: As described in the “Services” (page 83) chapter, additional authorization sources can be specified at the Service level. Policy Manager fetches role mapping attributes regardless of which authentication source the user or device was authenticated against.</p>
Backup Servers	<p>To add a backup server, click Add Backup. When the Backup 1 tab appears, you can specify connection details for a backup server (same fields as for primary server, specified below).</p> <p>To remove a backup server, select the server name and click Remove. Move Up or Move Down to change the server priority of the backup servers. This is the order in which Policy Manager attempts to connect to the backup servers.</p>
Cache Timeout	Policy Manager caches attributes fetched for an authenticating entity. This parameter controls the time period for which the attributes are cached.

The **Primary** Tab defines the settings for the primary server.

Figure 11-29 Generic SQL DB (Primary Tab)

Table 11-23 Generic SQL DB (Primary Tab)

Parameter	Description
Server Name	Enter the hostname or IP address of the database server.
Database Name	Enter the name of the database to retrieve records from.

Parameter	Description
Login Username/Password	<p>Enter the name of the user used to log into the database. This account should have read access to all the attributes that need to be retrieved by the specified filters.</p> <p>Enter the password for the user account entered in the field above.</p>
Timeout	Enter the time in seconds that Policy Manager waits before attempting to fail over from primary to the backup servers (in the order in which they are configured)
ODBC Driver	Select the ODBC driver (Postgres or MSSQL in this release) to connect to database.

The **Attributes** Tab defines the SQL DB query filters and the attributes to be fetched by using those filters.

Figure 11-30 Generic SQL DB (Attributes Tab)

Filter Name	Attribute Name	Alias Name	Enable as role
1. Authentication	department	department	true
	title	title	false

Table 11-24 Generic SQL DB Attributes Tab (Filter Listing Screen)

Tab	Parameter/Description
Filter Name / Attribute Name / Alias Name / Enable as Role	<p>Listing column descriptions:</p> <ul style="list-style-type: none"> • <i>Filter Name</i>: Name of the filter. • <i>Attribute Name</i>: Name of the SQL DB attributes defined for this filter. • <i>Alias Name</i>: For each attribute name selected for the filter, you can specify an alias name. • <i>Enable as Role</i>: Indicates whether an attribute has been enabled as a role.
Add More Filters	Brings up the filter creation popup.

The Filter Creation Popup defines a filter query and the related attributes to be fetched from the SQL DB store.

Figure 11-31 Generic SQL DB Filter Creation Popup (Configuration Tab)

Configure Filter

Configuration

Filter Name:

Filter Query:

```
SELECT department, title, user_credential(password) AS User_Password FROM
tips_auth_local_users WHERE ( expire_time is null OR expire_time > now() )
AND user_id = '#{Authentication:Username}'
```

	Name	Alias Name	Enable As Role	
1.	department	department	= true	
2.	title	title	= false	
3.	Click to add...			

Table 11-25 Generic SQL DB Filter Creation Popup (Configuration Tab)

Parameter	Description
Filter Name	Name of the filter
Filter Query	A SQL query to fetch the attributes from the user or device record in DB
Name / Alias Name / Enable as Role	<p><i>Name:</i> This is the name of the attribute</p> <p><i>Alias Name:</i> A friendly name for the attribute. By default, this is the same as the attribute name.</p> <p><i>Enable as Role:</i> Click here to enable this attribute value to be used directly as a role in an Enforcement Policy. This bypasses the step of having to assign a role in Policy Manager through a Role Mapping Policy.</p>

Token Server

The Generic SQL authentication source contains three tabs:

- The **General** Tab labels the authentication source and defines session details, authorization sources, and backup server details.

Figure 11-32 Token Server (General Tab)
Table 11-26 Token Server (General Tab)

Parameter	Description
Name/Description	Freeform label and description.
Type	In this context, <i>Token Server</i>
Use for Authorization	<p>This checkbox instructs Policy Manager to fetch role mapping attributes (or authorization attributes) from this authentication source. If a user or device successfully authenticates against this authentication source, then Policy Manager also fetches role mapping attributes from the same source (if this setting is enabled).</p> <p>This box is checked (enabled) by default</p>
Authorization Sources	<p>You can specify additional sources from which to fetch role mapping attributes. Select a previously configured authentication source from the drop down list, and click Add to add it to the list of authorization sources. Click Remove to remove it from the list.</p> <p>If Policy Manager authenticates the user or device from this authentication source, then it also fetches role mapping attributes from these additional authorization sources.</p> <p>Note: As described in the “Services” (page 83) chapter, additional authorization sources can be specified at the Service level. Policy Manager fetches role mapping attributes regardless of which authentication source the user or device was authenticated against.</p>

Parameter	Description
Backup Servers	<p>To add a backup server, click Add Backup. When the Backup 1 tab appears, you can specify connection details for a backup server (same fields as for primary server, specified below).</p> <p>To remove a backup server, select the server name and click Remove. Move Up or Move Down to change the server priority of the backup servers. This is the order in which Policy Manager attempts to connect to the backup servers. Server Timeout is the time in seconds that Policy Manager waits before attempting to fail over from primary to the backup servers (in the order in which they are configured)</p>

- The **Primary** Tab defines the settings for the primary server.

Figure 11-33 Token Server (Primary Tab)

Table 11-27 Token Server (Primary Tab)

Parameter	Description
Server Name/Port	Host name or IP address of the token server, and the UDP port at which the token server listens for RADIUS connections. The default port is 1812.
Secret	RADIUS shared secret to connect to the token server.

- The **Attributes** Tab defines the RADIUS attributes to be fetched from the token server. These attributes can be used in role mapping policies (See “Configuring a Role Mapping Policy” (page 144)). Policy Manager load all RADIUS vendor dictionaries in the type dropdown to help select the attributes.

Figure 11-34 Token Server (Attributes Tab)

GeneralPrimaryAttributesSummary

Type	Name	Enabled as Role	
1. Radius:IETF	Class	= false	
2. Radius:IETF	Callback-Number	= false	
3. <div></div>			
4. <div><div>Radius:IETF</div><div>Radius:Clavister</div><div>Radius:Cisco-VPN3000</div><div>Radius:Acc</div><div>Radius:Tropos</div><div>Radius:Cisco</div><div>Radius:ERX</div><div>Radius:CableLabs</div><div>Radius:Mikrotik</div><div>Radius:Cosine</div><div>Radius:JRadius</div><div>Radius:Cisco-BBSM</div><div>Radius:BinTec</div><div>Radius:Ascend</div><div>Radius:Roaring-Penguin</div><div>More choices</div></div>			

Back to Authentication Sources

Next >SaveCancel

Static Host List

The Static Host List authentication source contains three tabs:

- The **General** Tab labels the authentication source.

Figure 11-35 Static Host List (General Tab)

Configuration » Authentication » Sources » Add

Authentication Sources

GeneralStatic Host ListsSummary

Name:

Description:

Type:

Static Host List

Use for Authorization:

☐ Enable to use this authentication source to also fetch role mapping attributes

Authorization Sources:

Remove

View Details

Add

Back to Authentication Sources

Next >SaveCancel

Table 11-28 Static Host List (General Tab)

Parameter	Description
Name/ Description	Freeform label
Type	<i>Static Host List</i> , in this context.
Use for Authorza- tion/Authorization Sources	Not configurable

- The **Primary** Tab defines the settings for the primary server.

Figure 11-36 Static Host List (Static Host Lists Tab)

The screenshot shows the 'Static Host Lists' configuration window. It has three tabs: 'General', 'Static Host Lists' (selected), and 'Summary'. The 'Host List' section contains a dropdown menu with 'Handhelds' selected. To the right of the dropdown are four buttons: 'Remove', 'View Details', 'Modify', and 'Add'. A text label 'Add new Static Host List' is positioned to the right of the 'Add' button. At the bottom of the window, there is a 'Back to Authentication Sources' link and three buttons: 'Next >', 'Save', and 'Cancel'.

Table 11-29 Static Host List (Static Host Lists Tab)

Parameter	Description
Host List	Select a Static Host List from the drop down and Add to add it to the list. Click on Remove to remove the selected static host list. Click on View Details to view the contents of the selected static host list. Click on Modify to modify the selected static host list.

Note: Only Static Host Lists of type MAC Address List or MAC Address Regular Expression can be configured as authentication sources. (See “[Adding and Modifying Static Host Lists](#)” (page 155)).

Chapter 12: Identity - Users, Endpoints, Roles & Role Mapping

A Role Mapping Policy reduces client (user or device) identity or attributes associated with the request to *Role(s)* for Enforcement Policy evaluation. The roles ultimately determine differentiated access.

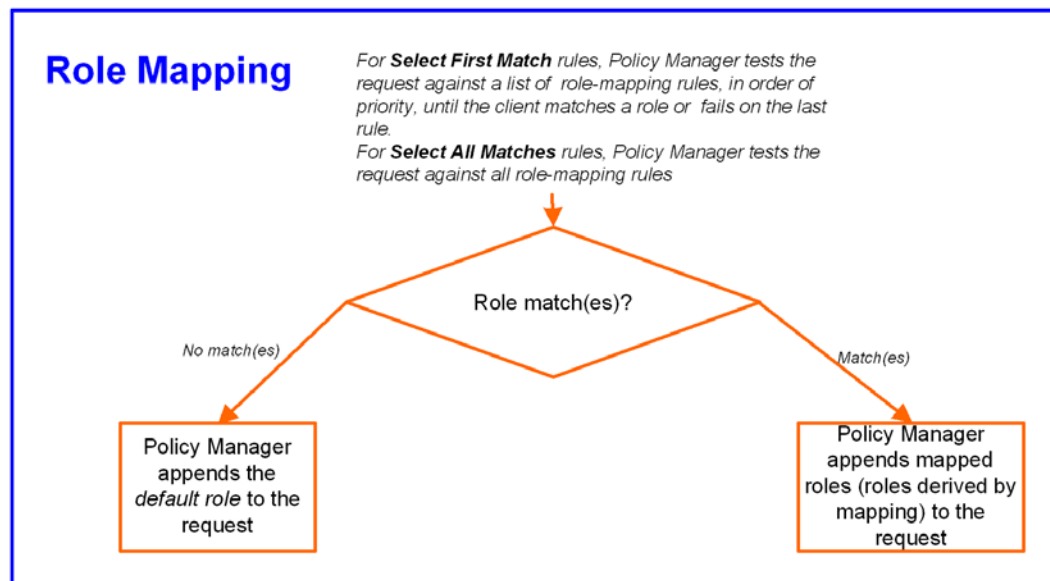
Architecture and Flow

Roles range in complexity from a simple user group (e.g., Finance, Engineering, or Human Resources) to a combination of a user group with some dynamic constraints (e.g., “San Jose Night Shift Worker” - - An employee in the Engineering department who logs in through the San Jose network device between 8 PM and 5 AM on weekdays). It can also apply to a list of s. A role can be:

- Discovered by Policy Manager through *role mapping* (“[Adding and Modifying Role Mapping Policies](#)” (page 144)). Roles are typically discovered by Policy Manager by retrieving attributes from the *authentication source*. *Filter rules* associated with the authentication source tell Policy Manager where to retrieve these attributes.
- Assigned automatically when retrieving attributes from the *authentication source*. Any attribute in the authentication source can be mapped directly to a role. (“[Adding and Modifying Authentication Sources](#)” (page 119))
- Associated directly with a user in the Policy Manager *local user* database (“[Adding and Modifying Local Users](#)” (page 149) and “[Adding and Modifying Guest Users](#)” (page 150)).
- Associated directly with a *static host list*, again through *role mapping* (“[Adding and Modifying Static Host Lists](#)” (page 155)).

At the Service level, you can create rules that associate a user with a role.

Figure 12-1 Role Mapping Process



Configuring a Role Mapping Policy

After authenticating a request, an Policy Manager *Service* invokes its *Role Mapping Policy*, resulting in assignment of a role(s) to the client. This role becomes the identity component of *Enforcement Policy* decisions.

Note: A Service can be configured without a Role Mapping Policy, but only one Role Mapping Policy can be configured for each Service.

Policy Manager ships with the following pre-configured roles:

- [Guest] - Role for guest access
- [TACACS Help Desk] - Policy Manager Admin Role, limited to views of the Monitoring screens
- [TACACS Network Admin] - Policy Manager Admin Role, limited to Configuration and Monitoring UI screens
- [TACACS Receptionist] - Policy Manager Guest Provisioning Role
- [TACACS Super Admin] - Policy Manager Admin Role with unlimited access to all UI screens

You may also configure other roles ([“Adding and Modifying Roles” \(page 147\)](#)).

Adding and Modifying Role Mapping Policies

From the **Services** page (**Configuration > Service**), you can configure role mapping for a new service (as part of the flow of the **Add Service** wizard), or modify an existing role mapping policy directly (**Configuration > Identity > Role Mappings**).

Figure 12-2 Role Mapping Policies

#	Name ▲	Description	Default Role
1.	Employee Roles	Role mapping policies for employees	Role_Engineer
2.	Enterprise Role Mapping Policy	Role mapping policy for all managed users	eTIPS_Guest
3.	Handheld Roles	Roles for handheld devices	Not_Handhelds
4.	RMP_DEPARTMENT		eTIPS_Guest
5.	Switch Port Role Mapping Policy		Unknown Client
6.	TG Role Mapping (AD)	AD Roles for traffic generator	eTIPS_Guest
7.	Unmanaged Clients Role Mapping	Roles for handheld devices	Not_Handhelds

When you click **Add Role Mapping** from any of these locations, Policy Manager displays the **Add Role Mapping** popup, which contains three tabs:

- The **Policy** Tab labels the method and defines the Default Role (the role to which Policy Manager defaults if the mapping policy does not produce a match for a given request).

Figure 12-3 Role Mapping (Policy Tab)
Table 12-1 Role Mapping (Policy Tab)

Parameter	Description
Policy Name / Description	Freeform label and description.
Default Role	Select the role to which Policy Manager will default when the role mapping policy does not produce a match.
View Details / Modify / Add new Role	Click on View Details to view the details of the default role. Click on Modify to modify the default role. Click on Add new Role to add a new role.

- The **Mapping Rules** Tab selects the evaluation algorithm, adds/edits/removes rules, and reorder rules.

In the **Rules Editor**, click **Add Rule** (button) to create a new rule, or select an existing rule (by clicking on the row) to **Edit Rule** (button) or **Remove Rule** (button).

Figure 12-4 Role Mapping (Mapping Rules Tab)

Conditions	Role Name
1. (Authorization:Avenda AD:department EQUALS Finance) OR (Authorization:Avenda AD:title EQUALS VP)	ROLE_FINANCE
2. (Authentication:Status EQUALS Machine) OR (Authorization:Avenda AD:memberOf EQUALS CorporateAssets)	ConferenceLaptop

Buttons: Add Rule, Move Up, Move Down, Edit Rule, Remove Rule

Navigation: Back to Role Mappings, Next >, Save, Cancel

When you select **Add Rule** or **Edit Rule**, Policy Manager displays the **Rules Editor** popup.

Figure 12-5 Rules Editor

Type	Name	Operator	Value
1. Authentication	Status	EQUALS	Machine
2. Authorization:Avenda AD	memberOf	EQUALS	CorporateAssets
3. Date	department	ELONGS_TO	Monday, Tuesday, Wednesday, Thursday, Friday

Matches ☒ ANY or ☐ ALL of the following conditions:

Actions

Role Name: ConferenceLaptop

Buttons: Save, Cancel

Table 12-2 Role Mappings Page (Rules Editor)

Label	Description
Type	<p>The rules editor appears throughout the Policy Manager interface. It exposes different namespace dictionaries depending on context. (Refer to “Namespaces” (page 314))</p> <p>In the role mapping context, Policy Manager allows attributes from following namespaces:</p> <ul style="list-style-type: none"> • Authorization:<authorization_source_instance> - Policy Manager shows each instance of the authorization source for which attributes have been configured to be fetched. (“Adding and Modifying Authentication Sources” (page 119)). Only those attributes that have been configured to fetched are shown in the attributes dropdown. • Authorization • Authentication • Certificate • Connection • Date • Device • GuestUser • Host • LocalUser • RADIUS - All enabled RADIUS vendor dictionaries
Name (of attribute)	Drop-down list of attributes present in the selected namespace.
Operator	<p>Drop-down list of context-appropriate (with respect to the attribute data type) operators.</p> <p>Operators have their obvious meaning; for stated definitions of operator meaning, refer to “Operators” (page 322).</p>
Value of attribute	Depending on attribute data type, may be a free-form (one or many line) edit box, a drop-down list, or a time/date widget.

When you save your Role Mapping configuration, it appears in the **Mapping Rules Tab** list. In this interface, you can select a rule (click and the background changes color), then use the various widgets to **Move Up**, **Move Down**, **Edit Rule** or **Remove Rule**.

Adding and Modifying Roles

Policy Manager lists all available roles in the Roles page. From the menu, select **Configuration > Identity > Roles**.

Figure 12-6 Roles

Configuration » Identity » Roles

Roles

[Add Roles](#)
[Import Roles](#)
[Export Roles](#)

Filter: contains Show records

#	<input type="checkbox"/>	Name ▲	Description
1.	<input type="checkbox"/>	ConferenceLaptop	ConferenceLaptopRole
2.	<input type="checkbox"/>	Developer	Development Team
3.	<input type="checkbox"/>	Device SuperAdmin	Super Administrator
4.	<input type="checkbox"/>	eTIPS_Guest	Guest User
5.	<input type="checkbox"/>	eTIPS_TACACS_Help_Desk	Help desk role for eTIPS Admin
6.	<input type="checkbox"/>	eTIPS_TACACS_Network_Admin	Network administrator role for eTIPS Admin
7.	<input type="checkbox"/>	eTIPS_TACACS_Receptionist	Receptionist role for eTIPS Admin
8.	<input type="checkbox"/>	eTIPS_TACACS_Super_Admin	Super administrator role for eTIPS Admin
9.	<input type="checkbox"/>	Handhelds	Generic Role for handheld devices
10.	<input type="checkbox"/>	IP Phones	IP Phones and ATAs

Showing 1-10 of 21

You can configure a role from within a Role Mapping Policy (**Add New Role**), or independently from the menu (**Configuration > Identity > Roles > Add Roles**). In either case, roles exist independently of an individual Service and can be accessed globally through the Role Mapping Policy of any Service.

When you click **Add Roles** from any of these locations, Policy Manager displays the **Add New Role** popup.

Figure 12-7 Add New Role

Add New Role

Name:

Description:

Table 12-3 Add New Role

Parameter	Description
Role Name / Description	Freeform label and description.

Local Users, Guest Users, Endpoints and Static Host List Configuration

The internal Policy Manager database (*[Local User Repository]*, *[Guest User Repository]*) supports storage of user records, when a particular class of users is not present in a central user repository (e.g., neither *Active Directory* nor other database); by way of an example of such a class of users, guest or contractor records can be stored in the local user repository .

Note: To authenticate local users from a particular Service, include *[Local User Repository]* among the Authentication Sources.

The **endpoints** table lists the endpoints that have authenticated requests to Policy Manager. These entries are automatically populated from the 802.1X, MAC-based authentications, and web authentications processed by Policy Manager. These can be further modified to add tags, known/unknown, disabled status.

A **static host list** comprises of list of MAC and IP addresses. These can be used as white or black lists to control access to the network.

Adding and Modifying Local Users

Policy Manager lists all local users in the **Local Users** page (**Configuration > Identity > Local Users**):

Figure 12-8 Local Users Listing

Configuration » Identity » Local Users

Local Users

Filter: UserID contains Go Clear Filter Show 10 records

[Add User](#)
[Import Users](#)
[Export Users](#)

#	<input type="checkbox"/>	User ID ▲	Name	Role	Status
1.	<input type="checkbox"/>	001e4cc18254	India Test Laptop	Role_Engineer	Enabled
2.	<input type="checkbox"/>	arthur	Arthur Denver	Senior_Mgmt	Enabled
3.	<input type="checkbox"/>	adhwadth	Adhwadth Marthy	Developer	Enabled
4.	<input type="checkbox"/>	avendaconference	Avenda Conference Room	ConferenceLaptop	Enabled
5.	<input type="checkbox"/>	shagya	Shagya Prasad 181	Role_Engineer	Enabled
6.	<input type="checkbox"/>	bob	Bill Gecko	Developer	Enabled
7.	<input type="checkbox"/>	carrie	Carrie Lipton	Senior_Mgmt	Enabled
8.	<input type="checkbox"/>	clay	Clay Pepp	Developer	Enabled
9.	<input type="checkbox"/>	donald	Donald Regis	TestQA	Enabled
10.	<input type="checkbox"/>	gabriel	Gabriel Hawthorne	Developer	Enabled

Showing 1-10 of 29 [▶▶](#)

Export Delete

- To add a local user, click **Add User** to display the **Add Local User** popup.

Figure 12-9 Add Local User

User ID:	<input type="text" value="gabriel"/>
Name:	<input type="text" value="Gabriel Hawthorne"/>
Password:	<input type="password" value="••••••••"/>
Verify Password:	<input type="password" value="••••••••"/>
Enable User	<input checked="" type="checkbox"/> (Check to enable local user)
Role:	<input type="text" value="Developer"/>

Attributes	
Attribute	Value
1. Phone	408-555-1212
2. Email	gabriel@acme.com
3. Designation	Consulting Engineer
4. Location	San Hacienda
5. Click to add...	

Table 12-4 Add Local User

Parameter	Description
User ID/ Name / Password/ Verify Password	Freeform labels and password.
Enable User	Uncheck to disable this user account.
Role	Select a static role for this local user.
Attributes	<p>Add custom attributes for this local user. Click on the “Click to add...” row to add custom attributes. By default, four custom attributes appear in the Attribute drop-down: Phone, Email, Sponsor, Designation. You can enter any name in the attribute field. All attributes are of String datatype. The value field can also be populated with any string. Each time you enter a new custom attribute, it is available for selection in Attribute dropdown for all local users.</p> <p>Note: All attributes entered for a local user are available in the role mapping rules editor under the <i>LocalUser</i> namespace.</p>

- To edit a local user, in the Local Users listing page, click on the name to display the **Edit Local User** popup.
- To delete a local user, in the Local Users listing page, select it (via checkbox) and click **Delete**.
- To export a local user, in the Local Users listing page, select it (via checkbox) and click **Export**.
- To export ALL local users, in the Local Users listing page, click **Export Users**.
- To import local users, in the Local Users listing page, click **Import Users**.

Adding and Modifying Guest Users

An administrator with the Policy Manager *Receptionist* role provisions users specifically as *Guests* (local users with a pre-defined role of Guest). From the menu, select **Configuration > Identity > Guest Users**.

Figure 12-10 Guest Users Listing

#	User Name ▲	Sponsor Name	Guest Type	Status	Expired	Source Application
1.	00-21-70-9C-85-2B		DEVICE	Enabled	Expired	GuestConnect
2.	11-22-33-44-55-66	foobar	DEVICE	Enabled	Expired	GuestConnect
3.	foobar		USER	Enabled	Valid	GuestConnect
4.	localguest		USER	Enabled	Valid	eTIPS
5.	m1esh12####		USER	Enabled	Expired	GuestConnect
6.	m1esh12####		USER	Enabled	Expired	GuestConnect
7.	santo		USER	Enabled	Valid	GuestConnect

Showing 1-7 of 7

Export Delete

Table 12-5 Guest Users Listing

Parameter	Description
User Name	Guest user name.
Sponsor Name	Sponsor who sponsored the guest.
Guest Type	USER (for guest users) and DEVICE (for devices registered from the GuestConnect product).
Status	Enabled/Disabled status.
Expired	Whether the guest/device account has expired
Source Application	Where this account was created: From Policy Manager or the GuestConnect guest provisioning product.

In the **Guest Users** listing:

- To add a guest user, click **Add User** to display the **Add New Guest User** popup.

Figure 12-11 Add New Guest User

Add New Guest User

Guest Type: ☒ USER ☐ DEVICE

User ID: johndoe

Password: vyWZkRN2aS Auto Generate

Expiry Time: ?

Enable Guest: ☒

Attributes

Attribute	Value
1. Company Name	= Foo Inc
2. Sponsor	= jane
3. Phone	= 408555
4. Click to add...	

Calendar: November, 2010. Today: 9. Time: 10:59. Select date.

Add Cancel

Figure 12-12 Add New Guest Device

Add New Guest User

Guest Type: ☐ USER ☒ DEVICE

MAC Address : 00-21-70-9C-85-2B

Expiry Time: 2010-11-16 11:04:36

Enable Guest: ☒

Attributes

Attribute	Value
1. Device Type	= Xbox 360
2. Sponsor	= johndoe
3. Click to add...	

Add Cancel

Table 12-6 Add New Guest User/Device

Parameter	Description
Guest Type	Add a guest user or a guest device
User ID/ Name / Password/ Verify Password (Guest User only)	Freeform labels and password. Click Auto Generate to auto-generate a password for the guest user.
MAC Address (Guest Device only)	MAC address of the guest device.
Enable Guest	Check to enable guest user.
Expiry Time	Use the date widget to select the date and time on which this Guest User's access expires.
Attributes	<p>Add custom attributes for this guest user. Click on the "Click to add..." row to add custom attributes. By default, six custom attributes appear in the Attribute drop-down: Company-Name, Location, Phone, Email, Sponsor, Designation. You can enter any name in the attribute field. All attributes are of String datatype. The value field can also be populated with any string. Each time you enter a new custom attribute, it is available for selection in Attribute dropdown for all guest users.</p> <p>Note: All attributes entered for a guest user are available in the role mapping rules editor under the <i>GuestUser</i> namespace.</p>

- *To edit a guest user*, in the Guest Users listing page, double-click on the name to display the **Edit Local User** popup.
- *To delete a guest user*, in the Guest Users listing page, select it (via checkbox) and click **Delete**.
- *To export a guest user*, in the Guest Users listing page, select it (via checkbox) and click **Export**.
- *To export ALL guest users*, in the Guest Users listing page, click **Export Users**.
- *To import guest users*, in the Guest Users listing page, click **Import Users**.

Adding and Modifying Endpoints

Policy Manager automatically lists all endpoints (that have authenticated) in the **Endpoints** page (**Configuration > Identity > Endpoints**):

Figure 12-13 Endpoints Listing

Configuration » Identity » Endpoints

Endpoints

Filter: contains Show records

#	<input type="checkbox"/>	MAC Address ▲	Status	Added by	Last Authenticated at	Authentication Records
1.	<input type="checkbox"/>	00-11-22-33-44-55	Known		-	-
2.	<input type="checkbox"/>	00-1A-4B-81-0B-DA	Unknown	eTIPS	Apr 01, 2010 12:10:04 PDT	<input type="button" value="View"/>
3.	<input type="checkbox"/>	00-1C-23-45-D0-CF	Unknown	eTIPS	Apr 01, 2010 12:16:36 PDT	<input type="button" value="View"/>
4.	<input type="checkbox"/>	00-1E-4C-C1-81-B4	Unknown	eTIPS	Apr 01, 2010 10:12:07 PDT	<input type="button" value="View"/>
5.	<input type="checkbox"/>	00-1F-29-AD-8A-65	Unknown	eTIPS	Apr 01, 2010 12:13:23 PDT	<input type="button" value="View"/>
6.	<input type="checkbox"/>	00-21-70-9C-85-2B	Unknown	eTIPS	Apr 01, 2010 12:07:36 PDT	<input type="button" value="View"/>
7.	<input type="checkbox"/>	90-84-0D-6D-A0-4E	Unknown	eTIPS	Apr 01, 2010 11:24:07 PDT	<input type="button" value="View"/>

Showing 1-7 of 7

- To view the authentication details of an endpoint, click **View** to display the **Endpoint Authentication Details** popup.

Figure 12-14 Endpoint Authentication Details

Endpoint Authentication Details

MAC Address

	Username	Device	Authentication	Start Time	End Time	eTIPS Server	Session ID
1		192.168.5.214	Success	2010/04/01 13:13:26		192.168.5.217	R0000034c-10-4bb4fe66
2		192.168.5.214	Success	2010/04/01 12:43:25		192.168.5.217	R00000346-10-4bb4f75c
3		192.168.5.214	Success	2010/04/01 12:13:23		192.168.5.217	R00000340-10-4bb4f052
4		192.168.5.214	Success	2010/04/01 11:43:21		192.168.5.217	R0000033a-10-4bb4e948
5		192.168.5.214	Success	2010/04/01 11:13:19		192.168.5.217	R00000333-10-4bb4e23e
6		192.168.5.214	Success	2010/04/01 10:43:17		192.168.5.217	R0000032b-10-4bb4db2f
7		192.168.5.214	Success	2010/04/01 10:13:09		192.168.5.217	R00000326-10-4bb4d423
8		192.168.5.214	Success	2010/04/01 09:43:05		192.168.5.217	R0000031f-10-4bb4cd17

- To manually add an endpoint, click **Add Endpoint** to display the **Add Endpoint** popup.

Figure 12-15 Add Endpoint

MAC Address	00-21-70-9C-85-2B
Description:	
Status	<input checked="" type="radio"/> Known client <input type="radio"/> Unknown client <input type="radio"/> Disabled client
Attributes	
Attribute	Value
1. Device Type	= Turnstile
2. Click to add...	
<div style="text-align: right;"> <input type="button" value="Add"/> <input type="button" value="Cancel"/> </div>	

Table 12-7 Add Endpoint

Parameter	Description
MAC Address	MAC address of the endpoint.
Status	Mark as Known, Unknown or Disabled client. The Known and Unknown status can be used in role mapping rules via the Authentication:MacAuth attribute. The Disabled status can be used to block access to a specific endpoint. This status is automatically set when an endpoint is blocked from the Endpoint Activity table (in the Live Monitoring section).
Attributes	<p>Add custom attributes for this endpoint. Click on the “Click to add...” row to add custom attributes. You can enter any name in the attribute field. All attributes are of String datatype. The value field can also be populated with any string. Each time you enter a new custom attribute, it is available for selection in Attribute dropdown for all endpoints.</p> <p>Note: All attributes entered for an endpoint are available in the role mapping rules editor under the <i>Endpoint</i> namespace.</p>

- *To edit an endpoint*, in the Endpoints listing page, click on the name to display the **Edit Endpoint** popup.

Notice that the **Policy Cache Values** section lists the role(s) assigned to the user and the posture status. Policy Manager can use these cached values in authentication requests from this endpoint. **Clear Cache** clears the computed policy results (roles and posture).

Figure 12-16 Edit Endpoint Popup

MAC Address	90840d6da04e
Description:	<input type="text"/>
Status	<input type="radio"/> Known client <input checked="" type="radio"/> Unknown client <input type="radio"/> Disabled client

Attribute	Value
1. Click to add...	

Roles	[User Authenticated], Senior_Mgmt
Posture Status	UNKNOWN (100)
Last Updated at	Nov 18, 2010 17:24:07 PST
Cache Expires at	Nov 18, 2010 17:24:07 PST

- To delete an endpoint, in the Endpoints listing page, select it (via checkbox) and click **Delete**.
- To export an endpoint, in the Endpoints listing page, select it (via checkbox) and click **Export**.
- To export ALL endpoints, in the Endpoints listing page, click **Export All Endpoints**.
- To import endpoints, in the Endpoints listing page, click **Import Endpoints**.

Adding and Modifying Static Host Lists

A static host list comprises a named list of MAC or IP addresses, which can be invoked:

- In Service and Role-mapping rules as a component.
- For non-responsive services on the network (for example, printers or scanners), as an Authentication Source.

Note: Only static host lists of type MAC address are available as authentication sources.

Note: A static host list often functions, in the context of the Service, as a *white list* or a *black list*.

Therefore, they are configured independently at the global level.

Figure 12-17 Static Host Lists (Listing Page)

Configuration » Identity » Static Host Lists

Static Host Lists

[Add Static Host List](#)
[Import Static Host Lists](#)
[Export Static Host Lists](#)

Filter: Name contains Go Clear Filter Show 10 records

#	Name	Format	Type	Description
1.	Handhelds	List	MACAddress	Handhelds Whitelist
2.	Macintosh and iPhone Clients	Regex	MACAddress	MAC Address list for Apple vendor endpoints
3.	SJ and Bangalore Endpoints	Regex	IPAddress	All San Jose & Bangalore Endpoints
4.	SJ Endpoints	Subnet	IPAddress	All San Jose Endpoints

Showing 1-4 of 4

Export Delete

In the **Static Host Lists** listing:

- To add a *Static Host List*, click **Add Static Host List** to display the **Add Static Host List** popup.

Figure 12-18 Add Static Host List

Edit Static Host List

Name: Handhelds

Description: Handhelds Whitelist

Host Format: ☐ Subnet ☐ Regular Expression ☒ List

Host Type: ☐ IP Address ☒ MAC Address

List: 00-23-df-21-9b-a7
00-21-e9-40-46-a5

Remove Host

Add Host

Save Cancel

Table 12-8 Add Static Host List

Parameter	Description
Name/ Description	Freeform labels and descriptions.
Host Format	Select a format for expression of the address: <i>subnet</i> , <i>IP address</i> , or <i>regular expression</i> (radio buttons).
Host Type	Select a host type: <i>IP Address</i> or <i>MAC Address</i> (radio buttons).
List	Use the Add Host and Remove Host widgets to maintain membership in the current <i>Static Host List</i> .

- To edit a *Static Host List* from the Static Host Lists listing page, click on the name to display the **Edit Static Host List** popup.
- To delete a *Static Host List* from the Static Host Lists listing page, select it (via checkbox) and click **Delete**.

- *To export a Static Host List*, in the Static Host Lists listing page, select it (via checkbox) and click **Export**.
- *To export ALL Static Host Lists*, in the Static Host Lists listing page, click **Export Static Host Lists**.
- *To import Static Host Lists*, in the Static Host Lists listing page, click **Import Static Host Lists**.

Chapter 13: Posture

Policy Manager provides several *posture* methods for health evaluation of clients requesting access. These methods all return *Posture Tokens* (E.g., Healthy, Quarantine) for use by Policy Manager for input into *Enforcement Policy*. One or more of these posture methods may be associated with a *Service*

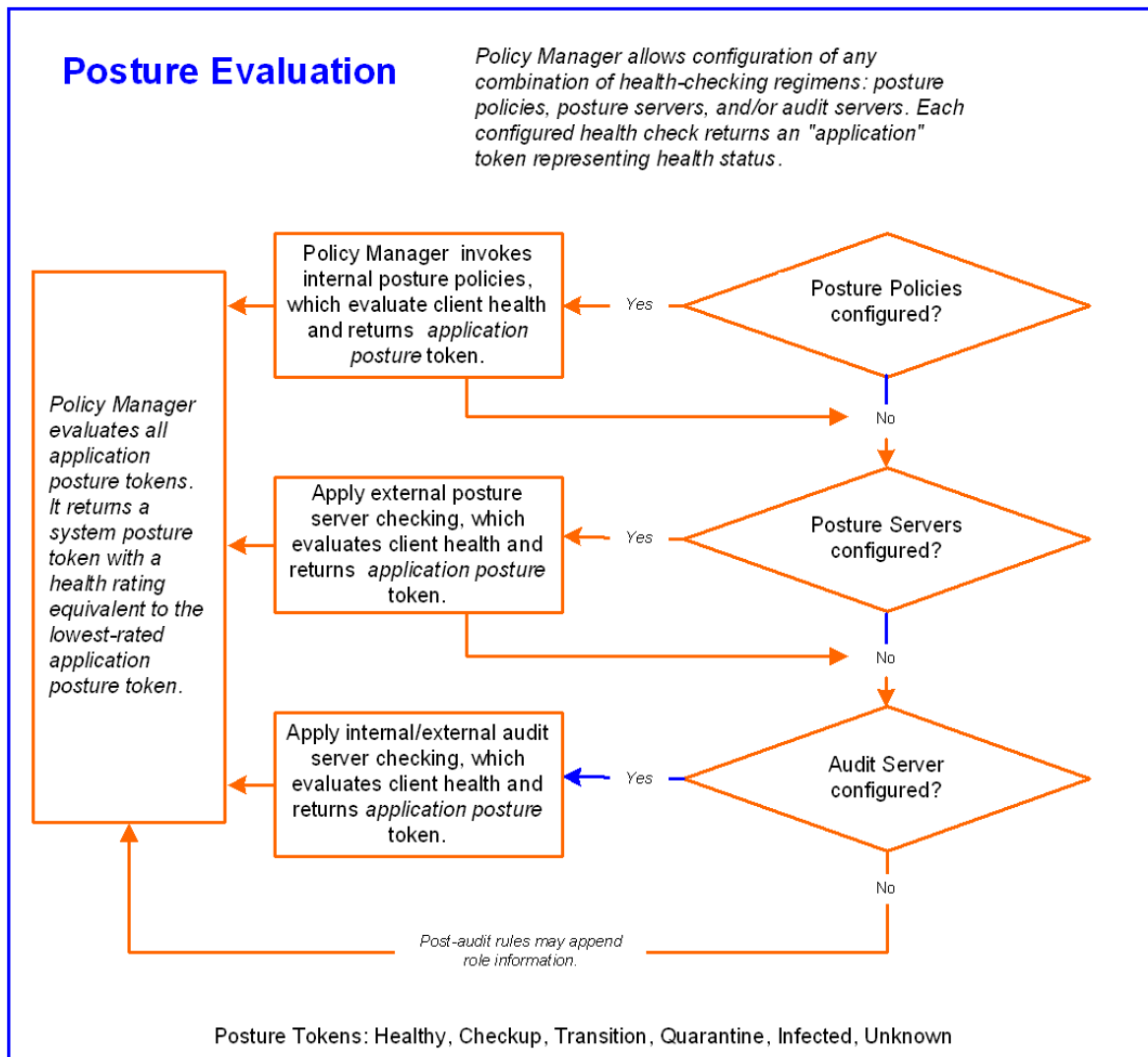
Architecture and Flow

Policy Manager supports three different types of posture checking:

- **Posture Policy.** Policy Manager supports four pre-configured posture plugins for Windows, one plugin for Linux and one plugin for MAC OS X, against which administrators can configure rules that test for specific attributes of client health and correlate the results to return Application Posture Tokens for processing by Enforcement Policies.
- **Posture Server.** Policy Manager can forward all or part of the posture data received from the client to a *Posture Server*. The Posture Server evaluates the posture data and returns Application Posture Tokens. Policy Manager supports the Microsoft NPS Server for Microsoft NAP integration.
- **Audit Server.** Audit Servers provide posture checking for unmanageable devices (i.e., devices lacking adequate posture agents or supplicants); in the case of such clients, the audit server's post-audit rules map clients to roles. Policy Manager supports two types of Audit Servers: NMAP audit server, primarily to derive roles from post-audit rules; NESSUS audit server, primarily used for vulnerability scans (and, optionally, post-audit rules).

[Figure 13-1: Posture Evaluation Process](#) illustrates the flow of control for posture evaluation.

Figure 13-1 Posture Evaluation Process



Policy Manager uses posture evaluation to assess client consistency with enterprise endpoint health policies, specifically with respect to:

- Operating system version/type
- Registry keys/services present (or absent)
- Antivirus/antispyware/firewall configuration
- Patch level of different software components
- Peer to Peer application checks
- Services to be running or not running
- Processes to be running or not running

Each configured health check returns an *application token* representing health:

- **Healthy.** Client is compliant: there are no restrictions on network access.

