

Dell Networking W-ClearPass Policy Manager 6.6



User Guide

Copyright Information

© Copyright 2016 Hewlett Packard Enterprise Development LP. Dell™, the DELL™ logo, and PowerConnect™ are trademarks of Dell Inc.

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

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

Open Source Code

This product includes code licensed under the GNU General Public License, the GNU Lesser General Public License, and/or certain other open source licenses.

About W-ClearPass Policy Manager	21
About the W-ClearPass Access Management System	21
About This Guide	21
Getting Started	21
W-ClearPass Access Management System Overview	22
Key Features	22
Advanced Policy Management	23
W-ClearPass Specifications	24
Accessing Configuration Information	29
Introduction	30
Start Here	30
Services	30
Authentication and Authorization	30
Identity	31
Posture	31
Enforcement	31
Network	31
Policy Simulation	31
Profile Settings	31
Importing and Exporting Information	32
Importing Information Into W-ClearPass	32
Exporting Information From W-ClearPass	33
Services	35
Services Architecture and Flow	35
Creating Service Templates	36
Creating Templates for W-ClearPass Services	36
Service Templates Provided	37
Services Supported for High Capacity Guest Mode	37
Viewing the List of Services	38
Viewing Existing Services	39
Adding and Removing Services	40
Reordering Services	43
802.1X Wired, 802.1X Wireless, and Dell 802.1X Wireless	45
Auto Sign-On	48
Dell VPN Access with Posture Checks	49
Certificate/Two-Factor Authentication for W-ClearPass Application Login	51

W-ClearPass Admin Access	53
W-ClearPass Admin SSO Login (SAML SP Service)	55
W-ClearPass Identity Provider (SAML IdP Service)	55
Device MAC Authentication	57
EDUROAM Service	58
Encrypted Wireless Access via 802.1X Public PEAP method	60
Guest Access	62
Guest Access Web Login	63
Guest Authentication with MAC Caching	64
Guest Social Media Authentication	66
OAuth2 API User Access	68
Onboard	68
Policy Manager Service Types	70
802.1X Wired	70
802.1X Wired - Identity Only	71
Dell 802.1X Wireless	71
802.1X Wireless - Identity Only	82
Dell 802.1X Wireless	83
Cisco Web Authentication Proxy	94
MAC Authentication	95
RADIUS Authorization	96
RADIUS Enforcement (Generic)	97
RADIUS Proxy	97
Dell W-Series Application Authentication	98
Dell W-Series Application Authorization	99
W-ClearPass OnConnect Enforcement	99
Event-Based Enforcement	101
TACACS+ Enforcement	103
Web-based Authentication	104
Web-based Health Check Only	104
Web-based Open Network Access	105
Monitoring	107
Live Monitoring: Access Tracker	107
About the Access Tracker	107
Customizing the Access Tracker	108
Viewing Access Tracker Session Details	110
Live Monitoring: Accounting	116
Modifying the Accounting Page Parameters	118
RADIUS Accounting Details > Summary Tab	119
RADIUS Accounting Record Details > Auth Sessions Tab	120
RADIUS Accounting Record Details > Utilization Tab	121
RADIUS Accounting Record Details > Details Tab	122
TACACS+ Accounting Record Details > Request Tab	124

TACACS+ Accounting Record Details > Auth Sessions Tab	125
TACACS+ Accounting Record Details > Details Tab	126
Live Monitoring: OnGuard Activity	127
About OnGuard Activity	127
Bouncing an Agent Using Non-SNMP	128
Bouncing a Client Using SNMP	131
Broadcasting a Message to Active Endpoints	132
Sending a Message to Selected Endpoints	133
Live Monitoring: Analysis and Trending	133
Live Monitoring: System Monitor	134
System Monitor Page	135
Process Monitor Page	136
Network Monitor Page	137
ClearPass Monitor Page	138
Profiler and Discovery	138
Profiler and Discovery: Endpoint Profiler	139
Profiler and Discovery: Network Discovery	140
About Network Discovery	140
Adding the Configurations to Query Seed Devices	141
Initiating a Network Discovery Scan	146
About Auto-Refresh	148
Importing and Viewing Discovered Network Devices	149
Viewing Discovered Endpoints	151
Audit Viewer	152
Introduction	152
Add Events	153
Modify Events	154
Remove Events	155
Event Viewer	155
About the Event Viewer	155
Creating an Event Viewer Report Using Default Values	156
Creating an Event Viewer Report Using Custom Values	156
Viewing Report Details	157
Data Filters	158
About Data Filters	158
Adding a Data Filter	159
Restoring Blacklisted Users to the Network	162
Authentication and Authorization	165
Supported Authentication Methods	165
Authentication and Authorization Architecture and Flow	165
Configuring Authentication Components	167
Adding and Modifying Authentication Methods	169
Adding a New Authentication Service	169

Modifying an Existing Authentication Service	170
Authorize Authentication Method	171
CHAP and EAP-MD5	171
EAP-FAST	172
EAP-GTC	177
EAP-MSCHAPv2	179
EAP-PEAP	179
EAP-PEAP-Public	182
EAP-PWD	185
EAP-TLS	186
EAP-TTLS	188
MAC-AUTH	191
MSCHAP	191
PAP	192
Adding and Modifying Authentication Sources	193
Generic LDAP and Active Directory	194
Generic SQL DB	207
HTTP	212
Kerberos	217
Okta	220
RADIUS Server	225
Static Host Lists	228
About Static Host Lists	228
Adding a Static Host List to ClearPass	228
Adding a Static Host List as an Authentication Source	230
Static Hosts Lists Configuration Summary	232
Token Server	232
Configuring Identity Settings	237
Configuring Single Sign-On	237
SAML Service Provider (SP) Configuration	237
SAML Identity Provider (IdP) Configuration	239
Managing Local Users	240
Adding a Local User	240
Modifying a Local User Account	242
Importing and Exporting Local Users	243
Setting Password Policy for Local Users	243
Disabling Local User Accounts	245
Adding and Modifying Endpoints	246
Viewing List of Authentication Endpoints	247
Viewing Endpoint Authentication Details	248
Triggering Actions Performed on Endpoints	248
Updating Device Fingerprints From a Hosted Portal	249
Manually Adding an Endpoint	250

Modifying an Endpoint	251
Managing Static Host Lists	253
About Static Host Lists	253
Adding a Static Host List	254
Static Hosts Lists Configuration Summary	256
Editing a Static Host List	256
Importing and Exporting Static Host Lists	256
Configuring a Role and Role Mapping Policy	257
Identity Roles Architecture and Workflow	257
Adding and Modifying Roles	259
Adding and Modifying Role Mapping Policies	259
Posture	263
Posture Architecture and Flow	263
Posture Policy	263
Audit Servers	263
Assessing Client Consistency	264
Application Token	264
System Token	265
Unified Agent System Tray Status Icons	265
About the Unified Agent	265
Unified Agent System Tray Icons	265
OnGuard-Only System Tray Icons	267
Creating a New Posture Policy	267
About ClearPass Posture	267
Creating a New Posture Policy	268
Configuring Posture Policy Agents and Hosts	269
Introduction	269
NAP Agent Posture Plug-ins	270
OnGuard Agent Posture Plug-ins	270
Configuring Posture Policy Plug-ins	272
Configuring OnGuard Agent Plugins	273
Configuring NAP Agent Plugins	320
Configuring Posture Policy Rules	324
Configuring Posture for Services	325
Configuring Audit Servers	327
Audit Service Flow Control	327
Default Audit Servers	328
Custom Audit Servers	331
Post-Audit Rules	340
Configuring Enforcement	343
Configuring Enforcement Policies	343
Configuring Enforcement Profiles	345
Adding an Enforcement Profile	346

Modifying an Existing Enforcement Profile	348
Agent Enforcement	348
Aruba Downloadable Role Enforcement	350
Aruba RADIUS Enforcement	360
Cisco Downloadable ACL Enforcement	362
Cisco Web Authentication Enforcement	364
ClearPass Entity Update Enforcement	366
CLI Based Enforcement	368
Filter ID Based Enforcement	370
Generic Application Enforcement	372
HTTP Based Enforcement	374
RADIUS Based Enforcement	375
RADIUS Change of Authorization (CoA)	377
Session Notification Enforcement	379
Session Restrictions Enforcement	381
SNMP Based Enforcement	386
TACACS+ Based Enforcement	387
VLAN Enforcement	389
Configuring Policy Simulation	393
Active Directory Authentication Simulation	393
Adding an Active Directory Simulation	394
Viewing the Simulation Results	394
Application Authentication Simulation	395
Simulation Tab	395
Attributes Tab	395
Results tab	396
Audit Simulation	396
Results Tab	397
Chained Simulation	398
Simulation Tab	398
Attributes Tab	398
Results Tab	400
Enforcement Policy Simulation	400
Simulation Tab	401
Attributes tab	403
Results Tab	403
RADIUS Authentication Simulation	404
Adding a RADIUS Authentication Simulation	404
Setting the Attributes to Be Tested	406
Viewing the Simulation Results	408
Role Mapping Simulation	409
Simulation Tab	409
Attributes Tab	411

Results Tab	411
Service Categorization Simulation	412
Simulation Tab	412
Attributes Tab	412
Results Tab	413
Import and Export Simulations	414
W-ClearPass Policy Manager Profile	415
W-ClearPass Profile Overview	415
Introduction	415
Enabling Endpoint Classification	415
Configuring CoA for an Endpoint-Connected Device	416
How W-ClearPass Profile Classifies Endpoints	417
Fingerprint Dictionaries	418
Viewing Live Endpoint Information for a Specific Device	419
About the Device Profile	420
Endpoint Information Collectors	420
DHCP Collector	421
W-ClearPass Onboard Collector	421
HTTP User-Agent Strings Collector	421
MAC OUI Collector	421
ActiveSync Plug-in Collector	422
W-ClearPass OnGuard Agent	422
SNMP Collector	422
Subnet Scan Collector	424
SNMP Configuration for Wired Network Profiling	426
Information Regarding SSH and WMI Configuration	427
Network Access Devices	429
Introduction	429
Adding and Modifying Network Devices	430
Adding a Network Device	430
Additional Tasks	437
Adding and Modifying Device Groups	438
Adding and Modifying Proxy Targets	440
Adding a Proxy Target	440
Configuring the Ingress Event Sources	441
Administration	443
W-ClearPass Guest Portal	444
Managing Admin Users	445
Changing the Administration Password	445
Adding an Admin User	446
Importing and Exporting Admin Users	447
Setting Password Policy for Admin Users	447
Disabling Admin User Accounts	448

Managing Admin Privileges	449
Overview	449
Defining Custom Admin Privileges	450
Creating Custom Administrator Privileges	452
Administrator Privilege XML File Structure	452
Administrator Privileges and IDs	453
Sample Administrator Privilege XML File	456
Server Configuration	457
Edit Server Configuration Settings	458
Set Date & Time	497
Change Cluster Password	499
Manage Policy Manager Zones	500
About Policy Manager Zones	500
Managing Policy Manager Zones	500
Mapping Policy Manager Zones	501
NetEvents Targets	502
Virtual IP Settings	504
Clear Machine Authentication Cache	504
Cluster-Wide Parameters	505
Make Subscriber	517
Collect Logs	518
Backup	519
Restore	520
Cleanup	521
Shutdown/Reboot	523
Drop Subscriber	523
Log Configuration	523
Service Log Configuration	524
System Level Configuration	525
Local Shared Folders	526
License Management	527
Licensing Page	527
Adding an Application License	528
Activating a Server License	529
Activating an Application License	530
Updating a Server License	531
Updating an Application License	532
SNMP Trap Receivers	533
SNMP Trap Receivers Main Page	533
Adding an SNMP Trap Server	533
Importing an SNMP Trap Server	534
Exporting All SNMP Trap Servers	535
Exporting an SNMP Trap Server	536