- **Checkup.** Client is compliant; however, there is an update available. This can be used to proactively remediate to healthy state.
- **Transient.** Client evaluation is in progress; typically associated with auditing a client. The network access granted is interim.
- **Quarantine.** Client is out of compliance; restrict network access, so the client only has access to the remediation servers.
- **Infected.** Client is infected and is a threat to other systems in the network; network access should be denied or severely restricted.
- **Unknown.** The posture token of the client is unknown.

Upon completion of all configured posture checks, Policy Manager evaluates all *application tokens* and calculates a *system token*, equivalent to the most restrictive rating for all returned application tokens. The *system token* provides the health posture component for input to the Enforcement Policy.

A Service can also be configured without any Posture policy.

Configuring Posture

At the Service level,

Figure 13-2 Posture Features at the Service Level

Configuration » Services » Edit - a802.1X Wireless Service

Services - a802.1X Wireless Service

Summary	Service	Authentication	Authorization	Roles	Posture	Audit	Enforcement
Validation Check: <input checked="" type="checkbox"/> Enable posture validation for end-hosts with posture agents							
Posture Policies: <div> Posture Policies: <div> Basic Linux Health Check Basic Windows Health Check --Select-- </div> <div> Remove View Details Modify Add </div> </div> Add new Posture Policy							
Default Posture Token: UNKNOWN (100)							
Remediate End-Hosts: <input checked="" type="checkbox"/> Enable auto-remediation of non-compliant end-hosts							
Remediation URL: http://remediation_internal.us.acme.com							
Posture Servers: <div> Posture Servers: <div> PS_NPS [RADIUS] </div> <div> Remove View Details Modify Add </div> </div> Add new Posture Server							

[Back to Services](#)
[Disable](#)
[Copy](#)
[Save](#)
[Cancel](#)

You can configure five features of posture:

Table 13-1 Posture Features at the Service Level

Configurable Component	How to Configure
Enable posture validation for end-hosts with posture agents	Select <i>Enable posture validation for end hosts with posture agents</i> (checkbox) to enable the posture policy feature.
Sequence of Posture Policies	<p>Select a Policy, then Move Up, Move Down, Remove, or View Details.</p> <p>To add a previously configured Policy, select from the Select drop-down list, then click Add.</p> <p>To configure a new Policy, click Add New Policy (link) and refer to “Adding and Modifying Posture Policies” (page 162).</p> <p>To edit the selected posture policy, click Modify and refer to “Adding and Modifying Posture Policies” (page 162)</p>
Sequence of Posture Servers	<p>Select a Posture Server, then Move Up, Move Down, Remove, or View Details.</p> <p>To add a previously configured Posture Server, select from the Select drop-down list, then click Add.</p> <p>To configure a new Posture Server, click Add New Posture Server (link) and refer to “Adding and Modifying Posture Servers” (page 189).</p> <p>To edit the selected posture server, click Modify and refer to “Adding and Modifying Posture Policies” (page 162)</p>
Enable auto-remediation of non-compliant end-hosts	<p>Select <i>Enable auto-remediation of non-compliant end-hosts</i> (checkbox) to enable the specified remediation server to enable auto-Remediation.</p> <p>Remediation server is optional. A popup appears on the client box, with the URL of the Remediation server.</p>

Adding and Modifying Posture Policies

Posture Policy. Policy Manager supports pre-configured posture plugins, against which administrators can configure rules that test for specific attributes of client health and correlate the results to posture tokens:

- *If you have NAP Agent (USHA) running on a NAP-compatible client (Windows 7, Windows Vista, Windows XP SP3, Windows Server 2008), use:*

ClearPass Windows Universal System Health Validator. Configurable checking for present/absent Registry Keys, Services and processes, and product-/version-/update- specific checking for Antivirus, Antispyware, and Firewall applications, checks for peer-to-peer applications or networks, and patch management applications.

- *If you have ClearPass Linux NAP Agent running on a Linux client (CentOS, Fedora, Red Hat Enterprise Linux, SUSE Linux Enterprise Desktop), use:*

ClearPass Linux Universal System Health Validator. Configurable checking for present/absent Services, and product-/version-/update- specific checking for Antivirus application, and Firewall configuration.

- *If you have a Microsoft NAP Agent running on the client, use:*
 - **Windows System Health Validator.** Configurable checking for required operating system versions and service packs.
 - **Windows Security Health Validator.** Configurable checking for Antivirus/Antispyware/Firewall applications, as well as automatic updates and security updates.
- *If you have ClearPass OnGuard Agent (dissolvable or persistent) running on the client (Windows 7, Windows Vista, Windows XP, Windows Server 2008, Windows 2000, Windows 2003, SUSE Linux, Redhat Enterprise Linux, Fedora Linux, CentOS Linux, MAC OS X), use:*
 - **ClearPass Windows Universal System Health Validator.** Configurable checking for present/absent Registry Keys and Services, and product-/version-/update- specific checking for Antivirus, Antispyware, and Firewall applications, and patch management applications.
 - **Windows System Health Validator.** Configurable checking for required operating system versions and service packs.
 - **ClearPass Linux Universal System Health Validator.** Configurable checking for present/absent services, and product-/version-/update- specific checking for Antivirus application, and Firewall configuration.
 - **ClearPass Mac OS X Universal System Health Validator.** Configurable checking for product-/version-/update- specific checking for Antivirus/Antispyware application, and Firewall configuration.

Note that ClearPass OnGuard Agent - both persistent and dissolvable forms it - can be used in the following scenarios:

- An environment that does not support 802.1X based authentication (legacy Windows Operating Systems, or legacy devices in the network)
- An OS that supports 802.1X natively, but does not have a built-in health agent. For example, MAC OS X.

Configuring Posture Policy Plugins

From the **Services** page (**Configuration > Service**), you can configure posture for a new service (as part of the flow of the **Add Service** wizard), or modify an existing posture policy or server directly (**Configuration > Posture > Posture Policies**, then click on its name in the **Posture Policies** listing page).

When you click **Add Posture Policy** from any of these locations, Policy Manager displays the **Add Posture Policy** page, which contains three configurable tabs:

- The **Policy** Tab labels the policy and defines operating system and the type of deployed agent.

Figure 13-3 Add Posture Policy (Policy Tab)

Table 13-2 Add Posture Policy

Parameter	Description
Name/Description	Freeform label and description.
Host Operating System	Select <i>Linux</i> , <i>Windows</i> or <i>Mac OS X</i> .
Posture Agent	<p><i>NAP Agent</i> - Use this to configure posture policies for host operating systems with an embedded NAP-compliant agent (Microsoft Windows NAP Agent or ClearPass Linux NAP Agent). Currently, the following OSes are supported: Microsoft Windows 7, Microsoft Windows Vista, Microsoft Windows XP SP3, Microsoft Windows Server 2008, and Linux OSes supported by ClearPass Linux NAP Agent.</p> <p><i>OnGuard Agent</i> - Use this to configure posture policies for guest or web portal based use cases (via a dissolvable Java-applet based agent), or for use cases where ClearPass (persistent) OnGuard Agent is installed on the endpoint. Currently, the following OSes are supported by the OnGuard Agent: Microsoft Windows 7, Microsoft Windows Vista, Microsoft Windows XP (SP2 or above), Microsoft Windows Server 2008, Microsoft Windows Server 2003, Microsoft Windows 2000, MAC OS X 10.5 or above, and Linux OSes supported by ClearPass Linux NAP Agent.</p>

- The **Posture Plugins** tab provides a selector for posture policy plugins. Select a plugin (by enabling its checkbox), then click **Configure**.

Figure 13-4 Add Posture Policy (Posture Plugins Tab) - Windows NAP Agent

Policy **Posture Plugins** Rules Summary

Select one/more plugins:

Plugin Name	Plugin Configuration	Status
<input type="checkbox"/> ClearPass Windows Universal System Health Validator	Configure View	-
<input type="checkbox"/> Windows System Health Validator	Configure View	-
<input type="checkbox"/> Windows Security Health Validator	Configure View	-

Back to Posture Policies Next > Save Cancel

Figure 13-5 Add Posture Policy (Posture Plugins Tab) - Linux NAP Agent

Policy **Posture Plugins** Rules Summary

Select one/more plugins:

Plugin Name	Plugin Configuration	Status
<input type="checkbox"/> ClearPass Linux Universal System Health Validator	Configure View	-

Back to Posture Policies Next > Save Cancel

Figure 13-6 Add Posture Policy (Posture Plugins Tab) - Windows OnGuard Agent

Policy **Posture Plugins** Rules Summary

Select one/more plugins:

Plugin Name	Plugin Configuration	Status
<input type="checkbox"/> ClearPass Windows Universal System Health Validator	Configure View	-
<input type="checkbox"/> Windows System Health Validator	Configure View	-

Back to Posture Policies Next > Save Cancel

Figure 13-7 Add Posture Policy (Posture Plugins Tab) - Linux OnGuard Agent

Policy **Posture Plugins** Rules Summary

Select one/more plugins:

Plugin Name	Plugin Configuration	Status
<input type="checkbox"/> ClearPass Linux Universal System Health Validator	Configure View	-

Back to Posture Policies Next > Save Cancel

Figure 13-8 Add Posture Policy (Posture Plugins Tab) - Mac OS X OnGuard Agent

Policy **Posture Plugins** Rules Summary

Select one/more plugins:

Plugin Name	Plugin Configuration	Status
<input type="checkbox"/> ClearPass Mac OS X Universal System Health Validator	Configure View	-

Back to Posture Policies Next > Save Cancel

Refer to the following sections for plugin-specific configuration instructions:

- “ClearPass Windows Universal System Health Validator - NAP Agent” (page 167)
- “Windows System Health Validator - NAP Agent” (page 185)
- “Windows Security Health Validator - NAP Agent” (page 187)
- “ClearPass Windows Universal System Health Validator - OnGuard Agent” (page 182)
- “ClearPass Linux Universal System Health Validator - OnGuard Agent” (page 185)
- “Windows System Health Validator - OnGuard Agent” (page 186)
- “ClearPass Mac OS X Universal System Health Validator - OnGuard Agent” (page 187)
- The **Rules** tab matches posture checking outcomes:
 - Passes all System Health Validator (SHV) checks
 - Passes one or more SHV checks
 - Fails all SHV checks
 - Fails one or more SHV checks

to specific posture tokens:

- **Healthy.** Client is compliant; there are no restrictions on network access.
- **Checkup.** Client is compliant; however, there is an update available. This can be used to proactively remediate to healthy state.
- **Transient.** Client evaluation is in progress; typically associated with auditing a client. The network access granted is interim.
- **Quarantine.** Client is out of compliance; restrict network access, so the client only has access to the remediation servers.
- **Infected.** Client is infected and is a threat to other systems in the network; network access should be denied or severely restricted.
- **Unknown.** The posture token of the client is unknown.

To commit a Condition/Action pairing, select them from their respective **Conditions** and **Actions** drop-down lists, then click **Save**.

Figure 13-9 Add Posture Policy (Rules Tab)

The screenshot displays the 'Add Posture Policy (Rules Tab)' interface. At the top, there are tabs for 'Policy', 'Posture Plugins', 'Rules', and 'Summary'. The 'Rules' tab is active, showing a 'Rules Evaluation Algorithm' set to 'First applicable'.

Below the tabs is a table with two columns: 'Conditions' and 'Posture Token'. The table contains one rule:

Conditions	Posture Token
1. Passes all SHV checks - ClearPass Windows Universal System Health Validator Windows System Health Validator Windows Security Health Validator	HEALTHY

Below the table are buttons: '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'.

Conditions:

- Select Plugin Checks: Fails one or more SHV checks
- Select Plugins:
 - ☐ ClearPass Windows Universal System Health Validator
 - ☒ Windows System Health Validator
 - ☒ Windows Security Health Validator

Actions:

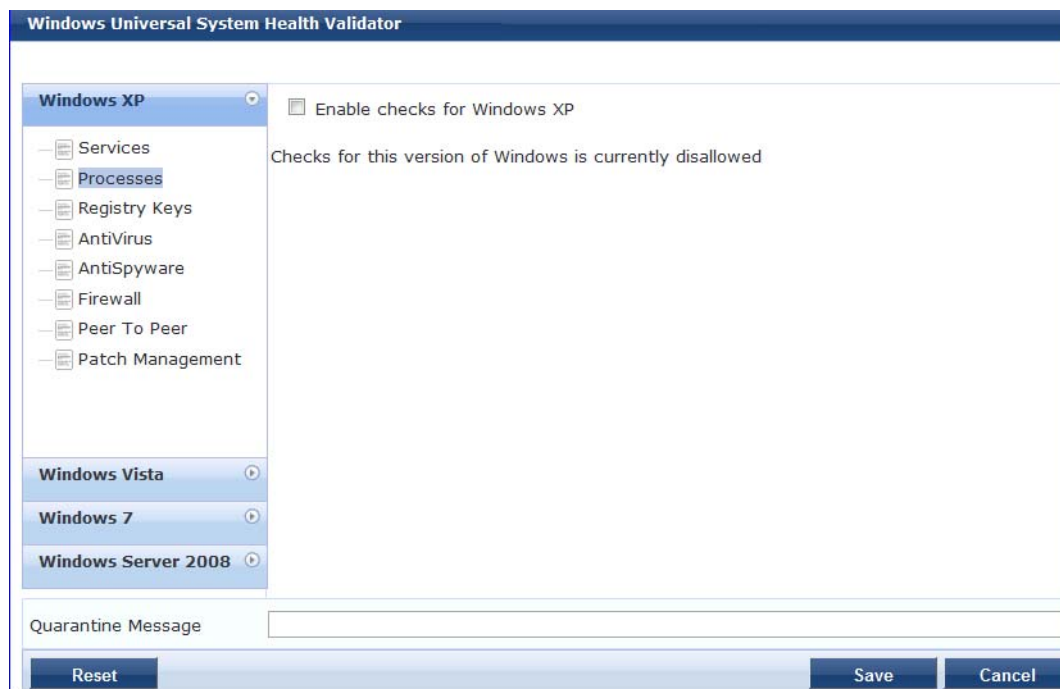
- Posture Token: QUARANTINE (20)

At the bottom of the 'Rules Editor' are 'Save' and 'Cancel' buttons.

At the bottom of the main interface are buttons: 'Back to Posture Policies', 'Next >', 'Save', and 'Cancel'.

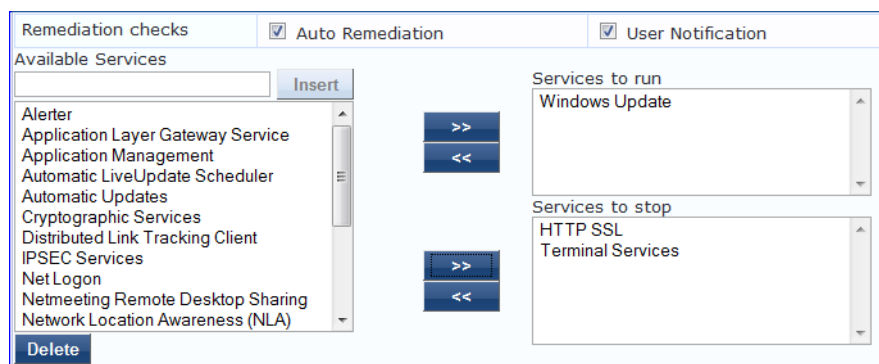
ClearPass Windows Universal System Health Validator - NAP Agent

The **ClearPass Windows Universal System Health Validator** page popup appears in response to actions in the **Posture Plugins** tab of the **Posture** configuration.

Figure 13-10 ClearPass Windows Universal System Health Validator - NAP Agent

Select a version of Windows and click the checkbox to enable checks for that version. Enabling checks for a specific version displays the corresponding set of configuration pages:

- The **Services** page provides a set of widgets for specifying specific services to be explicitly running or stopped.

Figure 13-11 Services Page**Table 13-3 Services Page**

Parameter	Description
Auto Remediation	Enable to allow auto remediation for service checks (Automatically stop or start services based on the entries in Service to run and Services to stop configuration).

Parameter	Description
User Notification	Enable to allow user notifications for service check policy violations.
Available Services	<p>This scrolling list contains a list of services that you can select and move to the Services to run or Services to stop panels (using their associated widgets). This list is different for the different OS types.</p> <p>Click the >> or << to add or remove, respectively, the services from the Service to run or Services to stop boxes.</p>
Insert	To add a service to the list of available services, enter its name in the text box adjacent to this button, then click Insert .
Delete	To remove a service from the list of available services, select it and click Delete .

- The **Processes** page provides a set of widgets for specifying specific processes to be explicitly present or absent on the system.

Figure 13-12 Processes Page (Overview)

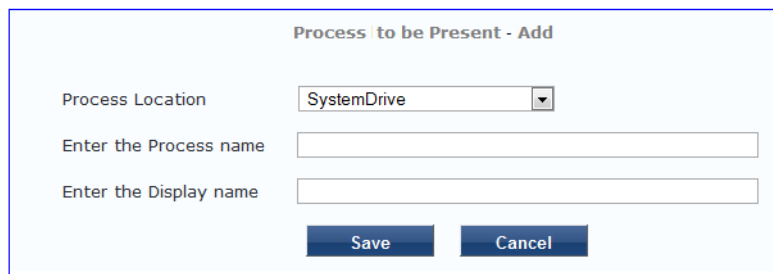
The screenshot shows a web interface for configuring processes. At the top, there are checkboxes for 'Remediation checks', 'Auto Remediation', and 'User Notification'. Below this, there are two main sections:

- Processes to be Present:** This section contains a table with two columns: 'Process Path' and 'Process Name'. There is an 'Add' button to the right of the table.
- Processes to be Absent:** This section contains a table with two columns: 'Process MD5 Sum' and 'Process Name'. There is an 'Add' button to the right of the table.

Table 13-4 Process Page (Overview - Pre-Add)

Parameter	Description
Auto Remediation	Enable to allow auto remediation for registry checks (Automatically add or remove registry keys based on the entries in Registry keys to be present and Registry keys to be absent configuration).
User Notification	Enable to allow user notifications for registry check policy violations.
Processes to be present/absent	Click Add to specify a process to be added, either to the Processes to be present or Processes to be absent lists.

Click **Add** for Process to be present to display the **Process** page detail.

Figure 13-13 Process to be Present Page (Detail)

Process to be Present - Add

Process Location

Enter the Process name

Enter the Display name

Table 13-5 Process to be Present Page (Detail)

Parameter	Description
Process Location	<p>Choose from one of the pre-defined paths, or choose None.</p> <ul style="list-style-type: none">• SystemDrive - For example, C:• SystemRoot - For example, C:\Windows• ProgramFiles - For example, "C:\Program Files"• HOMEDRIVE - For example, C:• HOMEPATH - For example, \Users\JohnDoe• None - By selecting None, you can enter a custom path name in the Process Name field.

Parameter	Description
Enter the Process name	<p>A pathname containing the process executable name. Some valid examples are listed below:</p> <ul style="list-style-type: none"> • If SystemRoot is specified in the Process Location field, then entering notepad.exe in this field specifies that the following full pathname for the process should be checked: %SystemRoot%\notepad.exe. Typically, this expands to: C:\Windows\notepad.exe • If ProgramFiles is specified in the Process Location field, then entering “Mozilla Firefox\firefox.exe” in this field specifies that the following full pathname for the process should be checked: “%ProgramFiles%\Mozilla Firefox\firefox.exe”. Typically, this expands to: “C:\Program Files\Mozilla Firefox\firefox.exe” • If None is specified in the Process Location field, then entering “\temp\usurf.exe” in this field specifies that the following full pathname for the process should be checked: “c:\temp\foo.exe” <p>Note that when the agent looks for running processes on the system, it looks for a process started from the specified location. For example, if the process to be running is specified to be C:\Windows\notepad.exe, the agent checks to see if there is a process running on the system that was started from the location C:\Windows. Even if the agent finds another process with the same name (notepad.exe) but started from a different location (C:\Temp), it will not match with what it is looking for. In this case, it will still start the process C:\Windows\notepad.exe.</p>
Enter the Display name	Enter a user friendly name for the process. This is displayed in end-user facing messages.

When you save your Process details, the key information appears in the **Processes to be present** page list.

Figure 13-14 Process to be Absent Page (Detail)

Process to be Absent - Add

Check Type : ☒ Process Name ☐ MD5 Sum

Enter the Process name

Enter the Display name

Save **Cancel**

Process to be Absent - Add

Check Type : ☐ Process Name ☒ MD5 Sum

MD5 Sum

Enter the Display name

Save **Cancel**

Table 13-6 Process to be Absent Page (Detail)

Parameter	Description
Check Type	<p>Select the type of process check to perform. The agent can look for</p> <ul style="list-style-type: none"> • Process Name - The agent looks for all processes that matches with the given name. For example, if notepad.exe is specified, the agent kills all processes whose name matches, regardless of the location from which these processes were started. • MD5 Sum - This specifies one or more (comma separated) MD5 checksums of the process executable file. For example, if there are multiple versions of the process executable, you can specify the MD5 sums of all versions here. The agent enumerates all running processes on the system, computes the MD5 sum of the process executable file, and matches this with the specified list. One or more of the matching processes are then terminated.
Enter the Display name	Enter a user friendly name for the process. This is displayed in end-user facing messages.

Figure 13-15 Process Page (Overview - Post Add)

Remediation checks

☒ Auto Remediation

☒ User Notification

Processes to be Present

Add

Process Path	Process Name	
SystemDrive	\\system32\\notepad.exe	

Processes to be Absent

Add

Process MD5 Sum	Process Name	
-	usurf.exe	
e1ab298bafc8ecca8c322a29c5fdc68c3f0ebc940fa292bb5f1d87dd544b5d60	UltraSurf	

- The **Registry** page provides a set of widgets for specifying specific registry keys to be explicitly present or absent.

Figure 13-16 Registry Page (Overview)

Remediation checks

☒ Auto Remediation

☒ User Notification

Registry keys to be present

Add

Key	Name	Value	Type	
-----	------	-------	------	--

Registry keys to be absent

Add

Key	Name	Value	Type	
-----	------	-------	------	--

Table 13-7 Registry Page (Overview - Pre-Add)

Parameter	Description
Auto Remediation	Enable to allow auto remediation for registry checks (Automatically add or remove registry keys based on the entries in Registry keys to be present and Registry keys to be absent configuration).
User Notification	Enable to allow user notifications for registry check policy violations.
Registry keys to be present/absent	Click Add to specify a registry key to be added, either to the Registry keys to be present or Registry keys to be absent lists.

Click **Add** for either condition to display the **Registry** page detail.

Figure 13-17 Registry Page (Detail)

Registry key to be Absent - Add

Select the Registry Hive HKEY_CLASSES_ROOT

Enter the Registry key
[eg: Software\SampleVendor\SampleApp\SampleKey]

Enter the Registry value name

Select the Registry value data type Any

Enter the Registry value data

Save
Cancel

Table 13-8 Registry Page (Detail)

Parameter	Description
Hive/Key/value (name, type, data)	Identifying information for a specific setting for a specific registry key.

When you save your Registry details, the key information appears in the **Registry** page list.

Figure 13-18 Registry Page (Overview - Post Add)

Remediation checks

☒ Auto Remediation

☒ User Notification

Registry keys to be present

Add

Key	Name	Value	Type	
HKEY_CLASSES_ROOT\software\SampleVendor\SampleApp\SampleKey	sdd	ddd	String	

Registry keys to be absent

Add

Key	Name	Value	Type	
HKEY_LOCAL_MACHINE\Software\Avenda\TestApp\Init	TestKeyName	@Ncdsnn	String	

- In the **Antivirus** page, you can specify that an Antivirus application must be on and allows drill-down to specify information about the Antivirus application.

In the **Antivirus** page, click **An Antivirus Application is On** to configure the Antivirus application information.

Figure 13-19 Antivirus Page (Overview - Before)

☐ An antivirus application is on

When enabled, the **Antivirus** detail page appears.

Figure 13-20 Antivirus Page (Detail 1)

☒ An antivirus application is on
 Remediation checks: ☒ Auto Remediation ☒ User Notification
 Product-specific checks: ☒ (Uncheck to allow any product)

Add

Antivirus	Prd Version	Eng Version	Dat Version	Last Scan	Rtp Check

Click **Add** to specify product, and version check information.

Figure 13-21 Antivirus Page (Detail 2)

Select the antivirus product: Symantec AntiVirus
 Product version check: Is Latest
 Engine version check: No Check
 Data file version check: No Check
 Last scan has been done before: 2 Day(s)
 Real-time Protection Status Check: ☐ No Check ☒ On ☐ Off

Save **Cancel**

When you save your Antivirus configuration, it appears in the **Antivirus** page list.

Figure 13-22 Antivirus Page (Overview - After)

☒ An antivirus application is on
 Remediation checks: ☒ Auto Remediation ☒ User Notification
 Product-specific checks: ☒ (Uncheck to allow any product)

Add

Antivirus	Prd Version	Eng Version	Dat Version	Last Scan	Rtp Check
Symantec AntiVirus	isLatest	no check	no check	2 Day(s)	on

Table 13-9 Antivirus Page

Interface	Parameter	Description
Antivirus Page	An Antivirus Application is On	Check the Antivirus Application is On checkbox to enable testing of health data for configured Antivirus application(s).
	Auto Remediation	Check the Auto Remediation checkbox to enable auto remediation of anti-virus status.
	User Notification	Check the User Notification checkbox to enable user notification of policy violation of anti-virus status.
	Uncheck to allow any product	Uncheck the Uncheck to allow any product checkbox to check whether any anti-virus application (any vendor) is running on the end host.

Interface	Parameter	Description
Antivirus Page (Detail 1)	Add	To <i>configure</i> Antivirus application attributes for testing against health data, click Add .
	Trashcan icon	To <i>remove</i> configured Antivirus application attributes from the list, click the trashcan icon in that row.
Antivirus Page (Detail 2)	Product/Version/ Last Check	<p>Configure the specific settings for which to test against health data. All of these checks may not be available for some products. Where checks are not available, they are shown in disabled state on the UI.</p> <ul style="list-style-type: none"> • Select the antivirus product - Select a vendor from the list • Product version check - No Check, Is Latest (requires registration with ClearPass portal), At Least, In Last N Updates (requires registration with ClearPass Portal) • Engine version check - Same choices as product version check. • Data file version check - Same choices as product version check • Last scan has been done before - Specify the interval in hours, days, weeks, or months. • Real-time Protection Status Check - on or off.

- In the **Antispyware** page, an administrator can specify that an Antispyware application must be on and allows drill-down to specify information about the Antispyware application.

In the **Antispyware** page, click **An Antispyware Application is On** to configure the Antispyware application information.

Figure 13-23 Antispyware Page (Overview Before)

A screenshot of the Antispyware page showing a single checkbox labeled "An antispyware application is on".

When enabled, the **Antispyware** detail page appears.

Figure 13-24 Antispyware Page (Detail 1)

A screenshot of the Antispyware page when the application is enabled. It shows a form with the following elements:

- A checked checkbox "An antispyware application is on".
- Two sections: "Remediation checks" with a checked "Auto Remediation" checkbox, and "User Notification" with a checked checkbox.
- "Product-specific checks" with a checked checkbox "(Uncheck to allow any product)".
- An "Add" button.
- A table header with columns: "Antispyware", "Prd Version", "Eng Version", "Dat Version", "Last Scan", and "Rtp Check".

Click **Add** to specify product, and version check information.

Figure 13-25 Antispyware Page (Detail 2)

Select the antispyware product: **AVG Anti-Malware [AntiSpyware]**

Product version check: **Is Latest**

Engine version check: **Is Latest**

Data file version check: **No Check**

Last scan has been done before: **Hour(s)**

Real-time Protection Status Check: ☒ No Check ☐ On ☐ Off

Save **Cancel**

Figure 13-26 Antispyware Page (Overview After)

☒ An antispyware application is on

Remediation checks: ☒ Auto Remediation ☒ User Notification

Product-specific checks: ☒ (Uncheck to allow any product)

Add

Antispyware	Prd Version	Eng Version	Dat Version	Last Scan	Rtp Check
AVG Anti-Malware [AntiSpyware]	isLatest	isLatest	no check	no check	nocheck

When you save your Antispyware configuration, it appears in the **Antispyware** page list.

The configuration elements are the same for anti-virus and antispyware products. Refer to the anti-virus configuration instructions above.

- In the **Firewall** page, you can specify that a Firewall application must be on and allows drill-down to specify information about the Firewall application.

Figure 13-27 Firewall Page (Overview Before)

☐ A firewall application is on

In the **Firewall** page, click **A Firewall Application is On** to configure the Firewall application information.

Figure 13-28 Firewall Page (Detail 1)

☒ A firewall application is on

Remediation checks: ☒ Auto Remediation ☒ User Notification

Product-specific checks: ☒ (Uncheck to allow any product)

Add

Firewall Product Name	Product Version
-----------------------	-----------------

When enabled, the **Firewall** detail page appears.

Figure 13-29 Firewall Page (Detail 2)

Select the firewall product: BitDefender Internet Security 2009

Product version is at least: 12

Save Cancel

When you save your Firewall configuration, it appears in the **Firewall** page list.

Figure 13-30 Firewall Page (Overview After)

☒ A firewall application is on

Remediation checks: ☒ Auto Remediation ☒ User Notification

Product-specific checks: ☒ (Uncheck to allow any product)

Add

Firewall Product Name	Product Version	
BitDefender Internet Security 2009	12	

Table 13-10 Firewall Page

Interface	Parameter	Description
Firewall Page	A Firewall Application is On	Check the Firewall Application is On checkbox to enable testing of health data for configured firewall application(s).
	Auto Remediation	Check the Auto Remediation checkbox to enable auto remediation of firewall status.
	User Notification	Check the User Notification checkbox to enable user notification of policy violation of firewall status.
	Uncheck to allow any product	Uncheck the Uncheck to allow any product checkbox to check whether any firewall application (any vendor) is running on the end host.
Firewall Page (Detail 1)	Add	<i>To configure</i> firewall application attributes for testing against health data, click Add .
	Trashcan icon	<i>To remove</i> configured firewall application attributes from the list, click the trashcan icon in that row.
Firewall Page (Detail 2)	Product/Version	<p>Configure the specific settings for which to test against health data. All of these checks may not be available for some products. Where checks are not available, they are shown in disabled state on the UI.</p> <ul style="list-style-type: none"> Select the firewall product - Select a vendor from the list Product version is at least - Enter the version of the product.

- The **Peer To Peer** page provides a set of widgets for specifying specific peer to peer applications or networks to be explicitly stopped. When you select a

peer to peer network, all applications that make use of that network are stopped.

Figure 13-31 Peer to Peer Page

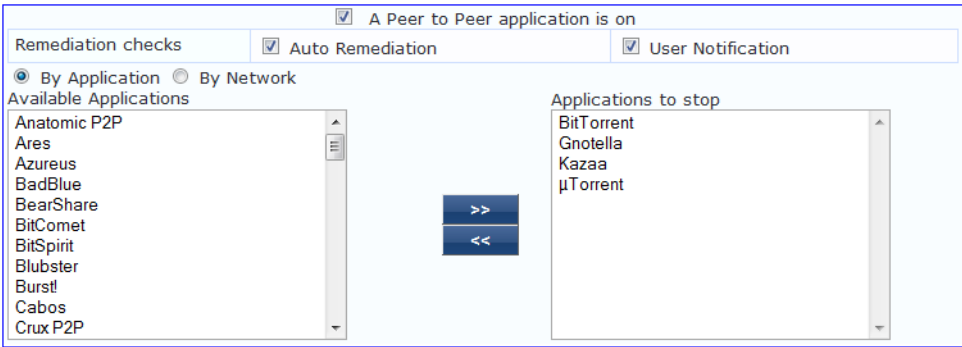


Table 13-11 Peer to Peer Page

Parameter	Description
Auto Remediation	Enable to allow auto remediation for service checks (Automatically stop peer to peer applications based on the entries in Applications to stop configuration).
User Notification	Enable to allow user notifications for peer to peer application/network check policy violations.
By Application / By Network	Select the appropriate radio button to select individual peer to peer applications or a group of applications that use specific p2p networks.
Available Applications	<p>This scrolling list contains a list of applications or networks that you can select and move to the Applications to stop panel.</p> <p>Click the >> or << to add or remove, respectively, the applications or networks from the Applications to stop box.</p>

- In the **Patches / Hot fixes** page, you can specify that a patch management application must be on and allows drill-down to specify information about the patch management application.

In the **Patches / Hot fixes** page, click **An patch management application is On** to configure the patch management application information.

Figure 13-32 Patches / Hot fixes Page (Overview - Before)



When enabled, the **Patches / Hot fixes** detail page appears.

Figure 13-33 Patches / Hot fixes Page (Detail 1)

Figure 13-33 shows the configuration options for patch management. At the top, there is a checkbox labeled "A patch management application is on" which is checked. Below this, there are three rows of checkboxes: "Remediation checks" with "Auto Remediation" checked, "User Notification" checked, and "Product-specific checks" with "(Uncheck to allow any product)" checked. An "Add" button is located to the right of these options. Below the options is a table with the following headers: "PM Product Name", "Product Version", "Status Check", and a trash icon. The table is currently empty.

Click **Add** to specify product, and version check information.

Figure 13-34 Patches / Hot fixes Page (Detail 2)

Figure 13-34 shows the configuration options for adding a new patch management product. It includes a dropdown menu for "Select the Patch Mgmt product" with "BigFix Enterprise Client" selected. Below this is a text input field for "Product version is at least" with "3.0" entered. There is also a dropdown menu for "Status Check Type" with "Enabled" selected. At the bottom are "Save" and "Cancel" buttons.

When you save your patches configuration, it appears in the **Patches / Hot fixes** page list.

Figure 13-35 Patches / Hot fixes Page (Overview - After)

Figure 13-35 shows the configuration options after saving a new patch management product. The configuration options are the same as in Figure 13-33. The table below now contains one row with the following data: "BigFix Enterprise Client" for "PM Product Name", "3.0" for "Product Version", and "Enabled" for "Status Check". A trash icon is visible at the end of the row.

Table 13-12 Patches / Hot fixes Page

Interface	Parameter	Description
Patches / Hot fixes Page	A patch management application is on	Check the Patches / Hot fixes Application is On checkbox to enable testing of health data for configured Antivirus application(s).
	Auto Remediation	Check the Auto Remediation checkbox to enable auto remediation of patch management status.
	User Notification	Check the User Notification checkbox to enable user notification of policy violation of patch management status.
	Uncheck to allow any product	Uncheck the Uncheck to allow any product checkbox to check whether any patch management application (any vendor) is running on the end host.

Interface	Parameter	Description
Patches / Hot fixes Page (Detail 1)	Add	To <i>configure</i> patch management application attributes for testing against health data, click Add .
	Trashcan icon	To <i>remove</i> configured patch management application attributes from the list, click the trashcan icon in that row.
Patches / Hot fixes Page (Detail 2)	Product/Version	<p>Configure the specific settings for which to test against health data. All of these checks may not be available for some products. Where checks are not available, they are shown in disabled state on the UI.</p> <ul style="list-style-type: none"> • Select the Patch Mgmt product - Select a vendor from the list • Product version is at least - Enter version number • Status check type - No check, Enabled, Disabled

- The **Windows Hotfixes** page provides a set of widgets for checking if specific Windows hotfixes are installed on the endpoint.

Figure 13-36 Windows Hotfixes Page

Table 13-13 Windows Hotfixes

Parameter	Description
Auto Remediation	Enable to allow auto remediation for hotfixes checks (Automatically trigger updates of the specified hotfixes).
User Notification	Enable to allow user notifications for hotfixes check policy violations.
Available Hotfixes	<p>The first scrolling list lets you select the criticality of the hotfixes. Based on this selection, the second scrolling list contains a list of hotfixes that you can select and move to the Hotfixes to be present panel (using their associated widgets).</p> <p>Click the >> or << to add or remove, respectively, the hotfixes from the Hotfixes to run boxes.</p>

- The **USB Devices** page provides configuration to control USB mass storage devices attached to an endpoint.

Figure 13-37 USB Devices
Table 13-14 USB Devices

Parameter	Description
Auto Remediation	Enable to allow auto remediation for USB mass storage devices attached to the endpoint (Automatically stop or eject the drive).
User Notification	Enable to allow user notifications for USB devices policy violations.
Remediation Action for USB Mass Storage Devices	<ul style="list-style-type: none"> No Action - Take no action; do not eject or disable the attached devices. Remove USB Mass Storage Devices - Eject the attached devices. Remove USB Mass Storage Devices - Stop the attached devices.

ClearPass Windows Universal System Health Validator - OnGuard Agent

The **ClearPass Windows Universal System Health Validator - OnGuard Agent** page popup appears in response to actions in the **Posture Plugins** p of the **Posture** configuration. (When you select **Windows** and **OnGuard Agent** from the posture policy page)

The OnGuard Agent version of the ClearPass Windows Universal System Health Validator supports all the features supported by the NAP Agent validator. In addition, it also supports two other Windows operating systems: Windows 2000 and Windows Server 2003.

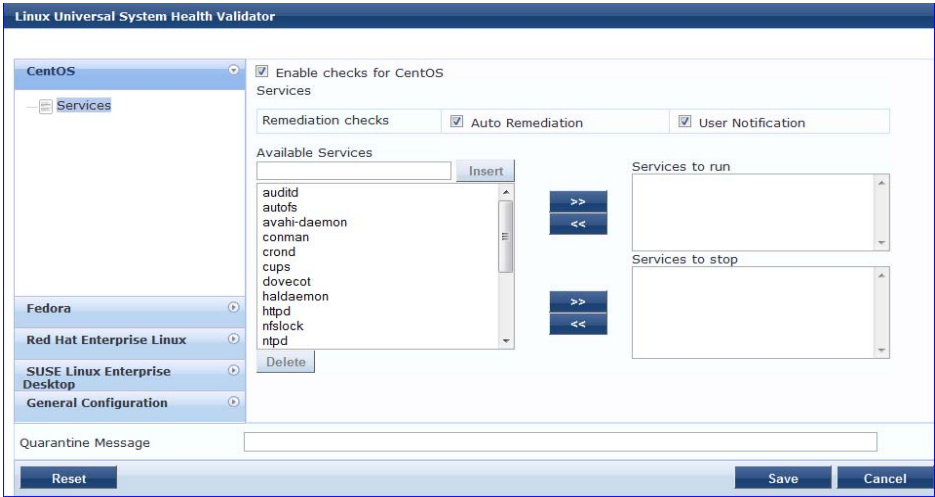
The Anti-Virus, Anti-Spyware, Firewall, Services, Patch Management, Process and Peer-to-Peer configuration steps described under the NAP Agent section also applies to the OnGuard Agent.

Note: Even though the UI allows configuring auto remediation, the **dissolvable** OnGuard Agent does not support this feature.

ClearPass Linux Universal System Health Validator - NAP Agent

The **ClearPass Linux Universal System Health Validator** page popup appears in response to actions in the **Posture Plugins** tab of the **Posture** configuration.

Figure 13-38 ClearPass Linux Universal system Health Validator - NAP Agent



Select a linux version and **Enable checks**for that version.

- The **Services** view appears automatically and provides a set of widgets for specifying specific services to be explicitly running or stopped.

Table 13-15 Services View

Parameter	Description
Auto Remediation	Enable to allow auto remediation for service checks (Automatically start or stop services based on the entries in Service to run and Service to stop configuration).
User Notification	Enable to allow user notifications for service status policy violations.
Available Services	This scrolling list contains a list of services that you can select and move to the Services to run or Services to stop panels (using their associated widgets).
Insert	To add a service to the list of selectable services, enter its name in the text box adjacent to this button, then click Insert .
Delete	To remove a service from the list of selectable services, select it and click Delete .

At the bottom left, the **General Configuration** section contains two pages: **Firewall Check** and **Antivirus Check**. Enable checkbox in either page display its respective configuration view:

Note: The configurations done in General Configuration section is applicable to all operating systems whose checks have been turned on.

Figure 13-39 General Configuration Section

The screenshot shows a web interface with a list of operating systems on the left: CentOS, Fedora, Red Hat Enterprise Linux, SUSE Linux Enterprise Desktop, and General Configuration. To the right of this list is a checkbox labeled 'Antivirus Check'. Below the list, there is a sidebar with two items: 'Antivirus' and 'Firewall', each with a small icon.

Select **Firewall Check** to display a view where you can specify Firewall parameters, specifically with respect to which ports may be open or blocked.

Figure 13-40 Firewall view

The screenshot shows the 'Firewall Check' configuration view. It has a title bar with a checked checkbox and the text 'Firewall Check'. Below the title bar, there are three tabs: 'Remediation checks', 'Auto Remediation' (checked), and 'User Notification' (checked). The main area contains several input fields: 'TCP ports to open', 'UDP ports to open', 'Block all other ports' (checkbox), 'TCP ports to block', and 'UDP ports to block'. At the bottom, there is an example text: 'Example: 90,100-200,256,1000-2000'.

- Select **Antivirus Check**, then click **Add** in the view that appears to specify Antivirus details.

Figure 13-41 Antivirus Check view

The screenshot shows the 'Antivirus Check' configuration view. It has a title bar with a checked checkbox and the text 'Antivirus Check'. Below the title bar, there is a label 'Select the Antivirus product' followed by a text input field containing 'AVG Anti-Virus'. Below this, there are three rows, each with a label and a dropdown menu: 'Product version check' with 'Is Latest', 'Engine version check' with 'Is Latest', and 'Data file version check' with 'Is Latest'. At the bottom right, there are two buttons: 'Save' and 'Cancel'.

When you save your Antivirus configuration, it appears in the **Antivirus** page list.

Figure 13-42 Antivirus Check

☒ Antivirus Check

Remediation checks ☒ Auto Remediation ☒ User Notification

Product-specific checks ☒ (Uncheck to allow any product)

Add

Product	Product Version	Engine Version	Dat file Version	
AVG Anti-Virus	isLatest	isLatest	isLatest	

Table 13-16 Antivirus Check

Interface	Parameter	Description
Antivirus Main view	Add	To <i>configure</i> Antivirus application attributes for testing against health data, click Add .
	Trashcan icon	To <i>remove</i> configured Antivirus application attributes from the list, click the trashcan icon in that row.
Antivirus Detail view	Product/Version/ Last Check	Configure the specific settings for which to test against health data. These fields all have their obvious meaning (described in the ClearPass Windows Universal System Health Validator section).

ClearPass Linux Universal System Health Validator - OnGuard Agent

The **ClearPass Linux Universal System Health Validator - OnGuard Agent** page popup appears in response to actions in the **Posture Plugins** tab of the **Posture** configuration (When you select **Linux** and **OnGuard Agent** from the posture policy page).

The dissolvable agent version of the ClearPass Linux Universal System Health Validator supports all the features supported by the NAP Agent validator except for the following:

- Auto-remediation
- Firewall status check and control

Windows System Health Validator - NAP Agent

This validator checks for current Windows Service Packs. An administrator can use the checkboxes to enable support of specific operating systems and to restrict access based on service pack level.

Figure 13-43 Windows System Health Validator (Overview)

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 System Health Validator - OnGuard Agent

This validator checks for current Windows Service Packs. The OnGuard Agent also supports legacy Windows operating systems such as Windows 2000 and Windows Server 2003. An administrator can use the checkboxes to enable support of specific operating systems and to restrict access based on service pack level.

Figure 13-44 Windows System Health Validator - OnGuard Agent (Overview)

Windows System Health Validator

Client computers can connect to your network, subject to the following checks -

☐ 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 2000**
Windows 2000 clients are allowed
☐ Restrict clients which have Service Pack less than

☒ **Windows Server 2003**
Windows Server 2003 clients are allowed
☐ Restrict clients which have Service Pack less than

Windows Security Health Validator - NAP Agent

This validator checks for the presence of specific types of security applications. An administrator can use the checkboxes to restrict access based on the absence of the selected security application types.

Figure 13-45 Windows Security Health Validator

ClearPass Mac OS X Universal System Health Validator - OnGuard Agent

The **ClearPass Mac OS X Universal System Health Validator** page popup appears in response to actions in the **Posture Plugins** tab of the **Posture** configuration.

Figure 13-46 ClearPass Mac OS X Universal System Health Validator - OnGuard Agent

Click the checkbox to enable checks for Mac OS X. Enabling checks displays the corresponding set of configuration pages:

- In the **Antivirus** page, you can specify that an Antivirus application must be on and allows drill-down to specify information about the Antivirus application.

In the **Antivirus** page, click **An Antivirus Application is On** to configure the Antivirus application information.

Figure 13-47 Antivirus Page (Overview - Before)

A screenshot of the Antivirus page overview. It shows a single entry with the text "An antivirus application is on" next to a small icon.

When enabled, the **Antivirus** detail page appears.

Figure 13-48 Antivirus Page (Detail 1)

A screenshot of the Antivirus page detail view. It shows a form with several sections:

- Antivirus Application Status:** A checkbox labeled "An antivirus application is on" is checked.
- Remediation checks:** A checkbox labeled "Auto Remediation" is checked.
- User Notification:** A checkbox labeled "User Notification" is checked.
- Product-specific checks:** A checkbox labeled "(Uncheck to allow any product)" is checked.
- Buttons:** An "Add" button is located at the bottom right.
- Table:** A table with columns: "Antivirus", "Prd Version", "Eng Version", "Dat Version", "Last Scan", and "Rtp Check".

Click **Add** to specify product, and version check information.

Figure 13-49 Antivirus Page (Detail 2)

A screenshot of the Antivirus page detail view configuration form. It contains the following fields:

- Select the antivirus product:** A dropdown menu showing "Trend Micro Security for Macintosh".
- Product version check:** A dropdown menu showing "Is Latest".
- Engine version check:** A dropdown menu showing "No Check".
- Data file version check:** A dropdown menu showing "Is Latest".
- Last scan has been done before:** A text input field followed by a "Hour(s)" dropdown menu.
- Real-time Protection Status Check:** Radio buttons for "No Check", "On" (selected), and "Off".
- Buttons:** "Save" and "Cancel" buttons at the bottom.

When you save your Antivirus configuration, it appears in the **Antivirus** page list. See [“ClearPass Windows Universal System Health Validator - NAP Agent”](#) (page 167) for antivirus page and field descriptions.

- In the **Antispyware** page, an administrator can specify that an Antispyware application must be on and allows drill-down to specify information about the Antispyware application.

In the **Antispyware** page, click **An Antispyware Application is On** to configure the Antispyware application information. See Antivirus configuration details above for description of the different configuration elements.

When you save your Antispyware configuration, it appears in the **Antispyware** page list.

The configuration elements are the same for anti-virus and antispyware products. Refer to the anti-virus configuration instructions above.

- In the **Firewall** page, you can specify that a Firewall application must be on and allows drill-down to specify information about the Firewall application.

In the **Firewall** page, click **A Firewall Application is On** to configure the Firewall application information.

When enabled, the **Firewall** detail page appears. See “ClearPass Windows Universal System Health Validator - NAP Agent” (page 167) for firewall page and field descriptions.

Adding and Modifying Posture Servers

Policy Manager can forward all or part of the posture data received from the client to Posture Servers. The Posture Server evaluates the posture data and returns Application Posture Tokens.

From the **Services** page (**Configuration > Service**), you can configure a posture server for a new service (as part of the flow of the **Add Service** wizard), or modify an existing posture server directly (**Configuration > Posture > Posture Servers**, then click on its name in the **Posture Servers** listing).

Figure 13-50 Posture Servers Listing Page

Configuration » Posture » Posture Servers

Posture Servers

[+ Add Posture Server](#)
[Import Posture Servers](#)
[Export Posture Servers](#)

Filter: Name contains Go Clear Filter Show 10 records

#	<input type="checkbox"/>	Name ▼	Description	Protocol	Default State
1.	<input type="checkbox"/>	PS_NPS	NAP Posture Server	RADIUS	UNKNOWN
2.	<input type="checkbox"/>	Avenda CCA CAM	Cisco Clean Access Manager GAMEv2 server	GAMEv2	UNKNOWN

Showing 1-2 of 2

Copy Export Delete

When you click **Add Posture Server** from any of these locations, Policy Manager displays the **Posture Servers** configuration page.

Figure 13-51 Add Posture Server Page

Configuration » Posture » Posture Servers » Add

Posture Servers

Posture Server Primary Server Backup Server Summary

Name:

Description:

Server Type: ☒ Microsoft NPS

Default Posture Token: UNKNOWN (100)

[Back to Posture Servers](#)

Depending on the **Protocol** and **Requested Credentials**, different tabs and fields appear. Refer to:

- “Microsoft NPS” (page 190)

Microsoft NPS

Use the Microsoft NPS server when you want Policy Manager to have health - NAP Statement of Health (SoH) credentials - evaluated by the Microsoft NPS Server.

Table 13-17 Microsoft NPS Settings (Posture Server tab)

Parameter	Description
Name/Description	Freeform label and description.
Server Type	Always <i>Microsoft NPS</i> .
Default Posture Token	Posture token assigned if the server is unreachable or if there is a posture check failure. Select a status from the drop-down list.

Figure 13-52 Microsoft NPS Settings (Primary and Backup Server tabs)

Posture Server Primary Server Backup Server Summary

RADIUS Server Name:

RADIUS Server Port: (default is 1812)

Shared Secret: Verify:

Timeout: 5 seconds

☐ Enable to use backup when primary does not respond

RADIUS Server Name:

RADIUS Server Port: (default is 1812)

Shared Secret: Verify:

Timeout: 5 seconds

[Back to Posture Servers](#)

Table 13-18 Microsoft NPS Settings (Primary and Backup Server tabs)

Parameter	Description
RADIUS Server Name/Port	Hostname or IP address and RADIUS server UDP port
Shared Secret	Enter the shared secret for RADIUS message exchange; the same secret has to be entered on the RADIUS server (Microsoft NPS) side
Timeout	How many seconds to wait before deeming the connection dead; if a backup is configured, Policy Manager will attempt to connect to the backup server after this timeout.
Note: For the backup server to be invoked on primary server failover, check the Enable to use backup when primary does not respond checkbox.	

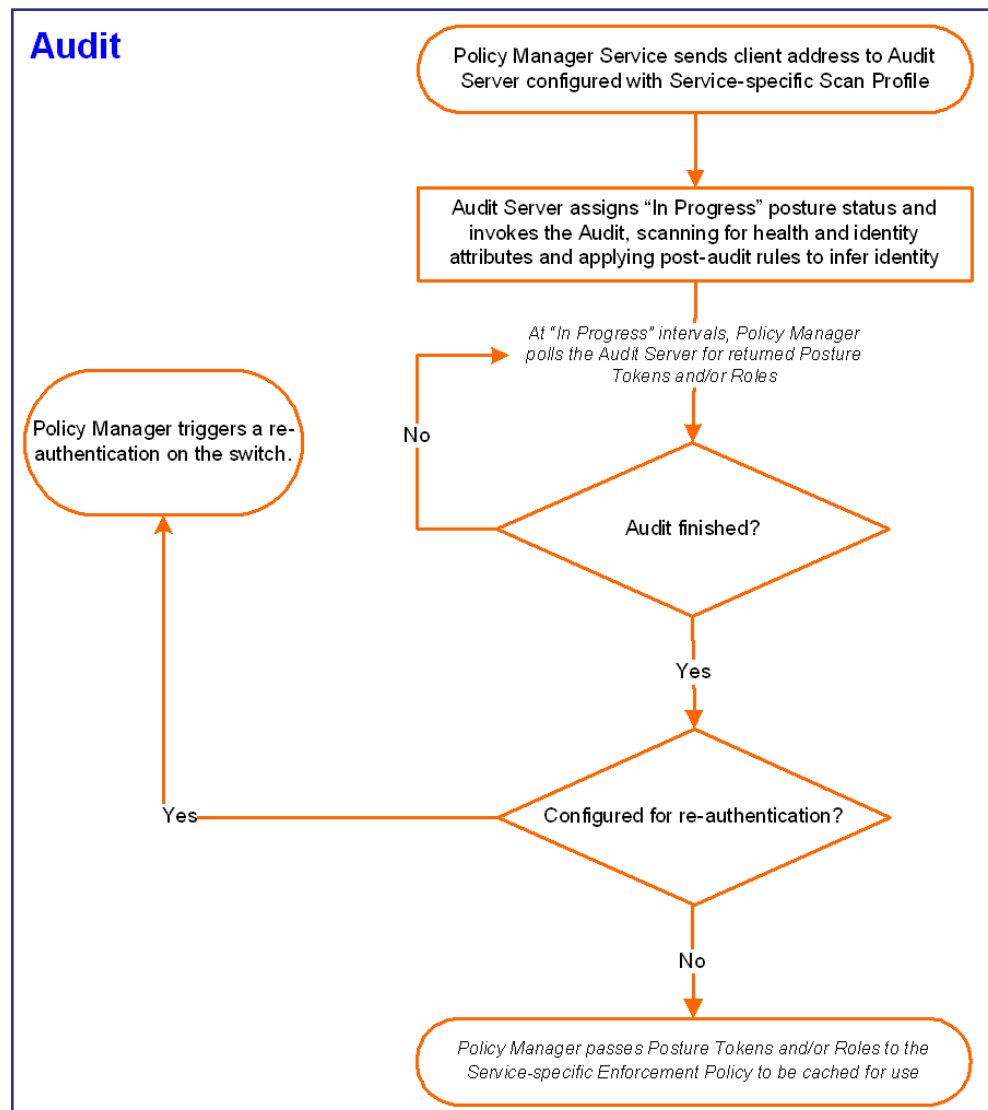
Chapter 14: Audit Servers

Audit Servers evaluate posture and/or role for unmanaged or unmanageable clients; that is, clients that lack an adequate posture agent or 802.1X supplicant (for example, printers, PDAs, or guest users may not be able to send posture credentials or identify themselves.) A Policy Manager Service can trigger an audit by sending a client ID to a pre-configured Audit Server, which returns attributes for role mapping and posture evaluation.

Architecture and Flow

Audit servers are configured at a global level. Only one audit server may be associated with a Service. The flow-of-control of the audit process occurs as follows:

Figure 14-1 Flow of Control of Policy Manager Auditing



Configuring Audit Servers

The Policy Manager server contains built-in Nessus (version 2.X) and NMAP servers. For enterprises with existing audit server infrastructure, or otherwise preferring external audit servers, Policy Manager supports these servers externally.

Built-In Audit Servers

When configuring an audit as part of an Policy Manager Service, you can select the default Nessus (*[Nessus Server]*) or NMAP (*[Nmap Audit]*) configuration.

Adding Auditing to An Policy Manager Service

1. Navigate to the Audit tab.

- To configure an audit server for a new service (as part of the flow of the *Add Service wizard*), navigate: **Configuration > Services > Add Services** (link) > **Audit** (tab).
- To modify an existing audit server, navigate: **Configuration > Posture > Audit Servers**, then select an audit server from the list.

2. Configure auditing.

Complete the fields in the **Audit** tab as follows:

Figure 14-2 Audit Tab

The screenshot shows the 'Configuration > Services > Add' page with the 'Services' section. The 'Audit' tab is selected among several tabs: Service, Authentication, Authorization, Roles, Audit, Enforcement, and Summary. The 'Audit' tab contains the following fields and options:

- Audit End-Hosts:** A checkbox labeled 'Enable auditing of end-hosts' which is checked.
- Audit Server:** A dropdown menu showing '--Select--'. To the right are buttons for 'View Details', 'Modify', and a link 'Add new Audit Server'.
- Audit Trigger Conditions:** A group of radio buttons:
 - Always
 - When posture is not available
 - For MAC authentication request (selected)
 - For known end-hosts only
 - For unknown end-hosts only
 - For all end-hosts
- Re-Authenticate End-Host:** A checkbox labeled 'Force re-authentication of the end-host after audit' which is checked.

At the bottom of the form, there is a 'Back to Services' button with a left arrow, and 'Next >', 'Save', and 'Cancel' buttons on the right.

Table 14-1 Audit Tab

Parameter	Description
Audit End-hosts	Select to enable auditing.

Parameter	Description
Audit Server/Add new Audit Server	<p>Select a built-in server profile from the list:</p> <ul style="list-style-type: none"> • The <i>[Nessus Server]</i> performs vulnerability scanning. It returns a <i>Healthy/Quarantine</i> result. • The <i>[Nmap Audit]</i> performs network port scans. The health evaluation always returns <i>Healthy</i>. The port scan gathers attributes that allow determination of Role(s) through post-audit rules. <p>Note: For Policy Manager to trigger an audit on an end-host, it needs to get the IP address of this end-host. The IP address of the end-host is not available at the time of initial authentication, in the case of 802.1X and MAC authentication requests. Policy Manager has a built-in DHCP snooping service that can examine DHCP request and response packets to derive the IP address of the end-host. For this to work, you need to use this service, Policy Manager must be configured as a DHCP “IP Helper” on your router/switch (in addition to your main DHCP server). Refer to your switch documentation for “IP Helper” configuration.</p> <p>To audit devices that have a static IP address assigned, it is recommended that a static binding between the MAC and IP address of the endpoint be created in your DHCP server. Refer to your DHCP Server documentation for configuring such static bindings.</p> <p>Note that Policy Manager does not issue IP address; it just examines the DHCP traffic in order to derive the IP address of the end-host.</p>
Trigger Conditions	<ul style="list-style-type: none"> • Always: Always perform an audit • When posture is not available: Perform audit only when posture credentials are not available in the request. <p>If you choose <i>For MAC Authentication Request</i>, Policy Manager presents three options:</p> <ul style="list-style-type: none"> • For known clients only. For example, when you want to reject unknown clients, but audit known clients for. Known clients are defined as those clients that are found in the authentication source(s) associated with this service. • For unknown clients only. For example, when known clients are assumed to be healthy, but you want to establish the identity of unknown clients and assign roles. Unknown client are those clients that are not found in any of the authentication sources associated with this service. • For all clients. For both known and unknown clients.
Re-authenticate client	<p>Check the checkbox for Force re-authentication of the client after audit to bounce the switch port or to force an 802.1X reauthentication (both done via SNMP).</p> <p>Note: Bouncing the port triggers a new 802.1X/MAC authentication request by the client. If the audit server already has the posture token and attributes associated with this client in its cache, it returns the token and the attributes to Policy Manager.</p>

Modifying Built-In Audit Servers

To reconfigure a default Policy Manager Audit Servers:

1. Open the audit server profile.

Navigate: **Configuration > Posture > Audit Servers > Audit** (page), then select an Audit Server. (from the listing).

Figure 14-3 Audit Servers Listing

The screenshot shows the 'Audit Servers' page under 'Configuration > Posture > Audit Servers'. It features a table with columns: #, Name, Description, and Type. There are three entries: 'eTIPS_Nessus_Server' (Type: NESSUS), 'eTIPS_Nmap_Audit' (Type: NMAP), and 'External Nessus Server (Sample)' (Type: NESSUS). Above the table is a filter section with a dropdown for 'Name', a 'contains' text box, a 'Go' button, a 'Clear Filter' button, and a 'Show 20 records' dropdown. To the right of the table are buttons for 'Copy', 'Export', and 'Delete'. At the top right, there are links: 'Add Audit Server', 'Import Audit Servers', and 'Export Audit Servers'.

#	Name	Description	Type
1.	eTIPS_Nessus_Server	Nessus server running in the eTIPS server	NESSUS
2.	eTIPS_Nmap_Audit	Nmap default configuration	NMAP
3.	External Nessus Server (Sample)		NESSUS

Showing 1-3 of 3

2. Modify the profile, plugins, and/or preferences.

- In the **Audit** tab, you can modify the **In Progress** and **Default** posture status.
- In the **Primary/Backup server** tabs, you can select **Add/Edit Scan Profile** to select plugins and preferences. Refer to “[Nessus Scan Profiles](#)” (page 200).

The built-in Policy Manager Nessus Audit Server ships with approximately 1000 of the most commonly used Nessus plugins. You can download others from <http://www.tenablesecurity.com>, in the form `all-2.0.tar.gz`. To upload them to the built-in Policy Manager Audit Server: **Administration > Server Manager > Server Configuration**, select **Upload Nessus Plugins** and select the downloaded file.

Figure 14-4 Upload Nessus Plugins Popup

The screenshot shows a 'Import from file' popup window. It has a 'Select File:' label next to a text box and a 'Browse...' button. Below that is a label 'Enter secret for the file (if any):' next to another text box. At the bottom right are 'Import' and 'Cancel' buttons.

- In the **Rules** tab, you can create post-audit rules for determining Role based on identity attributes discovered by the audit. Refer to “[Post-Audit Rules](#)” (page 204).

Custom Audit Servers

For enterprises with existing audit server infrastructure, or otherwise preferring custom audit servers, Policy Manager supports NISSUS (2.x and 3.x) (and NMAP scans using the NMAP plugin on these external Nessus Servers).

To configure a custom Audit Server:

1. Open the Audit page.

- To configure an audit server for a new service (as part of the flow of the *Add Service wizard*), navigate: **Configuration > Service > Audit** (tab), then click **Add new Audit Server**.
- To modify an existing audit server, navigate: **Configuration > Posture > Audit Server**, and select an audit server in the **Audit** tab.

2. Add a custom audit server.

When you click **Add Audit Server**, Policy Manager displays the **Add Audit Server** page.

Configuration settings vary depending on audit server type:

- “[NESSUS Audit Server](#)” (page 197)
- “[NMAP Audit Server](#)” (page 199)

NESSUS Audit Server

Policy Manager uses the NISSUS Audit Server interface primarily to perform vulnerability scanning. It returns a Healthy/Quarantine result.

The **Audit** tab identifies the server and defines configuration details.

Figure 14-5 NISSUS Audit Server (Audit Tab)

Configuration > Posture > Audit Servers > Add

Audit Servers

Audit	Primary Server	Backup Server	Rules	Summary
Name:	extern-nessus.acme.com			
Description:	External NISSUS 3.0 server			
Type:	<input type="radio"/> NMAP <input checked="" type="radio"/> NISSUS			
In-Progress Posture Status:	TRANSITION (15)			
Default Posture Status:	UNKNOWN (100)			

[Back to Audit Servers](#)
[Next >](#)
[Save](#)
[Cancel](#)

Table 14-2 NESSUS Audit Server (Audit Tab)

Parameter	Description
Name/Description	Freeform label and description.
Type	For purposes of an NESSUS-type Audit Server, always <i>NESSUS</i> .
In Progress Posture Status	Posture status during audit. Select a status from the drop-down list.
Default Posture Status	Posture status if evaluation does not return a condition/action match. Select a status from the drop-down list.

The **Primary** and **Backup Server** tabs specify connection information for the Nessus audit server.

Figure 14-6 NESSUS Audit Server (Primary & Backup Tabs)

The screenshot displays the configuration interface for the NESSUS Audit Server, divided into two main sections: Primary Server and Backup Server.

Primary Server Tab:

- Nessus Server Name:** extern-nessus.acme.com
- Nessus Server Port:** 1241 (default is 1241)
- Username:** admin
- Password:** [masked] **Verify:** [masked]
- Scan Profile:** default (with buttons for View Details, Modify, and Add/Edit Scan Profile)
- In-Progress Timeout:** 30 seconds

Backup Server Tab:

- Backup:** ☒ Enable to use backup when primary does not respond
- Nessus Server Name:** extern-nessus-backup.acme.com
- Nessus Server Port:** 1241 (default is 1241)
- Username:** admin
- Password:** [masked] **Verify:** [masked]
- Scan Profile:** default (with buttons for View Details, Modify, and Add/Edit Scan Profile)
- In-Progress Timeout:** 30 seconds

At the bottom of the interface, there is a navigation bar with a "Back to Audit Servers" link, a "Next >" button, and "Save" and "Cancel" buttons.

Table 14-3 NESSUS Audit Server (Primary & Backup Tabs)

Parameter	Description
Server Name and Port/ Username/ Password	Standard NESSUS server configuration fields. Note: For the backup server to be invoked on primary server failover, check the Enable to use backup when primary does not respond checkbox.
Scan Profile	You can accept the default Scan Profile or select Add/Edit Scan Profile to create other profiles and add them to the Scan Profile list. Refer to “Nessus Scan Profiles” (page 200).

The **Rules** Tab provides specifies rules for post-audit evaluation of the request to assign a role. Refer to “Post-Audit Rules” (page 204).

NMAP Audit Server

Policy Manager uses the NMAP Audit Server interface exclusively for network port scans. The health evaluation always returns *Healthy*. The port scan gathers attributes that allow determination of Role(s) through post-audit rules.

The **Audit** Tab labels the Server and defines configuration details.

Figure 14-7 **Audit Tab (NMAP)**

Configuration » Posture » Audit Servers » Add

Audit Servers

Audit

NMAP Options

Rules

Summary

Name:

Custom NMAP Profile

Description:

Customized NMAP profile for custom port scans

Type:

☒ NMAP ☐ NESSUS

In-Progress Posture Status:

TRANSITION (15)

Default Posture Status:

UNKNOWN (100)

Back to Audit Servers

Next >

Save

Cancel

Table 14-4 **Audit Tab (NMAP)**

Parameter	Description
Name/Description	Freeform label and description.
Type	For purposes of an NMAP-type Audit Server, always <i>NMAP</i> .
In Progress Posture Status	Posture status during audit. Select a status from the drop-down list.
Default Posture Status	Posture status if evaluation does not return a condition/action match. Select a status from the drop-down list.

The **NMAP Options** tab specifies scan configuration.

Figure 14-8 Options Tab (NMAP)
Table 14-5 Options Tab (NMAP)

Parameter	Description
TCP Scan	To specify a TCP scan, select from the TCP Scan drop-down list. Refer to NMAP documentation for more information on these options. NMAP option --scanflags.
UDP Scan	To enable, check the UDP Scan checkbox. NMAP option -sU.
Service Scan	To enable, check the Service Scan checkbox. NMAP option -sV.
Detect Host Operating System	To enable, check the Detect Host Operating System checkbox. NMAP option -A.
Port Range/ Host Timeout/ In Progress Timeout	Port Range - Range of ports to scan. NMAP option -p. Host Timeout - Give up on target host after this long. NMAP option --host-timeout In Progress Timeout - How long to wait before polling for NMAP results.

The **Rules** Tab provides specifies rules for post-audit evaluation of the request to assign a role. Refer to “[Post-Audit Rules](#)” (page 204).

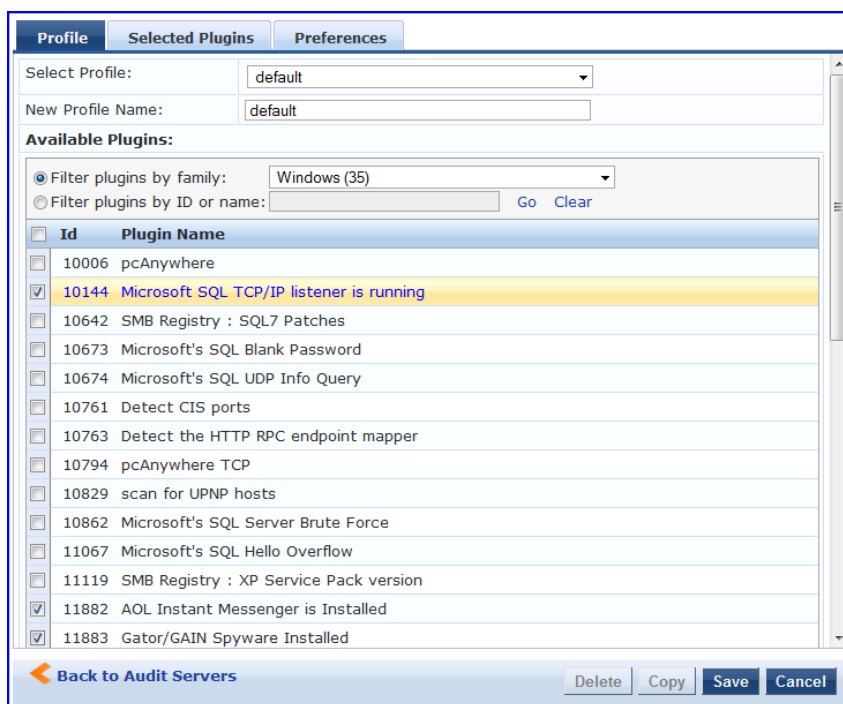
Nessus Scan Profiles

A scan profile contains a set of scripts (plugins) that perform specific audit functions. To Add/Edit Scan Profiles, select **Add/Edit Scan Profile** (link) from the **Primary Server** tab of the Nessus Audit Server configuration. The **Nessus Scan Profile Configuration** Page is displayed.

Figure 14-9 Nessus Scan Profile Configuration Page

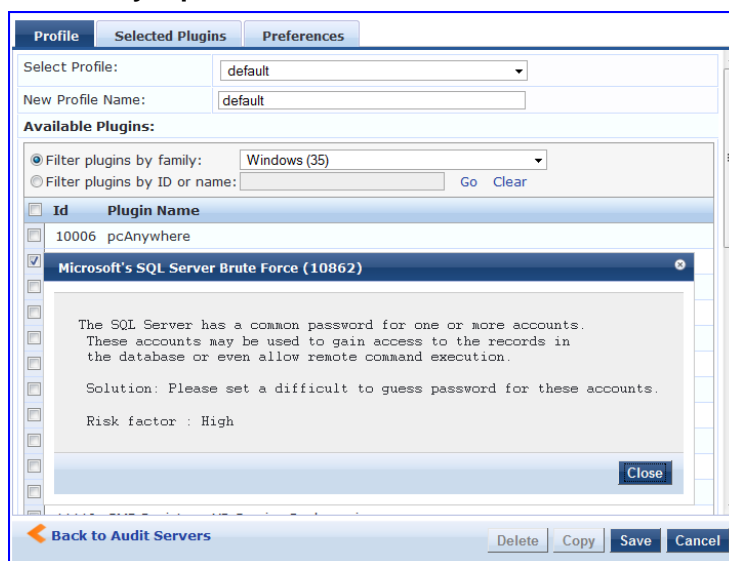
You can refresh the plugins list (after uploading plugins into Policy Manager, or after refreshing the plugins on your external Nessus server) by clicking **Refresh Plugins List**. The **Nessus Scan Profile Configuration** page provides three views for scan profile configuration:

- The **Profile** tab identifies the profile and provides a mechanism for selection of plugins:
 - From the **Filter plugins by family** drop-down list, select a family to display all available member plugins in the list below. You may also enter the name of a plugin in **Filter plugins by ID** or name text box.
 - Select one or more plugins by enabling their corresponding checkboxes (at left). Policy Manager will remember selections as you select other plugins from other plugin families.
 - When finished, click the **Selected Plugins** tab.

Figure 14-10 Nessus Scan Profile Configuration (Profile Tab)

- The **Selected Plugins** tab displays all selected plugins, plus any dependencies.

To display a synopsis of any listed plugin, click on its row.

Figure 14-11 Nessus Scan Profile Configuration (Profile Tab) - Plugin Synopsis

Note: Of special interest is the section of the synopsis entitled *Risks*.

To delete any listed plugin, click on its corresponding trashcan icon.

To change the vulnerability level of any listed plugin click on the link to change the level to one of HOLE, WARN, INFO, NOTE. This tells Policy Manager the vulnerability level that is considered to be assigned QUARANTINE status.

Figure 14-12 Nessus Scan Profile Configuration (Selected Plugins Tab)

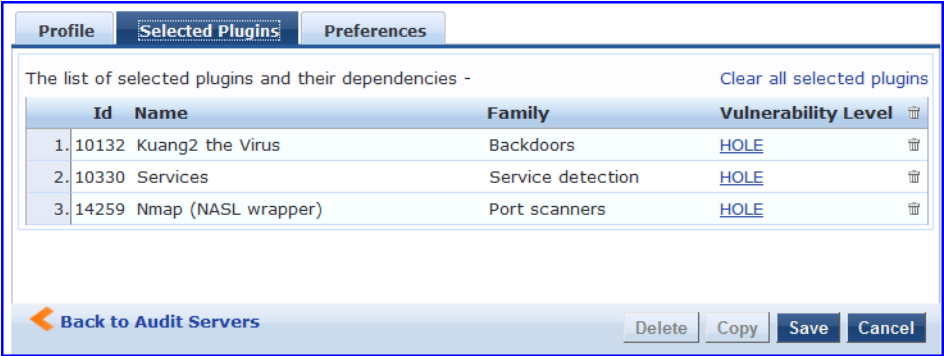
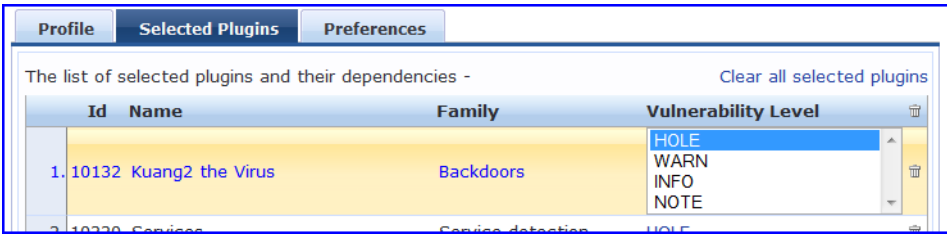


Figure 14-13 Nessus Scan Profile Configuration (Selected Plugins Tab) - Vulnerability Level



- For each selected plugin, the **Preferences** tab contains a list of fields that require entries.
- In many cases, these fields will be pre-populated. In other cases, you must provide information required for the operation of the plugin.
- By way of example of how plugins use this information, consider a plugin that must access a particular service, in order to determine some aspect of the client's status; in such cases, login information might be among the preference fields.

Figure 14-14 Nessus Scan Profile Configuration (Preferences Tab)

- Upon saving the profile, plugin, and preference information for your new (or modified) plugin, you can go to the **Primary/Backup Servers** tabs and select it from the **Scan Profile** drop-down list.

Post-Audit Rules

The **Rules** tab specifies rules for post-audit evaluation of the request to assign a role.

Figure 14-15 All Audit Server Configurations (Rules Tab)
Table 14-6 All Audit Server Configurations (Rules Tab)

Parameter	Description
Rules Evaluation Algorithm	<i>Select first matched</i> rule and return the role or <i>Select all matched</i> rules and return a set of roles.
Add Rule	Add a rule. Brings up the rules editor. See below.
Move Up/Down	Reorder the rules.
Edit Rule	Brings up the selected rule in edit mode.
Remove Rule	Remove the selected rule.

Figure 14-16 All Audit Server Configurations (Rules Editor)

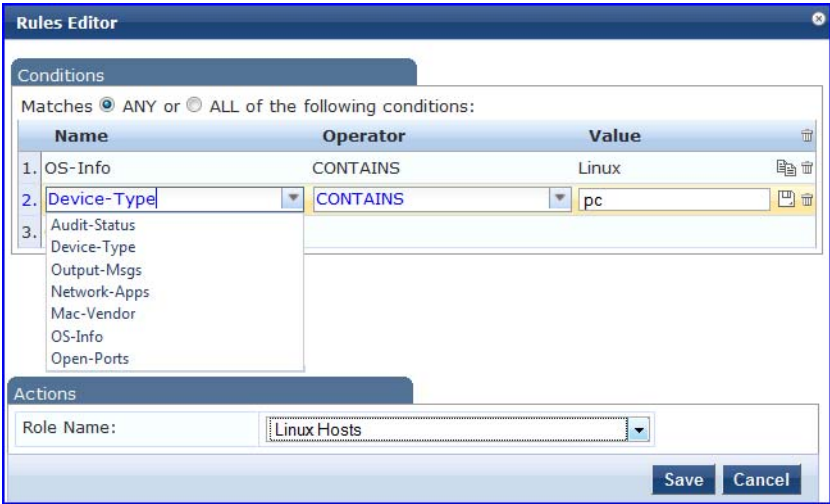


Table 14-7 All Audit Server Configurations (Rules Editor)

Parameter	Description
Conditions	The Conditions list includes five dictionaries: <i>Audit-Status</i> , <i>Device-Type</i> , <i>Output-Msgs</i> , <i>Mac-Vendor</i> , <i>Network-Apps</i> , <i>Open-Ports</i> , and <i>OS-Info</i> . Refer to “Namespaces” (page 314).
Actions	The Actions list includes the names of the roles configured in Policy Manager.
Save	To commit a Condition/Action pairing, click Save .

Chapter 15: Enforcement

Policy Manager controls network access by sending a set of access-control attributes to the request-originating Network Access Device (NAD).

Policy Manager sends these attributes by evaluating an *Enforcement Policy* associated with the service. The evaluation of Enforcement Policy results in one or more *Enforcement Profiles*; each Enforcement Profile wraps the access control attributes sent to the Network Access Device. For example, for RADIUS requests, commonly used Enforcement Profiles include attributes for VLAN, Filter ID, Downloadable ACL and Proxy ACL.

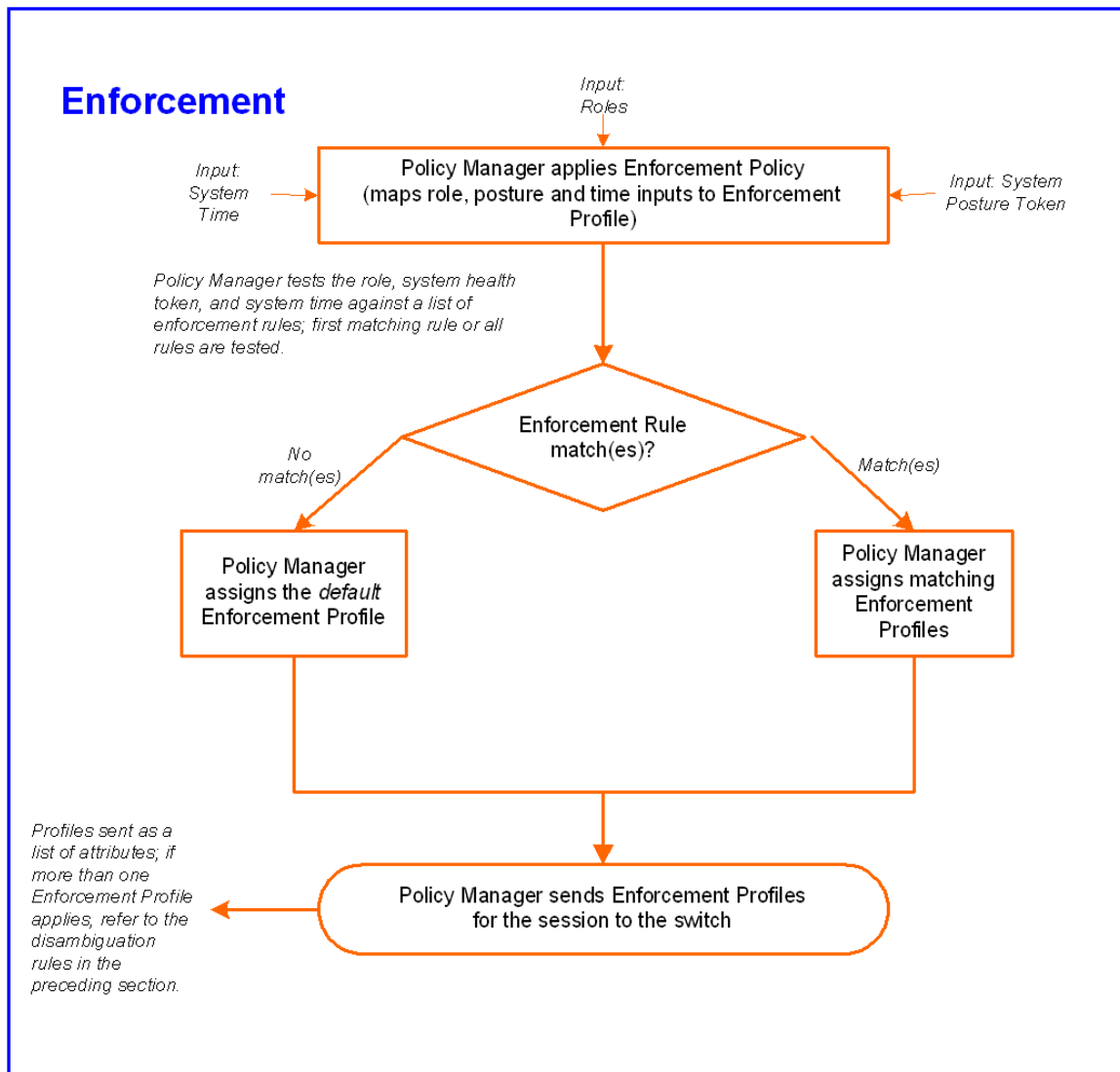
Architecture and Flow

To evaluate a request, a Policy Manager Application assembles the request's *client roles*, *client posture (system posture token)*, and *system time*. The calculation that matches these components to a pre-defined *Enforcement Profile* occurs inside of a black box called an *Enforcement Policy*.