Deleting an SNMP Trap Server	537
Syslog Targets	537
Syslog Targets Main Page	537
Adding a Syslog Target	538
Importing a Syslog Target	539
Exporting All Syslog Target	540
Exporting a Syslog Target	540
Deleting a Syslog Target	541
Syslog Export Filters	541
About Syslog Export Filters	542
Syslog Export Filters Page	542
Adding a Syslog Export Filter	542
Importing a Syslog Filter	550
Exporting All Syslog Filter	551
Exporting a Syslog Filter	552
Deleting a Syslog Filter	553
Messaging Setup	553
Configuring Messaging	553
Sending a Test Email Message	554
Sending a Test SMS Message	555
Endpoint Context Servers	555
Introduction	555
Endpoint Context Servers Page	556
Adding an Endpoint Context Server	556
Importing an Endpoint Context Server	558
Exporting All Endpoint Context Servers	559
Modifying an Endpoint Context Server	560
Polling an Endpoint Context Server	562
Deleting an Endpoint Context Server	562
Configuring Endpoint Context Server Actions	563
Filtering an Endpoint Context Server Action Report	563
Configuring Endpoint Context Server Actions	563
Adding machine-os and host-type Endpoint Attributes	567
Adding Vendor-Specific Endpoint Context Servers	568
Adding an AirWatch Endpoint Context Server	569
Adding an AirWave Endpoint Context Server	572
Adding an Aruba Activate Endpoint Context Server	574
Adding a ClearPass Cloud Proxy Endpoint Context Server	575
Adding a Google Admin Console Endpoint Context Server	577
Adding a Generic HTTP Endpoint Context Server	579
Integrating W-ClearPass with Infoblox	580
Integrating ClearPass with Juniper Networks SRX	594
Adding a JAMF Endpoint Context Server	604

Adding a MaaS360 Endpoint Context Server	606
Adding a MobileIron Endpoint Context Server	609
Adding a Palo Alto Networks Firewall Endpoint Context Server	611
Adding a Palo Alto Networks Panorama Endpoint Context Server	613
Adding an SAP Afaria Endpoint Context Server	614
Adding a SOTI Endpoint Context Server	616
Adding a XenMobile Endpoint Context Server	618
File Backup Servers	619
Server Certificate	621
Server Certificate Main Page	621
Server Certificate Type	622
Creating a Certificate Signing Request	624
Creating a Self-Signed Certificate	627
Exporting a Server Certificate	632
Importing a Server Certificate	632
Certificate Trust List	633
Certificate Trust List Main Page	633
Adding a Certificate	634
Viewing a Certificate Detail	634
Deleting a Certificate	634
Certificate Revocation Lists	635
About Certificate Revocation Lists	635
Adding a Certificate Revocation List	635
Deleting a Certificate Revocation List	636
Using ClearPass Dictionaries	636
RADIUS Dictionary	637
Import RADIUS Dictionary	638
TACACS+ Services Dictionary	638
Fingerprints Dictionary	640
Dictionary Attributes	641
Introduction	641
Adding a Dictionary Attribute	642
Modifying Dictionary Attributes	643
Importing Dictionary Attributes	643
Exporting All Dictionary Attributes	644
Exporting Selected Dictionary Attributes	645
Applications Dictionaries	645
Viewing an Application Dictionary	645
Deleting an Application Dictionary	646
Updating Policy Manager Software	646
Introduction	647
Software Updates Page	647
Install Update Dialog Box	649

Reinstalling a Patch	651
Uninstalling a Skin, Translation, or Plug-in	651
OnGuard Settings	651
Introduction	651
Accessing OnGuard Agent Support Charts	652
Configuring OnGuard Settings	652
OnGuard Global Agent Settings	654
About Global Agent Settings	654
Global Settings Parameters for OnGuard Agents	655
Global Agent Settings: Run OnGuard As Parameter	656
Contact Support	657
Remote Assistance	658
Remote Assistance Process Flow	658
Adding a Remote Assistance Session	659
Cluster Upgrade/Update Tool	661
Cluster Update Tool	661
About the Cluster Update Feature	661
Before Updating the Cluster	662
Updating the Cluster	662
Viewing Update Status	664
Cluster Upgrade Tool	666
Introduction	667
Cluster Upgrade Process Overview	667
Before You Upgrade	667
Installing the Cluster Upgrade Tool	668
Opening the Cluster Upgrade Tool	669
Upgrading the W-ClearPass Cluster	671
Viewing Upgrade Status	673
Steps in the Upgrade Tool's Automated Workflow	674
Sample Times Required for Upgrade	675
Troubleshooting	676
Configuring Processing for Ingress Events	677
Overview	677
Enabling Ingress Event Dictionaries	677
Configuring the Ingress Event Sources	678
Configuring the Ingress Receiving Ports	680
Configuring an Event-Based Enforcement Service	680
Introduction	680
Adding an Event-Based Enforcement Service	680
Associating the Enforcement Service with an Enforcement Policy	681
Enabling Ingress Events Processing	682
W-ClearPass Insight Reports	685
About W-ClearPass Insight	685

Introduction	685
Enabling Insight and Specifying a Master Insight Node	686
Launching Insight	687
About the Insight Dashboard	688
Dashboard Overview	688
Adding a Report Widget to the Dashboard Landing Page	689
Removing a Report Widget from the Dashboard Landing Page	689
Creating a Report or Alert From the Dashboard	690
Specifying the Date Range for Data Collection	691
Authentication Dashboard	692
Endpoints Dashboard	693
Guest Dashboard	694
Network Dashboard	695
Posture Dashboard	695
System Dashboard	696
System Monitor Dashboard	696
Searching the Insight Database	698
About Insight Search	698
Search Example	698
Creating Alerts	699
Introduction	699
Creating New Alerts	700
Modifying the User Watchlist	701
Adding or Removing Users from the Watchlist	704
Creating Reports	706
Overview	706
Settings Configuration	707
Report Filters Configuration	709
Specifying the Logo and Branding	710
Report Summary Page	711
Configured Reports Page	712
Viewing Reports	712
Insight Report Categories Reference	713
Introduction	714
Authentication Category Reports	714
Endpoint Category Reports	717
Guest Authentication Category Reports	718
Network Category Reports	720
OnGuard Category Reports	721
Onboard Category Report	723
RADIUS Authentication Category Reports	724
System Category Reports	726
TACACS Category Reports	727

Administration Operations	727
Overview	727
File Transfer Settings Configuration	728
Testing File Transfer Configuration	729
Database Settings Configuration	730
Managing Insight Admin Privileges	730
Overview	730
Viewing the Default Insight Admin Privileges	731
Defining Custom Insight Admin Privileges	731
Insight UI Differences for Read-Only Users	733
Command Line Interface	735
Cluster Commands	735
cluster drop-subscriber	735
cluster list	736
cluster make-publisher	736
cluster make-subscriber	736
cluster reset-database	737
cluster set-cluster-passwd	737
cluster sync-cluster-passwd	738
Configure Commands	738
configure date	738
configure dns	739
configure fips-mode	739
configure hostname	740
configure ip	740
configure ip6	741
configure mtu	742
configure timezone	743
Network Commands	743
network ip6	744
network ip	745
nslookup	746
network ping6	747
network ping	748
network reset	748
network traceroute6	749
network traceroute	749
Miscellaneous Commands	750
ad auth	750
ad netjoin	751
ad netleave	751
ad passwd-server	752
ad testjoin	752

alias	753
backup	753
cli session idle timeout	754
dump certchain	754
dump logs	754
dump servercert	755
exit	755
help	756
krb auth	756
krb list	756
ldapsearch	757
quit	757
restore	757
Service Commands	758
service <action> <service-name>	758
Show Commands	760
show all-timezones	760
show date	760
show dns	761
show domain	761
show fipsmode	762
show hostname	762
show ip	762
show license	763
show ntp	763
show sysinfo	764
show timezone	764
show version	765
SSH Timed Account Lockout	765
Introduction	765
SSH Account Lockout Configuration	766
SSH Account Lockout Alerts	768
SSH Account Lockout Behavior	768
System Commands	769
system apps-access-reset	769
system boot-image	769
system cleanup	770
system create-api-client	771
system gen-recovery-key	771
system gen-support-key	771
system install-license	771
system morph-vm	772
system refresh-license	773

system reset-server-certificate	773
system restart	773
system shutdown	774
system sso-reset	774
system start-rasession	774
system status-rasession	775
system terminate-rasession	775
system update	775
system upgrade	776
SNMP Private MIB, SNMP Traps, System Events, Error Codes	779
W-ClearPass SNMP Private MIB	779
Introduction	779
System MIB Entries	779
RADIUS Server MIB Entries	780
Policy Server MIB Entries	781
Web Authentication Server MIB Entries	783
TACACS+ Server MIB Entries	783
Network Traffic MIB Entries	784
W-ClearPass SNMP Traps and OIDs	784
Introduction	784
W-ClearPass SNMP Traps	785
SNMP Trap Details	786
SNMP Daemon Traps	787
SNMP Daemon Trap Events	787
Network Interface up and Down Events	787
Network Interface Status Traps	787
W-ClearPass Processes Stop and Start Events	788
Disk Space Threshold Traps	788
Disk Utilization Threshold Exceed Events	788
Process Status Traps	788
CPU Load Average Exceed Events for 1, 5, and 15 Minute Thresholds	796
CPU Load Average Traps	796
Important System Events	797
Admin User Interface Events	797
Admin Server Events	798
Async Service Events	798
W-ClearPass/Domain Controller Events	798
W-ClearPass System Configuration Events	798
W-ClearPass Update Events	799
Cluster Events	799
Command Line Events	799
Database Replication Services Events	799
Licensing Events	799

Policy Server Events	800
RADIUS/TACACS+ Server Events	800
Service Names	800
SNMP Events	801
Support Shell Events	801
System Auxiliary Service Events	801
System Monitor Events	801
Error Codes	802
Use Cases	807
802.1X Wireless Use Case	807
Configuring a Service	808
Creating a New Role Mapping Policy	809
Web Based Authentication Use Case	813
Configuring a Service	813
MAC Authentication Use Case	820
Configuring the Service	820
TACACS+ Use Case	823
Configuring the Service	823
Single Port Use Case	824
OnGuard Dissolvable Agent	825
Introduction	825
Native Agents Only Mode	825
Configuring Workflow in Native Agents Only Mode	826
End-to-End Flow in Native Agents Only Mode	827
Native Agents with Java Fallback Mode	830
Configuring Native Agents with Java Fallback Mode	830
End-to-end flow in Native Agents with Java Fallback Mode	831
Configuring Web Agent Flow - Java Only Mode	832
Configuring Web Agent Flow in W-ClearPass Policy Manager	832
Configuring Web Agent Flow in W-ClearPass Guest	833
Native Dissolvable Agent Supported Operating Systems and Browsers	835
OnGuard Dissolvable Agent Supported Browsers and Java Versions	839
Rules Editing and Namespaces	845
Namespaces	845
Application Namespace	846
Audit Namespaces	847
Authentication Namespaces	847
Authorization Namespaces	849
Certificate Namespaces	850
Connection Namespaces	851
Date Namespaces	852
Device Namespaces	852
Endpoint Namespaces	853

Guest User Namespaces	853
Host Namespaces	853
Local User Namespaces	853
Posture Namespaces	854
RADIUS Namespaces	854
TACACS Namespaces	855
Tips Namespaces	855
Variables	855
Operators	856

This chapter provides an overview of the W-ClearPass 6.6 Policy Manager Access Management System.

This chapter includes the following information:

- [About the W-ClearPass Access Management System](#)
- [Using the W-Policy Manager Dashboard](#)
- [Accessing Configuration Information](#)
- [Importing and Exporting Information](#)

About the W-ClearPass Access Management System

This section contains the following information:

- [About This Guide](#)
- [W-ClearPass Access Management System Overview](#)
- [Key Features](#)
- [Advanced Policy Management](#)
- [W-ClearPass Specifications](#)

About This Guide

Welcome to the W-ClearPass Policy Manager 6.6 *User Guide*.

The *W-ClearPass Policy Manager 6.6 User Guide* provides a general overview of W-ClearPass Policy Manager features, as well as detailed descriptions of the configuration settings used to manage and monitor your W-Policy Manager deployment.

Intended Audience

The intended audience for the *W-ClearPass Policy Manager 6.6 User Guide* includes customers, partners, and field Sales Engineers.

Please note that this document is not a training guide, and it is assumed that the reader has at minimum foundational training in W-ClearPass Essentials and, if possible, Dell Certified Professional (ACCP) certification.

The user of this guide should have a working knowledge of the following:

- AAA technologies (RADIUS, TACACS, 802.1X, MAC address authentication, and Web authentication)
- Layer-2 and Layer-3 networking
- User Identity stores, such as Active Directory



Providing information about network device configurations and capabilities is outside the scope of this guide. For information on these topics, refer to the documentation provided by the vendor of your network equipment.

Getting Started

If you are new to W-ClearPass Policy Manager, refer to the following sections:

- For a general description of W-ClearPass Policy Manager features, refer to the following topics in this section, [W-ClearPass Access Management System Overview](#) and [Key Features](#).
- For a description of how to use the Dashboard, see [Using the W-Policy Manager Dashboard on page 26](#).