Each *Enforcement Policy* contains a rule or set of rules for matching *Conditions* (role, posture and time) to *Actions* (Enforcement Profiles). For each request, it yields one or more matches, in the form of *Enforcement Profiles*, from which Policy Manager assembles access-control attributes for return to the originating NAD, subject to the following disambiguation rules:

- If an attribute occurs only once within an Enforcement Profile, transmit *as is*.
- If an attribute occurs multiple times *within the same Enforcement Profile*, transmit *as a multi-valued attribute*.
- If an attribute occurs *in more than one Enforcement Profile*, only transmit the value from the first Enforcement Profile in priority order.

Note: Optionally, each Enforcement Profile can have an associated group of NADs; when this occurs, Enforcement Profiles are only sent if the request is received from one of the NADs in the group. For example, you can have the same rule for VPN, LAN and WLAN access, with enforcement profiles associated with device groups for each type of access. If a device group is not associated with the enforcement profile, attributes in that profile are sent regardless of where the request originated.

Figure 15-1 Flow of Control of Policy Manager Enforcement

Configuring Enforcement Profiles

You configure Policy Manager Enforcement Profiles globally, but they must be referenced in an enforcement policy that is associated with a Service to be evaluated.

From the **Enforcement Policies** page (**Configuration > Enforcement > Policies**), you can configure an Enforcement Profile for a new enforcement policy (as part of the flow of the **Add Enforcement Policy** wizard), or modify an existing Enforcement Profile directly (**Configuration > Enforcement > Profiles**, then click on its name in the **Enforcement Profile** listing).

Figure 15-2 Enforcement Profiles Page

Configuration » Enforcement » Profiles

Enforcement Profiles

[Add Enforcement Profile](#)
[Import Enforcement Profiles](#)
[Export Enforcement Profiles](#)

Filter: contains Show records

#	<input type="checkbox"/>	Name ▲	Type	Description
1.	<input type="checkbox"/>	Access Switches Control	TACACS	TACACS+ Enforcement Profile for Access Switches
2.	<input type="checkbox"/>	Allow All Commands	TACACS	Allow all commands on the device
3.	<input type="checkbox"/>	AUTHFAIL_VLAN	RADIUS	VLAN to send on authentication failures
4.	<input type="checkbox"/>	Copy_of_AUTHFAIL_VLAN	RADIUS	VLAN to send on authentication failures
5.	<input type="checkbox"/>	DenyPrivilegedCommands	TACACS	Command Authorizations
6.	<input type="checkbox"/>	Departmental VLANs	RADIUS	
7.	<input type="checkbox"/>	Employee SNMP VLAN	SNMP	VLAN for employees
8.	<input type="checkbox"/>	EMPLOYEE_VLAN	RADIUS	Employee VLAN for wired access

Showing 1-20 of 30

Policy Manager comes pre-packaged with eight system-defined enforcement profiles:

- **[Allow Access Profile]**. System-defined RADIUS profile to allow network access; Policy Manager sends a RADIUS *AccessAccept* message with no attributes.
- **[Deny Access Profile]**. System-defined RADIUS profile to deny network access; Policy Manager sends a RADIUS *AccessReject* message with no attributes.
- **[Drop Access Profile]**. System-defined profile to drop the network access request; Policy Manager silently drops the RADIUS *AccessRequest* message.
- **[TACACS Deny Profile]**. System-defined TACACS+ profile to deny network device access through the TACACS+ protocol.
- There are several system-defined profiles associated with different vendors' RADIUS CoA actions.
 - **[Cisco - Terminate Session]** - Terminate a session on a Cisco device.
 - **[Cisco - Disable-Host-Port]** - Disable a port on a Cisco Ethernet switching device.
 - **[Cisco - Bounce-Host-Port]** - Perform link-up/link-down action on a Cisco Ethernet switching device.
 - **[Cisco - Reauthenticate-Session]** - Trigger a session reauthentication on a Cisco device.
 - **[HP - Terminate Session]** - Terminate a session on an HP device.
 - **[Aruba - Terminate Session]** - Terminate a session on an Aruba Wireless Controller.
- There are four built-in TACACS+ profiles that are mapped to the different administrator roles available in Policy Manager. These profiles can be used to give permissions to log into the Policy Manager UI.
 - **[TACACS Help Desk]**. System-defined profile to allow administrative access to Policy Manager using the *Helpdesk* role.

- **[TACACS Network Admin]**. System-defined profile to allow administrative access to Policy Manager using the *Network Administrator* role.
- **[TACACS Receptionist]**. System-defined profile to allow administrative access to Policy Manager using the *Receptionist* role.
- **[TACACS Super Admin]**. System-defined profile to allow administrative access to Policy Manager using the *Super Administrator* role.

From the **Enforcement Profile** page, when you click **Add Enforcement Profile**, Policy Manager displays the **Add Enforcement Profile** page:

Figure 15-3 Add Enforcement Profile Page

Configuration » Enforcement » Profiles » Add Enforcement Profile

Enforcement Profiles

Profile **Attributes** **Summary**

Template: VLAN Enforcement

- VLAN Enforcement
- Filter ID Based Enforcement
- RADIUS Based Enforcement
- RADIUS Change of Authorization (CoA)
- Agent Enforcement
- SNMP Based Enforcement
- CLI Based Enforcement
- TACACS+ Based Enforcement
- Cisco Downloadable ACL Enforcement
- Cisco Web Authentication Enforcement
- Arenda GuestConnect Enforcement
- Arenda Insight Enforcement
- Arenda Edge Filter Enforcement
- Generic Application Enforcement

Name:

Description:

Type: RADIUS

Action: ☒ Accept ☐ Reject ☐ Drop

Device Group List:

Remove	View Details	Modify	Add
--Select--			

[Back to Enforcement Profiles](#) [Next >](#) [Save](#) [Cancel](#)

Policy Manager comes pre-packaged with several enforcement profile templates:

- **VLAN Enforcement** - All RADIUS attributes for VLAN enforcement are pre-filled in this template.
- **Filter ID Based Enforcement** - All RADIUS attributes for filter-id based enforcement are pre-filled in this template.
- **RADIUS Based Enforcement** - Generic RADIUS template that can be filled with any attribute from the RADIUS vendor dictionaries loaded into Policy Manager.
- **RADIUS Change of Authorization (CoA)** - Enforcement profile that encapsulates CoA actions sent to the network device. Note that the system comes pre-packaged with default Enforcement Profiles for “Disconnect”

(Terminate Session) actions for the different supported vendor devices; there is no need to create profiles for these actions.

- TACACS+ Based Enforcement - TACACS+ based enforcement profile with UI customized for TACACS+ service & command authorization.
- SNMP Based Enforcement - Generic SNMP based enforcement profile with SNMP dictionaries for VLAN steering and Reset Connection.
- Cisco Downloadable ACL Enforcement - RADIUS based enforcement profile with UI customized for Cisco Downloadable ACL Enforcement.
- Cisco Web Authentication Enforcement - RADIUS based enforcement profile with pre-loaded attributes for enforcement for Cisco switch-hosted web authentication.
- Aruba GuestConnect Enforcement - Application specific enforcement profile with pre-loaded attributes for authorization of GuestConnect users.
- Aruba Insight Enforcement - Application specific enforcement profile with pre-loaded attributes for authorization of Insight users.
- Generic Application Enforcement - Application specific enforcement profile with customization attribute-value pairs for authorization of generic applications.
- CLI Based Enforcement - Enforcement profile that encapsulates CLI commands to be issued to the network device. The “Target Device” attribute specifies the device on which the “Command” attribute is executed.
- Agent Enforcement - Enforcement profile that encapsulates attributes sent to Aruba OnGuard agent. Attributes can be specified to bounce the client or to send a custom message to the client.

Table 15-1 Add Enforcement Profile Page

Parameter	Description
Name/ Description	Freeform label for enforcement profile.
Type	Auto-filled based on the selected template: RADIUS, TACACS, SNMP, Application, RADIUS_CoA
Action	Relevant only for RADIUS type enforcement profiles. Accept, Deny or Drop the request.
Device Group List	Associate the profile with pre-configured Device Groups. Add New Device Group to add a new device group. Add to add a device group from this drop-down list. Remove, View Details, Modify to remove, view the details of, or modify the selected enforcement profile, respectively. Note: This feature does not work with RADIUS CoA type Enforcement Profiles.

The remaining Enforcement Profile tabs vary in content, depending on the *Template Type* (auto-specified in the *Type* field when a *Template* has been selected):

- “RADIUS Enforcement Profiles” (page 212)
- “RADIUS CoA Enforcement Profiles” (page 214)
- “SNMP Enforcement Profiles” (page 214)
- “TACACS+ Enforcement Profiles” (page 215)
- “Application Enforcement Profiles” (page 218)
- “CLI Enforcement Profile” (page 219)
- “Agent Enforcement Profile” (page 219)

RADIUS Enforcement Profiles

RADIUS Enforcement Profiles contain name/value pairings of attributes from the RADIUS dictionaries; in this editing context, Policy Manager displays only those attributes marked in the dictionary with the *OUT* or *INOUT* qualifier.

Figure 15-4 RADIUS Enforcement Profile (Attributes Tab)

This figure illustrates rules for five sample profiles:

A—VLAN Enforcement; **B**— Filter ID Based Enforcement ;

C—Cisco Downloadable ACL Enforcement; **D**—Cisco Web Authentication Enforcement;

The screenshot displays the 'Attributes' tab of a RADIUS Enforcement Profile configuration interface. It shows five sample profiles, each with a table of attributes and values. The profiles are labeled A, B, C, and D on the right side of the interface.

Profile A: VLAN Enforcement

Type	Name	Value
Radius:IETF	Session-Timeout	= 3600
Radius:IETF	Termination-Action	= RADIUS-Request (1)
Radius:IETF	Tunnel-Type	= VLAN (13)
Radius:IETF	Tunnel-Medium-Type	= IEEE-802 (6)
Radius:IETF	Tunnel-Private-Group-Id	= Enter VLAN
6. Click to add...		

Profile B: Filter ID Based Enforcement

Type	Name	Value
Radius:IETF	Filter-Id	= Enter Filter Name
2. Click to add...		

Profile C: Cisco Downloadable ACL Enforcement

Type	Name	Value
Radius:Cisco	Cisco-IP-Downloadable-	= permit ip any any
2. Click to add...		

Profile D: Cisco Web Authentication Enforcement

Type	Name	Value
Radius:Cisco	Cisco-AVPair	= priv-lvl=15
Radius:Cisco	Cisco-AVPair	= proxyacl# 10=permit ip any any
3. Click to add...		

At the bottom of the interface, there are navigation buttons: "Back to Enforcement Profiles", "Next >", "Save", and "Cancel".

Figure 15-5 RADIUS Enforcement Profile (Attributes Tab) - Generic RADIUS Enforcement Profile

Type	Name	Value
1. Radius:IETF	User-Name	={}
Radius:IETF	User-Name	%{Authorization:Avenda AD:countryCode}
Radius:Clavister	Service-Type	%{Authorization:Avenda AD:department}
Radius:Cisco-VPN3000	Framed-Protocol	%{Authorization:Avenda AD:distinguishedName}
Radius:Acc	Framed-IP-Address	%{Authorization:Avenda AD:memberOf}
Radius:Tropos	Framed-IP-Netmask	%{Authorization:Avenda AD:msNPAllowDialin}
Radius:Cisco	Framed-Routing	%{Authorization:Avenda AD:name}
Radius:ERX	Filter-Id	%{Authorization:Avenda AD:title}
Radius:CableLabs	Framed-MTU	%{Authorization:Test RSA Token Server:IETF.Class}
Radius:Mikrotik	Framed-Compression	%{Authorization:Test RSA Token Server:IETF.Service-Type}
Radius:Cosine	Login-IP-Host	
Radius:Radius	Login-Service	
Radius:Cisco-BBSM	Login-TCP-Port	
Radius:BinTec	Reply-Message	
Radius:Ascend	Callback-Number	
Radius:Roaring-Penguin	Callback-Id	
More choices	More choices	
2. Click to add...		

Back to Enforcement Profiles Next > Save Cancel

Table 15-2 RADIUS Enforcement Profile (Attributes Tab)

Enforcement Profile Template	Description
A —VLAN Enforcement	Enforcement profile template to set IETF RADIUS standard VLAN attributes.
B —Filter ID Based Enforcement	Enforcement profile template to set IETF RADIUS standard filter ID attribute.
C —Cisco Downloadable ACL Enforcement	Enforcement profile template for Cisco IOS downloadable ACLs.
D —Cisco Web Authentication Enforcement	Enforcement profile template to set Cisco Web Authentication ACLs.

Enforcement Profile Template	Description
E—(Generic) RADIUS-Based Authentication	<p>Type is any RADIUS vendor dictionary that is pre-packaged with Policy Manager, or imported by the Administrator. This field is prepopulated with the dictionary names.</p> <p>Name is the name of the attribute from the dictionary selected in the Type field. The attribute names are prepopulated from the dictionary.</p> <p>Value is the value of the attribute. If the value has prepopulated values is the dictionary, these appear in a dropdown list. Otherwise, you can enter freeform text.</p> <p>An Enforcement Profile can also contain dynamic values (as received in the request or authentication handshake, or as derived by the Policy Manager policy system).</p> <p>For example, to set the name of the VLAN to the name of the role, enter <code>%{Tips:Role}</code> as the value for <code>RADIUS:IETF:Tunnel-Private-Group-Id</code>. These dynamic values must be entered in the following format, without any spaces: <code>%{namespace:attribute-name}</code>.</p> <p>For convenience, the value field also has a drop down that contains all the authorization attributes. You can use these directly to assign dynamic values in the profile. Refer to figure above.</p>

RADIUS CoA Enforcement Profiles

The RADIUS CoA Tab contains a template type and the actions associated with that template type.

The RADIUS CoA Enforcement Profile tab loads the CoA template attributes supported a specific template.

Table 15-3 RADIUS CoA Enforcement Profile (Attributes Tab)

Interface	Description
Select RADIUS CoA Template	<p>The supported template types are:</p> <p>Cisco - Disable-Host-Port, Cisco - Bounce-Host-Port, Cisco - Reauthenticate-Session, HP - Change-VLAN, HP - Generic-CoA</p>
Attributes	<p>The RADIUS (standard and vendor-specific) shown here are base on the CoA Template selected from the drop down. Fill in values for all entries marked “Enter value here”. The other pre-filled attributes must not be deleted, since the device requires these to be present.</p>

SNMP Enforcement Profiles

The SNMP Tab contains a VLAN identifier and timeout.

Figure 15-6 SNMP Enforcement Profile (SNMP Tab)

Attribute Name	Attribute Value
1. VLAN ID	= 150
2. Session Timeout (in seconds)	= 3600
3. VLAN ID	
4. Session Timeout (in seconds)	
Reset Connection (after the settings are applied)	

Back to Enforcement Profiles Next > Save Cancel

The SNMP Enforcement Profile **SNMP** tab loads the SNMP dictionary attributes supported by Policy Manager.

Table 15-4 SNMP Enforcement Profile (SNMP Tab)

Interface	Description
VLAN Id	VLAN ID to be sent to the device
Session Timeout	Session timeout in seconds.
Reset Connection (after the settings are applied)	Reset Connection is a primitive that does different actions based on the capabilities of the network device. For devices that support the 802.1X re-authentication, Policy Manager triggers a re-authentication; in other cases, it bounces the port.

TACACS+ Enforcement Profiles

TACACS+ Enforcement Profiles contain attribute-value pairs and other permissions related to administrative access to a network device. The built-in TACACS+ enforcement profiles can also be used to log into the Policy Manager UI. TACACS+ enforcement profiles use ARAP, Policy Manager:HTTP, PIX Shell, PPP:IP, PPP:IPX, PPP:LCP, Wireless-WCS:HTTP, CiscoWLC:Common and Shell namespaces to define service attributes.

Figure 15-7 TACACS+ Enforcement Profiles (Services Tab)

Configuration » Enforcement » Profiles » Add Enforcement Profile

Enforcement Profiles

Profile Services Commands Summary

Privilege Level: 15 (Privileged)

Selected Services:

Shell

Remove

--Select--

Add

--Select--

PIX Shell

PPP:IP

PPP:IPX

PPP:LCP

ARAP

eTIPS:HTTP

Service Attributes

Type	Name	=	Value	
1. Shell	priv_lvl	=	15	
2. Shell	timeout	=	180	
3. <input type="text"/>				
4. <input type="text"/>				

Shell

PIX Shell

PPP:IP

PPP:IPX

PPP:LCP

ARAP

eTIPS:HTTP

Back to Enforcement Profiles

Next > Save Cancel

Table 15-5 TACACS+ Enforcement Profiles (Services Tab)

Container	Description
Privilege Level	Enter a value, from 0 to 15. Note: Refer to your network device documentation for definitions of the different privilege levels.
Selected Services	<i>To add supported services, click Add.</i> <i>To remove a service, select it and click Remove.</i> Policy Manager supports <i>ARAP</i> , <i>eTIPS:HTTP</i> (Policy Manager administrative interface login), <i>PIX shell</i> , <i>Shell</i> , <i>PPP:IP</i> , <i>PPP:IPX</i> , <i>Wireless-WCS:HTTP</i> , <i>CiscoWLC:Common</i> and <i>PPP:LCP</i> .
Service Attributes	Once the services have been selected, you can select the attributes to send for those services. Some services have pre-defined attributes (which are automatically populated by Policy Manager in a drop down list in the Name field). You can also add custom attributes in the Name field. Add service attributes corresponding to the services selected in Selected Services . Policy Manager ships configured with attributes for some of the listed services.

Selections in the **Commands** tab configure commands and arguments allowed/disallowed for the selected **Service Type**.

Figure 15-8 TACACS+ Enforcement Profiles (Commands Tab)

The screenshot displays the 'Commands' tab of the TACACS+ Enforcement Profiles configuration. At the top, there are tabs for 'Summary', 'Profile', 'Services', and 'Commands'. Below the tabs, the 'Service Type' is set to 'Shell' (radio button selected), and 'Unmatched Commands' is checked with the label 'Enable to permit unmatched commands'. The main section is titled 'Commands' and contains a table with the following data:

Command	Arguments	Permit Action	Unmatched Arguments
1. show	vlan	Deny	Permit
2. show	interface	Deny	Deny

An overlay window titled 'Configure Tacacs Command Authorization' is shown. It has a 'Shell Command' field containing 'interface'. Below it is a table for 'Command Arguments' and 'Action':

Command Arguments	Action
1. vlan	Deny
2. Click to add...	

At the bottom of the overlay, 'Unmatched Arguments' is set to 'Permit' (radio button selected). 'Save' and 'Cancel' buttons are at the bottom right of the overlay. The main interface has a 'Back to Enforcement Profiles' link and 'Copy', 'Save', and 'Cancel' buttons at the bottom.

Table 15-6 Commands Tab (TACACS+ Enforcement Profiles)

Container	Description
Service Type	Select <i>Shell</i> or <i>PIX shell</i> radio button. Subsequent selections in this tab configure commands and arguments allowed/disallowed for this selection.
Unmatched Commands	Enable to permit commands that are not explicitly entered in the Commands field.

Container	Description
Commands	<p>Contains a list of the commands recognized for the specified Service Type:</p> <p><i>To add a command</i>, click Add. In the Configure Tacacs Command Authorization popup, enter values for:</p> <ul style="list-style-type: none"> • Command. A string for the command. This is followed by one or more command argument rows. <ul style="list-style-type: none"> • Command Arguments. The arguments for the command. • Action. Click on Enable to permit checkbox to permit use of this command argument. If this box is unchecked the column shows Deny and the command argument is not allowed. • Click Trashcan to delete the command argument. • Unmatched Arguments. Select Permit radio button to permit this command even if Policy Manager receives arguments for the command that it does not recognize. Select Deny radio button to deny the command if Policy Manager receives unrecognized arguments. <p><i>To save and exit</i>, click outside the row you are editing.</p> <p><i>To delete a command</i>, click the Trashcan icon for that row.</p>

Application Enforcement Profiles

Application Enforcement Profiles contain attribute-value pairs and other permissions related to authorization of users of Aruba Applications - GuestConnect and Insight. There are three different types of application enforcement profile templates that can be selected:

- Aruba GuestConnect Enforcement - Attributes for users of GuestConnect application.
- Aruba Insight Enforcement - Attributes for users of Insight application.
- Generic Application Enforcement - Attributes for users of any generic application.

Figure 15-9 Application Enforcement Profiles (Attributes Tab)

Configuration » Enforcement » Profiles » Add Enforcement Profile

Enforcement Profiles

Profile **Attributes** Summary

Attribute Name	Attribute Value	
1. Privilege-Level	= Sponsor	🗑
2. Sponsor-Profile-Name	= Enter Profile Name	🗑
3. <input type="text"/>	=	📁 🗑
4. <input type="text"/>		

Privilege-Level
 Sponsor-Profile-Name

Table 15-7 Application Enforcement Profiles (Attributes Tab)

Container	Description
Privilege-Level	Enter a predefined value: Admin, Sponsor, Helpdesk; or enter an application-specific custom value. Note: Sponsor is only valid for the GuestConnect application
Sponsor-Profile-Name	Valid only for GuestConnect application. This is the (case-sensitive) name of the sponsor profile defined in the GuestConnect application.

Besides the above attribute names custom attributes can be entered for other types of applications.

CLI Enforcement Profile

CLI Enforcement Profiles contain attribute-value pairs related to authorization of users/devices via CLI commands executed on a target network device.

Figure 15-10 CLI Enforcement Profile (Attributes Tab)

Configuration » Enforcement » Profiles » Add Enforcement Profile

Enforcement Profiles

Profile Attributes Summary

Attribute Name	Attribute Value	
1. Target Device	= %{Connection:NAD-IP-Address}	
2. Command	= Enter Command	
3. Click to add...		

Table 15-8 CLI Enforcement Profiles (Attributes Tab)

Container	Description
Target Device	Enter the device on which the CLI commands are executed. Typically, this is the edge device on which the user/endpoint connected (%{Connection:NAD-IP-Address}).
Command	Multiple commands (separated by a new line) that are executed on the target device.

Agent Enforcement Profile

Agent Enforcement Profiles contain attribute-value pairs related to enforcement actions sent to Aruba OnGuard Agent.

Figure 15-11 Agent Enforcement Profile (Attributes Tab)

Configuration » Enforcement » Profiles » Add Enforcement Profile

Enforcement Profiles

Profile Attributes Summary

Attribute Name	Attribute Value	
1. Bounce Client	= false	
2. Message	= Enter message here	
3. Click to add...		

Table 15-9 Agent Enforcement Profiles (Attributes Tab)

Container	Description
Bounce Client	If checked, the endpoint is bounced by the OnGuard agent (this feature is only available with the persistent agent)
Message	A custom message to send to the endpoint.
Session Timeout (in seconds)	Timeout after which the OnGuard agent forces a reauthentication on the endpoint.

Configuring Enforcement Policies

One and only one Enforcement Policy can be associated with each Service.

From the **Services** page (**Configuration > Service**), you can configure enforcement policy for a new service (as part of the flow of the **Add Service** wizard), or modify an existing enforcement policy (**Configuration > Enforcement > Enforcement Policies**, then click on its name in the **Enforcement Policies** listing page).

Figure 15-12 Enforcement Policies Listing Page

Configuration » Enforcement » Policies			
Enforcement Policies			
Add Enforcement Policy Import Enforcement Policies Export Enforcement Policies			
Filter:	Name	contains	Go Clear Filter
Showing	10	records	
#	Name ▲	Type	Description
1.	<input type="checkbox"/> AdminAccessPolicy	RADIUS	Cisco Wireless Controller Admin Access Policy
2.	<input type="checkbox"/> Avenda_Wireless_Access_Policy	RADIUS	Enforcement policy for Avenda wireless access
3.	<input type="checkbox"/> Device Command Authorization Policy	TACACS	Policy for device command authorization
4.	<input type="checkbox"/> Employee Enforcement Policy	RADIUS	Enforcement policies for corporate employees
5.	<input type="checkbox"/> Enterprise Enforcement Policy	RADIUS	Enforcement policies for local and remote employees
6.	<input type="checkbox"/> Entertainment-Xirus Enf. Policy	RADIUS	Entertainment Partners Demo Enforcement Policy
7.	<input type="checkbox"/> eTIPS_Admin_Network_Login_Policy	TACACS	Enforcement policy controlling access to eTIPS Admin
8.	<input type="checkbox"/> Guest_Access_policy	RADIUS	Guest Enforcement Policy, Limited Access
9.	<input type="checkbox"/> Handheld_Avenda_Wireless_Access_Policy	RADIUS	Enforcement policy for Avenda handheld wireless access
10.	<input type="checkbox"/> Handheld Enforcement	RADIUS	Enforcement for handheld devices
Showing 1-10 of 18			
Copy Export Delete			

When you click **Add Enforcement Policy**, Policy Manager displays the **Add Enforcement Policy** wizard page:

Figure 15-13 Add Enforcement Policy (Enforcement Tab)

Configuration » Enforcement » Policies » Add

Enforcement Policies

Enforcement Rules Summary

Name: Employee Access Enforcement

Description: Enforcement policy for employee access

Type: ☒ RADIUS ☐ TACACS+ ☐ WEBAUTH (SNMP/CLI) ☐ Application

Default Profile: -Select- [View Details](#) [Modify](#) [Add new Enforcement Profile](#)

[Back to Enforcement Policies](#) [Next >](#) [Save](#) [Cancel](#)

Table 15-10 Add Enforcement Policy (Enforcement Tab)

Parameter	Description
Name/Description	Freeform label and description.
Type	Select: <i>RADIUS</i> , <i>TACACS+</i> , <i>WebAuth (SNMP/CLI)</i> or <i>Application</i> . Based on this selection, the Default Profile list shows the right type of enforcement profiles in the dropdown list (See Below). Note: Web-based Authentication or WebAuth (HTTPS) is the mechanism used by authentications performed via a browser, and authentications performed via Aruba OnGuard. Both SNMP and CLI (SSH/Telnet) based Enforcement Profiles can be sent to the network device based on the type of device and the use case.
Default Profile	<p>An Enforcement Policy applies Conditions (roles, health and time attributes) against specific values associated with those attributes to determine the Enforcement Profile. If none of the rules matches, Policy Manager applies the Default Profile.</p> <p>Click Add new Enforcement Profile to add a new profile (This is integrated into the flow. Once you are done creating the profile, Policy Manager brings you back to the current page/tab.)</p>

In the **Rules** tab, click **New Rule** to display the **Rules Editor**:

Figure 15-14 Add Enforcement Policy (Rules Tab)

Enforcement Rules Summary

Rules Evaluation Algorithm: ☐ Select first match ☒ Select all matches

Enforcement Policy Rules:

	Conditions	Actions
1.	(Tips:Role MATCHES_ANY Role_Engineer Senior_Mgmt)	EMPLOYEE_VLAN
2.	(Tips:Role EQUALS eTIPS_Guest) AND (Tips:Posture EQUALS HEALTHY (0))	INTERNET_VLAN

[Add Rule](#) [Move Up](#) [Move Down](#) [Edit Rule](#) [Remove Rule](#)

[Back to Enforcement Policies](#) [Next >](#) [Save](#) [Cancel](#)

Figure 15-15 Add Enforcement Policy (Rules Editor)

The screenshot shows the 'Rules Editor' window. It has two main sections: 'Conditions' and 'Enforcement Profiles'.

Conditions Section:

Match ALL of the following conditions:

	Type	Name	Operator	Value	
1.	Tips	Posture	EQUALS	HEALTHY (0)	[Icon] [Icon]
2.	Tips	Role	MATCHES_ANY	Remote Worker role_engineer testqa	[Icon] [Icon]
3.	[Dropdown]				[Icon] [Icon]
4.	Date				

Enforcement Profiles Section:

Profile Names:

EMPLOYEE_VLAN
Remote Employee ACL

Move Up
Move Down
Remove

~Select~ [Add]

[Save] [Cancel]

Table 15-11 Add Enforcement Policy (Rules Tab)

Field	Description
Add/Edit Rule	Bring up the rules editor to add/edit a rule.
Move Up/Down	Reorder the rules in the enforcement policy.
Remove Rule	Remove a rule.

Table 15-12 Add Enforcement Policy (Rules Editor)

Field	Description
Conditions/Enforcement Profiles	<p>Select conditions for this rule. For each condition, select a matching action (Enforcement Profile).</p> <p>Note: A condition in an Enforcement Policy rule can contain attributes from the following namespaces: <i>Tips:Role</i>, <i>Tips:Posture</i>, and <i>Date</i>.</p> <p>Note: The value field for the <i>Tips:Role</i> attribute can be a role defined in Policy Manager, or a role fetched from the authorization source. (Refer to “Adding and Modifying Authentication Sources” (page 119) to see how Enable as Role can be turned on for a fetched attribute). Role names fetched from the authorization source can be entered freeform in value field.</p> <p>To commit the rule, click Save.</p>
Enforcement Profiles	<p>If the rule conditions match, attributes from the selected enforcement profiles are sent to Network Access Device. If a rule matches and there are multiple enforcement profiles, the enforcement profile disambiguation rules apply.</p>

Chapter 16: Network Access Devices

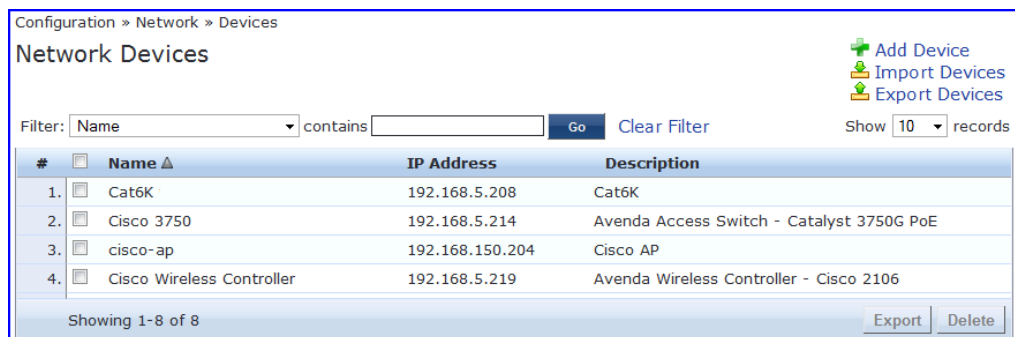
A *Policy Manager Device* represents a *Network Access Device* (NAD) that sends network access requests to Policy Manager, using the supported RADIUS, TACACS+, or SNMP protocol.

Adding and Modifying Devices

To connect with Policy Manager using the supported protocols, a NAD must belong to the global list of devices in the Policy Manager database.

Policy Manager lists all configured devices in the **Devices** page: **Configuration > Network > Devices**. From this interface:

Figure 16-1 Network Devices Page



Configuration » Network » Devices

Network Devices

Filter: Name contains Go Clear Filter Show 10 records

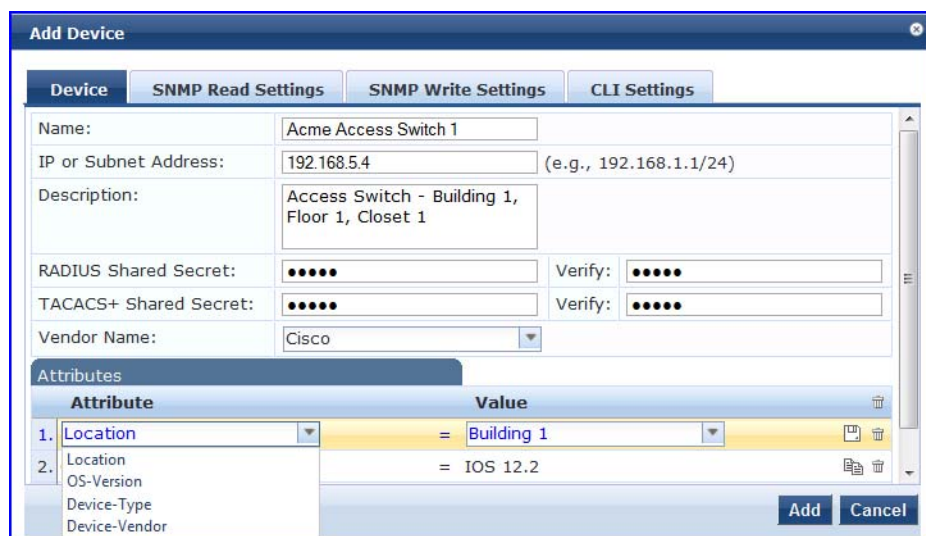
#	Name	IP Address	Description
1.	Cat6K	192.168.5.208	Cat6K
2.	Cisco 3750	192.168.5.214	Avenda Access Switch - Catalyst 3750G PoE
3.	cisco-ap	192.168.150.204	Cisco AP
4.	Cisco Wireless Controller	192.168.5.219	Avenda Wireless Controller - Cisco 2106

Showing 1-8 of 8

Export Delete

- To add a device, click **Add Device**, then complete the fields in the **Add Device** popup. In the **Device** tab,

Figure 16-2 Device Tab



Add Device

Device SNMP Read Settings SNMP Write Settings CLI Settings

Name: Acme Access Switch 1

IP or Subnet Address: 192.168.5.4 (e.g., 192.168.1.1/24)

Description: Access Switch - Building 1, Floor 1, Closet 1

RADIUS Shared Secret: Verify:

TACACS+ Shared Secret: Verify:

Vendor Name: Cisco

Attributes

Attribute	Value
1. Location	= Building 1
2. Location OS-Version	= IOS 12.2

Device-Type Device-Vendor

Add Cancel

Table 16-1 Device Tab

Container	Description
Name/ Description	Specify identity of the device.
IP Address or Subnet	Specify the IP address or the subnet (E.g., 192.168.5.0/24) of the device.
RADIUS/TACACS+ Shared Secret	Enter and confirm a Shared Secret for each of the two supported request protocols.
Vendor	<p>Optionally, specify the dictionary to be loaded for this device.</p> <p>Note: RADIUS:IETF, the dictionary containing standard set of RADIUS attributes, is always loaded.</p> <p>Note: When you specify a vendor here, the RADIUS dictionary associated with this vendor is automatically enabled.</p>
Enable RADIUS CoA RADIUS CoA Port	<p>Enable RADIUS Change of Authorization (RFC 3576/5176) for this device.</p> <p>Set the UDP port on the device to send CoA actions. Default value is 3799.</p>
Attributes	<p>Add custom attributes for this device. Click on the “Click to add...” row to add custom attributes. By default, four custom attributes appear in the Attribute dropdown: Location, OS-Version, Device-Type, Device-Vendor. You can enter any name in the attribute field. All attributes are of String datatype. The value field can also be populated with any string. Each time you enter a new custom attribute, it is available for selection in Attribute dropdown for all devices.</p> <p>Note: All attributes entered for a device are available in the role mapping rules editor under the <i>Device</i> namespace.</p>
Add/Cancel	Click Add to commit or Cancel to dismiss the popup.

In the **SNMP Read Settings** and **SNMP Write Settings** tabs,

Figure 16-3 SNMP Read/Write Settings Tabs

The screenshot shows a web interface titled "Add Device". It has four tabs: "Device", "SNMP Read Settings", "SNMP Write Settings", and "CLI Settings". The "SNMP Read Settings" tab is selected. It contains the following fields:

- Allow SNMP Read:** A checkbox labeled "Enable eTIPS to perform SNMP read operations".
- SNMP Read Setting:** A dropdown menu currently showing "SNMP v2 with community strings".
- Community String:** A text input field.
- Verify:** A text input field.

Below these fields, the "SNMP Write Settings" tab is partially visible, showing:

- Allow SNMP Write:** A checkbox labeled "Enable eTIPS to perform SNMP write operations".
- Default VLAN:** A text input field with a note "(VLAN setting for port when SNMP enforced session expires)".
- SNMP Write Setting:** A dropdown menu currently showing "SNMP v2 with community strings".
- Community String:** A text input field.
- Verify:** A text input field.

At the bottom right of the window are "Add" and "Cancel" buttons.

Figure 16-4 SNMP Read/Write Settings Tabs - SNMP v3 Details

This screenshot shows the "SNMP v3 Details" section. The "SNMP Read Setting" dropdown is set to "SNMP v3 with Authentication using SHA and with Privacy". Below this are the following fields:

- Username:** A text input field.
- Authentication Key:** A text input field.
- Verify:** A text input field.
- Privacy Key:** A text input field.
- Verify:** A text input field.

Table 16-2 SNMP Read/Write Settings Tabs

Container	Description
Allow SNMP Read/Write	Toggle to enable/disable SNMP Read/Write.
Default VLAN (SNMP Write only)	VLAN port setting after SNMP-enforced session expires.
SNMP Read/Write Setting	SNMP settings for the device.
Community String (SNMP v2 only)	
Username (SNMP v3 only)	Admin user name to use for SNMP read/write operations
Authentication Key (SNMP v3 only)	SNMP v3 with authentication option (SHA & MD5)
Privacy Key (SNMP v3 only)	SNMP v3 with privacy option
Add/Cancel	Click Add to commit or Cancel to dismiss the popup.

In the **CLI Settings** tab,

Figure 16-5 CLI Settings Tab
Table 16-3 CLI Settings Tab

Container	Description
Allow CLI Access	Toggle to enable/disable CLI access.
Access Type	Select SSH or Telnet. Policy Manager uses this access method to log into the device CLI.
Port	SSH or Telnet TCP port number.
Username/Password	Credentials to log into the CLI.
Username Prompt Regex (Telnet Only)	Regular expression for the username prompt. Policy Manager looks for this pattern to recognize the telnet username prompt.
Password Prompt Regex (Telnet Only)	Regular expression for the password prompt. Policy Manager looks for this pattern to recognize the telnet password prompt.
Command Prompt Regex (Telnet Only)	Regular expression for the command line prompt. Policy Manager looks for this pattern to recognize the telnet command line prompt.
Add/Cancel	Click Add to commit or Cancel to dismiss the popup.

- *To import a Device*, click **Import Devices**; in the **Import from File** popup, browse to select a file, then click **Import**. If you entered a secret key to encrypt the exported file, enter the same secret key to import the device back.
- *To export all Devices from the configuration*, click **Export Devices**; in the **Export to File** popup, specify a file path, then click **Export**. In the Export to File popup, you can choose to encrypt the exported data with a key. This protects data such as shared secret from being visible in the exported file. To import it back, you specify the same key that you exported with.

- To export a single Device from the configuration, select it (checkbox on left), then click **Export**; in the **Save As** popup, specify a file path, then click **Export**.
- To delete a single Device from the configuration, select it (checkbox on left), then click **Delete**; commit the deletion by selecting *Yes*, dismiss the popup by selecting *No*.

Adding and Modifying Device Groups

Policy Manager groups devices into *Device Groups*, which function as a component in Service and Role Mapping rules. Device Groups can also be associated with Enforcement Profiles; Policy Manager sends the attributes associated with these profiles only if the request originated from a device belonging to the device groups.

Administrators configure Device Groups at the global level. They can contain the members of the IP address of a specified subnet (or regular expression-based variation), or devices previously configured in the Policy Manager database.

Policy Manager lists all configured device groups in the **Device Groups** page: **Configuration > Network > Device Groups**. From this interface:

Figure 16-6 Device Groups Page

Configuration » Network » Device Groups

Network Device Groups

Filter: Name contains [] Go Clear Filter Show 10 records

#	<input type="checkbox"/>	Name ▲	Format	Description
1.	<input type="checkbox"/>	Bangalore Devices	Subnet	Devices in Bangalore
2.	<input type="checkbox"/>	Remote Bangalore	Subnet	Remote Bangalore Devices
3.	<input type="checkbox"/>	Remote San Jose	Subnet	San Jose VPN Devices
4.	<input type="checkbox"/>	San Jose Devices	Subnet	San Jose Switches

Showing 1-4 of 4

Export Delete

[Add Device Group](#)
[Import Device Groups](#)
[Export Device Groups](#)

- To add a Device Group, click **Add Device Group**. Complete the fields in the **Add New Device Group** popup:

Figure 16-7 Add New Device Group Popup

The figure shows three overlapping screenshots of the 'Add New Device Group' popup window. Each window has a title bar with a close button. The first window (top) shows the 'Subnet' format selected, with fields for Name ('Test Device Group'), Description ('This is a test device group'), and Subnet (with a hint '(e.g., 192.168.1.1/24)'). The second window (middle) shows the 'Regular Expression' format selected, with fields for Name ('Test Device Group 2'), Description ('This is a test device group 2'), and Regular Expression (with a hint '(e.g., ^192([0-9]*){3}\$)'). The third window (bottom) shows the 'List' format selected, with fields for Name ('Test Device Group 2'), Description ('This is a test device group 2'), and a List section containing 'Available Devices' (a list of IP addresses: 192.168.150.204, 192.168.150.60, 192.168.150.80, 192.168.5.12, 192.168.5.208, 192.168.5.214) and 'Selected Devices' (an empty list). There are 'Filter' buttons for both lists and '>>' and '<<' buttons between them. At the bottom right are 'Save' and 'Cancel' buttons.

Table 16-4 Add New Device Group Popup

Container	Description
Name/ Description/ Format	Specify identity of the device.
Subnet	Enter a subnet consisting of network address and the network suffix (CIDR notation); for example, 192.168.5.0/24
Regular Expression	Specify a regular expression that represents all IPv4 addresses matching that expression; for example, ^192([0-9]*){3}\$
List: Available/Selected Devices	Use the widgets to move device identifiers between Available and Selected. Click Filter to filter the list based on the text in the associated text box.
Save/Cancel	Click Save to commit or Cancel to dismiss the popup.

- Note: For SNMP enforcement on the network device, one or more of the following traps have to be configured on the device: Link Up trap, Link Down trap, MAC Notification trap. In addition, one or more of the following SNMP MIBs must be supported by the device:
 - RFC-1213 MIB, IF-MIB, BRIDGE-MIB, ENTITY-MIB, Q-BRIDGE-MIB, CISCO-VLAN-MEMBERSHIP-MIB, CISCO-STACK-MIB, CISCO-MAC-NOTIFICATION-MIB

These traps and MIBs enable Policy Manager to correlate the MAC address, IP address and switch port and switch information.

- *To import a Device Group*, click **Import Device Groups**; in the **Import from File** popup, browse to select a file, then click **Import**.
- *To export all Device Groups from the configuration*, click **Export Devices**; in the **Export to File** popup, specify a file path, then click **Export**.
- *To export a single Device Group from the configuration*, select it (checkbox on left), then click **Export**; in the **Save As** popup, specify a file path, then click **Export**.
- *To delete a single Device Group from the configuration*, select it (checkbox on left), then click **Delete**; commit the deletion by selecting *Yes*, dismiss the popup by selecting *No*.

Adding and Modifying Proxy Targets

In Policy Manager, a proxy target represents a RADIUS server (Policy Manager or third party) that is the target of a proxied RADIUS request. For example, when a branch office employee visits a main office and logs into the network, Policy Manager assigns the request to the first Service in priority order that contains a Service Rule for RADIUS proxy Services and appending the *domain* to the Username.

Proxy targets are configured at a global level. They can then be used in configuring RADIUS proxy Services. (Refer to [Policy Manager Service Types](#)).

Policy Manager lists all configured proxy servers in the **Proxy Servers** page: **Configuration > Network > Proxy Servers**

Figure 16-8 Proxy Targets Page

Configuration » Network » Proxy Targets

Proxy Targets

Filter: Name contains Go Clear Filter Show 10 records

#	Name	Hostname	Description
1.	BRANCH OFFICE PROXY	branch1proxy.avendasys.com	

Showing 1-1 of 1

Export Delete

- To add a Proxy Target, click **Add Proxy Target**. Complete the fields in the **Add Proxy Target** popup. You can also add a new proxy target from the **Services** page (**Configuration > Service** (as part of the follow of the **Add Service** wizard for a RADIUS Proxy Service Type).

Figure 16-9 Add Proxy Target Popup

Add Proxy Target

Name: SJ Branch Office Proxy

Description: SJ branch office proxy

Hostname: sjproxy.acme.com

Shared Secret:

Verify Shared Secret:

RADIUS Authentication Port: 1812 (Default is 1812)

RADIUS Accounting Port: 1813 (Default is 1813)

Save Cancel

Table 16-5 Add Proxy Target Popup

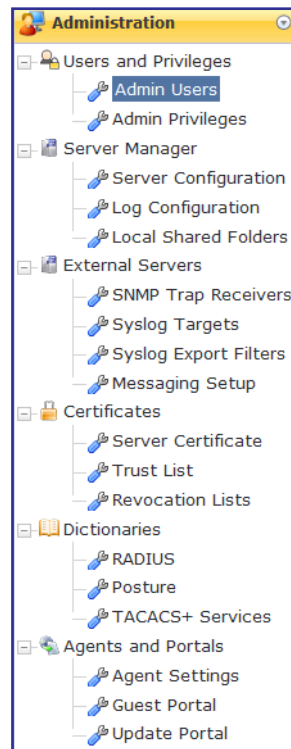
Container	Description
Name/Description	Freeform label and description.
Hostname/Shared Secret	RADIUS Hostname and Shared Secret. Use the same secret that you entered on the proxy target (refer to your RADIUS server configuration).
RADIUS Authentication Port	Enter the UDP port to send the RADIUS request. Default value for this port is 1812.
RADIUS Accounting Port	Enter the UDP port to send the RADIUS accounting request. Default value for this port is 1813.

- To import a Proxy Target, click **Import Proxy Targets**; in the **Import from File** popup, browse to select a file, then click **Import**.
- To export all Proxy Targets from the configuration, click **Export Proxy Targets**; in the **Export to File** popup, specify a file path, then click **Export**.

- *To export a single Proxy Target from the configuration, select it (checkbox on left), then click **Export**; in the **Save As** popup, specify a file path, then click **Export**.*
- *To delete a single Proxy Target from the configuration, select it (checkbox on left), then click **Delete**; commit the deletion by selecting *Yes*, dismiss the popup by selecting *No*.*

Chapter 17: Administration

All administrative activities including server configuration, log management, certificate and dictionary maintenance, portal definitions, and administrator user account maintenance are done from the Administration menus. The Policy Manager Administration menu provides the following interfaces for configuration:



- “Admin Users” (page 233)
- “Admin Privileges” (page 236)
- “Server Configuration” (page 237)
- “Log Configuration” (page 258)
- “Local Shared Folders” (page 260)
- “Snmp Trap Receivers” (page 261)
- “Syslog Targets” (page 264)
- “Syslog Export Filters” (page 266)
- “Messaging Setup” (page 269)
- “Server Certificate” (page 271)
- “Certificate Trust List” (page 276)
- “Revocation Lists” (page 277)
- “RADIUS Dictionaries” (page 279)
- “Posture Dictionaries” (page 280)
- “TACACS+ Services” (page 281)
- “Agent Settings” (page 283)
- “Guest Portal” (page 284)
- “Update Portal” (page 288)

Admin Users

The Policy Manager Admin Users menu t **Administration > Users and Privileges > Admin Users** provides the following interfaces for configuration:

- “Add User” (page 234)
- “Import Users” (page 235)
- “Export Users” (page 235)
- “Export” (page 235)

Figure 17-1 Admin Users

Administration » Users and Privileges » Admin Users

Admin Users

[Add User](#)
[Import Users](#)
[Export Users](#)

Filter: contains Show records

#	<input type="checkbox"/>	User ID ▲	Name	Privilege Level
1.	<input type="checkbox"/>	admin	Super Admin	Super Administrator
2.	<input type="checkbox"/>	fred	Fred Garcia	Help Desk
3.	<input type="checkbox"/>	ram	Ram Nath	Network Administrator
4.	<input type="checkbox"/>	stan	Stan Smith	Super Administrator

Showing 1-4 of 4

Table 17-1 Admin Users

Container	Description
Add User	Open Add User popup.
Import Users	Open Import Users popup.
Export Users	Export all users to an XML file.
Export	Export a selected to an XML file.
Delete	Delete a selected User.

Add User

Administration > Users and Privileges > Admin Users > Add (Admin) User

Figure 17-2 Add Admin User

Add Admin User

User ID:

Name:

Password:

Verify Password:

Privilege Level:

- Super Administrator
- Super Administrator
- Network Administrator
- Help Desk
- Receptionist

Table 17-2 Add Admin User

Container	Description
User ID	Specify identity and privilege level for a new administrator.
Name	
Password	
Verify Password	

Container	Description
Privilege Level	Select Privilege Level: <ul style="list-style-type: none"> • Help Desk • Super Administrator • Network Administrator • Receptionist • or any other custom privilege level
Add/Cancel	Add or dismiss changes.

Import Users

Administration > Users and Privileges > Admin Users > Import (Admin) Users (link)

Figure 17-3 Import (Admin) Users

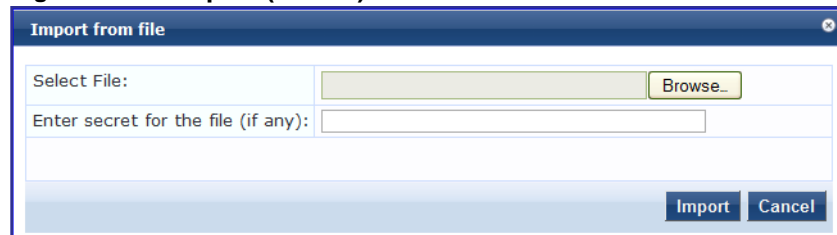


Table 17-3 Import (Admin) Users

Container	Description
Select file	Browse to select name of admin user import file.
Enter secret key for file (if any)	Enter the secret key used (while exporting) to protect the file.
Import/Cancel	Commit or dismiss import.

Export Users

Administration > Users and Privileges > Admin Users > Export Users (link).

The **Export (Admin) Users** link exports all (admin) users. Click **Export**. Your browser will display its normal **Save As** dialog, in which to enter the name of the XML file to contain the export.

Export

Administration > Users and Privileges > Admin Users > Export (button).

To export just one user, select it (checkbox at left) and click Export. Your browser will display its normal **Save As** dialog, in which to enter the name of the XML file to contain the export.

Admin Privileges

To display available Admin Privileges, **Administration > Users and Privileges > Admin Privileges**.

Figure 17-4 Admin Privileges

#	Name ▲	Description
1.	Help Desk	A help desk person logs in to troubleshoot problems reported by end users
2.	Network Administrator	A network administrator is allowed to configure all the policies in the system
3.	Receptionist	A receptionist is only allowed to configure guest users
4.	Super Administrator	A super administrator is allowed read/write access to all configuration elements

Showing 1-4 of 4

Import Admin Privileges

Administration > Users and Privileges > Admin Privileges > Import AdminPrivileges ([link](#))

Figure 17-5 Import (Admin) Privileges

Table 17-4 Import (Admin) Users

Container	Description
Select file	Browse to select name of admin privileges import file.
Enter secret key for file (if any)	Enter the secret key used (while exporting) to protect the file.
Import/Cancel	Commit or dismiss import.

Export Admin Privileges

Administration > Users and Privileges > Admin Privileges > Export Admin Privileges ([link](#)).

The **Export Admin Privileges** link exports all admin privileges. Click **Export**. Your browser will display its normal **Save As** dialog, in which to enter the name of the XML file to contain the export. Not that, once you export privileges, you can edit or create new ones and import these back into Policy Manager.

Export

Administration > Users and Privileges > Admin Privileges > Export (button).

To export just one admin privilege, select it (checkbox at left) and click Export. Your browser will display its normal **Save As** dialog, in which to enter the name of the XML file to contain the export.

Server Configuration

The Policy Manager Server Configuration menu provides the following interfaces for configuration:

- “Set Date/Time” (page 237)
- “Change Cluster Password” (page 239)
- “Make Subscriber” (page 239)
- “Upload Nessus Plugins” (page 240)
- “Collect Logs” (page 242)
- “Backup” (page 243)
- “Restore” (page 244)

Clicking on the server row provides the following interfaces for configuration:

- “Set Time Zone (Subscriber)” (page 245)
- “System Tab” (page 246)
- “Services Control Tab” (page 249)
- “Service Parameters Tab” (page 249)
- “System Monitoring Tab” (page 257)

Figure 17-6 Server Configuration

Administration » Server Manager » Server Configuration

Server Configuration

[Set Date & Time](#)
[Change Cluster Password](#)
[Upload Nessus Plugins](#)
[Cluster-Wide Parameters](#)

Publisher Server: etips [192.168.5.217]

#	Server Name ▲	Data Port	Management Port	Cluster Sync	Last Sync Time
1.	etips	-	192.168.5.217	Enabled	-
2.	etips2	-	192.168.5.220	Enabled	Mar 31, 2010 14:32:03 PDT

Showing 1-2 of 2

[Collect Logs](#)
[Backup](#)
[Restore](#)
[Shutdown](#)
[Reboot](#)
[Drop Subscriber](#)

Set Date/Time

Administration > Server Manager > Server Configuration > Set Date and Time, also available from a command line at “date” (page 301).

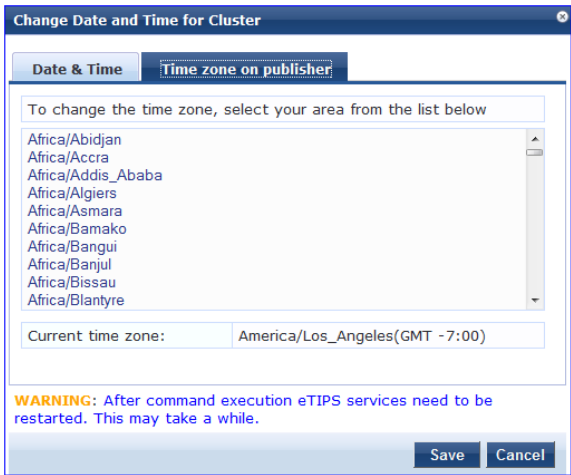
Figure 17-7 Change Date and Time
Table 17-5 Change date and time

Container	Description
Date in yyyy-mm-dd format	<i>To specify date and time</i> , use the indicated syntax. This is available only when Synchronize time with NTP server is unchecked.
Time in hh:mm:ss format	
Synchronize Time With NTP Server	<i>To synchronize with a Network Time Protocol Server</i> , enable this checkbox and specify the NTP servers. Only two servers may be specified.
NTP Servers	
Save/Cancel	Commit or dismiss changes. Note the warning in the popup regarding system restart upon saving.

Set Time Zone on Publisher

Administration > Server Manager > Server Configuration > Set Date and Time, also available from a command line at **“timezone”** (page 303). The time-zone list is shown in alphabetical order. Select a time zone and click **Save**. Note that this option is only available on the publisher. To set timezone on the subscriber, select the specific server and set timezone from the server-specific page.

Figure 17-8 Time zone on publisher



Change Cluster Password

Administration > Server Manager > Server Configuration > Change Cluster Password, also available from a command line at “set-cluster-passwd” (page 295).

Use this function to change cluster-wide password. **Note that this also changes the password of the CLI user - ‘appadmin’.**

Figure 17-9 Change Cluster Password

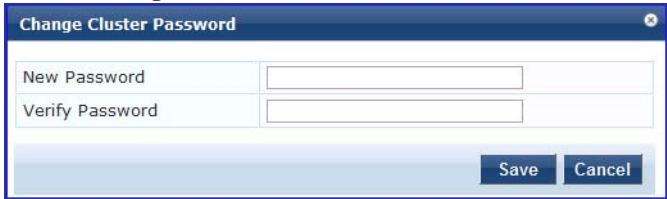


Table 17-6 Change Cluster Password

Container	Description
New Password	Enter and confirm password.
Verify Password	
Save/Cancel	Commit or dismiss changes.

Make Subscriber

In the Policy Manager cluster environment, the *Publisher node* acts as master. An Policy Manager cluster can contain only one Publisher node. Administration, configuration, and database write operations may occur only on this master node.

The Policy Manager appliance defaults to a Publisher node unless it is made a Subscriber node. Cluster commands can be used to change the state of the node, hence the Publisher can be made a Subscriber.

Administration > Server Manager > Server Configuration > Make Subscriber, also available from a command line at “[make-subscriber](#)” (page 294).

Figure 17-10 Add Subscriber Node

Table 17-7 Add Subscriber Node

Container	Description
Publisher IP	Specify publisher address and password. Note that the password specified here is the password for the CLI user <i>appadmin</i> .
Publisher Password	
Restore the local log database after this operation	Enable to restore the log database following addition of a subscriber node.
Save/Cancel	Commit or dismiss changes.

Upload Nessus Plugins

Administration > Server Manager > Server Configuration > Upload Nessus Plugins.

Figure 17-11 Upload Nessus Plugins

Table 17-8 Upload Nessus Plugins

Container	Description
Select File	Click Browse and select the plugins file with the extension tar.gz.
Enter secret for the file (if any)	Always leave this blank.
Import/Cancel	Load the plugins, or dismiss. If there are a large number of plugins, load time can be in the order of minutes.

Cluster-Wide Parameters

Administration > Server Manager > Server Configuration > Cluster-Wide Parameters

Table 17-9 Cluster-Wide Parameters

Container	Description
Policy result cache cleanup timeout	The number of minutes to store the role mapping and posture results derived by the policy engine during policy evaluation. This result can then be used in subsequent evaluation of policies associated with a service, if “Use cached Roles and Posture attributes from previous sessions” is turned on for the service. A value of 0 disables caching.
Maximum inactive time for an endpoint	The number of days to keep an endpoint in the endpoints table since its last authentication. If the endpoint has not authenticated for this period, the entry is removed from the endpoint table. 0 specifies no time limit.
Cleanup interval for session log details in the database	The Number of days to keep the following data in the Policy Manager DB: session logs (found on Access Tracker), event logs (found on Event Viewer), machine authentication cache.
Cleanup interval for information stored on disk	The Number of days to keep log files, report files, etc., written to disk.
System Alert Level	Alert notifications are generated for system events logged at this level or higher. Selecting INFO generates alerts for INFO, WARN and ERROR messages. Selecting WARN generates alerts for WARN and ERROR messages. Selecting ERROR generates alerts for ERROR messages.
Alert Notification Timeout	This indicates how often (in hours) alert messages are generated and sent out. Selecting “Disabled” disables alert generation.
Alert Notification - eMail Address	Comma separated list of email addresses to which alert messages are sent.
Alert Notification - SMS Address	Comma separated list of SMS addresses to which alert messages are sent. For example, 4085551212@txt.att.net.
Enable advanced archiving of session information	Enable archiving of session log information for Aruba’s advanced reporting and analytics application - Insight. If you have not deployed Insight, you can disable this by selecting FALSE from the dropdown.

Container	Description
Auto backup configuration options	<p>Off - Do not perform periodic backups.</p> <p>Config - Perform a periodic backup of only the configuration database.</p> <p>Config Session - Perform a periodic backup of both the configuration and log databases.</p>
Known or disabled endpoints cleanup interval	This controls how often (in days) endpoints with a status of Known or Disabled are cleaned up from the endpoints table.
Unknown endpoints cleanup interval	This controls how often (in days) endpoints with a status of Unknown are cleaned up from the endpoints table.
Maximum duration to archive session information	This controls the number of days to archive session log information. The “Enable advanced archiving of session information” has to be enabled for this parameter to take effect.
Free disk space threshold value	This controls the percentage below which disk usage warnings are issued in the Policy Manager Event Viewer. For example, a value of 30% indicates that a warning is issued if only 30% or below of disk space is available.
Free memory threshold value	This controls the percentage below which RAM usage warnings are issued in the Policy Manager Event Viewer. For example, a value of 30% indicates that a warning is issued if only 30% or below of RAM is available.
Expired guest accounts cleanup interval	This controls the cleanup interval of expired guest accounts; this is number of days after expiry that the cleanup happens. No cleanup is performed if the value is 0.

Collect Logs

Administration > Server Manager > Server Configuration > Collect Logs

Figure 17-12 Collect Logs

Collect Logs

Output file name:

Collect the following logs

- ☒ System logs
- ☐ Logs from all eTIPS services
- ☐ Capture network packets Duration of dump: secs.
- ☐ Diagnostic dumps from eTIPS services

☒ Specify date range

For number of days until today:

Start date in yyyy-mm-dd format:

End date in yyyy-mm-dd format:

Start **Cancel**

Table 17-10 Collect Logs

Container	Description
Output file name	Specify name of log file. The output file is a gzipped tar file (tar.gz extension).
Collect the following logs	Select: <ul style="list-style-type: none"> System Logs Logs from all Policy Manager services Capture network packets for the specified duration. Use this with caution, and use this only when you wish to debug a problem. System performance can be severely impacted. Diagnostic dumps from Policy Manager services
Specify date range	Enable to specify the date range; if selected, enter a number of days leading up to today or a start and end date.
Start date in yyyy-mm-dd format	
End date in yyyy-mm-dd format	
Start/Cancel	Commit or dismiss changes.

Backup

Administration > Server Manager > Server Configuration > Backup, also available from a command line at “[backup](#)” (page 307).

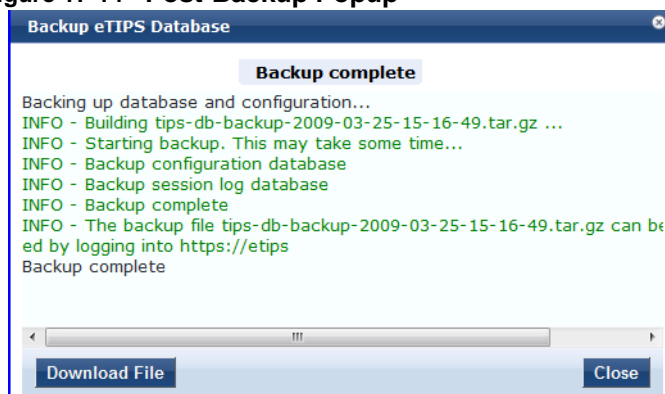
Figure 17-13 Backup Popup

Backup Tips Database

☒ Generate filename

Filename:

Start **Cancel**

Figure 17-14 Post-Backup Popup**Table 17-11 Backup**

Container	Description
Generate filename	Enable to have Policy Manager generate a filename; otherwise, specify Filename. Backup files are in the gzipped tar format (tar.gz extension). The backup file is automatically placed in the Shared Local Folder under folder type Backup Files (See “Local Shared Folders” (page 260)).
Filename	
Start/Cancel	Start backup/Dismiss popup.
Download File	After backup, download the file to your local machine. The operating system Save dialog pops up.

Restore

Administration > Server Manager > Server Configuration > Restore, also available from a command line at “[restore](#)” (page 310).

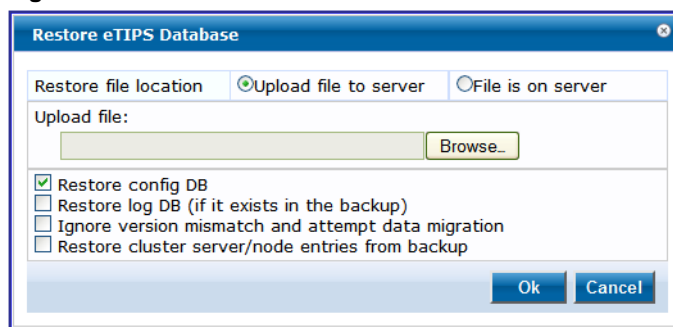
Figure 17-15 Restore

Table 17-12 Restore

Container	Description
Restore file location	Specify (radio button): <i>Upload file to server</i> or <i>File on server</i> .
Upload file	Browse to select name of backup file (shown only when Upload file to server radio button is selected).
Shared backup files present on the server	Select a file from the files in the local shared folders (See “ Local Shared Folders ” (page 260)). This is shown only when File on server radio button is selected.
Restore config DB	Enable to include the configuration database in the restore.
Restore log DB (if it exists in the backup).	Enable to include the log database in the restore.
Ignore version mismatch and attempt data migration	This option must be checked when you are migrating configuration and/or log data from a backup file that was created with a previous compatible version.
Restore cluster server/node entries from backup.	Enable to include the cluster server/node entries in the restore.
OK/Cancel	Commit or dismiss changes.

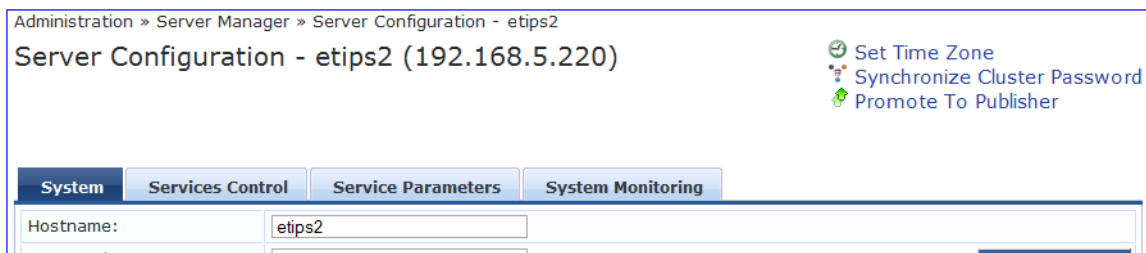
Shutdown/ Reboot

Administration > Server Manager > Server Configuration > Shutdown/Reboot. Shutdown or reboot the node from the UI.

Drop Subscriber

Administration > Server Manager > Server Configuration > Drop Subscriber. Drop a subscriber node from the cluster. Note that this button is not seen in a single node deployment.

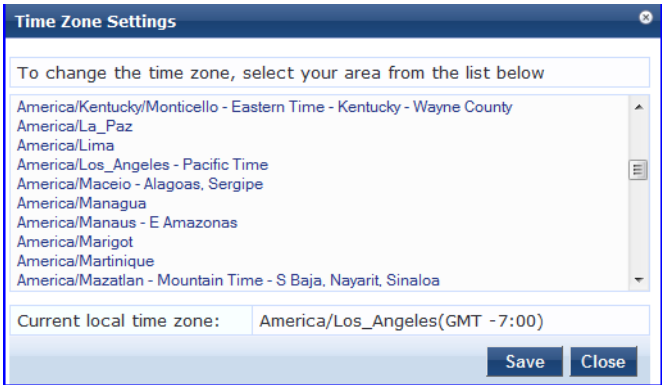
Set Time Zone (Subscriber)

Figure 17-16 Subscriber Operations

Administration > Server Manager > Server Configuration > <server-name> > Set Time Zone, also available from a command line at “[timezone](#)”

(page 303). The timezone list is shown in alphabetical order. Select a time zone and click **Save**. Note that this link is only seen for subscriber nodes.

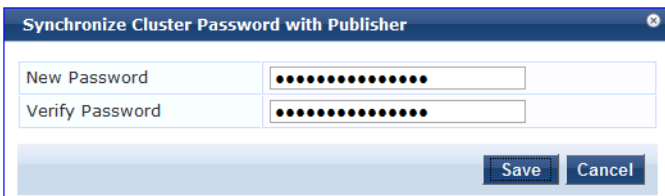
Figure 17-17 Set Time Zone



**Synchronize
Cluster
Password
(Subscriber)**

Administration > Server Manager > Server Configuration > <server-name> > Synchronize Cluster Password. If the subscriber node was down when the cluster password was changed on the publisher, this link provides a way for the subscriber to synchronize its password with the cluster password on the publisher. Enter the new cluster password in the popup.

Figure 17-18 Synchronize Cluster Password



**Promote To
Publisher**

Administration > Server Manager > Server Configuration > <server-name> > Promote To Publisher. A subscriber node can be manually promoted to a publisher node. The current publisher node is automatically demoted to a subscriber. This function can also be used if the publisher has to be taken out of the network for maintenance. One of the subscribers in the cluster can then be promoted to a publisher.

System Tab

Administration > Server Configuration - <servername> The attributes on this page can also be configured from the Command Line Interface (CLI) “Server Port Configuration” (page 1)

Figure 17-19 System Tab

Administration » Server Manager » Server Configuration - etips [Set Time Zone](#)

Server Configuration - etips (192.168.5.217)

System Services Control Service Parameters System Monitoring

Hostname:

AD Domain: [Leave Domain](#) [Join Domain](#)

AD Domain: [Leave Domain](#) [Join Domain](#)

Management Port:

IP Address:

Subnet Mask:

Default Gateway:

Data/External Port:

IP Address:

Subnet Mask:

Default Gateway:

DNS Settings:

Primary DNS:

Secondary DNS:

[Back to Server Configuration](#) [Save](#) [Cancel](#)

Table 17-13 System

Container	Description
Hostname	Hostname of Policy Manager appliance. It is not necessary to enter the fully qualified domain name here.
AD Domain	Active Directory Domain Name (optional) - Use only if you need to authenticate users against Active Directory. Select Join Domain to join an Active Directory domain. See below.
Management Port: IP Address	Management interface IP address. You access the Policy Manager UI via the management interface.
Management Port: Subnet Mask	Management interface Subnet Mask
Management Port: Default Gateway	Default gateway for management interface
Data Port: IP Address	Data interface IP address. All authentication and authorization requests arrive on the data interface.
Data Port: Subnet Mask	Data interface Subnet Mask
Data Port: Default Gateway	Default gateway for data interface
DNS: Primary DNS	Primary DNS for name lookup
DNS: Secondary DNS	Secondary DNS for name lookup

Join Domain - Click on this button to join this Policy Manager appliance to an Active Directory domain.

Leave Domain - Click on this button to disassociate this Policy Manager appliance from an Active Directory domain.

Note: For most use case, if you have multiple nodes in the cluster you must join each node to the same Active Directory domain.

Figure 17-20 Join Active Directory Domain

Table 17-14 System Tab

Container	Description
Domain Controller	Fully qualified name of the Active Directory domain controller
Short Name - NETBIOS name (optional)	<p>The short name or NETBIOS name of the domain. Enter this value only if this is different from your regular Active Directory domain name. If this is different from your domain name (usually a shorter name), enter that name here. Contact your AD administrator about the NETBIOS name.</p> <p>Note: If you enter an incorrect value for the NETBIOS name, you see a warning message in the UI. If you see this warning message, leave the domain by clicking on the Leave Domain button (which replaces the Join Domain button once you join the domain. After leaving the domain, join again with the right NETBIOS name.</p>

Container	Description
Domain Controller name conflict	<p>In some deployments (especially if there are multiple domain controllers, or if the domain name has been wrongly entered in the last step), the domain controller FQDN returned by the DNS query can be different from what was entered. In this case, you may:</p> <ul style="list-style-type: none"> • Continue to use the domain controller name that you entered • Use the domain controller name returned by the DNS query • Abort the Join Domain operation.
Use default domain admin user	Check this box to use the <i>Administrator</i> user name to join the domain
User Name	User ID of the domain administrator account
Password	Password of the domain administrator account

Services Control Tab

Administration > Server Configuration - <servername> View status and control (stop or start) Policy Manager services from this page.

Figure 17-21 Services Control Tab


System

Services Control

Service Parameters

System Monitoring

Service Name	Status	Action
1. Async DB write service	Running	Stop
2. Async network services	Running	Stop
3. DB change notification server	Running	Stop
4. DB replication service	Running	Stop
5. Domain service	Running	Stop
6. Policy server	Running	Stop
7. Radius server	Running	Stop
8. System auxiliary services	Running	Stop
9. System monitor service	Running	Stop
10. Tacacs server	Running	Stop

 Back to Server Configuration

Save

Cancel

Service Parameters Tab

Administration > Server Configuration - <servername> Change system parameters of the services from this page.

Figure 17-22 Policy Server Service Parameters

Parameter Name	Parameter Value	Default Value
Machine Authentication Cache Timeout	86400 seconds	86400
Authentication Thread Pool Size	20 threads	20
LDAP Primary Retry Interval	600 seconds	600
External Posture Server Thread Pool Size	5 threads	5
External Posture Server Primary Retry Interval	600 seconds	600
Audit SPT Default Timeout	600 seconds	600
Number of request processing threads	4 threads	
Audit Primary Retry Interval	600 seconds	600
Audit IP Lookup Session Timeout	120 seconds	120

Table 17-15 Policy Server Service Parameters

Service Parameter	Description
Machine Authentication Cache Timeout	This specifies the time (in seconds) for which machine authentication entries are cached by Policy Manager
Authentication Thread Pool Size	This specifies the number of threads to use for LDAP/AD and SQL connections.
LDAP Primary Retry Interval	Once a primary LDAP server is down, Policy Manager connects to one of the backup servers. This parameter specifies how long Policy Manager waits before it tries to connect to the primary server again.
External Posture Server Thread Pool Size	This specifies the number of threads to use for posture servers.
External Posture Server Primary Retry Interval	Once a primary posture server is down, Policy Manager connects to one of the backup servers. This parameter specifies how long Policy Manager waits before it tries to connect to the primary server again.
Audit SPT Default Timeout	Time for which Audit success or error response is cached in policy server.
Number of request processing threads	Maximum number of threads used to process requests.
Audit Primary Retry Interval	Once a primary audit server is down, Policy Manager connects to one of the backup servers. This parameter specifies how long Policy Manager waits before it tries to connect to the primary server again.
Audit IP Lookup Session Timeout	Temporary session timeout returned for a request that triggers an audit, and Policy Manager needs to lookup IP address for the MAC address of the host before proceeding with audit

Figure 17-23 RADIUS Server Service Parameters

System	Services Control	Service Parameters	System Monitoring
Select Service: RADIUS server			
Parameter Name	Parameter Value	Default Value	
Proxy			
Maximum Response Delay	<input type="text" value="5"/> seconds	5	
Maximum Reactivation Time	<input type="text" value="120"/> seconds	120	
Maximum Retry Counts	<input type="text" value="5"/> retries	5	
Security			
Reject Packet Delay	<input type="text" value="1"/> seconds	1	
Maximum Attributes	<input type="text" value="200"/> attributes	200	
Main			
Authentication Port	<input type="text" value="1812"/> , <input type="text" value="1645"/>	1812, 1645	
Accounting Port	<input type="text" value="1813"/> , <input type="text" value="1646"/>	1813, 1646	
Maximum Request Time	<input type="text" value="30"/> seconds	30	
Cleanup Time	<input type="text" value="5"/> seconds	5	
Local DB Authentication Source Connection Count	<input type="text" value="32"/>	32	
AD/LDAP Authentication Source Connection Count	<input type="text" value="32"/>	32	
SQL DB Authentication Source Connection Count	<input type="text" value="32"/>	32	
TLS Session Cache Limit	<input type="text" value="10000"/> sessions	10000	
Thread Pool			
Maximum Number of Threads	<input type="text" value="50"/> threads	50	
Number of Initial Threads	<input type="text" value="25"/> threads	25	
EAP-FAST			
Master Key Expire Time	<input type="text" value="1"/> weeks	1 weeks	
Master Key Grace Time	<input type="text" value="3"/> weeks	3 weeks	
PACs are valid across cluster	<input type="text" value="true"/>	true	

Table 17-16 RADIUS Server Service Parameters

Service Parameter	Description
Proxy	
Maximum Response Delay	Time delay before retrying a proxy request, if the target server has not responded
Maximum Reactivation Time	Time to elapse before retrying a dead proxy server
Maximum Retry Counts	Maximum number of times to retry a proxy request if the target server doesn't respond
Security	
Reject Packet Delay	Delay time before sending an actual RADIUS Access-Reject after the server decides to reject the request
Maximum Attributes	Maximum number of RADIUS attributes allowed in a request
Main	
Authentication Port	Ports on which radius server listens for authentication requests. Default values are 1645, 1812

Service Parameter	Description
Accounting Port	Ports on which radius server listens for accounting requests. Default values are 1646, 1813
Maximum Request Time	Maximum time allowed for a processing a request after which it is considered timed out
Cleanup Time	Time to cache the response sent to a RADIUS request after sending it. If the RADIUS server gets a duplicate request for which the response is already sent, the cached response is resent if the duplicate request arrives within this time period.
Local DB Authentication Source Connection Count	Maximum number of Local DB DB connections opened
AD/LDAP Authentication Source Connection Count	Maximum number of AD/LDAP connections opened
SQL DB Authentication Source Connection Count	Maximum number of SQL DB
TLS Session Cache Limit	Number of TLS sessions to cache before purging the cache (used in TLS based 802.1X EAP Methods)
Thread Pool	
Maximum Number of Threads	Maximum number of threads in the RADIUS server thread pool to process requests
Number of Initial Threads	Initial number of thread in the RADIUS server thread pool to process requests
EAP-FAST	
Master Key Expire Time	Lifetime of a generated EAP-FAST master key
Master Key Grace Time	Grace period for a EAP-FAST master key after its lifetime. If a client presents a PAC that is encrypted using the master key in this period after its TTL, it is accepted and a new PAC encrypted with the latest master key is provisioned on the client
PACs are valid across cluster	Whether PACs generated by this server are valid across the cluster or not

Figure 17-24 Tips System Services Parameters

Select Service:	Tips system services		
Parameter Name	Parameter Value	Default Value	Allowed Values
HTTP Proxy			
Proxy Server	<input type="text"/>		
Port	<input type="text" value="3128"/>	3128	
Username	<input type="text"/>		
Password	<input type="text"/>		

You can use these service parameters if all your http traffic flows through a proxy server. Policy Manager relies on an http connection to the Aruba update portal in order to download the latest version information for posture services.