- For a list of common configuration tasks and pointers to information about how to perform each task, refer to [Accessing Configuration Information on page 29](#).
- If you are planning a new W-ClearPass Policy Manager deployment, refer to the *W-ClearPass Deployment Guide*. The *W-ClearPass Deployment Guide* is organized in a way that presents the recommended sequence in which W-ClearPass deployment should take place, and makes the major deployment tasks easy to implement.

W-ClearPass Access Management System Overview

The W-ClearPass Policy Manager™ Access Management System provides a window into your network and covers all your access security requirements from a single platform. You get complete views of mobile devices and users and have total control over what they can access.

With W-ClearPass, IT can centrally manage network policies, automatically configure devices and distribute security certificates, admit guest users, assess device health, and even share information with third-party solutions—through a single pane of glass, on any network and without changing the current infrastructure.

Role-Based and Device-Based Access

The W-ClearPass Policy Manager platform provides role-based and device-based network access control for employees, contractors, and guests across any wired, wireless, and VPN infrastructure.

W-ClearPass works with any multivendor network and can be extended to business and IT systems that are already in place.

Self-Service Capabilities

W-ClearPass delivers a wide range of unique self-service capabilities. Users can securely onboard their own devices for enterprise use or register AirPlay, AirPrint, Digital Living Network Alliance (DLNA), and Universal Plug and Play (UPnP) devices that are enabled for sharing, sponsor guest Wi-Fi access, and even set up sharing for Apple TV and Google Chromecast.

Leveraging Contextual Data

The power of W-ClearPass comes from integrating ultra-scalable AAA (authentication, authorization, and accounting) with policy management, guest network access, device onboarding, and device health checks with a complete understanding of context.

From this single W-ClearPass policy and AAA platform, contextual data is leveraged across the network to ensure that users and devices are granted the appropriate access privileges.

W-ClearPass leverages a user's role, device, location, application use, and time of day to execute custom security policies, accelerate device deployments, and streamline network operations across wired networks, wireless networks, and VPNs.

Third-Party Security and IT Systems

W-ClearPass can be extended to third-party security and IT systems using REST-based APIs to automate work flows that previously required manual IT intervention. W-ClearPass integrates with mobile device management to leverage device inventory and posture information, which enables well-informed policy decisions.

Key Features

W-ClearPass's key features are as follows:

- Bring Your Own Device (BYOD) Certificate Authority for secure self service onboarding
- Auto Sign-On and single sign-on (SSO) support via Security Assertion Markup Language (SAML) v2.0

- Social network and Cloud application SSO via OAuth2, Facebook, Twitter, LinkedIn, Office365, Google Apps, and so on
- Enterprise reporting, monitoring, and alerting
- Role-based network access enforcement for multivendor Wi-Fi, wired, and VPN networks
- High performance, scalability, High Availability, and load balancing
- A Web-based user interface that simplifies policy configuration and troubleshooting
- Network Access Control (NAC), Network Access Protection (NAP) posture and health checks, and Mobile Device Management (MDM) integration for mobile device posture checks
- Advanced reporting of all user authentications and failures
- HTTP/RESTful APIs for integration with third-party systems, Internet security, and MDM
- Device profiling and self-service onboarding
- Guest access with extensive branding and customization and sponsor-based approvals
- IPv6 administration support

Advanced Policy Management

W-ClearPass advanced policy management support includes:

- **Employee access**

W-ClearPass offers user and device authentication based on 802.1X, non-802.1X, and Web Portal access methods. To strengthen security in any environment, you can concurrently use multiple authentication protocols, such as PEAP, EAP-FAST, EAP-TLS, EAP-TTLS, and EAP-PEAP-Public.

For fine-grained control, you can use attributes from multiple identity stores, such as Microsoft Active Directory, LDAP-compliant directory, Open Database Connectivity (ODBC)-compliant SQL database, token servers, and internal databases across domains within a single policy.

Additionally, you can add posture assessments and remediation to existing policies at any time.

- **Device profiling**

W-ClearPass provides a profiling service that discovers and classifies all endpoints, regardless of device type. You can obtain a variety of contextual data (such as MAC OUIs, DHCP fingerprinting, and other identity-centric device data) and use this data within policies.

Stored profiling data identifies device profile changes and dynamically modifies authorization privileges. For example, if a printer appears as a Windows laptop, W-ClearPass Policy Manager can automatically deny access.

- **Access for unmanaged endpoints**

Unmanaged non-802.1X devices (such as printers, IP phones, and IP cameras) can be identified as *known* or *unknown* upon connecting to the network. The identity of these devices is based on the presence of their MAC address in an external or internal database.

- **Secure configuration of personal devices**

W-ClearPass Onboard fully automates the provisioning of any Windows, Mac OS X, iOS, Android, Chromebook, and Ubuntu devices via a built-in captive portal. Valid users are redirected to a template-based interface to configure required SSIDs and 802.1X settings, and download unique device credentials.

Additional capabilities include the ability for IT to revoke and delete credentials for lost or stolen devices, and the ability to configure mobile email settings for Exchange ActiveSync and VPN clients on some device types.

- **Customizable visitor management**

W-ClearPass Guest simplifies work flow processes so that receptionists, employees, and other non-IT staff can create temporary guest accounts for secure Wi-Fi and wired network access. Self-registration allows guests to create their credentials.

- **Device health checks**

W-ClearPass OnGuard, as well as separate OnGuard persistent or dissolvable agents, performs advanced endpoint posture assessments. Traditional NAC health-check capabilities ensure compliance and network safeguards before devices connect.

You can use information about endpoint integrity (such as status of anti-virus, anti-spyware, firewall, and peer-to-peer applications) to enhance authorization policies. Automatic remediation services are also available for non-compliant devices.

W-ClearPass Specifications

W-ClearPass Policy Manager

- Comprehensive identity-based policy engine
- Posture agents for Windows, Macintosh OS X, and Linux operating systems
- Built-in AAA services: RADIUS, TACACS+, and Kerberos
- Web, 802.1X, and non-802.1X authentication and authorization
- Reporting, analytics, and troubleshooting tools
- External captive portal redirect to multivendor equipment
- Interactive policy simulation and monitor mode utilities
- Deployment templates for any network type, identity store, and endpoint

Framework and Protocol Support

- RADIUS, RADIUS CoA, TACACS+, Web authentication, and SAML v2.0
- EAP-FAST (EAP-MSCHAPv2, EAP-GTC, EAP-TLS)
- PEAP (EAP-MSCHAPv2, EAP-GTC, EAP-TLS, EAP-PEAP-Public)
- TTLS (EAP-MSCHAPv2, EAP-GTC, EAP-TLS, EAP-MD5, PAP, CHAP)
- EAP-TLS
- PAP, CHAP, MSCHAPv1, MSCHAPv2, and EAP-MD5
- Wireless and wired 802.1X and VPN
- Microsoft Network Access Protection (NAP) and Network Access Control (NAC)
- Windows machine authentication
- MAC address authentication (non-802.1X devices)
- Audit based on port and vulnerability scans

Supported Identity Stores

- Microsoft Active Directory
- Kerberos
- Any LDAP-compliant directory
- Any ODBC-compliant SQL server
- Token servers
- Built-in SQL store
- Built-in static-hosts list

Using the W-Policy Manager Dashboard

The W-Policy Manager Dashboard organizes and presents the key information about the status and performance of the current W-ClearPass server or cluster, as well as a set of Quick Links to the most commonly used functions, such as configuring policies, viewing the Access Tracker, and so on.

The Dashboard information is illustrated in interactive bar chart, graph, and table formats.

To customize the Dashboard layout to display the information you most want to see (as described in [Table 1](#)), drag and drop from the list of the Widget elements on the left pane to one of the available Dashboard slots in the right pane.

Table 1: *Dashboard Widget Summary*

 Alerts <i>Latest Alerts</i>	To view the table with latest system level events, drag and drop the Alerts widget to the Dashboard. Clicking on a row drills down to the Event Viewer.
 All Requests <i>Trend all Policy Manager requests</i>	To view the graph that displays all requests processed by W-Policy Manager over the past week, drag and drop the All Requests widget. - Processed requests include RADIUS, TACACS+, and WebAuth requests. - Clicking on each bar in the graph drills down to the Access Tracker page and shows the requests for the selected day.
 Applications <i>Launch other ClearPass Applications</i>	To view the links to the Dell Insight, Guest, and Onboard applications that are integrated with W-Policy Manager, drag and drop the Applications widget to the Dashboard.
 Authentication Status <i>Trend Successful and Failed authentications</i>	To view a graph of the failed and successful requests over the past week, drag and drop the Authentication Status to the Dashboard. - This graph 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 to the Access Tracker page that shows the failed and successful requests for the day specified.
 Cluster Status <i>Monitor the status of the entire cluster</i>	To view the status of all nodes in a cluster, drag and drop the Cluster Status widget to the Dashboard. The following fields are shown for each node: Status: Shows the overall health status of the cluster. Green indicates healthy status. Red indicates connectivity problems or high CPU or high memory utilization. The status also shows red when a node is out-of-sync with the rest of the cluster. Host Name: Specifies the name of the host and IP address of the node. Zone: The configured cluster zone. Server Role: Indicates whether the cluster node is a publisher or subscriber.

Table 1: Dashboard Widget Summary (Continued)

	• Last Replication: Date of the last replication. • Status: Indicates the status of the cluster node.
 Device Category <i>Device Categories</i>	To view the chart that shows the graph of all profiled devices categorized into the following categories: • Access Points • Computer • Conflict Indicates a conflict occurred in the categorization of the device. • Datacenter Appliance • Game Console • Monitoring Devices • Network Boot Agents • Physical Security • Printer • Router • Server • Smart Device • Switch • Unknown Indicates devices that are not included in the Profiler database. • VOIP phone
 Device Family <i>Device Family</i>	To view the device family of a particular device category: 1. Drag and drop the Device Category widget to the Dashboard. 2. From the drop-down, select the device category. The device family is displayed. For example, selecting Computer would show that the device family is <i>Windows</i>.
 Endpoint Profiler Summary <i>Endpoint profiling details</i>	To view a display that shows the number of smart devices, computers, and unmanaged devices, as well as the total number of devices defined by the Endpoint Profiler for this W-ClearPass server, drag and drop the Endpoint Profiler Summary widget to the Dashboard.
 Failed Authentications <i>Track the latest failed authentications</i>	• To view the table with the latest failed authentications, drag and drop the Failed Authentications widget to the Dashboard. • Clicking on a row drills down to the Access Tracker page and shows failed requests sorted by timestamp, with the latest request displayed on the top.
 Health Status <i>Trend Healthy and Unhealthy requests</i>	To view the graph of the healthy and unhealthy requests over the past week, drag and drop the Health Status widget. • <i>Healthy requests</i> are the requests to which the health state was deemed to be healthy based on the posture data sent from the client.

Table 1: Dashboard Widget Summary (Continued)

	• <i>Unhealthy requests</i> are the requests to which the health state was deemed to be <i>quarantined</i> (posture data received but health status is not compliant) or <i>unknown</i> (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 to the Access Tracker page that shows the healthy and unhealthy requests for the last week.
 Latest Authentications <i>Latest Authentications</i>	To view the table with the latest authentications, drag and drop the Latest Authentications widget to the Dashboard. • Clicking on a row in the table drills down to the Access Tracker page that shows requests sorted by timestamp with the latest request displayed on the top.
 MDM Discovery Summary <i>Mobile Device Management discovery details</i>	To view the charts that show the endpoints discovered, drag and drop the MDM Discovery Summary widget to the Dashboard. • The endpoints are displayed in separate charts based on the endpoint's operating system. • Clicking a chart drills down to the Configuration > Identity > Endpoints page. The results depends on the operating system selected. For example, if you click the Android devices chart, you can view the list of only Android devices in the Endpoints page.
 OnGuard Clients Summary <i>OnGuard Clients details</i>	To view a display that shows the number of Linux, Mac, and Windows OnGuard clients, as well as the total number of OnGuard clients for this W-ClearPass server, drag and drop the OnGuard Clients Summary to the Dashboard.
 Quick Links <i>Launch configuration interfaces with a single click</i>	To view the links to the following configuration tasks, drag and drop the Quick Links widget to the Dashboard: • Start Configuring Policies • Manage Services • Access Tracker • Analysis and Trending • Network Devices • Server Manager • W-ClearPass Guest • W-ClearPass Onboard
 Request Processing Time <i>Trend total request processing time</i>	To view the trend of total request processing time, drag and drop the Request Processing Time widget to the Dashboard.

Table 1: Dashboard Widget Summary (Continued)

 Service Categorization <i>Monitor Service Categorization of authentications</i>	To view the bar chart with each bar representing a categorized W-Policy Manager service request, drag and drop the Service Categorization widget to the Dashboard. Clicking on a bar drills down to the Access Tracker that shows the requests that were categorized into a specific service.
 Successful Authentications <i>Track the latest successful authentications</i>	To view a table with the latest successful authentications, drag and drop the Successful Authentications widget to the Dashboard. Clicking on a row in the table drills down to the Access Tracker page that shows successful requests sorted by timestamp, with the latest request displayed on the top.
 System CPU Utilization <i>CPU usage for last 30 mins</i>	To view the CPU usage for the last 30 minutes, drag and drop the System CPU Utilization widget to the Dashboard. - The widget displays the CPU utilization time in minutes and percentage for System, User, and IO Wait time, indicated by color. - CPU utilization is presented in five-minute increments.
 System Summary <i>Snapshot of system usage</i>	To view the Percentage Used statistics for the following components, drag and drop the System Summary widget to Dashboard: - Main Memory - Swap Memory - Disk - Swap Disk

Accessing Configuration Information

This section contains the following information:

- [Introduction](#)
- [Start Here](#)
- [Services](#)
- [Authentication and Authorization](#)
- [Identity](#)
- [Posture](#)
- [Enforcement](#)
- [Network](#)
- [Policy Simulation](#)
- [Profile Settings](#)

Introduction

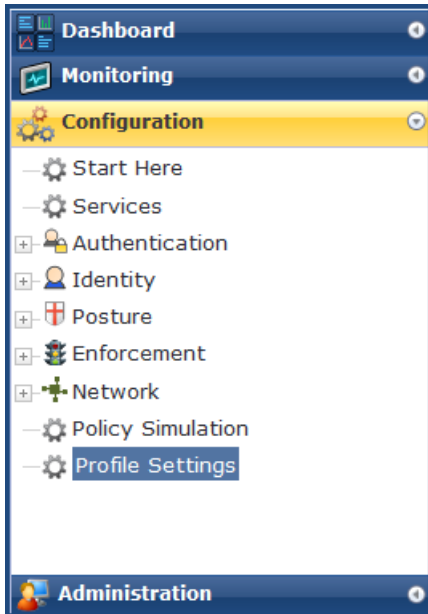
This section provides pointers to information on how to configure the primary configuration tasks in W-ClearPass Policy Manager.

You can access all these configuration tasks via the W-ClearPass **Configuration** menu.

To access the W-ClearPass **Configuration** menu, select **Configuration**.

The **Configuration** menu appears (see [Figure 1](#)):

Figure 1: ClearPass Policy Manager Configuration Menu



Start Here

The W-ClearPass Policy Manager **Start Here** page provides the ability to create templates for services that will allow you to define baseline policies and require specific data when you create services.

For more information, see [Creating Service Templates on page 36](#).

Services

The **Services** page provides options to add, modify, and remove a service. For more information, refer to the following sections:

- [Services Architecture and Flow on page 35](#)
- [Policy Manager Service Types on page 70](#)

This page also shows the current list and order of services that W-ClearPass Policy Manager keeps track of during authentication and authorization.

Authentication and Authorization

The **Authentication** page provides options to configure the following components:

- Authentication Method
- Authentication Source
- Authorization Source

For more information, refer to the following sections:

- [Adding and Modifying Authentication Methods on page 169](#)
- [Adding and Modifying Authentication Sources on page 193](#)
- [Configuring Authentication Components on page 167](#)

Identity

The **Identity** page provides options on the settings required to configure W-ClearPass Policy Manager Identity settings. For more information, refer to the following sections:

- [Configuring Single Sign-On on page 237](#)
- [Managing Local Users on page 240](#)
- [Adding and Modifying Endpoints on page 246](#)
- [Managing Static Host Lists on page 253](#)

Posture

The **Posture** page provides options to configure posture policies and audit servers. For more information, refer to the following sections:

- [Posture Architecture and Flow on page 263](#)
- [Configuring Audit Servers on page 327](#)

Enforcement

The **Enforcement** page provides options to configure the Enforcement Profiles globally and to reference in an enforcement policy that is associated with a service.

For more information, refer to the following section:

- [Enforcement Architecture and Flow on page 1](#)

Network

The **Network** page provides options to configure the Network Access Device (NAD) that sends network access requests to W-Policy Manager using the supported RADIUS, TACACS+, or SNMP protocol. The NAD in this context is usually a mobility controller or a switch.

For more information, refer to the following sections :

- [Adding and Modifying Network Devices on page 430](#)
- [Adding and Modifying Device Groups on page 438](#)
- [Adding and Modifying Proxy Targets on page 440](#)

Policy Simulation

The **Policy Simulation** page provides options to configure the **Policy Simulation** utility that applies a set of request parameters as input against a given policy component.

- For more information, refer to [Configuring Policy Simulation on page 393](#).

Profile Settings

The **Profile Settings** page provides options to configure Profiles, which is a W-Policy Manager module that automatically classifies endpoints using attributes obtained from software components called *Collectors*.

For more information, refer to the following sections:

- [W-ClearPass Profile Overview on page 415](#)

- [About the Device Profile on page 420](#)
- [Endpoint Information Collectors on page 420](#)

Importing and Exporting Information

This section contains the following information:

- [Importing Information Into W-ClearPass](#)
- [Exporting Information From W-ClearPass](#)

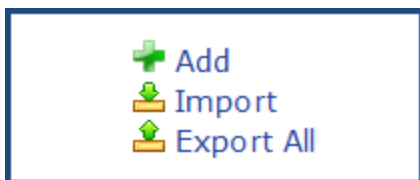
The option to import or export is available from many W-ClearPass components, such as services, authentication methods, authentication sources, and enforcement policies.

Importing Information Into W-ClearPass

Most pages in W-Policy Manager allow you to import configuration and administration-related information.

This information is stored as an XML file, which can be password protected. For information about the tags and attributes in the XML file, refer to Appendix B, "Using the W-ClearPass Configuration API" in the *W-ClearPass Deployment Guide*.

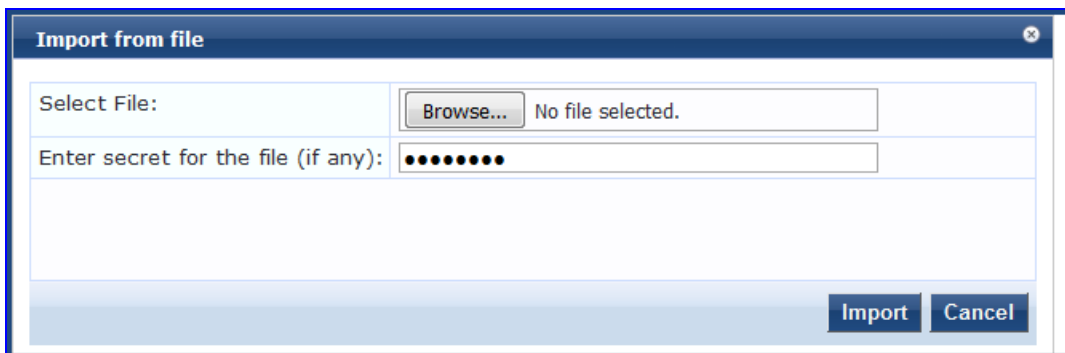
In the top-right corner of the configuration pages, the **Add**, **Import**, and **Export All** options are displayed:



To import information into W-ClearPass:

1. Click the **Import** link.
The **Import from file** dialog box opens.

Figure 2: *Import From File Page*



2. Click **Choose File**.
3. Browse to the file you want to import.
 - You must select an XML file in the correct format.
 - See Appendix B, "Using the W-ClearPass Configuration API" in the *W-ClearPass Deployment Guide* for more information about the format and contents of XML files.
 - If you have exported files from different locations within W-Policy Manager, ensure that you are selecting the correct file.
4. If the file is password protected, enter the password in the **Enter secret for the file (if any)** field.

5. Click **Import**.

Exporting Information From W-ClearPass

Most pages in W-Policy Manager allow you to export configuration and administration-related information.

To export multiple items, select the check boxes in the rows of the specific items that you want to export.

The configuration and administration information is exported as an XML file; you can set this file to be password protected (see [Table 2](#) for details).

To export information from W-ClearPass:

1. Click the **Export All** link at the top-right corner of the configuration page.
The **Export to File** dialog opens.

Figure 3: *Export to File Dialog*



2. Specify the export parameters based on [Table 2](#).
3. Click **Export**.
4. Enter the XML file name in the **Save As** dialog box.
5. Click **Save**.

[Table 2](#) describes the **Export to file** parameters:

Table 2: *Export to File Dialog Parameters*

Parameter	Action/Description
Export file with password protection	1. To export the file with password protection, choose Yes .
Secret Key/ Verify Secret	2. Enter the secret key. Then reenter the secret key.

This chapter describes the following topics:

- [Services Architecture and Flow](#)
- [Creating Service Templates](#)
- [Viewing the List of Services](#)
- [Policy Manager Service Types](#)

The W-Policy Manager policy model groups policy components that serve a specific type of request into the **Services** page.

Services Architecture and Flow

Service Classification

W-Policy Manager services are classified as follows:

- **Parents** of their policy components, which are wrapped hierarchically and coordinated in processing requests.
- **Siblings** of other W-Policy Manager services within an order that determine the sequence in which they are tested against requests.
- **Children** of W-Policy Manager, which test requests against their rules to find a matching service for each request.

Service Flow Control

The flow control for requests follows this sequence:

1. W-Policy Manager tests for the first request-to-service-rule match.
2. The matching service coordinates execution of its policy components.
3. Those policy components process the request to return enforcement profiles to the network access device and, optionally, return the posture results to the client.

Approaches to Creating a New Service

There are two approaches to creating a new service in W-ClearPass:

Bottom-Up

1. Create all the policy components first as needed:
 - Authentication method
 - Authentication source
 - Role-mapping policy
 - Posture policy
 - Audit servers
 - Enforcement profiles
 - Enforcement policy
2. Create the service using the **Service** creation wizard.

Top-Down

1. Start with the **Service** creation wizard.

2. Create the associated policy components as and when required, all in the same flow.

To help you get started, W-ClearPass provides 17 service types or templates. If these service types do not suit your needs, you can create a new service using custom rules (as described in the next section [Creating Service Templates](#)).

Creating Service Templates

This section includes the following information:

- [Creating Templates for W-ClearPass Services](#)
- [Service Templates Provided](#)
- [Services Supported for High Capacity Guest Mode](#)

Service templates provide a way to simply step through the template-creation process, so you can easily create services and define components, such as role-mapping policies, enforcement policies, and network devices.

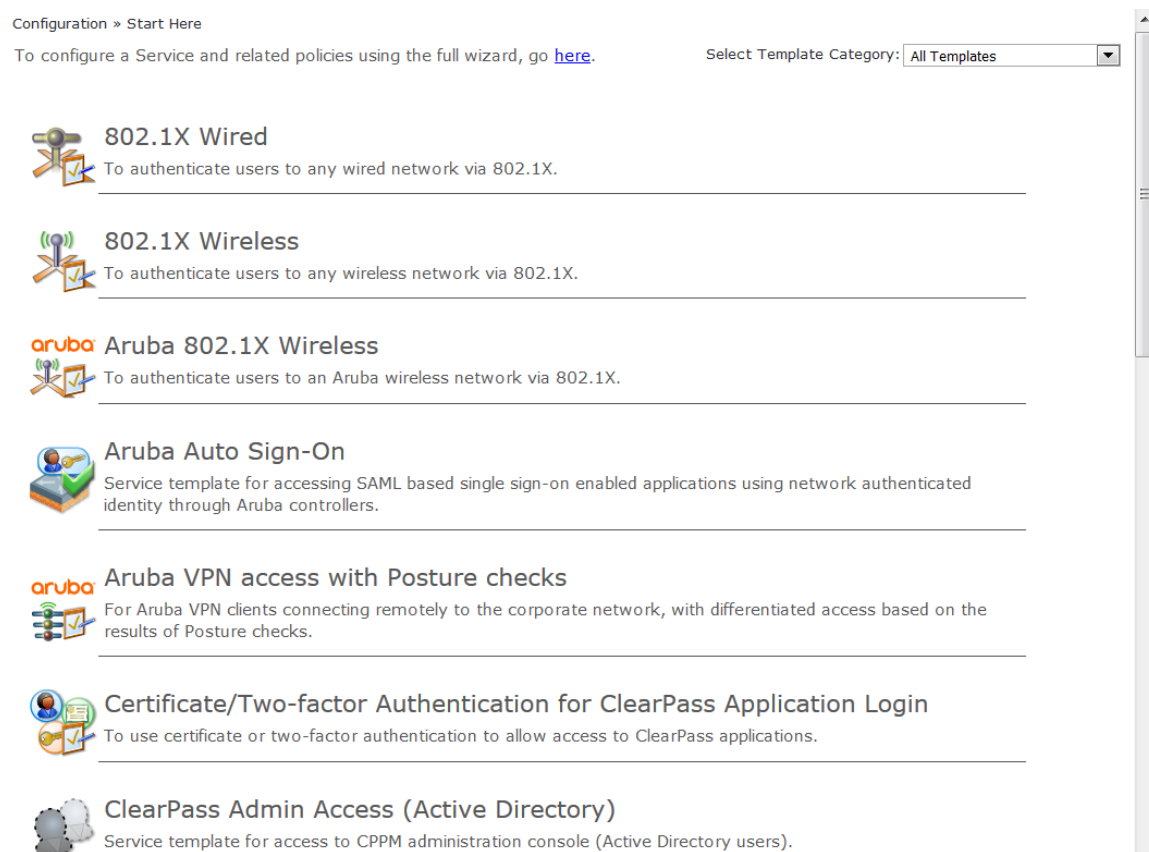
Creating Templates for W-ClearPass Services

To create templates for services for which you can define baseline policies and require specific data:

1. Navigate to the **Configuration > Start Here** page.

The Start Here page opens.