Table 17-17 Tips System Services Parameters

Service Parameter	Description
Proxy Server	Hostname or IP address of the proxy server
Port	Port at which the proxy server listens for http traffic
Username	Username to authenticate with proxy server
	Password to authenticate with proxy server

Figure 17-25 TACACS+ Service Parameters

Parameter Name	Parameter Value	Default Value
TACACS+ Profiles Cache Timeout	86400 seconds	86400

Table 17-18 TACACS+ Service Parameters

Service Parameter	Description
TACACS+ Profiles Cache Timeout	This specifies the time (in seconds) for which TACACS+ profile result entries are cached by Policy Manager

Tips Network Services Parameters aggregate service parameters from the following services:

- DhcpSnooper Service
- Snmp Service
- WebAuth Service
- Posture Service

Figure 17-26 Tips Network Services Parameters

Select Service: Tips network services

Parameter Name	Parameter Value	Default Value	Allowed Values
DhcpSnooper			
MAC to IP Request Hold time	<input type="text" value="120"/> seconds	120	60-300
DHCP Request Probation Time	<input type="text" value="30"/> seconds	30	10-60
SnmpService			
SNMP Timeout	<input type="text" value="4"/> seconds	4	2-30
SNMP Retries	<input type="text" value="1"/> retries	1	1-5
LinkUp Timeout	<input type="text" value="5"/> seconds	5	3-15
IP Address Cache Timeout	<input type="text" value="600"/> seconds	600	12-1200
Uplink Port Detection Threshold	<input type="text" value="5"/>	5	0-20
SNMP v2c Trap Community	<input type="text" value="....."/>	public	
SNMP v3 Trap Username	<input type="text" value="avenda"/>	avenda	
SNMP v3 Trap Authentication Protocol	<input type="text"/>		
SNMP v3 Trap Privacy Protocol	<input type="text"/>		
SNMP v3 Trap Authentication Key	<input type="text"/>		
SNMP v3 Trap Privacy Key	<input type="text"/>		
WebAuthService			
Max time to determine network device where client is connected	<input type="text" value="5"/> seconds	5	0-100
PostureService			

Figure 17-27 DHCP Snooping Service

DhcpSnooper				
MAC to IP Request Hold time	<input type="text" value="120"/>	seconds	120	60-300
DHCP Request Probation Time	<input type="text" value="30"/>	seconds	30	10-60

Table 17-19 DHCP Snooping Service Parameters

Service Parameter	Description
MAC to IP Request Hold time	Number of seconds to wait before responding to a query to get IP address corresponding to a MAC address. Any DHCP message received in this time period will refresh the MAC to IP binding. Typically, audit service will request for a MAC to IP mapping as soon the RADIUS request is received, but the client may take some more time receive and IP address through DHCP. This wait period takes into account the latest DHCP IP address that the client got
DHCP Request Probation Time	Number of seconds to wait before considering the MAC to IP binding received in a DHCPREQUEST message as final. This wait would handle cases where client receives a DHCPNAK for a DHCPREQUEST and receives a new IP address after going through the DHCPDISCOVER process again

Figure 17-28 SNMP Service Parameters

SnmpService				
SNMP Timeout	4	seconds	4	2-30
SNMP Retries	1	retries	1	1-5
LinkUp Timeout	5	seconds	5	3-15
IP Address Cache Timeout	600	seconds	600	12-1200
Uplink Port Detection Threshold	5		5	0-20
SNMP v2c Trap Community	*****		public	
SNMP v3 Trap Username	avenda		avenda	
SNMP v3 Trap Authentication Protocol				
SNMP v3 Trap Privacy Protocol				
SNMP v3 Trap Authentication Key				
SNMP v3 Trap Privacy Key				

Table 17-20 SNMP Service Parameters

Service Parameter	Description
SNMP Timeout	Seconds to wait for an SNMP response from the network device
SNMP Retries	Number of retries for SNMP requests
LinkUp Timeout	Seconds to wait before processing link-up traps. If a MAC notification trap arrives in this time, SNMP service will not try to poll the switch for MAC addresses behind a port for link-up processing
IP Address Cache Timeout	Duration in seconds for which MAC to IP lookup response is cached
Uplink Port Detection Threshold	Limit for the number of MAC addresses found behind a port after which the port is considered an uplink port and not considered for SNMP lookup and enforcement
SNMP v2c Trap Community	Community string that must be checked in all incoming SNMP v2 traps
SNMP v3 Trap Username	SNMP v3 Username to be used for all incoming traps
SNMP v3 Trap Authentication Protocol	SNMP v3 Authentication protocol for traps. Must be one of MD5, SHA or empty (to disable authentication)
SNMP v3 Trap Privacy Protocol	SNMP v3 Privacy protocol for traps. Must be one of DES_CBC or empty (to disable privacy)
SNMP v3 Trap Authentication Key	SNMP v3 authentication key and privacy key for incoming traps
SNMP v3 Trap Privacy Key	

Figure 17-29 Posture Service Parameters

PostureService				
Audit Thread Pool Size	20	threads	20	5-40
Audit Result Cache Timeout	600	seconds	600	1-864000
Audit Host Ping Timeout	60	seconds	60	1-300

Table 17-21 Posture Service Parameters

Service Parameter	Description
Audit Thread Pool Size	This specifies the number of threads to use for connections to audit servers.
Audit Result Cache Timeout	This specifies the time (in seconds) for which audit result entries are cached by Policy Manager
Audit Host Ping Timeout	This specifies the number of seconds for which Policy Manager pings an end-host before giving up and deeming the host to be unreachable.

Table 17-22 Webauth Service Parameters

Service Parameter	Description
Max time to determine network device where client is connected	In some usage scenarios where the web authentication request does not originate from the network device, Policy Manager has to determine the network device to which the client is connect through an out-of-band SNMP mechanism. The network device deduction can take some time. This parameter specifies the maximum time to wait for Policy Manager to determine the network device to which the client is connected.

Figure 17-30 System Monitor Service Parameters

Parameter Name	Parameter Value	Default Value
Free Disk Space Threshold	30 %	30
1 Min CPU load average Threshold	3 %	3
5 Min CPU load average Threshold	2 %	2
15 Min CPU load average Threshold	1 %	1

Table 17-23 System Monitor Service Parameters

Service Parameter	Description
Free Disk Space Threshold	This parameter monitors the available disk space. If the available disk free space falls below the specified threshold (default 30%), then system sends SNMP traps to the s configured.
1 Min CPU load average Threshold	These parameters monitor the CPU load average of the system, specifying thresholds for 1-min, 5-min and 15-min averages, respectively. If any of these loads exceed the associated maximum value then system sends traps to the trap servers configured.
5 Min CPU load average Threshold	
15 Min CPU load average Threshold	

System Monitoring Tab

Administration > Server Configuration - <servername> Configure the SNMP parameters, so external Management Information Base (MIB) browsers can browse the system level MIB objects exposed by the Policy Manager appliance.

Figure 17-31 System Monitoring Tab

SystemServices ControlService ParametersSystem Monitoring

System Location:

System Contact:

SNMP Configuration:

Version:V3

User Name:

Security Level:NOAUTH_NOPRIV

Authentication Protocol:MD5

Authentication key:

Verify:

Privacy Protocol:DES

Privacy Key:

Verify:

SystemServices ControlService ParametersSystem Monitoring

System Location:

System Contact:

SNMP Configuration:

Version:V2C

Community String:.....

Verify:.....

Table 17-24 System Monitoring Tab Details

Service Parameter	Description
System Location	Policy Manager appliance location and contact information
System Contact	
SNMP Configuration: Version	V1, V2C or V3
SNMP Configuration: Community String	Read community string.
SNMP Configuration: SNMP v3: Username	Username to use for SNMP v3 communication
SNMP Configuration: SNMP v3: Security Level	One of NOAUTH_NOPRIV (no authentication or privacy), AUTH_NOPRIV (authenticate, but no privacy), AUTH_PRIV (authenticate and keep the communication private)
SNMP Configuration: SNMP v3: Authentication Protocol	Authentication protocol (MD5 or SHA) and key
SNMP Configuration: SNMP v3: Authentication key	

Service Parameter	Description
SNMP Configuration: SNMP v3: Privacy Protocol	Privacy protocol (DES or AES) and key
SNMP Configuration: SNMP v3: Privacy Key	

Log Configuration

The Policy Manager Log Configuration menu at **Administration > Server Manager > Log Configuration** provides the following interface for configuration:

Figure 17-32 Log Configuration (Services Level tab)

Administration » Server Manager » Log Configuration

Log Configuration

Select Server: 192.168.5.217

Service Log Configuration | System Level

Select Service: Multi-master cache

- Policy server
- Radius server
- Tacacs server
- Admin server
- DB change notification server
- DB replication service
- Syslog client service
- Tips network services
- Async network services
- Multi-master cache

Module Log Level Settings: ☒ Enable to override default log level

Default Log Level: WARN

Module Name	Log Level
1. Rules Engine	WARN
2. Xpip Server	WARN
3. Database	INFO
4. AD/LDAP	INFO
5. Request Handling	DEBUG
6. Common Framework	INFO
7. External Posture Validation	WARN
8. Internal Posture Validation	ERROR
9. Audit Server support	FATAL
10. SOAP API	INFO

Table 17-25 Log Configuration (Services Level tab)

Container	Description
Select Server	Specify the server for which to configure logs. All nodes in the cluster appear in the drop down list.
Select Service	Specify the service for which to configure logs.

Container	Description
Module Log Level Settings	<i>Enable</i> to set log level for each module individually (listed in decreasing level of verbosity. For optimal performance you must run Policy Manager with log level set to ERROR or FATAL): <ul style="list-style-type: none"> • DEBUG • INFO • WARN • ERROR • FATAL If <i>disabled</i> all module level logs are set to the default log level.
Default Log Level	
Module & Log Level	If Override default log level is enabled, select log levels for each of the available modules (listed in decreasing level of verbosity): <ul style="list-style-type: none"> • DEBUG • INFO • WARN • ERROR • FATAL
Restore Defaults/Save	Click Save to save changes or Restore Defaults to restore default settings.

Figure 17-33 Log Configuration (System Level tab)

Administration » Server Manager » Log Configuration

Log Configuration

Select Server:

Service Log Configuration

System Level

Number of log files:	<input type="text" value="6"/> (default is 6 files)
Limit each log file size to:	<input type="text" value="10"/> MB (default is 10 MB)

Syslog Settings:

Syslog Server:	<input type="text"/>
Syslog Server Port:	<input type="text" value="514"/> (default is 514)

Service Name	Enable Syslog	Syslog Filter Level
1. Policy server	<input type="checkbox"/>	WARN
2. Radius server	<input type="checkbox"/>	WARN
3. Tacacs server	<input type="checkbox"/>	WARN
4. Admin server	<input type="checkbox"/>	WARN
5. Syslog client service	<input type="checkbox"/>	WARN
6. Tips network services	<input type="checkbox"/>	WARN

Table 17-26 Log Configuration (System Level tab)

Container	Description
Select Server	Specify the server for which to configure logs.
Number of log files	Number of log files of a specific module to keep at any given time. Once a log file reaches the specified size (see below), Policy Manager rolls the log over to another file until the specified number of log files is reached; once this log files exceed this number, Policy Manager overwrites the first numbered file.
Limit each log file size to	Limit each log file to this size, before log rolls over to the next file
Syslog Server Syslog Port	Specify the syslog server and port number. Policy Manager will send the configured module logs to this syslog server.
Service Name Enable Syslog Syslog Filter Level	Name of the service to enable syslog output for, and the log level.
Restore Defaults/Save	Click Save to save changes or Restore Defaults to restore default settings.

Local Shared Folders

To view backup files, log files, and generated reports: **Administration > Server Manager > Local Shared Folders**.

Select the specific folder from the **Select folder** drop-down list. Currently supported folder types are listed below:

- Backup files - Database backup files backed up manually (tar.gz format)
- Log files - Log files backed up via the Collect Logs mechanism (tar.gz format)
- Generated Reports - Historical reports auto-generated on a configured schedule from the Reporting screens (PDF and CSV formats)
- Automated Backup files - Database backup files backed up automatically on a daily basis (tar.gz format)

Select any file in the listing to download it to your local computer. The browser download box appears.

Figure 17-34 Local Shared Folders

Administration » Server Manager » Local Shared Folders

Local Shared Folders

Select folder: Backup files

- Backup files
- Log files
- Generated Reports
- Automated Backup files

#	File Name	File Size	Last Modified Time
1.	tips-db-backup-2009-03-25-15-16-49.tar.gz	3.08 MB	Mar 25, 2009 15:16:52 PDT
2.	eTIPS_Backup_Mar24.tar.gz	2.95 MB	Mar 24, 2009 11:09:16 PDT
3.	restore-2009-03-20-00-16-07-backup.tar.gz	325.23 KB	Mar 19, 2009 17:16:08 PDT
4.	setup-2009-03-20-00-05-40-backup.tar.gz	0.54 KB	Mar 19, 2009 17:05:40 PDT

Snmp Trap Receivers

Policy Manager sends SNMP traps that expose the following server information:

- **System uptime.** Conveys information about how long the system is running
- **Network interface statistics [up/down].** Provides information if the network interface is up or down.
- **Process monitoring information.** Check for the processes that should be running. Maximum and minimum number of allowed instances. Sends traps if there is a change in value of maximum and minimum numbers.
- **Disk usage.** Check for disk space usage of a partition. The agent can check the amount of available disk space, and make sure it is above a set limit. The value can be in % as well. Sends traps if there is a change in the value.
- **CPU load information.** Check for unreasonable load average values. For example if 1 minute CPU load average exceeds the configured value [in percentage] then system would send the trap to the configured destination.
- **Memory usage.** Report the memory usage of the system.

The Policy Manager SNMP Trap Configuration page at **Administration > External Servers > SNMP Trap Receivers** provides the following interfaces for configuration:

- “Add SNMP Trap Server” (page 262)
- “Import SNMP Trap Server” (page 263)
- “Export SNMP Trap Server” (page 263)
- “Export” (page 263)

Figure 17-35 Snmp Trap Receivers Listing Page

Administration » External Servers » SNMP Trap Receivers

SNMP Trap Receivers

[Add SNMP Trap Server](#)
[Import SNMP Trap Server](#)
[Export SNMP Trap Server](#)

Filter: HostAddress contains Go Clear Filter Show 10 records

#	Host Address	Description
1.	192.168.150.3	Trap Receiver 1
2.	192.168.150.8	SNMP Trap Receiver 2

Showing 1-2 of 2

Export Delete

Table 17-27 Snmp Trap Configuration

Container	Description
Add Trap Server	Opens Add Trap Server popup.
Import Trap Server	Opens Import Trap Server popup.
Export Trap Server	Opens Export Trap Server popup.
Export	Opens Export popup.
Delete	To delete an <i>SNMP Trap Configuration</i> , select it (checkbox at left) and click Delete .

Add SNMP Trap Server

To add a trap server: **Administration > External Servers > SNMP Trap Receivers > Add Trap Server**.

Figure 17-36 Add SNMP Trap Server

Add SNMP Trap Server

Host Address: 192.168.24.33

Description: CentralView SNMP Trap Receiver

SNMP Version: V2C

Community String: Verify:

Server Port: 162

Save Cancel

Table 17-28 Add SNMP Trap Server

Container	Description
Host Address	Trap destination hostname or ip address. Note: This server must have an <i>SNMP trap receiver or trap viewer</i> installed.
Description	Freeform description.
SNMP Version	V1 or V2C.

Container	Description
Community String /Verify Community String	Community string for sending the traps.
Server Port	Port number for sending the traps; by default, port 162. Note: Configure the trap server firewall for traffic on this port.
Save/Cancel	Click Save to commit the configuration or Cancel to dismiss.

Import SNMP Trap Server

Administration > External Servers > SNMP Trap Receivers > Import Trap Server

Figure 17-37 Import SNMP Trap Server

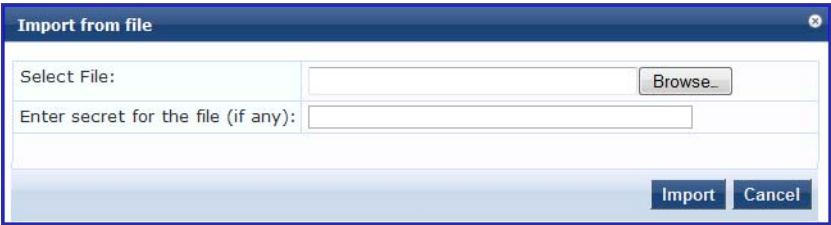


Table 17-29 Import from file

Container	Description
Select File	Browse to the SNMP Trap Server configuration file to be imported.
Enter secret for the file (if any)	If the file was exported with a secret key for encryption, enter the same key here.
Import/Cancel	Click Import to commit, or Cancel to dismiss the popup.

Export SNMP Trap Server

Administration > External Servers > SNMP Trap Receivers > Export Trap Server (link).

The **Export Trap Server** link exports all configured SNMP Trap Receivers. Click **Export Trap Server**. Your browser will display its normal **Save As** dialog, in which to enter the name of the XML file to contain the SNMP trap server configuration.

Export

Administration > External Servers > SNMP Trap Receivers **Export** (button).

To export a trap server, select it (checkbox at left) and click **Export**. Your browser will display its normal **Save As** dialog, in which to enter the name of the XML file to contain the export.

Syslog Targets

Policy Manager can export session data (seen in the “[Access Tracker](#)” (page 13)), audit records (seen in the “[Audit Viewer](#)” (page 35)) and event records (seen in the “[Event Viewer](#)” (page 37)). This information can be sent to one or more syslog targets (servers). You configure syslog targets from this page.

The Policy Manager Syslog Targets page at **Administration > External Servers > Syslog Targets** provides the following interfaces for configuration:

- “Add Syslog Target” (page 264)
- “Import Syslog Target” (page 265)
- “Export Syslog Target” (page 265)
- “Export” (page 266)

Figure 17-38 Syslog Target Listing Page

Administration » External Servers » Syslog Targets

Syslog Targets

Filter: Host Address contains Go Clear Filter Show 20 records

#	<input type="checkbox"/>	Host Address ▲	Description
1.	<input type="checkbox"/>	192.168.5.179	Kiwi syslog target
2.	<input type="checkbox"/>	192.168.5.233	My Test Syslog Target

Showing 1-2 of 2

Export Delete

Table 17-30 Syslog Target Configuration

Container	Description
Add Syslog Target	Opens Add Syslog Target popup.
Import Syslog Target	Opens Import Syslog Target popup.
Export Syslog Target	Opens Export Syslog Target popup.
Export	Opens Export popup.
Delete	To delete a Syslog Target, select it (checkbox at left) and click Delete .

Add Syslog Target

To add a Syslog Target: **Administration > External Servers > Syslog Targets > Add Syslog Target**.

Figure 17-39 Add Syslog Target

The screenshot shows a dialog box titled "Add Syslog Target". It has three input fields: "Host Address" containing "192.168.12.44", "Description" containing "Kangaroo Syslog Target", and "Server Port" containing "514". At the bottom right, there are two buttons: "Save" and "Cancel".

Table 17-31 Add Syslog Target

Container	Description
Host Address	Syslog server hostname or IP address.
Description	Freeform description.
Server Port	Port number for sending the syslog messages; by default, port 514.
Save/Cancel	Click Save to commit the configuration or Cancel to dismiss.

Import Syslog Target

Administration > External Servers > Syslog Targets > Import Syslog Target

Figure 17-40 Import Syslog Target

The screenshot shows a dialog box titled "Import from file". It has two input fields: "Select File:" with a "Browse..." button, and "Enter secret for the file (if any):". At the bottom right, there are two buttons: "Import" and "Cancel".

Table 17-32 Import from file

Container	Description
Select File	Browse to the Syslog Target configuration file to be imported.
Enter secret for the file (if any)	If the file was exported with a secret key for encryption, enter the same key here.
Import/Cancel	Click Import to commit, or Cancel to dismiss the popup.

Export Sylog Target

Administration > External Servers > Syslog Targets > Export Syslog Target (link).

The **Export Syslog Target** link exports all configured syslog targets. Click **Export Syslog Target**. Your browser will display its normal **Save As** dialog, in which to enter the name of the XML file to contain the Syslog Target configuration.

Export

Administration > External Servers > Syslog Targets (button).

To export a syslog target, select it (checkbox at left) and click **Export**. Your browser will display its normal **Save As** dialog, in which to enter the name of the XML file to contain the export.

Syslog Export Filters

Policy Manager can export session data (seen in the “[Access Tracker](#)” (page 13)), audit records (seen in the “[Audit Viewer](#)” (page 35)) and event records (seen in the “[Event Viewer](#)” (page 37)). You configure Syslog Export Filters to tell Policy Manager where to send this information, and what kind of information should be sent (through Data Filters).

The Policy Manager Syslog Targets page at **Administration > External Servers > Syslog Targets** provides the following interfaces for configuration:

- “[Add Syslog Filter](#)” (page 267)
- “[Import Syslog Filter](#)” (page 269)
- “[Export Syslog Filter](#)” (page 269)
- “[Export](#)” (page 269)

Figure 17-41 Syslog Filters Listing Page

Administration » External Servers » Syslog Export Filters

Syslog Export Filters

Add Syslog Filter

Import Syslog Filter

Export Syslog Filter

Filter:

Name

 contains

Go

Clear Filter

Show

20

 records

#	<div></div> Name ▲	Description	Export Template	Status
1.	<div></div> Audit Records Stream	This is the syslog export filter to stream System Audit records to external syslog target	Audit Records	<div>Disable</div>
2.	<div></div> Failed Authentications Stream	This is the syslog export filter to stream all the failed authentications to syslog target	Session Logs	<div>Disable</div>
3.	<div></div> Failed Requests Stream	Stream all failed requests to external syslog	Session Logs	<div>Disable</div>
4.	<div></div> Logged in Session Stream	This is the syslog export filter to stream all the logged in session information to the syslog target.	Session Logs	<div>Disable</div>
5.	<div></div> System Events Stream	This is the syslog export filter to stream System Events to external syslog target	System Events	<div>Disable</div>

Showing 1-5 of 5

Export

Delete

Table 17-33 Syslog Export Filters Configuration

Container	Description
Add Syslog Filter	Opens Add Syslog Filter page (Administration > External Servers > Syslog Export Filters > Add).
Import Syslog Filter	Opens Import Syslog Filter popup.
Export Syslog Filter	Opens Export Syslog Filter popup.
Enable/Disable	Click the toggle button Enable/Disable to enable or disable the syslog filter.
Export	Opens Export popup.
Delete	<i>To delete a Syslog Filter</i> , select it (checkbox at left) and click Delete .

Add Syslog Filter

To add a Syslog Filter: **Administration > External Servers > Syslog Filters > Add Syslog Filter**.

Figure 17-42 Add Syslog Filters (General Tab)

Administration » External Servers » Syslog Export Filters » Add

Syslog Export Filters

General | Filter and Columns | Summary

Name: Passed Radius requests

Description: Stream passed radius requests to syslog

Export Template: Session Logs

Syslog Server: 192.168.5.233 (selected)
 192.168.5.233
 192.168.5.179

Buttons: Modify, Add new Syslog target, Back to Syslog Filters, Next >, Save, Cancel

Table 17-34 Add Syslog Target (General Tab)

Container	Description
Name/Description	Freeform label.
Export Template	Session Logs, Audit Records or System Events
Syslog Server	A drop down list shows all Syslog Targets configured. (Refer to “ Add Syslog Target ” (page 264)).
Modify/Add new syslog target	Click to Modify the selected syslog target. Or Add new syslog target (link) to add a new syslog target.
Save/Cancel	Click Save to commit the configuration or Cancel to dismiss.

If you selected Session Logs as the export template in the **General** tab, a new tab **Filter and Columns** appears. In this tab you specify the Data Filter (See “Add Filter” (page 40)) you want to use; specifying a data filter filters the rows that are sent to the syslog target. You may also select the columns that are sent to the syslog target.

Figure 17-43 Add Syslog Filters (Filter and Columns Tab)

Table 17-35 Add Syslog Filters (Filter and Columns Tab)

Container	Description
Data Filter	Specify the data filter. The data filter limits the type of records sent to syslog target.
Modify/ Add new Data filter	Modify the selected data filter, or add a new one.
Columns Selection	<p>This provides a way to limit the type of columns sent to syslog. There are Predfined Field Groups, which are column names grouped together for quick addition to the report. For example, <i>Logged in users</i> field group seven pre-defined columns. When you click <i>Logged in users</i> the seven columns automatically appear in the Selected Columns list.</p> <p>Additional Fields are available to add to the reports. You can select the type of attributes (which are the different table columns available in the session database) from the Available Columns Type drop down list. Policy Manager populates these column names by extracting the column names from existing sessions in the session database. Once you select a column from the Available Columns Type, the columns appear in the box below. From here you can click >> to add the selected column to the Selected Columns list. Click << to remove a column from the Selected Columns list.</p>

Import Syslog Filter

Administration > External Servers > Syslog Filters > Import Syslog Filter

Figure 17-44 Import Syslog Filter

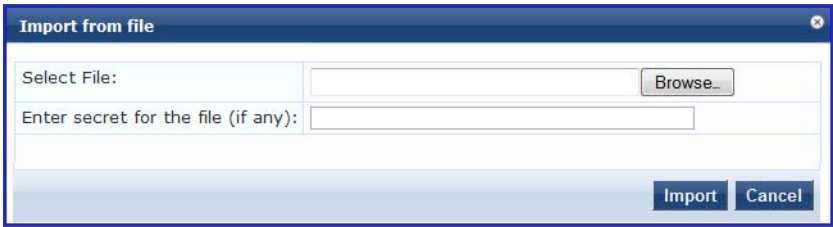


Table 17-36 Import from file

Container	Description
Select File	Browse to the Syslog Filter configuration file to be imported.
Enter secret for the file (if any)	If the file was exported with a secret key for encryption, enter the same key here.
Import/Cancel	Click Import to commit, or Cancel to dismiss the popup.

Export Syslog Filter

Administration > External Servers > Syslog Filters > Export Syslog Filter (link).

The **Export Syslog Filter** link exports all configured syslog filters. Click **Export Syslog Filter**. Your browser will display its normal **Save As** dialog, in which to enter the name of the XML file to contain the Syslog Filer configuration.

Export

Administration > External Servers > Syslog Filters (button).

To export a syslog filter, select it (checkbox at left) and click **Export**. Your browser will display its normal **Save As** dialog, in which to enter the name of the XML file to contain the export.

Messaging Setup

The Policy Manager Messaging Setup menu at **Administration > Server Manager > Messaging Setup** provides the following interface for configuration:

Figure 17-45 Messaging Setup (SMTP Servers)

Administration » External Servers » Messaging Setup

Messaging

Configure the SMTP mail servers for email and SMS notifications : Select Server : 192.168.5.217 ▼

SMTP Servers

Mobile Service Providers

☒ Use the same settings for sending both emails and SMSes

Common SMTP settings

Server name:	<input type="text"/>	<input type="checkbox"/> Use SSL
User Name:	<input type="text"/>	Port: <input type="text" value="25"/>
Password:	<input type="text"/> <input type="checkbox"/> Show Password	Connection timeout: <input type="text" value="30"/> seconds
Default from address:	<input type="text"/>	

Save

Table 17-37 Messaging Setup (SMTP Servers Tab)

Container	Description
Select Server	Specify the server for which to configure messaging. All nodes in the cluster appear in the drop down list.
Use the same settings for sending both emails and SMSes	Check this box to configure the same settings for both your SMTP and SMS email servers. This box is checked, by default.
Server name	Fully qualified domain name or IP address of the server.
Username/password	If your email server requires authentication for sending email messages, enter the credentials here.
Default from address	All emails sent out will have this from address in the message.
Use SSL	Use secure SSL connection for communications with the server.
Port	This is TCP the port number that the SMTP server listens on.
Connection timeout	Timeout for connection to the server (in seconds).

Figure 17-46 Messaging Setup (Mobile Service Providers tab)

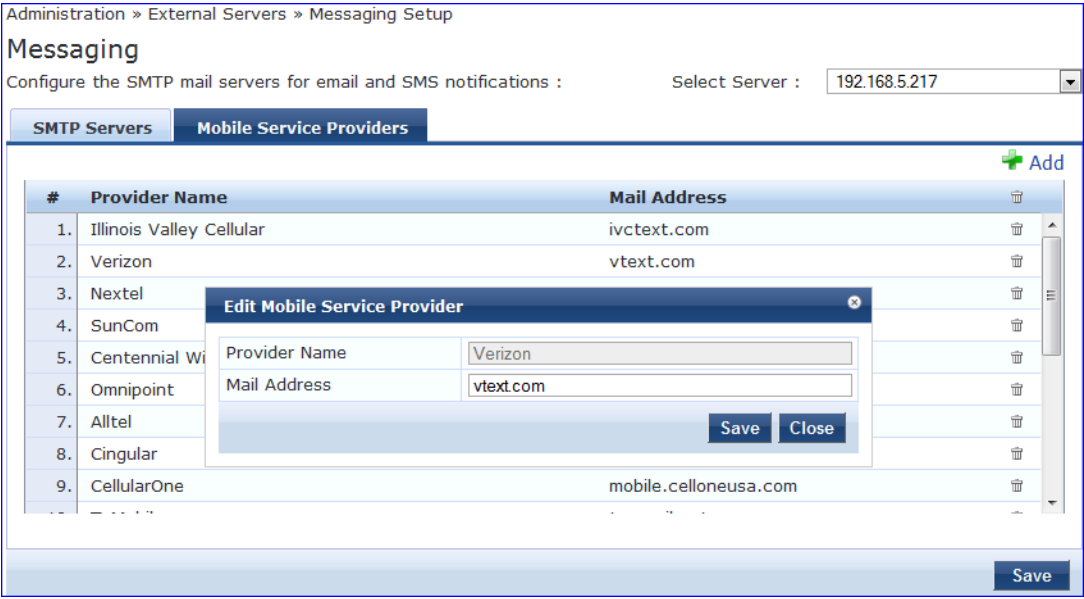


Table 17-38 Messaging Setup (Mobile Service Providers tab)

Container	Description
Add	Add a mobile service provider
Provider Name	Name of the provider
Mail Address	Domain name of the provider

Certificates

The Policy Manager Certificates menu provides the following interfaces for configuration:

- “Server Certificate” (page 271)
- “Certificate Trust List” (page 276)
- “Revocation Lists” (page 277)

Server Certificate

The Policy Manager Server Certificate menu at **Administration > Certificates > Server Certificates** provides the following interfaces for configuration:

- “Create Self-Signed Certificate” (page 272)
- “Create Certificate Signing Request” (page 274)
- “Export Server Certificate” (page 275)
- “Import Server Certificate” (page 276)

Figure 17-47 Server Certificates

Administration » Certificates » Server Certificate

Server Certificate

Create Self-Signed Certificate
Create Certificate Signing Request

Select Server: 192.168.5.217

Certificate Field	Field Value
Subject:	O=eTIPS, CN=etips
Issued by:	O=eTIPS, CN=etips
Issue Date:	Thu Mar 19 2009 17:12:55 GMT-0700 (Pacific Daylight Time)
Expiry Date:	Fri Mar 19 2010 17:12:55 GMT-0700 (Pacific Daylight Time)
Validity Status:	Valid
Signature Algorithm:	SHA1withRSA
Key Format:	X.509

Export Import

Table 17-39 Server Certificate

Container	Description
Create Self-Signed Certificate	Open Create Self-Signed Certificate popup.
Create Certificate Signing Request	Open Create Certificate Signing Request popup.
Select Server	Select a server in the cluster for server certificate operations.
Export	Open Export popup.
Import	Open Import popup.

Create Self-Signed Certificate

Administration > Certificates > Server Certificate > Create Self-Signed Certificate

Figure 17-48 Create Self-Signed Certificate

Create Self-Signed Certificate

Common Name (CN): etips

Organization (O): Avenda Systems

Organizational Unit (OU): Engineering

State (ST): CA

Country (C): US

Location (L): San Jose

Subject Alternate Name (SAN): email:admin@us.avendasys.com

Private Key Password: ••••

Verify Private Key Password: ••••

Key Length: 1024 bits

Digest Algorithm: SHA-1

Valid for: 180 days

Submit Cancel

Figure 17-49 Generated Self Signed Certificate

Create Self-Signed Certificate	
Subject DN:	L=San Jose, C=US, ST=CA, O=Avenda Systems, OU=Engineering, CN=etips
Issuer DN:	L=San Jose, C=US, ST=CA, O=Avenda Systems, OU=Engineering, CN=etips
Subject Alternate Name (SAN):	email:admin@us.avendasys.com
Issue Date/Time:	Thu Mar 26 08:48:45 PDT 2009
Expiry Date/Time:	Tue Sep 22 08:48:45 PDT 2009
Validity Status:	Valid
Signature Algorithm:	SHA1WithRSAEncryption
Public Key Format:	X.509
<input type="button" value="Install"/> <input type="button" value="Cancel"/>	

Table 17-40 Create Self-Signed Certificate

Container	Description
Common Name (CN)	Name associated with this entity: <i>host name, IP address or other meaningful name.</i> Required.
Organization (O)	Name of the organization. Optional.
Organizational Unit (OU)	Name of a department, division, section, or other meaningful name. Optional.
State (ST)	State, country, and/or another meaningful location. Optional.
Country (C)	
Location (L)	
Subject Alternate Name (SAN)	Alternative names for the specified Common Name. Note that SAN has to be in the form email: <i>email_address</i> , URI: <i>uri</i> , IP: <i>ip_address</i> , dns: <i>dns_name</i> or rid: <i>id</i> Optional.
Private Key Password	Specify and verify password.
Verify Private Key Password	Required.
Key Length	Select length for the generated private key: <i>512, 1024 or 2048.</i>
Digest Algorithm	Select message digest algorithm to use: <i>SHA-1, MD5 and MD2.</i>
Valid for	Specify duration in days.

Container	Description
Submit/Cancel	On submit, Policy Manager generates a popup containing the self-signed certificate. Click on the Install button to install the certificate on the selected server. Note: All services are restarted; you must relogin into the UI to continue.

Create Certificate Signing Request

Administration > Certificates > Create Certificate Signing Request. Create a self-signed certificate to be signed by a CA.

Figure 17-50 Create Certificate Signing Request

Figure 17-51 Generated Certificate Signing Request

```

-----BEGIN CERTIFICATE REQUEST-----
MIIB+TCCAWICAQAwBTEOMAwGA1UEAxMFZXRRpcHMxZDAsBgNVBAsTC0Vud21uZWVyaW5nMRcwFQYDVQQKEw5BdmVuZGEGU3lzdGVtczELMAkGA1UECBMQ0ExCzAJBgNVBAYTA1VTMRIwEAYDVQQHEw1CYW5nYVxvcmlUaW8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAN7cuQZLWFQQSooLIN4K07zLf8p7Cx91zbEanQ8629hf0ojJbeRiS8vjWmFuMEoz0CPcfXB11/ENCfDIwq83st+xJMxNsMD/JFa/ThFIou8JTnvdMw6m9KJaAr5EBgda+r19MQ9WK5Qk+JgzIzIVj7cj2jQ1loibvqTNzTBG65NagMBAAGgTDBKBgkqhkiG9w0BCQ4xPTA7MCQGA1UdEQQdMBuBGWFkbW1uQG1uZG1hLmF2ZW5kYXN5cy5jb20wEwYDVRO1BAwwCgYIKwYBBQUHAEwDQYJKoZIhvcNAQEFBQADgYEAwb8Ss9Q1lDxcckvo/c+UMZ/H6hhdABKwqTCzv0431f1gIFTB+NucX62s4Meqn2KS+SLwXK072dJEcrKhHd1ZJSWSJnD4Ms5U8JNJJV5nCcW7RWugieZKmacVchPDN4LPWKkplzcFoypxDeAQ910iCSgv2ZILmIQhE9IXFnzzUWdo=
-----END CERTIFICATE REQUEST-----

```

Copy and paste this into the web form in the enrollment process

Table 17-41 Create Certificate Signing Request

Container	Description
Common Name (CN)	Name associated with this entity: <i>host name, IP address or other meaningful name.</i> Required.
Organization (O)	Name of the organization. Optional.
Organizational Unit (OU)	Name of a department, division, section, or other meaningful name. Optional.
State (ST)	State, country, and/or another meaningful location. Optional.
Country (C)	
Location (L)	
Subject Alternate Name (SAN)	Alternative names for the specified Common Name. Optional.
Private Key Password	Specify and verify password.
Verify Private Key Password	Required.
Key Length	Select length for the generated private key: <i>512, 1024 or 2048.</i>
Digest Algorithm	Select message digest algorithm to use: <i>SHA-1, MD5 and MD2.</i>
Submit/Cancel	<p>On submit, Policy Manager generates a popup containing the certificate signing request for copying/pasting into the web form that you typically use to get the certificate signed by a CA.</p> <p><i>To create a file containing the certificate signing request, click Download CSR File. A .csr file is downloaded to your local computer.</i></p> <p><i>To download the generated private key file, click Download Private Key File.</i></p> <p>Note: Make sure that you save the downloaded private key in a secure place.</p>

Export Server Certificate

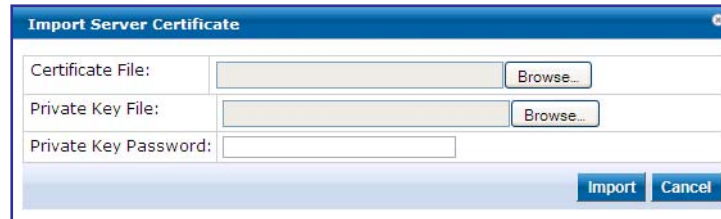
Administration > Certificates > Server Certificates > **Export** (button).

The **Export** button saves the file `ServerCertificate.zip`. The zip file has the server certificate (.crt file) and the private key (.pvk file).

Import Server Certificate

Administration > Certificates > Server Certificates > Import (button)

Figure 17-52 Import



The dialog box titled "Import Server Certificate" contains three input fields: "Certificate File:" with a "Browse..." button, "Private Key File:" with a "Browse..." button, and "Private Key Password:" with a text input field. At the bottom right are "Import" and "Cancel" buttons.