Figure 4: *Start Here Page (Partial View)*



2. Fill in the various fields that are presented in the templates—W-Policy Manager then creates the configuration elements that are needed for that particular service.

Service Templates Provided

W-ClearPass provides the following service templates:

- [802.1X Wired, 802.1X Wireless, and Dell 802.1X Wireless on page 45](#)
- [Auto Sign-On on page 48](#)
- [Dell VPN Access with Posture Checks on page 49](#)
- [Certificate/Two-Factor Authentication for W-ClearPass Application Login on page 51](#)
- [W-ClearPass Admin Access on page 53](#)
- [W-ClearPass Admin SSO Login \(SAML SP Service\) on page 55](#)
- [W-ClearPass Identity Provider \(SAML IdP Service\) on page 55](#)
- [Device MAC Authentication on page 57](#)
- [EDUROAM Service on page 58](#)
- [Encrypted Wireless Access via 802.1X Public PEAP method on page 60](#)
- [Guest Access on page 62](#)
- [Guest Access Web Login on page 63](#)
- [Guest Authentication with MAC Caching on page 64](#)
- [Guest Social Media Authentication on page 66](#)
- [OAuth2 API User Access on page 68](#)
- [Onboard on page 68](#)

Services Supported for High Capacity Guest Mode

The following service templates are supported when the **High Capacity Guest (HCG)** mode is enabled:

- W-ClearPass Admin Access (Active Directory)
- W-ClearPass Admin SSO Login (SAML SP Service)
- W-ClearPass Identity Provider (SAML IdP Service)
- Encrypted Wireless Access via 802.1X Public PEAP method
- Guest Access
- Guest Access - Web Login
- Guest MAC Authentication
- OAuth2 API User Access

The following service types are supported when the **HCG** mode is enabled:

- MAC Authentication
- RADIUS Authorization
- RADIUS Enforcement
- RADIUS Proxy
- Dell Application Authentication
- Dell Application Authorization
- TACACS+ Enforcement
- Web-based Authentication
- Web-based Open Network Access

Authentication Methods Used in HCG Mode

The following authentication methods are used in service templates in the **HCG** mode:

- PAP
- CHAP
- MSCHAP
- EAP_MD5
- MAC_AUTH
- AUTHORIZE
- EAP_PEAP_PUBLIC

Viewing the List of Services

The **Services** page shows the current list and order of services that W-ClearPass Policy Manager follows during authentication and authorization. You can use the configured default service types or you can add additional services. Services included in square brackets "[]" indicate default services.

To view the list of services on the current W-ClearPass server:

Navigate to **Configuration > Services**.

The **Services** page opens:

Figure 5: Services Page

Configuration » Services
Services

 Add
 Import
 Export All

Filter: Name contains Go Clear Filter Show 100 records

#	Order	Name	Type	Template	Status
1.	1	Radius-generic-suri	RADIUS	RADIUS Enforcement (Generic)	
2.	2	App-auth	Application	Aruba Application Authentication	
3.	3	MAB-suri	RADIUS	MAC Authentication	
4.	4	1X-Wireless	RADIUS	802.1X Wireless	
5.	5	Health-only	WEBAUTH	Web-based Health Check Only	
6.	6	Tacacs-suri	TACACS	TACACS+ Enforcement	
7.	7	[Policy Manager Admin Network Login Service]	TACACS	TACACS+ Enforcement	
8.	8	Guest Operator Logins	Application	Aruba Application Authentication	
9.	9	[AirGroup Authorization Service]	RADIUS	RADIUS Enforcement (Generic)	
10.	10	[Aruba Device Access Service]	TACACS	TACACS+ Enforcement	
11.	11	[Guest Operator Logins]	Application	Aruba Application Authentication	
12.	12	suri-captive Guest Access	RADIUS	RADIUS Enforcement (Generic)	
13.	13	Web-auth	WEBAUTH	Web-based Authentication	

Showing 1-13 of 13

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

The following table describes the **Services** parameters:

Table 3: Services Page Parameters

Parameter	Description
Name	Displays the name of the service.
Type	Displays the type of authentication associated with the service. For example, RADIUS, Web Authentication, and TACACS.
Template	Specifies the type of the service template to create a service.

Table 3: Services Page Parameters (Continued)

Parameter	Description
Status	Displays the status of the service. A green/red icon indicates enabled/disabled state. Click the icon to toggle the status of a service between Enabled and Disabled . NOTE: If a service is in Monitor mode, an [m] indicator is displayed next to the Status icon.

For more information, see:

- [Adding Services on page 1](#)
- [Modifying Services on page 1](#)
- [Reordering Services on page 43](#)

Viewing Existing Services

You can view all configured services in a list or drill down to individual services in the **Services** page.

1. To view a list of services that you can filter by phrase or sort by order, navigate to **Configuration > Services**.
2. In the **Services** page, select the name of a **Service** to view its details.

The following figure displays the **Services** tab with the list of services with the sorting tool:

Figure 6: List of Services with Sorting Tool

The screenshot shows the 'Services' page with the 'Summary' tab selected. The service details are as follows:

- Name:** 1X-Wireless
- Description:** 802.1X Wireless Access Service
- Type:** 802.1X Wireless
- Status:** Disabled
- Monitor Mode:** ☐ Enable to monitor network access without enforcement
- More Options:** ☐ Authorization ☐ Posture Compliance ☐ Audit End-hosts ☐ Profile Endpoints ☐ Accounting Proxy

Below the details is the 'Service Rule' section, which shows a table of 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...			

The **Summary** tab provides the detailed information about the selected service with the link to other tabs.

For example, to add authentication sources and authentication methods, click **Authentication**.

The following figure displays the **Summary** tab with service details:

Figure 7: Details for an Individual Service

Services - 1X-Wireless

Summary	Service	Authentication	Roles	Enforcement												
Service Details: Name: 1X-Wireless Description: 802.1X Wireless Access Service Type: 802.1X Wireless Status: Disabled Monitor Mode: Disabled More Options: -																
Service Rule Match 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>EQUALS</td> <td>Wireless-802.11 (19)</td> </tr> <tr> <td>2. Radius:IETF</td> <td>Service-Type</td> <td>BELONGS_TO</td> <td>Login-User (1), Framed-User (2), Authenticate-Only (8)</td> </tr> </tbody> </table>					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)
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)													
Authentication: Authentication Methods: 1. [EAP PEAP] 2. [EAP FAST] 3. [EAP TLS] 4. [EAP TTLS] 5. [EAP MSCHAPv2] 6. [MSCHAP] 7. [PAP] Authentication Sources: 1. 172.31.1.11 [Active Directory] 2. [Local User Repository] [Local SQL DB] Strip Username Rules: user:@																
Roles: Role Mapping Policy: -																
Enforcement:																

Adding and Removing Services

You can modify a list of services by creating a new service, and modifying or deleting an existing service.

Creating a New Service

To create a new service:

1. Navigate to **Configuration > Services**.

The **Services** page opens.

Figure 8: Services Page

Configuration > Services

Services

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

Filter: Name contains [] Go Clear Filter

Show 100 records

#	Order	Name	Type	Template	Status
1.	1	Radius-generic-suri	RADIUS	RADIUS Enforcement (Generic)	❌
2.	2	App-auth	Application	Aruba Application Authentication	✅
3.	3	MAB-suri	RADIUS	MAC Authentication	✅
4.	4	1X-Wireless	RADIUS	802.1X Wireless	✅
5.	5	Health-only	WEBAUTH	Web-based Health Check Only	✅
6.	6	Tacacs-suri	TACACS	TACACS+ Enforcement	✅
7.	7	[Policy Manager Admin Network Login Service]	TACACS	TACACS+ Enforcement	✅
8.	8	Guest Operator Logins	Application	Aruba Application Authentication	✅
9.	9	[AirGroup Authorization Service]	RADIUS	RADIUS Enforcement (Generic)	✅
10.	10	[Aruba Device Access Service]	TACACS	TACACS+ Enforcement	❌
11.	11	[Guest Operator Logins]	Application	Aruba Application Authentication	✅
12.	12	suri-captive Guest Access	RADIUS	RADIUS Enforcement (Generic)	✅
13.	13	Web-auth	WEBAUTH	Web-based Authentication	✅

Showing 1-13 of 13

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

2. Click **Add**.

The **Add Services** dialog opens.

Figure 9: Add Services Page

Configuration » Services » Add

Services

Service	Authentication	Authorization	Roles	Posture	Enforcement	Audit	Profiler	Summary
Type:	DELL W-Series Wireless							
Name:								
Description:	DELL 802.1X Wireless Access Service							
Monitor Mode:	☐ Enable to monitor network access without enforcement							
More Options:	☒ Authorization ☒ Posture Compliance ☒ Audit End-hosts ☒ Profile Endpoints							
Service Rule								
Matches ☐ ANY or ☒ ALL of the following conditions:								
Type	Name	Operator	Value					
1. Radius:IETF	NAS-Port-Type	EQUALS	Wireless-802.11 (19)					
2. Radius:IETF	Service-Type	BELONGS_TO	Login-User (1), Framed-User (2), Authenticate-Only (8)					
3. Radius:Aruba	Aruba-Essid-Name	EXISTS						
4. Click to add...								

Table 4 describes the **Services** configuration parameters. Note that the available settings vary, depending upon the service type selected.

Table 4: Services Page

Parameter	Action/Description
Type	Select the desired service type from the drop-down list. When working with service rules, you can select from the following namespace dictionaries: • Application: The type of application for this service. • Authentication: The Authentication method to be used for this service. • Connection: Originator address (Src-IP-Address, Src-Port), Destination address (Dest-IP-Address, Dest-Port), and Protocol • Device: Filter the service based on a specific device type, vendor, operating system location, or controller ID. • Date: Time-of-Day, Day-of-Week, or Date-of-Year • Endpoint: Filter based on endpoint information such as enabled/disabled, device, OS, location, and more. • Host: Filter based on host Name, OSType, FQDN, UserAgent, CheckType, UniqueID, Agent-Type, and InstalledSHAs, • RADIUS: W-ClearPass 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 (link). The notation RADIUS:IETF refers to the RADIUS attributes defined in RFC 2865 and associated RFCs. As the name suggests, RADIUS namespace is only available if the request type is RADIUS. • Any other supported namespace: See Rules Editing and Namespaces on page 845 for an exhaustive list of namespaces and their descriptions. 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.
Name	Enter the name or label for the service you want to create.
Description	Enter a description that provides additional information to identify the service. This field is

Table 4: Services Page (Continued)

Parameter	Action/Description
	optional.
Monitor Mode	Optionally check the Enable to monitor network access without enforcement 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. W-Policy Manager also allows <i>Policy Simulation</i> (Monitoring > Policy Simulation), where the administrator can test the results of a particular configuration of policy components.
More Options	Select any of the available check boxes to enable the configuration tabs for those options. The available check boxes varies based on the type of service that is selected and may include one or more of the following: • Authorization: Select an authorization source from the drop-down list to add the source or select the Add new Authentication Source link to create a new source. • Posture Compliance: Select a Posture Policy from the drop-down list to add the policy or create a new policy by clicking the link. Select the default Posture token. Specify whether to enable auto-remediation of non-compliant end hosts. If this is enabled, then enter the Remediation URL. You can specify the Posture Server from the drop-down list or add a new server by clicking the Add new Posture Server link. • Audit End-hosts: Select an Audit Server, either built-in or customized. Refer to Configuring Audit Servers on page 327 for audit server configuration steps. For this type of service, you can perform audit Always, When posture is not available, or For MAC authentication requests. You can specify to trigger an audit always, when posture is not available, or for MAC authentication requests. If For MAC authentication requests is specified, then you can perform an audit For known end-hosts only or For unknown end hosts only, or For all end hosts. Known end hosts 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, Policy Manager re-applies policies on the network device by one of the following ways: ■ No Action: The audit does not apply policies on the network device after this audit. ■ Do SNMP bounce: This option bounces the switch port or force an 802.1X re-authentication (both done using SNMP). NOTE: Bouncing the port triggers a new 802.1X or 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. ■ Trigger RADIUS CoA action: This option sends a RADIUS CoA command to the network device by Policy Manager. • Optionally configure Profiler settings. Select one or more Endpoint Classification items from the drop down list, then select the RADIUS CoA action. You can also create a new action by selecting the Add new RADIUS CoA Action link.

Creating a Service by Copying an Existing Service



You can perform a service copy operation only on a Publisher node.

To create a service template by making a copying an existing service:

From the **Services** page, select the check box by a service, then click **Copy**.

Modifying a Service

For full access in modifying a service, you must log in to the Publisher node.

To modify an existing service:

1. From the **Services** page, click the check box for the service you want to modify.

The **Configuration > Services > Edit > <service name>** dialog opens.

Figure 10: *Edit Services Dialog*

Configuration » Services » Edit - [AirGroup Authorization Service]
Services - [AirGroup Authorization Service]

Summary **Service** Authentication Roles Enforcement

Service:

Name:	[AirGroup Authorization Service]
Description:	Authorization service for AirGroup device access
Type:	RADIUS Enforcement (Generic)
Status:	Enabled
Monitor Mode:	Disabled
More Options:	-

Service Rule

Match ALL of the following conditions:

Type	Name	Operator	Value
1. Radius:IETF	Called-Station-Id	EQUALS	AirGroup
2. Radius:IETF	Service-Type	EQUALS	Authorize-Only (17)

Authentication:

Authentication Methods:	[Allow All MAC AUTH]
Authentication Sources:	[Guest Device Repository]
Strip Username Rules:	-

Roles:

Role Mapping Policy:	[AirGroup Version Match]

Enforcement:

Use Cached Results:	Disabled
Enforcement Policy:	[AirGroup Enforcement Policy]

2. Select the **Service** tab to edit the service information.

3. Modify the parameters as needed, then click **Save**.

You can also disable or enable a service from the **Edit Services** dialog page by clicking **Disable** or **Enable** in the lower right of the page.

Removing a Non-Default Service

To remove a non-default service:

1. From the **Services** page, select the check box for the non-default service you want to remove.
2. Click **Delete**.

Reordering Services

W-ClearPass 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.

To change the order of the services:

1. Navigate to the **Configuration > Services** page.

The **Services** page appears.

Figure 11: Services Page Reorder Button

2. Click the **Reorder** button (located on the lower-right portion of the page).

The Reorder Services page appears.

3. Click the service you want to move to another position in the order (see [Figure 12](#)).

In this example, we will move **Guest Operator Logins** at the 5th position to the 2nd position.

Figure 12: Selecting the Service to Be Reordered

Configuration > Services > Reorder

Reorder Services

To reorder services, click on a service you want to move. Click on another service where you want to move the previously selected service.

Order	Name	Service Details:
1	[Policy Manager Admin Network Login Service]	Name: [Guest Operator Logins]
2	[Insight Operator Logins]	Template: Aruba Application Authentication
3	[AirGroup Authorization Service]	Type: Application
4	[Aruba Device Access Service]	Description: Authentication service for Guest application
5	[Guest Operator Logins]	Status: Enabled

Service Rule

```
(
  (Application:Name EQUALS Guest)
  AND (Authentication:Type NOT_EQUALS SSO) )
AND (Connection:Protocol EQUALS Application)
```

4. Select the position where you want to move the service (see [Figure 13](#)).

Figure 13: Selecting the Destination Order Position

Configuration > Services > Reorder

Reorder Services

To reorder services, click on a service you want to move. Click on another service where you want to move the previously selected service.

Order	Name	Service Details:
1	[Policy Manager Admin Network Login Service]	Name: [Guest Operator Logins]
2	[Insight Operator Logins]	Template: Aruba Application Authentication
3	[AirGroup Authorization Service]	Type: Application
4	[Aruba Device Access Service]	Description: Authentication service for Guest application
5	[Guest Operator Logins]	Status: Enabled

Service Rule

```
(
  (Application:Name EQUALS Guest)
  AND (Authentication:Type NOT_EQUALS SSO) )
AND (Connection:Protocol EQUALS Application)
```

5. Click the selected destination position (see [Figure 14](#)).

The service is now moved to its new position in the services order.

Figure 14: Service Moved to New Order Position

Configuration > Services > Reorder

Reorder Services

To reorder services, click on a service you want to move. Click on another service where you want to move the previously selected service.

Order	Name	Service Details:
1	[Policy Manager Admin Network Login Service]	Name: [Policy Manager Admin Network Login Service]
2	[Guest Operator Logins]	Template: TACACS+ Enforcement
3	[Insight Operator Logins]	Type: TACACS
4	[AirGroup Authorization Service]	Description: Service for access to Policy Manager Admin for network users
5	[Aruba Device Access Service]	Status: Enabled

Service Rule

```
(
  (Connection:NAD-IP-Address EQUALS 127.0.0.1) )
AND (Connection:Protocol EQUALS TACACS)
```

6. Click **Save**.

You return to the Services page, which shows the service in its new order and displays the message:

Services have been reordered successfully.

802.1X Wired, 802.1X Wireless, and Dell 802.1X Wireless

The **802.1X Wired** template is designed for wired end-hosts connecting through an Ethernet LAN with authentication using IEEE 802.1X. The **802.1X Wired** template allows configuration of both identity and posture-based policies.

The **802.1X Wireless** template is intended for wireless end-hosts connecting through an 802.11 wireless access device or controller with authentication using IEEE 802.1X. The **802.1X Wireless** template allows configuring both identity and posture based policies.

The **Dell W-Series 802.1X Wireless** template is designed for wireless end-hosts connecting through a Dell W-Series 802.11 wireless access device or controller with authentication using IEEE 802.1X (service rules customized for Dell WLAN controllers).



All three templates are configured using identical parameters.

Figure 15: Service Templates - 802.1X Wired Service Template

Service Templates - 802.1X Wired

General Authentication Wired Network Settings Posture Settings Enforcement Details

Name Prefix*: Dot1xWired

Description

For end-hosts connecting through an Ethernet LAN, with authentication via IEEE 802.1X. This template configures AD Authentication Source; joins this node to an AD Domain; creates Enforcement Policy for AD based attributes; creates Network Access Device.

Back to Start Here Delete Next > Add Service Cancel

To add a new service for the selected service template,

1. Specify a unique **Name Prefix** (applies only to the selected template) in the **General** tab.
2. Update the required fields in the **Authentication** and **Enforcement Details** sections.
3. Click **Add Service**.

An entry for the new set of configuration is created under the **Services, Roles, Role Mapping, Enforcement Policies** and **Profiles** menus.



The sections shown in the figure and listed above are not same for all service templates. It is recommended to customize the respective templates when you add a new service.

Once you add a new service to the service template, the service denoted by the **Name Prefix** appears in the **Select Prefix** drop-down. Selecting a prefix from the drop-down populates the existing configuration for the service.

4. Edit the changes and click **Edit Service** to save the changes.

Deleting a Service

To delete a service:

1. Select the appropriate service from the **Select Prefix** drop-down
2. Click **Delete**.

All the configured entries under the **Services, Authentication Source, Roles, Role Mapping, Enforcement Policies** and **Profiles** menu are deleted if these entities were created from the service template.



When you edit or delete the entities of a service, a message is displayed at the top of the entity page stating that the selected entity was created through the service template.

Do not delete entities used in service configurations that are not created using the service template.

The following table describes the parameters in the 802.1X Wired, 802.1X Wireless, and Dell W-Series 802.1X Wireless service templates:

Table 5: 802.1X Wired, 802.1X Wireless, and Dell W-Series 802.1X Wireless Service Template Parameters

Parameter	Action/Description
General	
Select Prefix	1. Select a prefix from the existing list of prefixes. This populates the preconfigured information in the Authentication and Enforcement Details sections. The Name Prefix field is not editable.
Name Prefix	2. Enter a prefix that is appended to services using this template. Use this to identify the services that use templates.
Authentication	
Select Authentication Source	1. Select any available authentication source from the list. The information updated in the Authentication and Enforcement Details tabs will be auto-populated.
Active Directory Name	2. Enter the name of the Active Directory. This field is mandatory.
Description	3. Enter a description that helps you to identify the characteristics of this template. This field is mandatory.
Server	4. Enter the hostname or the IP address of the Active Directory server. This field is mandatory.
Port	5. Enter the TCP port where the server is listening for a connection. This field is mandatory.
Identity	6. Enter the Distinguished Name (DN) of the administrator account. This field is mandatory.
Password	7. Enter the account password. This field is mandatory.
NetBIOS	8. Enter the server Active Directory domain name. This field is mandatory.
Base DN	9. Enter the DN of the node in your directory tree from which to start searching for records. This field is mandatory.
Enforcement Details	
Attribute	The attributes defined in the Authentication Source are listed here.

Table 5: 802.1X Wired, 802.1X Wireless, and Dell W-Series 802.1X Wireless Service Template Parameters
(Continued)

Parameter	Action/Description
Name	- Configure an optional enforcement policy based on the following attributes: - Email - Name - Phone - UserDN - Company - member of - Title For example, you can configure an enforcement policy for a contractor specifying that "If Name equals <contractor_name>, then assign the [Contractor] Role."
Attribute Value	Enter the active directory attribute value for the selected name in the Attribute Name field.
VLAN ID	Enter the standard RADIUS-IETF VLAN ID.
Wired Network Settings	
Select Switch	Select any switch from the drop-down list.
Device Name	Enter the name of the device.
IP Address	Enter the IP address of the device.
Vendor Name	Select the manufacturer of the wired controller.
RADIUS Shared Secret	Enter the shared secret that is configured on the controller and inside W-Policy Manager to send and receive RADIUS requests.
Enable RADIUS CoA	Select to enable RADIUS initiated Change of Authorization (CoA) on the network device.
RADIUS CoA Port	Specifies the default port 3799 if RADIUS CoA is enabled. Change this value only if you defined a custom port on the network device.
Wireless Network Settings	
Wireless controller name	Enter the name of the wireless controller.
Controller IP Address	Enter the IP address of the wireless controller.
Vendor Name	Select the manufacturer of the wireless controller.
RADIUS Shared Secret	Enter the shared secret that is configured on the controller and W-Policy Manager to send and receive RADIUS requests.

Table 5: 802.1X Wired, 802.1X Wireless, and Dell W-Series 802.1X Wireless Service Template Parameters (Continued)

Parameter	Action/Description
Enable RADIUS CoA	5. Select to enable RADIUS initiated CoA on the network device.
RADIUS CoA Port	Specifies the default port 3799 if RADIUS CoA is enabled. 6. Change this value only if you defined a custom port on the network device.
Posture Settings	
Enable Posture Checks	7. Select the check box to perform health checks post authentication. This enables the Host Operating System and Quarantine Message fields.
Host Operating System	8. Select the operating system: Windows , Linux , or Mac OS X .
Quarantine Message	9. Specify the quarantine message that will appear on the client.

Auto Sign-On

The **Auto Sign-On** service template allows you to access the SAML-based single sign on enabled applications (such as W-Policy Manager, Guest, Onboard, and W-ClearPass Insight) using a network authenticated (802.1X) identity through controllers.

The following figure displays the **Auto Sign-On** service template :

Figure 16: Auto Sign-On Service Template

Service Templates - Aruba Auto Sign-On

General	Authentication	Enforcement Details	SP Details
Name Prefix*: ASO-Service-Template			
Description For accessing SAML based single sign-on enabled applications using network authenticated identity through Aruba controllers.			
Back to Start Here Delete Next > Add Service Cancel			

The following table describes the **Auto Sign-On** service template parameters:

Table 6: W-ClearPass Auto Sign-On Service Template Parameters

Parameter	Action/Description
General	
Select Prefix	Select a prefix from the existing list of prefixes. This field populates the pre-configured information in the Authentication , SP details , and Enforcement Details sections. The Name Prefix field is not editable.
Name Prefix	Enter a prefix that you want to append to services using this template. Use this to identify services that use templates.