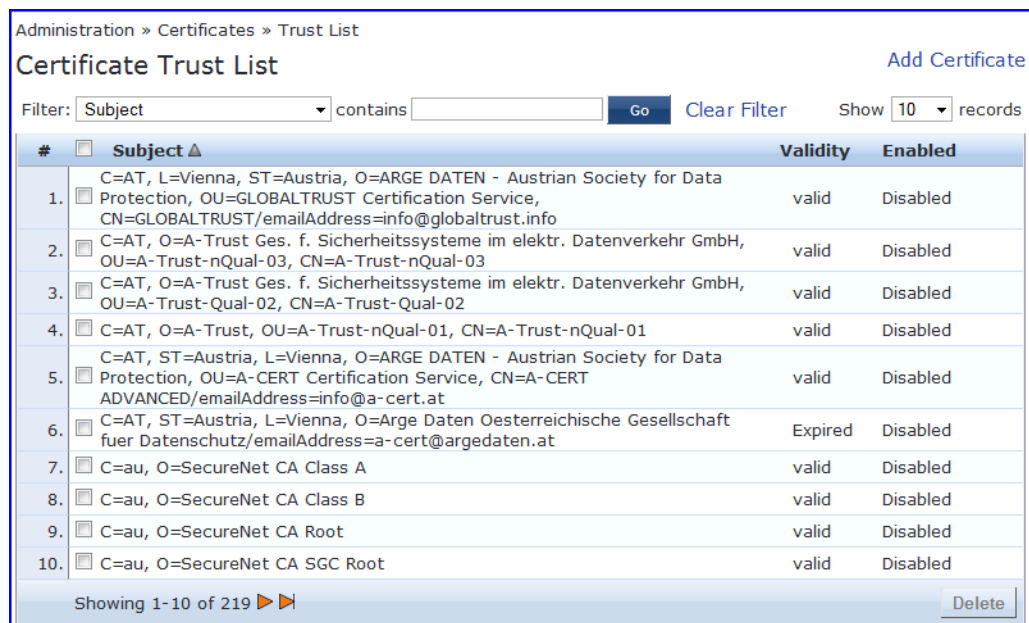
Table 17-42 Import

Container	Description
Certificate File	Browse to the certificate file to be imported.
Private Key File	Browse to the private key file to be imported.
Private Key Password	Specify the private key password.
Import/Cancel	Click Import to commit, or Cancel to dismiss the popup.

Certificate Trust List

To display the list of trusted Certificate Authorities (CAs), **Administration > Certificates > Certificate Trust List**. To add a certificate, click **Add Certificate**; to delete a certificate, select it (checkbox on left) and click **Delete**.

Figure 17-53 Certificate Trust List



The interface shows the "Certificate Trust List" under "Administration » Certificates ». It includes a search filter (Subject, contains), a "Go" button, a "Clear Filter" button, and a "Show 10 records" dropdown. The table lists 10 certificates with columns for #, Subject, Validity, and Enabled. A "Delete" button is at the bottom right.

#	Subject	Validity	Enabled
1.	C=AT, L=Vienna, ST=Austria, O=ARGE DATEN - Austrian Society for Data Protection, OU=GLOBALTRUST Certification Service, CN=GLOBALTRUST/emailAddress=info@globaltrust.info	valid	Disabled
2.	C=AT, O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH, OU=A-Trust-nQual-03, CN=A-Trust-nQual-03	valid	Disabled
3.	C=AT, O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH, OU=A-Trust-Qual-02, CN=A-Trust-Qual-02	valid	Disabled
4.	C=AT, O=A-Trust, OU=A-Trust-nQual-01, CN=A-Trust-nQual-01	valid	Disabled
5.	C=AT, ST=Austria, L=Vienna, O=ARGE DATEN - Austrian Society for Data Protection, OU=A-CERT Certification Service, CN=A-CERT ADVANCED/emailAddress=info@a-cert.at	valid	Disabled
6.	C=AT, ST=Austria, L=Vienna, O=Arge Daten Oesterreichische Gesellschaft fuer Datenschutz/emailAddress=a-cert@argedaten.at	Expired	Disabled
7.	C=au, O=SecureNet CA Class A	valid	Disabled
8.	C=au, O=SecureNet CA Class B	valid	Disabled
9.	C=au, O=SecureNet CA Root	valid	Disabled
10.	C=au, O=SecureNet CA SGC Root	valid	Disabled

Showing 1-10 of 219

Table 17-43 Certificate Trust List

Container	Description
Subject	The Distinguished Name (DN) of the subject field in the certificate
Validity	This indicates whether the CA certificate has expired.
Enabled	Whether this CA certificate is enabled or not.

To view the details of the certificate, click on a certificate row. From the **View Certificate Details** popup you can **Enable** the CA certificate. When you enable a CA certificate, Policy Manager considers the entity whose certificate is signed by this CA to be trusted.

Add Certificate

Administration > Certificates > Certificate Trust List > Add Certificate (link)

Figure 17-54 Add Certificate
Table 17-44 Add Certificate

Container	Description
Certificate File	Browse to select certificate file.
Add Certificate/Cancel	Click Add Certificate to commit, or Cancel to dismiss the popup.

Revocation Lists

To display available Revocation Lists, **Administration > Certificates > Revocation Lists**. To add a revocation list, click **Add Revocation List**; to delete a revocation list, select it (checkbox on left) and click **Delete**.

Figure 17-55 Revocation Lists

Table 17-45 Revocation Lists

Container	Description
Add Revocation List	Click to launch the Add Revocation List popup.
Delete	<i>To delete a revocation list</i> , select it (checkbox at left) and click Delete .

Add Revocation List

Administration > Certificates > Revocation Lists > Add Revocation List
(link)

Figure 17-56 Add Certificate Revocation List
Table 17-46 Add Certificate Revocation List

Container	Description
Distribution URL	Specify the distribution URL (e.g., <code>http://crl.verisign.com/Class3InternationalServer.crl</code>) to fetch the certificate revocation list.
Auto Update	<i>Update whenever CRL is updated</i> to update the CRL at intervals specified in the list. Enable <i>Periodically update</i> , to check periodically and at the specified frequency (in days).

Dictionaries

The Policy Manager Dictionaries menu provides the following interfaces for configuration:

- “RADIUS Dictionaries” (page 279)
- “Posture Dictionaries” (page 280)
- “TACACS+ Services” (page 281)

All of these interfaces provide the option to **Import Dictionary**, which applies to any vendor- or service-attribute Dictionary.

RADIUS Dictionaries

To add a new vendor dictionary, click on Import Dictionary. To edit an existing dictionary, export an existing dictionary, edit the exported XML file, and then import the dictionary. To view the contents of the RADIUS dictionary, sorted by *Vendor Name*, *Vendor ID*, or *Vendor Prefix*, navigate to: **Administration > Dictionaries > RADIUS**.

Figure 17-57 RADIUS

Administration » Dictionaries » RADIUS

RADIUS Dictionaries

Import Dictionary

Filter: Vendor Name contains Go Clear Filter Show 10 records

#	Vendor Name ▲	Vendor ID	Vendor Prefix	Enabled
1	3com	43	3com	false
2	3GPP	10415	3GPP	false
3	3GPP2	5535	3GPP2	false
4	Acc	5	Acc	false
5	ADSL-Forum	3561	ADSL-Forum	false
6	Airespace	14179	Airespace	true
7	Alcatel	3041	Alcatel	false
8	Alteon	1872	Alteon	false
9	Alvarion	12394	Alvarion	false
10	Aruba	14823	Aruba	false

Showing 1-10 of 85

Table 17-47 RADIUS

Container	Description
Import Dictionary	Click to open the Import Dictionary popup. Import the dictionary (XML file).

Click on a vendor row to see all the attributes and their data type. For example, click on vendor IETF to see all IETF attributes and their data type.

Figure 17-58 RADIUS IETF Dictionary Attributes

RADIUS Attributes

Vendor Name: IETF (0)

#	Attribute Name	ID	Type	In/Out
1.	User-Name	1	String	in out
2.	User-Password	2	String	in
3.	CHAP-Password	3	String	in
4.	NAS-IP-Address	4	IPv4Address	in
5.	NAS-Port	5	Integer32	in
6.	Service-Type	6	Integer32	in out
7.	Framed-Protocol	7	Integer32	in out
8.	Framed-IP-Address	8	IPv4Address	in out
9.	Framed-IP-Netmask	9	IPv4Address	in out
10.	Framed-Routing	10	Integer32	out

Disable Export Close

Table 17-48 RADIUS Dictionary Attributes

Container	Description
Export	Click to save the dictionary file in XML format. You can make modifications to the dictionary and import the file back into Policy Manager.
Enable/Disable	Enable or disable this dictionary. Enabling a dictionary makes it appear in the Policy Manager rules editors (Service rules, Role mapping rules, etc.).

Posture Dictionaries

To add a new vendor posture dictionary, click on Import Dictionary. To edit an existing dictionary, export an existing dictionary, edit the exported XML file, and then import the dictionary.

To view the contents of the Posture dictionary, sorted by *Vendor Name*, *Vendor ID*, *Application Name*, or *Application ID*, navigate to: **Administration > Dictionaries > Posture**.

Figure 17-59 Posture

Administration » Dictionaries » Posture

Posture Dictionaries

Import Dictionary

Filter: Vendor Name contains Go Clear Filter Show 10 records

#	Vendor Name ▲	Vendor ID	Application Name	Application ID
1.	Avenda Systems	25427	WindowsSHV	65281
2.	Avenda Systems	25427	LinuxSHV	65280
3.	Avenda Systems	25427	Audit	6
4.	Cisco	9	Audit	6
5.	Cisco	9	Host Intrusion Protection Service	5
6.	Cisco	9	Firewall	4
7.	Cisco	9	Anti-Virus	3
8.	Cisco	9	Host	2
9.	Cisco	9	Posture Agent	1
10.	Microsoft	311	WindowsSHV	65408

Showing 1-10 of 15

Table 17-49 Posture

Container	Description
Import Dictionary	Click to open the Import Dictionary popup.

Click on a vendor row to see all the attributes and their data type. For example, click on vendor Microsoft/System SHV to see all the associated posture attributes and their data type.

Figure 17-60 Posture Dictionary

Posture Attributes				
Vendor Name:		Microsoft (311)		
Application Name:		SystemSHV (65280)		
#	Attribute Name	ID	Type	In/Out
1.	Application-Posture-Token	1	Unsigned32	out
2.	System-Posture-Token	2	Unsigned32	out
3.	SoH	3	SoH	in
4.	SoHR	4	SoH	out
				Export Close

Table 17-50 Posture Dictionary Attributes

Container	Description
Export	Click to save the posture dictionary file in XML format. You can make modifications to the dictionary and import the file back into Policy Manager.

TACACS+ Services

To add a new TACACS+ service dictionary, click on Import Dictionary. To add or modify attributes in an existing service dictionary, select the dictionary, export it, make edits to the XML file, and import it back into Policy Manager.

To view the contents of the TACACS+ service dictionary, sorted by *Name* or *Display Name*, navigate to: **Administration > Dictionaries > TACACS+ Services**.

Figure 17-61 TACACS+ Services

Administration » Dictionaries » TACACS+ Services			Import Dictionary Export Dictionary	
TACACS+ Services Dictionaries				
Filter: <input type="text" value="Name"/>		contains <input type="text"/>	Go	Clear Filter
		Show <input type="text" value="10"/> records		
#	Name ▲	Display Name		
1.	<input type="checkbox"/> arap	ARAP		
2.	<input type="checkbox"/> eTIPS:http	eTIPS:HTTP		
3.	<input checked="" type="checkbox"/> pixshell	PIX Shell		
4.	<input type="checkbox"/> ppp:ip	PPP:IP		
5.	<input type="checkbox"/> ppp:ipx	PPP:IPX		
6.	<input type="checkbox"/> ppp:lcp	PPP:LCP		
7.	<input type="checkbox"/> shell	Shell		
Showing 1-7 of 7			Export	Delete

Table 17-51 TACACS+ Service

Container	Description
Import Dictionary	Click to open the Import Dictionary popup. Import the dictionary (XML file).
Export Dictionary	Export all TACACS+ services into one XML file containing multiple dictionaries

To export a specific service dictionary, select a service and click on **Export**.

To see all the attributes and their data types, click on a service row. For example, click on shell service to see all shell service attributes and their data type.

Figure 17-62 Shell Service Dictionary Attributes

#	Name	Display Name	Type	Allowed Values
1.	acl	Access control list	String	-
2.	autocmd	Auto command	String	-
3.	callback-line	Callback line	String	-
4.	callback-rotary	Callback rotary	String	-
5.	idletime	Idle time	Unsigned32	-
6.	nocallback-verify	No callback verify	String	true, false
7.	noescape	No escape	String	true, false
8.	nohangup	No hangup	String	true, false
9.	priv-lvl	Privilege level	Unsigned32	-
10.	timeout	Timeout	Unsigned32	-

Import Dictionary

Administration > Dictionaries > Posture | RADIUS > Import Dictionary

Note: The imported file is in XML format. To view a sample of this XML format, export a dictionary file and open it in an XML viewer.

Figure 17-63 Import from file
Table 17-52 Import from file

Container	Description
Select File / Enter secret for the file	Browse to the dictionary file to be imported. Enter the secret key (if any) that was used to export the dictionary.

Container	Description
Import/Cancel	Click Import to commit, or Cancel to dismiss the popup.

Agent Settings

Administration > Agents and Portals > Agent Settings

Use this page to configure the agent deployment packages. Once the configuration is saved, agent deployment packages are created for Microsoft Windows and MAC OS X operating systems and placed at a fixed URL on the Policy Manager appliance. This URL can then be published to the user community. The agent deployment packages can also be downloaded to another location.



Figure 17-64 Agent Settings

Administration » Agents and Portals » Agent Settings -

Avenda Agent Settings -

Agent Version: 1.0.0.24496

Agent Installers

 Windows	http://192.168.5.31/agent/installer/windows/AvendaOnGuardInstall.exe
 Mac OS X	http://192.168.5.31/agent/installer/mac/AvendaOnGuardInstall.dmg

Agent Customization

Managed Interfaces: ☒ Wired ☒ Wireless ☐ VPN ☐ Other

Mode: Authenticate with health checks

Username Text:

Password Text:

Client Certificate Check: ☐ Enable to use a certificate from User keystore during authentication

Agent action when an update is available: Download Installer

External Captive Portal Support

Enter the URL of a web page that can be accessed only after a successful authentication (e.g., <http://www.avendasys.com>). A network device that is configured for captive portal-based authentication redirects requests to this URL to an authentication page.

URL:

Save Cancel

Table 17-53 Agent Settings

Container	Description
Agent Version	Current agent version.
Agent Installers	The URLs for the different agent deployment packages.
Managed Interfaces	Select the type of interfaces that OnGuard will manage on the endpoint.

Container	Description
Mode	<p>Select one of:</p> <ul style="list-style-type: none"> • Authenticate - no health checks. • Check health - no authentication. OnGuard does not collect username/password. • Authenticate with health checks. OnGuard collects username/password and also performs health checks on the endpoint.
Username/Password text	The label for the username/password field on the OnGuard agent. This setting is not valid for the “Check health - no authentication” mode.
Client certificate check	Enable to also perform client certificate based authentication. OnGuard extracts the client certificate from the logged in user’s certificate store and presents this in the TLS exchange with Policy Manager.
Agent action when an update is available	This setting determines what the agent does when an update is available. Options are Ignore, Download Installer, Notify User.
URL	In a captive portal scenario, the network device presents a captive portal page prior to user authentication. This portal page is presented when the user browses to a URL that is not authorized to be accessed prior to authentication. Enter such a URL here.
Save/Cancel	Commit the update information and generate new deployment packages.

Guest Portal

Administration > Agents and Portals > Guest Portal

Click on any of the four editable sections (areas C, D, F, G, H, I and J) of this page to customize the content for your enterprise:

Figure 17-65 Guest Portal

Administration » Portals » Guest Portal Global Portal Settings

Guest Portal


Name:	default	A
Portal URL:	https://etips/agent/portal/	B
Select Mode:	<div> <div>Authenticate - no health checks (HTML form)</div> <div>Authenticate - no health checks (HTML form)</div> <div>Authenticate - no health checks (Java applet)</div> <div>Check health - no authentication (Java applet)</div> <div>Authenticate with health checks (Java applet)</div> <div>Authenticate with optional health checks (Dual mode)</div> </div>	C
	<div> <div>Username</div> <div>:</div> <div></div> </div> <div> <div>Password</div> <div>:</div> <div></div> </div> <div>Submit</div>	D
Resource Files:	No resource files were uploaded. A ZIP archive containing resource files is supported <div>Upload</div>	E1
Customize Portal:	<input checked="" type="radio"/> Use default template <input type="radio"/> Upload custom template	E
Title	Guest Access Portal - Aruba Systems	F
Logo Image		G
Header	Guests must login with the username and password provided to access the network	H
Footer	<p>Note: If you can not access an enterprise resource, it may be because you are in the quarantine network. Please visit Aruba Networks Guest Policy for more information</p>	I
Copyright	© Copyright 2011 Aruba Networks. All rights reserved.	J

Table 17-54 Guest Portal

Container	Description
Global Portal Settings	<p>Attribute names and value configuration for the portal.</p> <p><i>UsernameFormat:</i> Format of username sent in authentication requests. This can be used in service rules (Authentication:Full-Username attribute) to write different service rules for different portals.</p> <p><i>SharedSecret:</i> Secret shared with a Wireless Controller (for example, Xirrus Wireless Controller) when Policy Manager is configured as an external captive portal on the network device.</p> <p><i>ShowOriginalPageRedirectLink:</i> Show a link that will take the user to the original page (prior to being redirected to the captive portal).</p>




Container	Description
C-Select Mode	<p>Select from the following for different modes of the portal:</p> <ul style="list-style-type: none"> • Authenticate - no health validation (HTML Form) - Policy Manager presents a simple HTML form with the username and password. Health credentials are not collected from the client. • Authenticate - no health validation (Java Applet) - Policy Manager presents an applet based form with the username and password. Health credentials are not collected from the client. Note that, the Java applet collects the MAC address of all interfaces on the client. In the case of a simple HTML form, Policy Manager would have to perform the extra step of DHCP snooping to collect the MAC address of the client. • Authenticate with health checks (Java Applet) - Policy Manager prompts the user for username and password, and also collects client health credentials by means of a Java applet downloaded to the page. • Authenticate with optional health checks (Dual mode) - User is presented with a simple HTML form. User can choose to load the Java applet by clicking on a link on this page; the java applet (dissolvable agent) also collects health information. • Check Health - no authentication (Java applet) - Username/password are not collected. Health is evaluated via a Java applet.
A-Name	A- Name is 'default'.
B-Portal URL	B - This is the URL that presents the guest portal page.
D-Username/Password label	(Note that this is automatically generated by Policy Manager).
F-Portal HTML Page Title String	Click on the logo image (G) to browse and select an image for the banner.
G-Logo Image	Click on the Username/Password labels (D) to change the respective label strings.
H-Header Message	Click on one of the highlighted regions (on the text) to edit and save the HTML.
I-Footer Message	
J-Copyright Message	

Container	Description
E1-Resource Files	<p>Click on Upload link to upload a zipped archive of resource files consisting of images, style sheets, scripts, etc. These are hosted on the Policy Manager appliance and can be referenced by prefixing the <code>_eTIPS_GUEST_PORTAL_RESOURCE_</code> to the patch component. For example, if there is a file named logo.jpg in the zipped archive, refer to this resource as <code>"_eTIPS_GUEST_PORTAL_RESOURCE_/logo.jpg"</code> on the guest portal page.</p> <p>Once the zipped archive is successfully uploaded, a screen showing the contained files is shown:</p>

Figure 17-66 Uploaded Resource Files

Resource Files:

4 resource files are uploaded (Size: 211.8 KB)

 Update  Download  Delete

Resource Files Details

Name	Size	Modified
cam.jpg	51.2 KB	2010/10/26 17:33:00
chappatte.jpg	70 KB	2010/10/26 17:34:02
dcr0656l.jpg	24.9 KB	2010/10/26 17:30:56
keefe.jpg	68.9 KB	2010/10/26 17:33:16

To reference the uploaded resource, use `_eTIPS_GUEST_PORTAL_RESOURCE_/<filename>`

E-Customize Portal	<p>Use default template to edit the different fields as described above. To import a custom HTML file to be used as the guest portal, select Upload custom template. Note that the following macros must be present in the custom HTML template:</p> <ul style="list-style-type: none"> <code>_eTIPS_GUEST_PORTAL_HEADER_</code> <code>_eTIPS_GUEST_PORTAL_BODY_</code> <code>_eTIPS_GUEST_PORTAL_FORM_</code>
Save/Cancel	Click Save to save changes, or Cancel to keep the default page.

Figure 17-67 Custom HTML Template Upload

Sample template

Upload Web Page

```

_eTIPS_GUEST_PORTAL_HEADER_
</head>
<body>
_eTIPS_GUEST_PORTAL_BODY_
<!-- Add page contents -->
eTIPS_GUEST_PORTAL_FORM
<!-- Add more page contents -->
<!-- Add Copyright -->
</body>

```

Save Cancel

Update Portal

Administration > Agents and Portals > Update Portal

Use the Update portal to sign up for live updates for Aruba-supported antivirus, antispyware, and other security software. Updates are done every hour.

Note: This does not include updates to the Policy Manager software. To update the Policy Manager software, refer to “[Updating the Policy Manager Software](#)” (page 3).

Figure 17-68 Update Portal

Administration » Portals » Update Portal

Update Portal

Not signed up for live updates, please register for [eTIPS updates](#)

User name:

Password: Verify:

Save Register Cancel

Table 17-55 Aruba Portal

Container	Description
Pre-Registration	
Policy Manager updates (link)	Click to register and turn on live updates. You are redirected to the Support page where you can register for updates. A username and password are emailed to the email address that you entered at the time of registration.

Container	Description
Post-Registration	
Username	Identity and login information for the update system. Enter the username and password you receive after the registration process.
Password	
Save/Cancel	Commit the update information or dismiss the dialog.

Appendix A: Command Line Interface

The Policy Manager command line provides commands of the following types:

- “Cluster Commands” (page 293)
- “Configure Commands” (page 296)
- “Network Commands” (page 297)
- “Service commands” (page 300)
- “Show Commands” (page 301)
- “System commands” (page 303)
- “Miscellaneous Commands” (page 306)
- “VM-Only Commands” (page 311)

Available Commands

Command
<i>ad auth</i> See <i>Miscellaneous Commands</i>
<i>ad netleave</i> See <i>Miscellaneous Commands</i>
<i>ad netjoin</i> See <i>Miscellaneous Commands</i>
<i>ad testjoin</i> See <i>Miscellaneous Commands</i>
<i>alias</i> See <i>Miscellaneous Commands</i>
<i>backup</i> See <i>Miscellaneous Commands</i>
<i>cluster drop-subscriber</i>
<i>cluster list</i>
<i>cluster make-publisher</i>
<i>cluster make-subscriber</i>
<i>cluster reset-database</i>
<i>cluster set-cluster-passwd</i>
<i>cluster set-local-passwd</i>

Command
<i>configure date</i>
<i>configure dns</i>
<i>configure hostname</i>
<i>configure ip</i>
<i>configure timezone</i>
dump certchain See <i>Miscellaneous Commands</i>
dump logs See <i>Miscellaneous Commands</i>
dump servercert See <i>Miscellaneous Commands</i>
exit See <i>Miscellaneous Commands</i>
help See <i>Miscellaneous Commands</i>
<i>kerb auth</i> See <i>Miscellaneous Commands</i>
<i>kerb list</i> See <i>Miscellaneous Commands</i>
<i>ldapsearch</i> See <i>Miscellaneous Commands</i>
<i>network ip</i>
<i>network nslookup</i>
<i>network ping</i>
<i>network traceroute</i>
<i>network reset</i>
quit See <i>Miscellaneous Commands</i>
restore See <i>Miscellaneous Commands</i>
<i>service activate</i>
<i>service deactivate</i>
<i>service list</i>

Command
<i>service</i> restart
<i>service</i> start
<i>service</i> status
<i>service</i> stop
<i>show</i> date
<i>show</i> dns
<i>show</i> domain
<i>show</i> all-timezones
<i>show</i> hostname
<i>show</i> ip
<i>show</i> license
<i>show</i> timezone
<i>show</i> version
<i>system</i> boot-image
<i>system</i> gen-support-key
<i>system</i> update
<i>system</i> restart
<i>system</i> shutdown
<i>system</i> install-license
<i>system</i> upgrade

Cluster Commands

The Policy Manager command line interface includes the following *cluster* commands:

- “drop-subscriber” (page 294)
- “list” (page 294)
- “make-publisher” (page 294)
- “make-subscriber” (page 294)
- “reset-database” (page 295)
- “set-cluster-passwd” (page 295)
- “set-local-passwd” (page 295)

drop-subscriber	Removes specified subscriber node from the cluster.								
Syntax	<pre>cluster drop-subscriber [-f] [-i <IP Address>] -s</pre> <p>where:</p> <table border="1"> <thead> <tr> <th>Flag/Parameter</th><th>Description</th></tr> </thead> <tbody> <tr> <td>-f</td><td>Force drop, even for down nodes</td></tr> <tr> <td>-i <IP Address></td><td>Management IP address of the node. If not specified and the current node is a subscriber, Policy Manager drops the current node.</td></tr> <tr> <td>-s</td><td>Do not reset the database on the dropped node. Note: By default, Policy Manager drops the current node (if a subscriber) from the cluster.</td></tr> </tbody> </table>	Flag/Parameter	Description	-f	Force drop, even for down nodes	-i <IP Address>	Management IP address of the node. If not specified and the current node is a subscriber, Policy Manager drops the current node.	-s	Do not reset the database on the dropped node. Note: By default, Policy Manager drops the current node (if a subscriber) from the cluster.
Flag/Parameter	Description								
-f	Force drop, even for down nodes								
-i <IP Address>	Management IP address of the node. If not specified and the current node is a subscriber, Policy Manager drops the current node.								
-s	Do not reset the database on the dropped node. Note: By default, Policy Manager drops the current node (if a subscriber) from the cluster.								
Example	<pre>[appadmin]# cluster drop-subscriber -f -i 192.168.1.1 -s</pre>								

list	Lists the cluster nodes.
Syntax	<pre>cluster list</pre>
Example	<pre>[appadmin]# cluster list cluster list Publisher : Management port IP=192.168.5.227 Data port IP=None [local machine]</pre>

make-publisher	Makes this node a publisher.
Syntax	<pre>cluster make-publisher</pre>
Example	<pre>[appadmin]# cluster make-publisher ***** * WARNING: Executing this command will promote the * * current machine (which must be a subscriber in the * * cluster) to the cluster publisher. Do not close the * * shell or interrupt this command execution. * ***** Continue? [y Y]: y</pre>

make-subscriber	Makes this node a subscriber to the specified publisher node.
Syntax	<pre>make-subscriber -i <IP Address> [-l]</pre> <p>where:</p>

Flag/Parameter	Description
-i <IP Address>	Required. Publisher IP address.
-l	Optional. Restore the local log database after this operation.

Example `[appadmin]# cluster make-subscriber -i 192.168.1.1 -p !alore -l`

reset-database Resets the local database and erases its configuration.

Syntax `cluster reset-database`

Returns `[appadmin]# cluster reset-database`

```
*****
* WARNING: Running this command will erase the Policy Man-
* ager
* configuration and leave the database with default
* configuration. You will lose all the configured data.
* Do not close the shell or interrupt this command
* execution.
*****
Continue? [y|Y]: y
```

set-cluster-passwd Changes the cluster password on all publisher nodes. Executed on the publisher; prompts for the new cluster password.

Syntax `cluster set-cluster-passwd`

Returns `[appadmin]# cluster set-cluster-passwd`

```
cluster set-cluster-passwd
Enter Cluster Passwd: santaclara
Re-enter Cluster Passwd: santaclara
INFO - Password changed on local (publisher) node
Cluster password changed
```

set-local-passwd Changes the local password. Executed locally; prompts for the new local password.

Syntax `cluster sync-local-password`

Returns `[appadmin]# cluster set-local-password`

```
cluster sync-local-passwd
Enter Password: !alore
Re-enter Password: !alore
```

Configure Commands

The Policy Manager command line interface includes the following *configuration* commands:

- “date” (page 296)
- “dns” (page 296)
- “hostname” (page 297)
- “ip” (page 297)
- “timezone” (page 297)

date

Sets *System Date, Time* and *Time Zone*.

Syntax `configure date -d <date> [-t <time>] [-z <timezone>]`
 or
`configure date -s <ntpserver> [-z <timezone>]`
 where:

Flag/Parameter	Description
-s <ntpserver>	Optional. Synchronize time with specified NTP server.
-d <date>	Required. <i>Syntax:</i> yyyy-mm-dd
-t <time>	Optional. <i>Syntax:</i> hh:mm:ss
-z <timezone>	Optional. <i>Syntax:</i> To view the list of supported timezone values, enter: <code>show all-timezones</code> .

Example 1 Specify date/time/timezone:

```
[appadmin]# configure date -d 2007-06-22 -t 12:00:31 -z America/Los_Angeles
```

Example 2 Synchronize with a specified NTP server:

```
[appadmin]# -s <ntpserver>
```

dns

Configure DNS servers. At least one DNS server must be specified; a maximum of three DNS servers can be specified.

Syntax `configure dns <primary> [secondary] [tertiary]`

Example 1 `[appadmin]# configure dns 192.168.1.1`

Example 2 `[appadmin]# configure dns 192.168.1.1 192.168.1.2`

Example 3 `[appadmin]# configure dns 192.168.1.1 192.168.1.2 192.168.1.3`

hostname	Configures the hostname.								
Syntax	<code>configure hostname <hostname></code>								
Example	<code>[appadmin]# configure hostname sun.us.arubanetworks.com</code>								
ip	Configures IP address, netmask and gateway.								
Syntax	<code>configure ip <mgmt data> <ipaddress> netmask <netmask address> gateway <gateway address></code> where: <table><tr><th>Flag/Parameter</th><th>Description</th></tr><tr><td><code>ip <mgmt data> <ip address></code></td><td><ul style="list-style-type: none">• Network interface type: <i>mgmt</i> or <i>data</i>• Server ip address.</td></tr><tr><td><code>netmask <netmask address></code></td><td>Netmask address.</td></tr><tr><td><code>gateway <gateway address></code></td><td>Gateway address.</td></tr></table>	Flag/Parameter	Description	<code>ip <mgmt data> <ip address></code>	<ul style="list-style-type: none">• Network interface type: <i>mgmt</i> or <i>data</i>• Server ip address.	<code>netmask <netmask address></code>	Netmask address.	<code>gateway <gateway address></code>	Gateway address.
Flag/Parameter	Description								
<code>ip <mgmt data> <ip address></code>	<ul style="list-style-type: none">• Network interface type: <i>mgmt</i> or <i>data</i>• Server ip address.								
<code>netmask <netmask address></code>	Netmask address.								
<code>gateway <gateway address></code>	Gateway address.								
Example	<code>[appadmin]# configure ip data 192.168.5.12 netmask 255.255.255.0 gateway 192.168.5.1</code>								

timezone	Configures time zone interactively.
Syntax	<code>configure timezone</code>
Example	<code>[appadmin]# configure timezone</code> <code>configure timezone</code> ***** * WARNING: When the command is completed Policy Manager services * * are restarted to reflect the changes. * ***** Continue? [y Y]: y

Network Commands

The Policy Manager command line interface includes the following *network* commands:

- “ip” (page 298)
- “nslookup” (page 299)

- “ping” (page 299)
- “reset” (page 299)
- “traceroute” (page 300)

ip

Add, delete or list custom routes to the data or management interface routing table.

Syntax `network ip add <mgmt|data> [-i <id>] [<-s <SrcAddr>] [<-d <DestAddr>]>`

Add a custom routing rule.

where:

Flag/Parameter	Description
<mgmt data>	Specify management or data interface
-i <id>	id of the network ip rule. If unspecified, the system will auto-generate an id. Note that the id determines the priority in the ordered list of rules in the routing table.
-s <SrcAddr>	Optional. Specifies the ip address or network (for example, 192.168.5.0/24) or 0/0 (for all traffic) of traffic originator. Only one of SrcAddr or DstAddr must be specified.
-d <DestAddr>	Optional. Specifies the destination ip address or network (for example, 192.168.5.0/24) or 0/0 (for all traffic). Only one of SrcAddr or DstAddr must be specified.

Syntax `network ip del <-i <id>>`

Delete a rule.

where:

Flag/Parameter	Description
-i <id>	Id of the rule to delete.

Syntax `network ip list`

List all routing rules.

Syntax `network ip reset`

Reset routing table to factory default setting. All custom routes are removed.

Example 1 `[appadmin]# network ip add data -s 192.168.5.0/24`

Example 2 `[appadmin]# network ip add data -s 192.168.5.12`

Example 3 `[appadmin]# network ip list`

nslookup

Returns IP address of host using DNS.

Syntax `nslookup -q <record-type> <host>`

where:

Flag/Parameter	Description
<record-type>	Type of DNS record. For example, A, CNAME, PTR
<host>	Host or domain name to be queried.

Example 1 `[appadmin]# nslookup sun.us.arubanetworks.com`

Example 2 `[appadmin]# nslookup -q SRV arubanetworks.com`

ping

Tests reachability of the network host.

Syntax `network ping [-i <SrcIpAddr>] [-t] <host>`

where:

Flag/Parameter	Description
-i <SrcIpAddr>	Optional. Originating IP address for ping.
-t	Optional. Ping indefinitely.
<host>	Host to be pinged.

Example `[appadmin]# network ping -i 192.168.5.10 -t sun.us.arubanetworks.com`

reset

Reset network data port.

Syntax `network reset <port>`

where:

Flag/Parameter	Description
<port>	Required. Name of network port to reset.

Example `[appadmin]# network reset data`

traceroute

Prints route taken to reach network host.

Syntax `network traceroute <host>`

where:

Flag/Parameter	Description
<host>	Name of network host.

Example `[appadmin]# network traceroute sun.us.arubanetworks.com`

Service commands

The Policy Manager command line interface includes the following *service* commands:

- start
- stop
- status
- restart
- activate
- deactivate
- list

These commands in this section have identical syntax; therefore, this section presents them as variations on <action>.

<action>

Activates the specified Policy Manager service.

Syntax `service <action> <service-name>`

where:

Flag/Parameter	Description
action	Choose an action: <i>activate</i> , <i>deactivate</i> , <i>list</i> , <i>restart</i> , <i>start</i> , <i>status</i> , or <i>stop</i> .
service-name	Choose a service: <i>tips-policy-server</i> , <i>tips-admin-server</i> , <i>tips-system-auxiliary-server</i> , <i>tips-radius-server</i> , <i>tips-tacacs-server</i> , <i>tips-dbwrite-server</i> , <i>tips-repl-server</i> , or <i>tips-sysmon-server</i> .

Example 1 `[appadmin]# service activate tips-policy-server`

Example 2 `[appadmin]# service list all`
`service list`
Policy server [tips-policy-server]
Admin UI service [tips-admin-server]
System auxiliary services [tips-system-auxiliary-server]
Radius server [tips-radius-server]
Tacacs server [tips-tacacs-server]
Async DB write service [tips-dbwrite-server]
DB replication service [tips-repl-server]
System monitor service [tips-sysmon-server]

Example 3 `[appadmin]# service status tips-domain-server`

Show Commands

The Policy Manager command line interface includes the following *show* commands:

- “all-timezones” (page 301)
- “date” (page 301)
- “dns” (page 302)
- “domain” (page 302)
- “hostname” (page 302)
- “ip” (page 302)
- “license” (page 303)
- “timezone” (page 303)
- “version” (page 303)

<hr/>	
all-timezones	Interactively displays all available timezones
Syntax	show all-timezones
Example	<code>[appadmin]# show all-timezones</code> Africa/Abidjan Africa/Accra WET Zulu
<hr/>	
date	Displays <i>System Date</i> , <i>Time</i> , and <i>Time Zone</i> information.
Syntax	show date
Example	<code>[appadmin]# show date</code> Wed Jul 30 14:33:39 UTC 2008

dns Displays DNS servers.

Syntax show dns

Example [appadmin]# **show dns**
 show dns
 =====
 DNS Information

 Primary DNS : 192.168.5.3
 Secondary DNS : <not configured>
 Tertiary DNS : <not configured>
 =====

domain Displays *Domain Name*, *IP Address*, and *Name Server* information.

Syntax show domain

Example [appadmin]# **show domain**

hostname Displays hostname.

Syntax show hostname

Example [appadmin]# **show hostname**
 show hostname
 wolf

ip Displays IP and DNS information for the host.

Syntax show ip

Example [appadmin]# **show ip**
 show ip
 =====
 Device Type : Management Port

 IP Address : 192.168.5.227
 Subnet Mask : 255.255.255.0
 Gateway : 192.168.5.1
 =====
 Device Type : Data Port

 IP Address : <not configured>
 Subnet Mask : <not configured>
 Gateway : <not configured>
 =====
 DNS Information

 Primary DNS : 192.168.5.3
 Secondary DNS : <not configured>
 Tertiary DNS : <not configured>
 =====

license	Displays the license key.
Syntax	show license
Example	<pre>[appadmin]# show license show license</pre>
timezone	Displays current system timezone.
Syntax	show timezone
Example	<pre>[appadmin]# show timezone show timezone</pre>
version	Displays Policy Manager software version hardware model.
Syntax	show version
Example	<pre>[appadmin]# show version ===== Policy Manager software version : 2.0(1).6649 Policy Manager model number : ET-5010 =====</pre>

System commands

The Policy Manager command line interface includes the following *system* commands:

- “boot-image” (page 303)
- “gen-support-key” (page 304)
- “install-license” (page 304)
- “restart” (page 304)
- “shutdown” (page 305)
- “update” (page 305)
- “upgrade” (page 305)

boot-image	Sets system boot image control options.
Syntax	<pre>system boot-image [-l] [-a <version>]</pre> where:

Flag/Parameter	Description
-l	Optional. List boot images installed on the system.
-a <version>	Optional. Set active boot image version, in <i>A.B.C.D</i> syntax.

Example `[appadmin]# system boot-image`

gen-support-key Generates the support key for the system.

Syntax `system gen-support-key`

Example `[appadmin]# system gen-support-key`
`system gen-support-key`
`Support key='01U2FsdGVkX1+/WS9jZKQajERyzXhM8mF6zAKrzxrHvaM='`

install-license Replace the current license key with a new one.

Syntax `system install-license <license-key>`
where:

Flag/Parameter	Description
<license-key>	Mandatory. This is the newly issued license key.

Example `[appadmin]# system install-license`

restart Restart the system

Syntax `system restart`

Example `[appadmin]# system restart`
`system restart`

```
*****
* WARNING: This command will shutdown all applications *
* and reboot the system                                *
*****
Are you sure you want to continue? [y|Y]: y
```

shutdown Shutdown the system

Syntax system shutdown

Example [appadmin]# **system shutdown**

```
*****
* WARNING: This command will shutdown all applications *
* and power off the system                               *
*****
Are you sure you want to continue? [y|Y]: y
```

update Manages updates.

Syntax system update [-i user@hostname:/<filename> | http://hostname/<filename>]
system update [-u <patch-name>]
system update [-l]

where:

Flag/Parameter	Description
-i user@hostname:/<filename> http://hostname/<filename>	Optional. Install the specified patch on the system.
-u <patch-name>	Optional. Uninstall the patch. (For exact patch names, refer to [-l] in this table.)
-l	Optional. List the patches installed on the system.

Example [appadmin]# **system update**

upgrade Upgrades the system.

Syntax system upgrade <filepath>

where:

Flag/Parameter	Description
<filepath>	Required. Enter filepath, using either syntax provided in the two examples provided.

Example 1 [appadmin]# **system upgrade admin@sun.us.arubanetworks.com:/tmp/PolicyManager-x86-64-upgrade-71.tgz**

Example 2 [appadmin]# **system upgrade http://sun.us.arubanetworks.com/downloads/PolicyManager-x86-64-upgrade-71.tgz**

Miscellaneous Commands

The Policy Manager command line interface includes the following *miscellaneous* commands:

- “ad auth” (page 306)
- “ad netjoin” (page 306)
- “ad netleave” (page 307)
- “ad testjoin” (page 307)
- “alias” (page 307)
- “backup” (page 307)
- “dump certchain” (page 308)
- “dump logs” (page 308)
- “dump servercert” (page 309)
- “exit” (page 309)
- “help” (page 309)
- “krb auth” (page 309)
- “krb list” (page 310)
- “ldapsearch” (page 310)
- “quit” (page 311)
- “restore” (page 310)

ad auth

Authenticate the user against AD.