Table 6: *W-ClearPass Auto Sign-On Service Template Parameters (Continued)*

Parameter	Action/Description
Authentication	
Select Authentication Source	Select an authentication source from the list. The information provided in the Authentication , Enforcement Details , and SP details tabs are auto-populated.
Active Directory Name	Enter the hostname or the IP address of the Active Directory server. This field is mandatory.
Description	Enter a description that helps you to identify the characteristics of this template. This field is mandatory.
Server	Enter the hostname or the IP address of the Active Directory server. This field is mandatory.
Identity	Enter the DN of the administrator account. This field is mandatory.
NETBIOS	Enter the server Active Directory domain name. This field is mandatory.
Base DN	Enter the DN of the administrator account. This field is mandatory.
Password	Enter the account password. This field is mandatory.
Port	Enter the TCP port where the server is listening for a connection. This value defaults to 389 . This field is mandatory.
Enforcement Details	
Create new Enforcement Policy	Configure an optional enforcement policy based on the following attributes: • Department • Email • Name • Phone • UserDN • company • memberOf • Title
SP Details	
SP URL	Enter the Service Provider (SP) URL.
Attribute Name	Enter attribute names and assign values to those names. These name/value pairs are included in SAML responses.
Attribute Value	

Dell VPN Access with Posture Checks

This template authenticates Dell VPN clients connecting remotely to corporate networks. Differentiated access is based on the result of posture checks. This template:

- Configures an AD authentication source
- Joins this node to the AD domain

- Creates an enforcement policy for AD-based attributes
- Creates a NAD



Posture checks are not performed if the **High Capacity Guest** mode is enabled in the cluster.



You can view only the default user role in the **Dell User Roles for different access privileges** tab if the **HCG** mode is enabled in the cluster.

The following figure displays the **Dell VPN Access with Posture Checks** service template:

Figure 17: Dell VPN access with Posture checks Service Template

Configuration » Start Here

Service Templates - Aruba VPN access with Posture checks

General | Authentication | Aruba Wireless Controller for VPN access | Aruba User Roles for different access privileges

Name Prefix*: VPN-Service-Template

Description

For Aruba VPN clients connecting remotely to the corporate network, with differentiated access based on the results of Posture checks. This template configures an AD Authentication Source; joins this node to the AD Domain; creates Enforcement Policy for AD based attributes; creates Network Access Device.

[Back to Start Here](#) [Delete](#) [Next >](#) [Add Service](#) [Cancel](#)

The following table describes the **Dell VPN Access with Posture Checks** service template parameters:

Table 7: Dell VPN Access with Posture Checks Service Template Parameters

Parameter	Description
General	
Select Prefix	Select a prefix from the existing list of prefixes. This populates the pre-configured information in the Authentication Dell Wireless Controller for VPN Settings and Dell User Roles for different access privileges sections. The Name Prefix field is not editable.
Name Prefix	Enter a prefix that you want to append to services using this template. Use this to identify services that use templates.
Authentication	
Select Authentication Source	Select an authentication source from the list. The information provided in the Authentication, Dell Wireless Controller for VPN Settings , and Dell User Roles for different access privileges sections are auto-populated.
Active Directory Name	Enter the Active Directory name.
Description	Enter a description that helps you to identify the characteristics of this template.
Server	Enter the hostname or the IP address of the Active Directory server.
Identity	Enter the Distinguished Name of the administrator account.
NETBIOS	Enter the server Active Directory domain name.
Base DN	Enter the DN of the node in your directory tree from which to start searching for records.

Table 7: Dell VPN Access with Posture Checks Service Template Parameters (Continued)

Parameter	Description
Password	Enter the account password.
Port	Enter the TCP port where the server is listening for a connection.
Dell Wireless Controller for VPN Access	
Select Wireless Controller	Select a wireless controller from the drop-down list.
Wireless controller name	Enter the name given to the wireless controller.
Controller IP Address	Enter the wireless controller's IP address.
Vendor Name	Select the manufacturer of the wireless controller.
RADIUS Shared Secret	Enter the shared secret that is configured on the controller and inside W-Policy Manager to send and receive RADIUS requests.
Enable RADIUS CoA	Select this option to enable RADIUS initiated CoA on the network device.
RADIUS CoA Port	Specifies the default port 3799 if RADIUS CoA is enabled. Change this value only if you defined a custom port on the network device.
Dell User Roles for different access privileges - Create a new Enforcement Policy	
Initial Role (before posture checks)	Enter the initial role of the client before posture checks are performed.
Quarantined Role (failed posture checks)	Enter the role of clients that fail posture checks.
Healthy Role (passed posture checks)	Enter the role of the client after a posture check is passed and deemed healthy.

Certificate/Two-Factor Authentication for W-ClearPass Application Login

This template allows administrators and operators to log in to W-ClearPass using a smart card and TLS (Transport Layer Security) certificates.

To log in using a smart card and TLS certificates, ensure that the services are configured using the **Certificate/Two-Factor Authentication for ClearPass Application Login** service template.

The following figure displays the **Certificate/Two-Factor Authentication for ClearPass Application Login** service template:

Figure 18: *Certificate/Two-Factor Authentication Service Template*

Service Templates - Certificate/Two-factor Authentication for ClearPass Application Login

General Service Rule Authentication IdP Details Enforcement Details

Name Prefix*: Cert-Two-factor

Description

To use certificate or two-factor authentication to allow access to ClearPass applications. This configures SAML-based Single Sign-On (SSO) for access to CPPM, Insight, Guest and Operator screens via ClearPass Identity Provider (IdP). This also allows to configure ClearPass IdP to support certificate or two-factor authentication for SAML based logins.

[Back to Start Here](#) [Delete](#) [Next >](#) [Add Service](#) [Cancel](#)

Specify the **Certificate/Two-Factor Authentication for ClearPass Application Login** service template parameters as described in the following table:

Table 8: *W-ClearPass Certificate/Two-Factor Authentication Service Template Parameters*

Parameter	Action/Description
General	
Select Prefix	1. Select a prefix from the existing list of prefixes. This field populates the pre-configured information in the Authentication , SP details , and Enforcement Details sections. The Name Prefix field is not editable.
Name Prefix	2. Enter a prefix that you want to append to services using this template. Use this to identify services that use templates.
Service Rule	
Application	3. Select the application for which SAML-based Single Sign-On (SSO) should be enabled from the following options: Policy Manager , Guest , Insight , and Onboard .
Authentication	
Select Authentication Source	4. Select an authentication source from the list. The information provided in the Authentication , Enforcement Details , and SP details tabs are auto-populated.
Active Directory Name	5. Enter the hostname or the IP address of the Active Directory server. This field is mandatory.
Description	6. Enter a description that helps you to identify the characteristics of this template. This field is mandatory.
Server	7. Enter the hostname or the IP address of the Active Directory server. This field is mandatory.
Port	8. Enter the TCP port where the server is listening for a connection. The default value is value defaults to 389 . This field is mandatory.
Identity	9. Enter the DN of the administrator account. This field is mandatory.

Table 8: W-ClearPass Certificate/Two-Factor Authentication Service Template Parameters (Continued)

Parameter	Action/Description
Password	10. Enter the account password. This field is mandatory.
NETBIOS	11. Enter the server Active Directory domain name. This field is mandatory.
Base DN	12. Enter the Distinguished Name (DN) of the administrator account. This field is mandatory.
IdP Details	
Page Name	13. Select the Web Login pages from the drop-down list. For more information, see the next section, Creating a New Web Login Page .
Enforcement Details	
Certificate Attribute - Super Admin Condition	14. Select the certificate attribute from the drop-down list. 15. Enter the value in the Super Admin Condition field that matches the Certificate Attribute value to provide the super administrator access.
Certificate Attribute - Read Only Admin Condition	16. Select the certificate attribute from the drop-down list. 17. Enter the value in the Read Only Admin Condition field that matches the Certificate Attribute value to provide the Read-Only administrator access.
Certificate Attribute - Help Desk Admin Condition	18. Select the certificate attribute from the drop-down list. 19. Enter the value in the Help Desk Admin Condition field that matches the Certificate Attribute value to provide the help desk administrator access.

Creating a New Web Login Page

To create a new Web Login page:

1. Click the **Add New Guest Web Login page** link.
This opens the W-ClearPass Guest application in which you can create a new **Guest Web Login** page.
2. To log in using a smart card and TLS certificates, navigate to **ClearPass Guest > Configuration > Pages > Web Logins**.
3. In the **Vendor Settings** field, select **Single Sign On -SAML Identity Provider**.
 - a. When you select **Optional - Request a client certificate from the user**, but allow none from the **Client Certificate** field, the user needs to provide a certificate, username, and password.
 - b. When you select **Required - Require a client certificate from the user** from the **Client Certificate** field, the user needs to provide only certificates for authentication.
This enables the **Authentication** field with the following options:
 - **Certificate only - No username or password required:** Requires only certificate authentication.
 - **Credentials - Also require a username and password:** Requires the username and password.

W-ClearPass Admin Access

This template is designed for services that authenticate users against Active Directory (AD).

Use Active Directory attributes to determine appropriate privilege levels for W-ClearPass Policy Manager admin access.

The following figure displays the **W-ClearPass Admin Access** service template:

Figure 19: *W-ClearPass Admin Access Service Template*

Service Templates - ClearPass Admin Access (Active Directory)

General Authentication Role Mapping

Name Prefix*: CPPM_Admin_Access

Description

Service that authenticates users against Active Directory (AD) and uses AD attributes to determine appropriate privilege level for ClearPass Policy Manager admin access.

Back to Start Here Delete Next > Add Service Cancel

Specify the **W-ClearPass Admin Access** service template parameters as described in the following table:

Table 9: *W-ClearPass Admin Access Service Template Parameters*

Parameter	Action/Description
General	
Select Prefix	Select a prefix from the existing list of prefixes. This populates the preconfigured information in the Authentication and Role Mapping sections. The Name Prefix field is not editable.
Name Prefix	Enter a prefix that you want to append to services using this template. Use this to identify services that use templates.
Authentication: Create an Active Directory Authentication Source	
Select Authentication Source	Select an authentication source from the list. The information updated in the Authentication and Role Mapping tabs are auto-populated.
Active Directory Name	Enter the hostname or the IP address of the Active Directory server. This field is mandatory.
Description	Enter a description that helps to identify the characteristics of this template. This field is mandatory.
Server	Enter the hostname or the IP address of the Active Directory server. This field is mandatory.
Port	Enter the TCP port where the server is listening for a connection. This field is mandatory.
Identity	Enter the Distinguished Name (DN) of the administrator account. This field is mandatory.
Password	Enter the account password. This field is mandatory.
NetBIOS	Enter the server Active Directory domain name. This field is mandatory.
Base DN	Enter the DN of the administrator account. This field is mandatory.
Role Mapping	
Attribute Name	Select the Active Directory attribute.

Table 9: W-ClearPass Admin Access Service Template Parameters (Continued)

Parameter	Action/Description
Super Admin Condition	Defines the various privilege levels.
Read Only Admin Condition	
Help Desk Condition	

W-ClearPass Admin SSO Login (SAML SP Service)

This application service template allows Security Asserting Markup Language (SAML) based Single Sign-On (SSO) authenticated users to access Policy Manager, Guest, Insight, and Operator pages.

The following figure displays the **W-ClearPass Admin SSO Login** service template:

Figure 20: ClearPass Admin SSO Login (SAML SP Service) Service Template

Service Templates - ClearPass Admin SSO Login (SAML SP Service)

The following table describes the **W-ClearPass Admin SSO Login** service template parameters:

Table 10: W-ClearPass Admin SSO Login Service Template Parameters

Parameter	Description
General	
Select Prefix	Select a prefix from the existing list of prefixes. This populates the pre-configured information in the Service Rule tab. The Name Prefix field is not editable.
Name Prefix	Enter a prefix that you want to append to services using this template. Use this to identify services that use templates.
Service Rule	
Application	Select the application that single-sign-on-authenticated administrative users can access.

W-ClearPass Identity Provider (SAML IdP Service)

This template is designed for services that act as an Identity Provider (IdP). This IdP feature allows the Layer-2 device, RADIUS server, and SAML IdP to work together and deliver application-based single sign-on using network authentication information.

The following figure displays the **W-ClearPass Identity Provider (SAML IdP Service)** service template:

Figure 21: *Identity Provider (SAML IdP Service)*

Service Templates - ClearPass Identity Provider (SAML IdP Service)

General | Authentication | SP Details

Name Prefix*: IdP-SAML

Description

To provide a SAML based single sign-on service that can be used by other applications.