Syntax `ad auth --username=<username>`
 where:

Flag/Parameter	Description
<username>	Required. username of the authenticating user.

Example `[appadmin]# ad auth --username=mike`

ad netjoin

Joins host to the domain.

Syntax `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.

Example `[appadmin]# ad netjoin atlas.us.arubanetworks.com`

ad netleave Removes host from the domain.

Syntax `ad netleave`

Example `[appadmin]# ad netleave`

ad testjoin Tests if the netjoin command succeeded. Tests if Policy Manager is a member of the AD domain.

Syntax `ad testjoin`

Example `[appadmin]# ad testjoin`

alias Creates or removes aliases.

Syntax `alias <name>=<command>`
where:

Flag/Parameter	Description
<name>=<command>	Sets <name> as the alias for <command>.
<name>=	Removes the association.

Example 1 `[appadmin]# alias sh=show`

Example 2 `[appadmin]# alias sh=`

backup Creates backup of Policy Manager configuration data. If no arguments are entered, the system auto-generates a filename and backups up the configuration to this file.

Syntax `backup [-f <filename>] [-L] [-P]`
where:

Flag/Parameter	Description
-f <filename>	Optional. Backup target. If not specified, Policy Manager will auto-generate a filename.

Flag/Parameter	Description
-L	Optional. Do not backup the log database configuration
-P	Optional. Do not backup password fields from the configuration database

Example `[appadmin]# backup -f PolicyManager-data.tar.gz`
`Continue? [y|Y]: y`

dump certchain Dumps certificate chain of any SSL secured server.

Syntax `dump certchain <hostname:port-number>`
 where:

Flag/Parameter	Description
<hostname:port-number>	Specifies the hostname and SSL port number.

Example 1 `[appadmin]# dump certchain ldap.acme.com:636`
`dump certchain`

dump logs Dumps Policy Manager application log files.

Syntax `dump logs -f <output-file-name> [-s yyyy-mm-dd] [-e yyyy-mm-dd]`
`[-n <days>] [-t <log-type>] [-h]`
 where:

Flag/Parameter	Description
-f <output-file-name>	Specifies target for concatenated logs.
-s yyyy-mm-dd	Optional. Date range start (default is today).
-e yyyy-mm-dd	Optional. Date range end (default is today).
-n <days>	Optional. Duration in days (from today).
-t <log-type>	Optional. Type of log to collect.
-h	Specify (print help) for available log types.

Example 1 `[appadmin]# dump logs -f tips-system-logs.tgz -s 2007-10-06 -e 2007-10-17 -t SystemLogs`

Example 2 `[appadmin]# dump logs -h`

dump servercert Dumps server certificate of SSL secured server.

Syntax `dump servercert <hostname:port-number>`
 where:

Flag/Parameter	Description
<hostname:port-number>	Specifies the hostname and SSL port number.

Example 1 `[appadmin]# dump servercert ldap.acme.com:636`

exit Exits shell.

Syntax `exit`

Example `[appadmin]# exit`

help Display the list of supported commands

Syntax `help <command>`

Example `[appadmin]# help`

<code>help</code>	
<code>alias</code>	Create aliases
<code>backup</code>	Backup Policy Manager data
<code>cluster</code>	Policy Manager cluster related commands
<code>configure</code>	Configure the system parameters
<code>dump</code>	Dump Policy Manager information
<code>exit</code>	Exit the shell
<code>help</code>	Display the list of supported commands
<code>netjoin</code>	Join host to the domain
<code>netleave</code>	Remove host from the domain
<code>network</code>	Network troubleshooting commands
<code>quit</code>	Exit the shell
<code>restore</code>	Restore Policy Manager database
<code>service</code>	Control Policy Manager services
<code>show</code>	Show configuration details
<code>system</code>	System commands

krb auth Does a kerberos authentication against a kerberos server (such as Microsoft AD)

Syntax `krb auth <user@domain>`
 where:

Flag/Parameter	Description
<user@domain>	Specifies the username and domain.

Example `[appadmin]# krb auth mike@corp-ad.acme.com`

krb list Lists the cached kerberos tickets

Syntax `krb list`

Example `[appadmin]# krb list`

ldapsearch The Linux ldapsearch command to find objects in an LDAP directory. (Note that only the Policy Manager-specific command line arguments are listed below. For other command line arguments, refer to ldapsearch man pages on the Internet).

Syntax `ldapsearch -B <user@hostname>`

where:

Flag/Parameter	Description
<user@hostname>	Specifies the username and the full qualified domain name of the host. The -B command finds the bind DN of the LDAP directory.

Example `[appadmin]# ldapsearch -B admin@corp-ad.acme.com`

restore Restores Policy Manager configuration data from the backup file

Syntax `restore user@hostname:/<backup-filename> [-l] [-i] [-c|-C] [-p] [-s]`

where:

Flag/Parameter	Description
user@hostname:/<backup-filename>	Specify filepath of restore source.
-c	Restore configuration database (default).
-C	Do not restore configuration database.
-l	Optional. If it exists in the backup, restore log database.
-i	Optional. Ignore version mismatch errors and proceed.
-p	Optional. Force restore from a backup file that does not have password fields present.
-s	Optional. Restore cluster server/node entries from the backup. (Node entries disabled on restore.)

Example `[appadmin]# restore user@hostname:/tmp/tips-backup.tgz -l -i -c -s`

quit	Exits shell.
Syntax	<code>quit</code>
Example	<code>[appadmin]# quit</code>

VM-Only Commands

The command line interface for VM edition of Policy Manager supports the following *VM-Only* commands:

- “[configure vmhost](#)” (page 311)
- “[show vmhost](#)” (page 311)

configure vmhost	Configure VM host details and the credentials required to access the service console commands. This information is required to activate the Policy Manager VM.						
Syntax	<code>configure vmhost -s <server-name> -u <username></code> where: <table> <tr> <th>Flag/Parameter</th><th>Description</th></tr> <tr> <td><code><server-name></code></td><td>Required. VM host server name.</td></tr> <tr> <td><code><username></code></td><td>Required. VM host service console username.</td></tr> </table>	Flag/Parameter	Description	<code><server-name></code>	Required. VM host server name.	<code><username></code>	Required. VM host service console username.
Flag/Parameter	Description						
<code><server-name></code>	Required. VM host server name.						
<code><username></code>	Required. VM host service console username.						
Example	<code>[appadmin]# configure vmhost -s esx40-srv1.us.arubanet-works.com -u root</code>						

show vmhost	Shows configured VM host information, including connection status.
Syntax	<code>show vmhost</code>
Example	<pre>[appadmin]# show vmhost ----- Server address : esx40-srv1.us.arubanetworks.com Username : root Password : ***** Connection status : Connection successful =====</pre>

Appendix B: Rules Editing & Namepsaces

In the Policy Manager administration User Interface (UI) you use the same editing interface to create different types of objects:

- Service rules
- Role mapping policies
- Internal ure policies
- Enforcement policies
- Enforcement profiles
- Post-audit rules
- Proxy attribute pruning rules
- Filters for Access Tracker and activity reports
- Attributes editing for policy simulation

When editing all these elements, you are presented with a tabular interface with the same column headers:

- *Type* - Type is the namespace from which these attributes are defined. This is a drop-down list that contains namespaces defined in the system for the current editing context.
- *Name* - Name is the name of the attribute. This is a drop-down list with the names of the attributes present in the namespace.
- *Operator* - Operator is a list of operators appropriate for the data type of the attribute. The drop-down menu shows the operators appropriate for data type on the left (that is, the attribute).
- *Value* - The value is the value of the attribute. Again, depending on the data type of the attribute, the value field can be a free-form one-line edit box, a free-form multi-line edit box, a drop-down menu containing pre-defined values (enumerated types), or a time or date widget.

In some editing interfaces (for example, enforcement profile and policy simulation attribute editing interfaces) the operator does not change; it is always the EQUALS operator.

Providing a uniform tabular interface to edit all these elements enables you to use the same steps while configuring these elements. Also, providing a context-sensitive editing experience (for names, operators and values) takes the guess-work out of configuring these elements.

The following sections describe namespaces and operators in more detail.

Namespaces

There are multiple namespaces exposed in the rules editing interface. The namespaces exposed depend upon what you are editing. For example, when you are editing posture policies you work with the posture namespace; when you are editing service rules you work with, among other namespaces, the RADIUS namespace, but not the posture namespace.

Enumerated below are the namespaces you will find in the different rules editing contexts:

- *RADIUS Namespace* - Dictionaries in the RADIUS namespace come pre-packaged with the product. The administration interface does provide a way to add new dictionaries into the system (See [“RADIUS Dictionaries” \(page 279\)](#) for more information). RADIUS namespace has the notation RADIUS:Vendor, where Vendor is the name of the Company that has defined attributes in the dictionary. Sometimes, the same vendor has multiple dictionaries, in which case the "Vendor" portion has the name suffixed by the name of device or some other unique string. IETF is a special vendor for the dictionary that holds the attributes defined in the RFC 2865 and other associated RFCs. Policy Manager comes pre-packaged with a number of vendor dictionaries. Some examples of dictionaries in the RADIUS namespace are: RADIUS:IETF, RADIUS:Cisco, RADIUS:Juniper.

RADIUS namespace appears in the following editing contexts:

- Service rules: All RADIUS namespace attributes that can appear in a request (the ones marked with the IN or INOUT qualifier)
- RADIUS Enforcement profiles: All RADIUS namespace attributes that can be send back to a RADIUS client (the ones marked with the OUT or INOUT qualifier)
- Role mapping policies
- Policy simulation attributes
- Post-proxy attribute pruning rules
- Filter rules for Access Tracker and Activity Reports
- *Posture Namespace* - Dictionaries in the posture namespace come pre-packaged with the product. The administration interface does provide a way to add new dictionaries into the system (See [“Posture Dictionaries” \(page 280\)](#) for more information). Posture namespace has the notation Vendor:Application, where Vendor is the name of the Company that has defined attributes in the dictionary, and Application is the name of the application for which the attributes have been defined. The same vendor typically has different dictionaries for different applications. Some examples of dictionaries in the posture namespace are: Avenda:LinuxSHV, Microsoft:SystemSHV, Microsoft:WindowsSHV Trend:AV

Posture namespace appears in the following editing contexts:

- Internal posture policies conditions - Attributes marked with the IN qualifier
- Internal posture policies actions - Attributes marked with the OUT qualifier
- Policy simulation attributes
- Filter rules for Access Tracker and Activity Reports
- *Authorization Namespaces* - Policy Manager supports a number of types of authorization sources. Authorization sources from which values of attributes can be retrieved to create role mapping rules have their own separate namespaces (prefixed with *Authorization:*). They are:
 - *Authorization* - The authorization namespace has one attribute: sources. The values are prepopulated with the authorization sources defined in Policy Manager. Use this to check for the authorization source(s) from which attributes were extracted for the authenticating entity.
 - *AD Instance Namespace* - For each instance of an Active Directory authentication source, there is an AD instance namespace that appears in the rules editing interface. The AD instance namespace consists of all the attributes that were defined when the authentication source was created. These attribute names are pre-populated in the UI for administrative convenience. For Policy Manager to fetch the values of attributes from Active Directory, you need to define filters for that authentication source (see [“Adding and Modifying Authentication Sources”](#) (page 119) for more information).
 - *LDAP Instance Namespace* - For each instance of an LDAP authentication source, there is an LDAP instance namespace that appears in the rules editing interface. The LDAP instance namespace consists of all the attributes that were defined when the authentication source was created. These attribute names are pre-populated in the UI for administrative convenience. For Policy Manager to fetch the values of attributes from an LDAP-compliant directory, you need to define filters for that authentication source (see [“Adding and Modifying Authentication Sources”](#) (page 119) for more information).
 - *SQL Instance Namespace* - For each instance of an SQL authentication source, there is an SQL instance namespace that appears in the rules editing interface. The SQL instance namespace consists of attributes names that you have defined when you created an instance of this authentication source. The attribute names are pre-populated for administrative convenience. For Policy Manager to fetch the values of attributes from a SQL-compliant database, you need to define filters for that authentication source.
 - *RSAToken Instance Namespace* - For each instance of an RSA Token Server authentication source, there is an RSA Token Server instance namespace that appears in the rules editing interface. The RSA Token Server instance namespace consists of attributes names that you have

defined when you created an instance of this authentication source. The attribute names are pre-polluted for administrative convenience.

- *Sources*- This is the list of the authorization sources from which attributes were fetched for role mapping.

Authorization namespaces appear in the following editing contexts:

- Role mapping policies
- *Date Namespace* - The date namespace has three pre-defined attributes defined: Time-of-Day, Day-of-Week and Date-of-Year. Depending on the attribute selected in the UI, the operator and value fields change. For Day-of-Week, the operators supported are BELONG_TO and NOT_BELONGS_TO, and the value field shows a multi-select list box with days from Monday through Sunday. The Time-of-Day attribute shows a time widget in the value field. The Date-of-Year attribute shows a date, month and year widget in the value field. The operators supported for Date-of-Year and Time-of-Day attributes are the similar to the ones supported for the integer data type (See Operators section for more details).

Date namespace appears in the following editing contexts:

- Service rules
- Role mapping policies
- Enforcement policies
- Filter rules for Access Tracker and Activity Reports
- *Connection Namespace* - The connection namespace can be used in role mapping policies to define roles based on where the protocol request originated from and where it terminated. The connection namespace has the following pre-defined attributes:

Attribute	Description
Src-IP-Address	Src-IP-Address and Src-Port are the IP address and port from which the request (RADIUS, TACACS+, etc.) originated
Src-Port	
Dest-IP-Address	Dst-IP-Address and Dst-Port are the IP address and port at which Policy Manager received the request (RADIUS, TACACS+, etc.)
Dest-Port	
Protocol	Request protocol: RADIUS, TACACS+, WebAuth
NAD-IP-Address	IP address of the network device from which the request originated
Client-Mac-Address	MAC address of the client

Client-Mac-Address-Colon, Client-Mac-Address-Dot, Client-Mac-Address-Hyphen, Client-Mac-Address-Nodelim	Client MAC address in different formats
Client-IP-Address	IP address of the client (if known)

Connection namespace appears in the following editing contexts:

- Service rules
- Role mapping policies
- *Authentication Namespace* - The authentication namespace can be used in role mapping policies to define roles based on what kind of authentication method was used or what the status of the authentication is. The attribute names and possible values with descriptions are shown in the table below:

Attribute Name	Values
InnerMethod	PAP CHAP MSCHAP EAP-GTC EAP-MSCHAPv2 EAP-MD5 EAP-TLS
OuterMethod	PAP CHAP MSCHAP EAP-MD5 EAP-TLS EAP-TTLS EAP-FAST EAP-PEAP
Phase1PAC	<i>None</i> - No PAC was used to establish the outer tunnel in the EAP-FAST authentication method <i>Tunnel</i> - A tunnel PAC was used to establish the outer tunnel in the EAP-FAST authentication method <i>Machine</i> - A machine PAC was used to establish the outer tunnel in the EAP-FAST authentication method; machine PAC is used for machine authentication (See “EAP-FAST” (page 108)).

Attribute Name	Values
Phase2PAC	<p><i>None</i> - No PAC was used instead of an inner method handshake in the EAP-FAST authentication method</p> <p><i>UserAuthPAC</i> - A user authentication PAC was used instead of the user authentication inner method handshake in the EAP-FAST authentication method</p> <p><i>PosturePAC</i> - A posture PAC was used instead of the posture credential handshake in the EAP-FAST authentication method</p>
Posture	<p><i>Capable</i> - The client is capable of providing posture credentials</p> <p><i>Collected</i> - Posture credentials were collected from the client</p> <p><i>Not-Capable</i> - The client is not capable of providing posture credentials</p> <p><i>Unknown</i> - It is not known whether the client is capable of providing credentials</p>
Status	<p><i>None</i> - No authentication took place</p> <p><i>User</i> - The user was authenticated</p> <p><i>Machine</i> - The machine was authenticated</p> <p><i>Failed</i> - Authentication failed</p> <p><i>AuthSource-Unreachable</i> - The authentication source was unreachable</p>
MacAuth	<p><i>NotApplicable</i> - Not a MAC Auth request</p> <p><i>Known Client</i> - Client MAC address was found in an authentication source</p> <p><i>Unknown Client</i> - Client MAC address was not found in an authentication source</p>
Username	The username as received from the client (after the strip user name rules are applied)
Full-Username	The username as received from the client (before the strip user name rules are applied)
Source	The name of the authentication source used to authenticate the user

Authentication namespace appears in the following editing contexts:

- Role mapping policies
- *Certificate Namespace* - The certificate namespace can be used in role mapping policies to define roles based on attributes in the client certificate presented by the end host. Client certificates are presented in mutually authenticated 802.1X EAP methods (EAP-TLS, PEAP/TLS, EAP-FAST/TLS). The attribute names and possible values with descriptions are shown in the table below:

Attribute Name	Values
Version	Certificate version
Serial-Number	Certificate serial number
Subject-DN, Subject-DC, Subject-UID, Subject-CN, Subject-GN, Subject-SN, Subject-C, Subject-L, Subject-ST, Subject-O, Subject-OU, Subject-emailAddress	Attributes associated with the subject (user or machine, in this case). Not all of these fields are populated in a certificate.
Issuer-DN, Issuer-DC, Issuer-UID, Issuer-CN, Issuer-GN, Issuer-SN, Issuer-C, Issuer-L, Issuer-ST, Issuer-O, Issuer-OU, Issuer-emailAddress	Attributes associated with the issuer (Certificate Authorities or the enterprise CA). Not all of these fields are populated in a certificate.
Subject-AltName-Email, Subject-AltName-DNS, Subject-AltName-URI, Subject-AltName-DirName, Subject-AltName-IPAddress, Subject-AltName-RegisteredID, Subject-AltName-msUPN	Attributes associated with the subject (user or machine, in this case) alternate name. Not all of these fields are populated in a certificate.

Certificate namespace appears in the following editing contexts:

- Role mapping policies
- *Tips Namespace* - Tips namespace has two pre-defined attributes: Role and Posture. Values are assigned to these attributes at run-time after Policy Manager evaluates role mapping and posture related policies. The value for the Role attribute is a set of roles assigned by the either the role mapping policy or the post-audit policy. The value value of the Role attribute can also be a dynamically fetched “Enable as role” attribute from the authorization source. The value for the Posture attribute is one of HEALTHY, CHECKUP, TRANSITION, QUARANTINE, INFECTED or UNKNOWN. The posture value is computed after Policy Manager evaluates internal posture policies, gets posture status from posture servers or audit servers.

Tips namespace appears in the following editing contexts:

- Enforcement policies
- *Host Namespace* - Host namespace has a number of pre-defined attributes: Name, OStype, FQDN, UserAgent, CheckType, UniqueID, AgentType and InstalledSHAs. Host:Name, Host:OStype, Host:FQDN, Host:AgentType, Host:InstalledSHAs are only populated when request is originated by a Microsot NAP-compatible agent. UserAgent and CheckType are present when Policy Manager acts as a Web authentication portal.
- *Endpoint Namespace* - Endpoint namespace has the following attributes: Disabled By, Disabled Reason, Enabled By, Enabled Reason, Info URL. Use

these attributes look for attributes of authenticating endpoints (present in the Policy Manager endpoints list).

- *Device Namespace* - Device namespace has the attributes associated with the network device that originated the request. Device namespace has four pre-defined attributes: Location, OS-Version, Device-Type and Device-Vendor. Custom attributes also appear in the attribute list if they are defined as custom tags for the device. Note that these attributes can be used only if you have pre-populated the values for these attributes when a network device is configured in Policy Manager.
- *LocalUser Namespace* - LocalUser namespace has the attributes associated with the local user (resident in the Policy Manager local user database) who authenticated in this session. As the name suggests, this namespace is only applicable if a local user authenticated. LocalUser namespace has four pre-defined attributes: Phone, Email, Sponsor and Designation. Custom attributes also appear in the attribute list if they are defined as custom tags for the local user. Note that these attributes can be used only if you have pre-populated the values for these attributes when a local user is configured in Policy Manager.
- *GuestUser Namespace* - GuestUser namespace has the attributes associated with the guest user (resident in the Policy Manager guest user database) who authenticated in this session. As the name suggests, this namespace is only applicable if a guest user authenticated. GuestUser namespace has six pre-defined attributes: Company-Name, Location, Phone, Email, Sponsor and Designation. Custom attributes also appear in the attribute list if they are defined as custom tags for the guest user. Note that these attributes can be used only if you have pre-populated the values for these attributes when a guest user is configured in Policy Manager.
- *Audit Namespace* - Dictionaries in the audit namespace come pre-packaged with the product. Audit namespace has the notation Vendor:Audit, where Vendor is the name of the Company that has defined attributes in the dictionary. An example of a dictionary in the audit namespace is: Avenda Systems:Audit or Qualys:Audit.
 - Audit namespace appears when editing post-audit rules (See [“Built-In Audit Servers”](#) (page 194) for more information)
 - Avenda Systems:Audit namespace appears when editing post-audit rules for NESSUS and NMAP audit servers. The attribute names and possible values with descriptions are shown in the table below:

Attribute Name	Values
Audit-Status	AUDIT_SUCCESS, AUDIT_INPROGRESS or AUDIT_ERROR
Device-Type	Type of device returned by an NMAP port scan
Output-Msgs	The output message returned by Nessus plugin after a vulnerability scan

Attribute Name	Values
Network-Apps	String representation of the open network ports (http, telnet, etc.)
Mac-Vendor	Vendor associated with MAC address of the host
OS-Info	OS information string returned by NMAP
Open-Ports	The port numbers of open applications on the host

- *Tacacs Namespace* - Tacacs namespace has the attributes associated with attributes available in a TACACS+ request. Available attributes are AvendaAVPair, UserName and AuthSource.
- *Application Namespace* - Application namespace has a name attribute. This attribute is an enumerated type currently containing the following string values: GuestConnect, Insight, Edge..

Variables

Variables are populated with the connection-specific values. Variable names (prefixed with % and enclosed in curly braces; for example, %{Username}”) can be used in filters, role mapping, enforcement rules and enforcement profiles. Policy Manager does in-place substitution of the value of the variable during runtime rule evaluation. The following built-in variables are supported in Policy Manager:

Variable	Description
%{attribute-name}	<i>attribute-name</i> is the alias name for an attribute that you have configured to be retrieved from an authentication source. See “Adding and Modifying Authentication Sources” (page 119).
%{RADIUS:IETF:MAC-Address-Colon}	MAC address of client in aa:bb:cc:dd:ee:ff format
%{RADIUS:IETF:MAC-Address-Hyphen}	MAC address of client in aa-bb-cc-dd-ee-ff format
%{RADIUS:IETF:MAC-Address-Dot}	MAC address of client in aabb.ccdd.eeff format
%{RADIUS:IETF:MAC-Address-NoDelim}	MAC address of client in aabbccddeeff format

Note that you can also use any other dictionary-based attributes (or namespace attributes defined in this chapter) as variables in role mapping rules, enforcement rules, enforcement profiles and LDAP or SQL filters. For example, you can use %{RADIUS:IETF:Calling-Station-ID} or %{RADIUS:Airespace:Airespace-Wlan-Id} in rules or filters.

Operators

The rules editing interface in Policy Manager supports a rich set of operators. The type of operators presented in the UI is based on the data type of the attribute for which the operator is being used. Wherever the data type of the attribute is not known, the UI treats that attribute as a string type. The following table lists the operators presented for common attribute data types:

Attribute Type	Operators
String	EQUALS, NOT_EQUALS, CONTAINS, NOT_CONTAINS, BEGINS_WITH, NOT_BEGINS_WITH, ENDS_WITH, NOT_ENDS_WITH, BELONGS_TO, NOT_BELONGS_TO, EQUALS_IGNORE_CASE, NOT_EQUALS_IGNORE_CASE, MATCHES_REGEX, NOT_MATCHES_REGEX, EXISTS, NOT_EXISTS
Integer	EQUALS, NOT_EQUALS, GREATER_THAN, GREATER_THAN_OR_EQUALS, LESS_THAN, LESS_THAN_OR_EQUALS, EXISTS, NOT_EXISTS, BELONGS_TO, NOT_BELONGS_TO
Time or Date	EQUALS, NOT_EQUALS, GREATER_THAN, GREATER_THAN_OR_EQUALS, LESS_THAN, LESS_THAN_OR_EQUALS, IN_RANGE
Day	BELONGS_TO, NOT_BELONGS_TO
List (Example: Role)	EQUALS, NOT_EQUALS, MATCHES_ANY, NOT_MATCHES_ANY, MATCHES_ALL, NOT_MATCHES_ALL, MATCHES_EXACT, NOT_MATCHES_EXACT
Group (Example: Calling-Station-Id, NAS-IP-Address)	BELONGS_TO_GROUP, NOT_BELONGS_TO_GROUP, and all string data types

The following table describes all the operator types:

Operator	Description
EQUALS	True if the run-time value of the attribute matches the configured value. For string data type, this is a case-sensitive comparison. E.g., <code>RADIUS:IETF:NAS-Identifier EQUALS "SJ-VPN-DEVICE"</code>

Operator	Description
CONTAINS	<p>For string data type, true if the run-time value of the attribute is a substring of the configured value.</p> <p>E.g., <code>RADIUS:IETF:NAS-Identifier CONTAINS "VPN"</code></p>
BEGINS_WITH	<p>For string data type, true if the run-time value of the attribute begins with the configured value.</p> <p>E.g., <code>RADIUS:IETF:NAS-Identifier BEGINS_WITH "SJ-"</code></p>
ENDS_WITH	<p>For string data type, true if the run-time value of the attribute ends with the configured value.</p> <p>E.g., <code>RADIUS:IETF:NAS-Identifier ENDS_WITH "DEVICE"</code></p>
BELONGS_TO	<p>For string data type, true if the run-time value of the attribute matches a set of configured string values.</p> <p>E.g., <code>RADIUS:IETF:Service-Type BELONGS_TO Login-User, Framed-User, Authenticate-Only</code></p> <p>For integer data type, true if the run-time value of the attribute matches a set of configured integer values.</p> <p>E.g., <code>RADIUS:IETF:NAS-Port BELONGS_TO 1, 2, 3</code></p> <p>For day data type, true if run-time value of the attribute matches a set of configured days of the week.</p> <p>E.g., <code>Date:Day-of-Week BELONGS_TO MONDAY, TUESDAY, WEDNESDAY</code></p> <p>When Policy Manager is aware of the values that can be assigned to BELONGS_TO operator, it populates the value field with those values in a multi-select list box; you can select the appropriate values from the presented list. Otherwise, you must enter a comma separated list of values.</p>
EQUALS_IGNORE_CASE	<p>For string data type, true if the run-time value of the attribute matches the configured value, regardless of whether the string is upper case or lower case.</p> <p>E.g., <code>RADIUS:IETF:NAS-Identifier EQUALS_IGNORE_CASE "sj-vpn-device"</code></p>
MATCHES_REGEX	<p>For string data type, true if the run-time value of the attribute matches the regular expression in the configured value.</p> <p>E.g., <code>RADIUS:IETF:NAS-Identifier MATCHES_REGEX sj-device[1-9]-dev*</code></p>
EXISTS	<p>For string data type, true if the run-time value of the attribute exists. This is a unary operator.</p> <p>E.g., <code>RADIUS:IETF:NAS-Identifier EXISTS</code></p>
GREATER_THAN	<p>For integer, time and date data types, true if the run-time value of the attribute is greater than the configured value.</p> <p>E.g., <code>RADIUS:IETF:NAS-Port GREATER_THAN 10</code></p>

Operator	Description
GREATER_THAN_OR_EQUALS	For integer, time and date data types, true if the run-time value of the attribute is greater than or equal to the configured value. E.g., RADIUS:IETF:NAS-Port GREATER_THAN_OR_EQUALS 10
LESS_THAN	For integer, time and date data types, true if the run-time value of the attribute is less than the configured value. E.g., RADIUS:IETF:NAS-Port LESS_THAN 10
LESS_THAN_OR_EQUALS	For integer, time and date data types, true if the run-time value of the attribute is less than or equal to the configured value. E.g., RADIUS:IETF:NAS-Port LESS_THAN_OR_EQUALS 10
IN_RANGE	For time and date data types, true if the run-time value of the attribute is less than or equal to the first configured value and less than equal to the second configured value. E.g., Date:Date-of-Year IN_RANGE 2007-06-06,2007-06-12
MATCHES_ANY	For list data types, true if any of the run-time values in the list matches one of the configured values. E.g., Tips:Role MATCHES_ANY HR,ENG,FINANCE
MATCHES_ALL	For list data types, true if all of the run-time values in the list are found in the configured values. E.g., Tips:Role MATCHES_ALL HR,ENG,FINANCE. In this example, if the run-time values of Tips:Role are HR,ENG,FINANCE,MGR,ACCT the condition evaluates to true.
MATCHES_EXACT	For list data types, true if all of the run-time values of the attribute match all of the configured values. E.g., Tips:Role MATCHES_ALL HR,ENG,FINANCE. In this example, if the run-time values of Tips:Role are HR,ENG,FINANCE,MGR,ACCT the condition evaluates to false, because there are some values in the configured values that are not present in the run-time values.
BELONGS_TO_GROUP	For group data types, true if the run-time value of the attribute belongs to the configured group (either a static host list or a network device group, depending on the attribute). E.g., RADIUS:IETF:Calling-Station-Id BELONGS_TO_GROUP Printers.

Appendix C: **Software Copyright and License Statements**

This appendix lists the copyright notices for the binary distribution from Aruba Networks. A copy of the source code is available for portions of the software whose copyright statement requires Aruba Networks to publish any modified source code. To cover the costs of duplication and shipping, there is a nominal cost to obtain the source code material. To obtain a copy of the source code, contact info@arubanetworks.com.

Copyright statements for portions of software are listed below.

Postgres Copyright

PostgreSQL is Copyright © 2004-2010 by the PostgreSQL Global Development Group and is distributed under the terms of the license of the University of California below.

Permission to use, copy, modify, and distribute this software and its documentation for any purpose, without fee, and without a written agreement is hereby granted, provided that the above copyright notice and this paragraph and the following two paragraphs appear in all copies.

IN NO EVENT SHALL THE UNIVERSITY OF CALIFORNIA BE LIABLE TO ANY PARTY FOR DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, INCLUDING LOST PROFITS, ARISING OUT OF THE USE OF THIS SOFTWARE AND ITS DOCUMENTATION, EVEN IF THE UNIVERSITY OF CALIFORNIA HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

THE UNIVERSITY OF CALIFORNIA SPECIFICALLY DISCLAIMS ANY WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE SOFTWARE PROVIDED HEREUNDER IS ON AN "AS-IS" BASIS, AND THE UNIVERSITY OF CALIFORNIA HAS NO OBLIGATIONS TO PROVIDE MAINTENANCE, SUPPORT, UPDATES, ENHANCEMENTS, OR MODIFICATIONS.

GNU LGPL

Version 2, June 1991

Copyright (C) 1991 Free Software Foundation, Inc.

51 Franklin St, Fifth Floor, Boston, MA 02110-1301, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

[This is the first released version of the library GPL. It is numbered 2 because it goes with version 2 of the ordinary GPL.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Library General Public License, applies to some specially designated Free Software Foundation software, and to any other libraries whose authors decide to use it. You can use it for your libraries, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library, or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link a program with the library, you must provide complete object files to the recipients so that they can relink them with the library, after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

Our method of protecting your rights has two steps: (1) copyright the library, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the library.

Also, for each distributor's protection, we want to make certain that everyone understands that there is no warranty for this free library. If the library is modified by someone else and passed on, we want its recipients to know that what they have is not the original version, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that companies distributing free software will individually

obtain patent licenses, thus in effect transforming the program into proprietary software. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License, which was designed for utility programs. This license, the GNU Library General Public License, applies to certain designated libraries. This license is quite different from the ordinary one; be sure to read it in full, and don't assume that anything in it is the same as in the ordinary license.

The reason we have a separate public license for some libraries is that they blur the distinction we usually make between modifying or adding to a program and simply using it. Linking a program with a library, without changing the library, is in some sense simply using the library, and is analogous to running a utility program or application program. However, in a textual and legal sense, the linked executable is a combined work, a derivative of the original library, and the ordinary General Public License treats it as such.

Because of this blurred distinction, using the ordinary General Public License for libraries did not effectively promote software sharing, because most developers did not use the libraries. We concluded that weaker conditions might promote sharing better.

However, unrestricted linking of non-free programs would deprive the users of those programs of all benefit from the free status of the libraries themselves. This Library General Public License is intended to permit developers of non-free programs to use free libraries, while preserving your freedom as a user of such programs to change the free libraries that are incorporated in them. (We have not seen how to achieve this as regards changes in header files, but we have achieved it as regards changes in the actual functions of the Library.) The hope is that this will lead to faster development of free libraries.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, while the latter only works together with the library.

Note that it is possible for a library to be covered by the ordinary General Public License rather than by this special one.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Library General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

- a) The modified work must itself be a software library.
- b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.
- c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.
- d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table,

the facility still operates, and performs whatever part of its purpose remains meaningful. (For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also compile or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

- b) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.
- c) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.
- d) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

- a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.
- b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its

terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Library General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

GNU GPL

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we

have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

- a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
- b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.
- c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you

provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

- a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
- b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
- c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system

on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system

in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

Lighthttpd License

Copyright (c) 2004, Jan Kneschke, incremental

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of the 'incremental' nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHER-

WISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Apache License

Version 2.0, January 2004

<http://www.apache.org/licenses/>

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall

not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

1. You must give any other recipients of the Work or Derivative Works a copy of this License; and
2. You must cause any modified files to carry prominent notices stating that You changed the files; and

3. You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

4. If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any

Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

OpenSSL License

```
/*
=====

* Copyright (c) 1998-2007 The OpenSSL Project. All rights reserved.

*

* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
*
* 1. Redistributions of source code must retain the above copyright
* notice, this list of conditions and the following disclaimer.
*
* 2. Redistributions in binary form must reproduce the above copyright
* notice, this list of conditions and the following disclaimer in
* the documentation and/or other materials provided with the
```

- * distribution.
- *
- * 3. All advertising materials mentioning features or use of this
- * software must display the following acknowledgment:
- * "This product includes software developed by the OpenSSL Project
- * for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)"
- *
- * 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
- * endorse or promote products derived from this software without
- * prior written permission. For written permission, please contact
- * openssl-core@openssl.org.
- *
- * 5. Products derived from this software may not be called "OpenSSL"
- * nor may "OpenSSL" appear in their names without prior written
- * permission of the OpenSSL Project.
- *
- * 6. Redistributions of any form whatsoever must retain the following
- * acknowledgment:
- * "This product includes software developed by the OpenSSL Project
- * for use in the OpenSSL Toolkit (<http://www.openssl.org/>)"
- *
- * THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS"
- AND ANY
- * EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT
- LIMITED TO, THE
- * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS
- FOR A PARTICULAR

* PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR

* ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,

* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT

* NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;

* LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)

* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,

* STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)

* ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED

* OF THE POSSIBILITY OF SUCH DAMAGE.

*

=====

*

* This product includes cryptographic software written by Eric Young

* (eay@cryptsoft.com). This product includes software written by Tim

* Hudson (tjh@cryptsoft.com).

*

*/

Original SSLeay License

/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)

- * All rights reserved.
- *
- * This package is an SSL implementation written
- * by Eric Young (eay@cryptsoft.com).
- * The implementation was written so as to conform with Netscapes SSL.
- *
- * This library is free for commercial and non-commercial use as long as
- * the following conditions are aheared to. The following conditions
- * apply to all code found in this distribution, be it the RC4, RSA,
- * lhash, DES, etc., code; not just the SSL code. The SSL documentation
- * included with this distribution is covered by the same copyright terms
- * except that the holder is Tim Hudson (tjh@cryptsoft.com).
- *
- * Copyright remains Eric Young's, and as such any Copyright notices in
- * the code are not to be removed.
- * If this package is used in a product, Eric Young should be given attribution
- * as the author of the parts of the library used.
- * This can be in the form of a textual message at program startup or
- * in documentation (online or textual) provided with the package.
- *
- * Redistribution and use in source and binary forms, with or without
- * modification, are permitted provided that the following conditions
- * are met:
- * 1. Redistributions of source code must retain the copyright
- * notice, this list of conditions and the following disclaimer.

- * 2. Redistributions in binary form must reproduce the above copyright
- * notice, this list of conditions and the following disclaimer in the
- * documentation and/or other materials provided with the distribution.
- * 3. All advertising materials mentioning features or use of this software
- * must display the following acknowledgement:
- * "This product includes cryptographic software written by
- * Eric Young (eay@cryptsoft.com)"
- * The word 'cryptographic' can be left out if the routines from the library
- * being used are not cryptographic related :-).
- * 4. If you include any Windows specific code (or a derivative thereof) from
- * the apps directory (application code) you must include an acknowledgement:
- * "This product includes software written by Tim Hudson (tjh@crypt-
- * soft.com)"
- *
- * THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS" AND
- * ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT
- * LIMITED TO, THE
- * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS
- * FOR A PARTICULAR PURPOSE
- * ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CON-
- * TRIBUTORS BE LIABLE
- * FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEM-
- * PLARY, OR CONSEQUENTIAL
- * DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT
- * OF SUBSTITUTE GOODS
- * OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS
- * INTERRUPTION)
- * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY,
- * WHETHER IN CONTRACT, STRICT

* LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY

* OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF

* SUCH DAMAGE.

*

* The licence and distribution terms for any publically available version or

* derivative of this code cannot be changed. i.e. this code cannot simply be

* copied and put under another distribution licence

* [including the GNU Public Licence.] */

OpenLDAP License

The OpenLDAP Public License

Version 2.8, 17 August 2003

Redistribution and use of this software and associated documentation ("Software"), with or without modification, are permitted provided that the following conditions are met:

1. Redistributions in source form must retain copyright statements and notices,
2. Redistributions in binary form must reproduce applicable copyright statements and notices, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution, and
3. Redistributions must contain a verbatim copy of this document. The OpenLDAP Foundation may revise this license from time to time. Each revision is distinguished by a version number. You may use this Software under terms of this license revision or under the terms of any subsequent revision of the license.

THIS SOFTWARE IS PROVIDED BY THE OPENLDAP FOUNDATION AND ITS CONTRIBUTORS ``AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OPENLDAP FOUNDATION, ITS CONTRIBUTORS, OR THE AUTHOR(S) OR OWNER(S) OF THE SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PRO-

CUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The names of the authors and copyright holders must not be used in advertising or otherwise to promote the sale, use or other dealing in this Software without specific, written prior permission. Title to copyright in this Software shall at all times remain with copyright holders.

OpenLDAP is a registered trademark of the OpenLDAP Foundation. Copyright 1999-2003 The OpenLDAP Foundation, Redwood City, California, USA. All Rights Reserved. Permission to copy and distribute verbatim copies of this document is granted.

gSOAP Public License

Portions created by gSOAP are Copyright (C) 2001-2004 Robert A. van Engelen, Genivia inc. All Rights Reserved.

THE SOFTWARE IN THIS PRODUCT WAS IN PART PROVIDED BY GENIVIA INC AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE." 