[Back to Start Here](#) [Delete](#) [Next >](#) [Add Service](#) [Cancel](#)

The following table describes the **W-ClearPass Identity Provider (SAML IdP Service)** service template parameters:

Table 11: *W-ClearPass Identity Provider (SAML IdP Service) Service Template Parameters*

Parameter	Description
General	
Select Prefix	Select a prefix from the existing list of prefixes. This populates the pre-configured information in the Authentication and SP Details sections. The Name Prefix field is not editable.
Name Prefix	Enter a prefix that you want to append to services using this template. Use this to identify services that use templates.
Authentication	
Select Authentication Source	Select an authentication source from the list, the information updated in the Authentication and SP Details tabs are auto-populated.
Active Directory Name	Enter the hostname or the IP address of the Active Directory server. This field is mandatory.
Description	Enter a description that helps you to identify the characteristics of this template. This field is mandatory.
Server	Enter the hostname or the IP address of the Active Directory server. This field is mandatory.
Identity	Enter the DN of the administrator account. This field is mandatory.
NetBIOS	Enter the Active Directory server domain name. This field is mandatory.
Base DN	Enter the DN of the administrator account. This field is mandatory.
Password	Enter the account password. This field is mandatory.
Port	Enter the TCP port where the server is listening for a connection. This field is mandatory.
SP Details	

Table 11: W-ClearPass Identity Provider (SAML IdP Service) Service Template Parameters (Continued)

Parameter	Description
SP URL	Enter the Service Provider (SP) URL.
Attribute Name	Enter the name of the attributes and assign values to those names. These name/value pairs are included in SAML responses.
Attribute Value	

Device MAC Authentication

This template is designed for authenticating guest devices based on their MAC address.

You can limit the network access for guest devices that do not have user directly associated with them for a specific duration in days or by the bandwidth limit.

The following figure displays the **Device MAC Authentication** service template:

Figure 22: Device MAC Authentication Service Template

Service Templates - Device MAC Authentication

Specify the parameters in the **Device MAC Authentication** service template as described in the following table:

Table 12: Device MAC Authentication Template Parameters

Parameter	Action/Description
General	
Select Prefix	Select a prefix from the existing list of prefixes. This populates the preconfigured information in the Authentication and SP Details sections. The Name Prefix field is not editable.
Name Prefix	Enter a prefix that you want to append to services using this template. Use this to identify services that use templates.
Network Settings	
Select Device	Select a preconfigured device from the drop-down list. To create a new device, leave this field blank and enter the remaining fields.
Device Name	The name of the device is populated automatically based on the device selected from the Select Device field. If you create a new device, enter the name of the device.
IP Address	The IP address of the device is populated automatically based on the device selected from the

Table 12: Device MAC Authentication Template Parameters (Continued)

Parameter	Action/Description
	Select Device field. If you create a new device, enter the name of the device.
Vendor Name	The name of the manufacturer of the device is populated automatically based on the device selected from the Select Device field. If you create a new device, enter the name of the manufacturer of the device.
RADIUS Shared Secret	Enter the shared secret that is configured on the controller and in W-Policy Manager to send and receive RADIUS requests.
Enable RADIUS CoA	Select to enable RADIUS initiated Change of Authorization (CoA) on the network device.
RADIUS CoA Port	Specifies the default port 3799 if RADIUS CoA is enabled. Change this value only if you defined a custom port on the network device.
Device Access Restrictions	
Days allowed for access	Select the days on which network access is allowed.
Maximum bandwidth allowed per device	Enter a number to set an upper limit for the amount of data in megabytes to which a device is allowed per day. A value of 0 (zero), the default, means no limit is set.

EDUROAM Service

This template is designed for the following scenarios:

- Local campus users connecting to eduroam from the local wireless network.
- Roaming users from an eduroam campus connecting to their campus network.
- Roaming users connecting from local campus or other campuses that are part of the eduroam federation.



You cannot view the **EDUROAM** service template if the **HCG** mode is enabled in the cluster.

The following figure displays the **EDUROAM** service template:

Figure 23: *EDUROAM Service Template*

Service Templates - EDUROAM service

General Service Rule Authentication Wireless Network Settings Federation Level RADIUS Server (FLR)

Name Prefix*: EDUROAM

Description

Services are generated for: Local campus users connecting to eduroam from the local wireless network; roaming users from an eduroam campus connecting to their campus network; roaming users connecting from local campus or other campuses that are part of the eduroam federation.

[Back to Start Here](#) [Delete](#) [Next >](#) [Add Service](#) [Cancel](#)

The following table describes the parameters used in the **EDUROAM** service template:

Table 13: *EDUROAM Service Template Parameters*

Parameter	Description
General	
Select Prefix	Select a prefix from the existing list of prefixes. This populates the pre-configured information in the Authentication , Service Rule , Wireless , and Federation Level Radius Server (FLR) tabs. The Name Prefix field is not editable.
Name Prefix	Enter a prefix that you want to append to services using this template. Use this to identify services that use templates.
Service Rule	
Enter domain details	Enter the domain name of the network. For example, @edunet.ucla.com. This field is mandatory.
Select Vendor	Select the vendor of the network device. This field is mandatory.
Authentication	
Select Active Directory	Select an authentication source from the list, the information updated in the Authentication , Wireless , and Federation Level Radius Server (FLR) tabs are auto-populated.
Active Directory Name	Enter the hostname or the IP address of the Active Directory server. This field is mandatory.
Description	Enter a description that helps you identify the characteristics of this template. This field is mandatory.
Server	Enter the hostname or the IP address of the Active Directory server. This field is mandatory.
Identity	Enter the DN of the administrator account. This field is mandatory.
NETBIOS	Enter the server Active Directory domain name. This field is mandatory.
Base DN	Enter the DN of the administrator account. This field is mandatory.
Password	Enter the account password. This field is mandatory.

Table 13: EDUROAM Service Template Parameters (Continued)

Parameter	Description
Port	Enter the TCP port where the server is listening for a connection. This field is mandatory.
Wireless Network Settings	
Select wireless controller	Select a wireless controller from the drop-down list.
Wireless controller name	Enter the name given to the wireless controller.
Controller IP Address	Enter the IP address of the wireless controller.
Vendor Name	Select the manufacturer of the wireless controller.
RADIUS Shared Secret	Enter the shared secret that is configured on the controller and inside W-Policy Manager to send and receive RADIUS requests.
Enable RADIUS CoA	Select to enable RADIUS initiated CoA on the network device.
RADIUS CoA Port	Specifies the default port 3799 if RADIUS CoA is enabled. Change this value only if you defined a custom port on the network device.
Federation Level RADIUS Server (FLR)	
Host Name	Enter the hostname of the federation RADIUS server.
IP Address	Enter the IP address of the federation RADIUS server.
Vendor Name	Select the manufacturer of the wireless controller.
RADIUS Shared Secret	Enter the shared secret that is configured on the controller and inside W-Policy Manager to send and receive RADIUS requests.
Enable RADIUS CoA	Select to enable RADIUS initiated CoA on the network device.
RADIUS CoA Port	Specifies the default port 3799 if RADIUS CoA is enabled. Change this value only if you defined a custom port on the network device.
RADIUS Authentication Port	Enter a port number here.
RADIUS Accounting Port	Enter a port number here.

Encrypted Wireless Access via 802.1X Public PEAP method

This template is designed for providing encrypted wireless access to users using fixed 802.1X PEAP credentials. This template configures an **EAP PEAP Public** type authentication method and creates enforcement policy for network access.

The following figure displays the **Encrypted Wireless Access via 802.1X Public PEAP method** service template:

Figure 24: *Encrypted Wireless Access via 802.1X Public PEAP method Service Template*

Service Templates - Encrypted Wireless Access via 802.1X Public PEAP method

General Wireless Network Settings Authentication Method Access Restrictions

Name Prefix*: service_template_Encrypted_Wireless_Access

Description

For wireless end-hosts connecting through an 802.11 wireless access device or controller, with authentication via IEEE 802.1X. This template configures an EAP PEAP Public type Authentication Method; creates Enforcement Policy for network access; creates Network Access Device.

[Back to Start Here](#) [Delete](#) [Next >](#) [Add Service](#) [Cancel](#)

The following table describes the parameters used in the **Encrypted Wireless Access via 802.1X Public PEAP method** service template:

Table 14: *Encrypted Wireless Access via 802.1X Public PEAP Method Service Template Parameters*

Parameter	Description
General	
Name Prefix	Enter a prefix that you want to append to services using this template. You can use this to identify services that use templates.
Wireless Network Settings	
Select wireless controller	Select a wireless controller from the drop-down list.
Wireless controller name	Enter the name given to the wireless controller.
Controller IP Address	Enter the IP address of the wireless controller.
Vendor Name	Select the manufacturer of the wireless controller.
RADIUS Shared Secret	Enter the shared secret that is configured on the controller and inside W-Policy Manager to send and receive RADIUS requests.
Enable RADIUS CoA	Select to enable RADIUS initiated CoA on the network device.
RADIUS CoA Port	Specifies the default port 3799 if RADIUS CoA is enabled. Change this value only if you defined a custom port on the network device.
Authentication Method	
Public Username	Enter public username for EAP PEAP Public type authentication method.
Public Password	Enter password for EAP PEAP Public type authentication method.
Access Restrictions	
Days allowed for access	Select the days on which network access is allowed.

Guest Access

This template is designed for authenticating guest users who log in using captive portal. Guests must re-authenticate after session expiry. Guest access can be restricted based on day of the week, bandwidth limit, and number of unique devices used by the guest user.

The following figure displays the **Guest Access** service template:

Figure 25: *Guest Access Service Template*

Service Templates - Guest Access

General | Wireless Network Settings | Posture Settings | Guest Access Restrictions

Name Prefix*: Guest_Access

Description

For authenticating guest users who login via captive portal. Guests must re-authenticate after their session ends. Network access can be restricted based on day of the week or bandwidth limit used by the guest user. Posture checks can be enabled, optionally, to validate the client device for AntiVirus, AntiSypware, Firewall status. These results will determine the enforcement for the device.

[Back to Start Here](#) [Delete](#) [Next >](#) [Add Service](#) [Cancel](#)

The following table describes the parameters used in the **Guest Access** service template:

Table 15: *Guest Access Service Template Parameters*

Parameter	Description
General	
Select Prefix	Select any one prefix from the existing list of prefixes. This populates the pre-configured information in the Wireless Network Settings and Guest Access Restrictions sections. The Name Prefix field is not editable.
Name Prefix	Enter a prefix that you want to append to services using this template. Use this to identify services that use templates.
Wireless Network Settings	
Wireless SSID for Guest access	Enter the SSID value here.
Select wireless controller	Select the wireless controller from the drop-down list if you already configured.
Wireless controller name	Enter the name of the wireless controller.
Controller IP Address	Enter the wireless controller's IP address.
Vendor Name	Select the manufacturer of the wireless controller.
RADIUS Shared Secret	Enter the shared secret that is configured on the controller and inside W-Policy Manager to send and receive RADIUS requests.
Enable RADIUS CoA	Select to enable RADIUS initiated CoA on the network device.

Table 15: Guest Access Service Template Parameters (Continued)

Parameter	Description
RADIUS CoA Port	Specifies the default port 3799 if RADIUS CoA is enabled. Change this value only if you defined a custom port on the network device.
Posture Settings	
Enable Posture Checks	Select the check box to perform health checks post authentication. This enables the Host Operating System and Quarantine Message fields.
Host Operating System	Select the operating system: Windows, Linux, or Mac OS X.
Quarantine Message	Specify the quarantine message that will appear on the client.
Guest Access Restrictions	
Days allowed for access	Select the duration in number of days to enable on which the guest users are allowed network access.
Maximum bandwidth allowed per user	Enter a number to set an upper limit for the amount of data in megabytes to which a user is allowed per day. A value of 0 (zero), the default, means no limit is set.

Guest Access Web Login

This service authenticates guests logging in using the Guest portal. To use this service, create a **Guest Web Login** page that sets the **Pre-Auth Check** option to **AppAuth - Check** using **Dell Application Authentication**.

The following figure displays the **Guest Access Web Login** service template:

Figure 26: Guest Access Web Login Service Template

Service Templates - Guest Access - Web Login

General	Service Rule	Guest Access Restrictions
Name Prefix*: Guest_Access_Web_Login Description Create a service that performs an authentication check for guests logging in via guest portal. To use this service, create a Guest web login page with the Pre-Auth Check set to "App Auth - check using Aruba Application Authentication". Back to Start Here Delete Next > Add Service Cancel		

The following table describes the **Guest Access Web Login** service template parameters:

Table 16: *Guest Web Login Service Template Parameters*

Parameter	Description
General	
Select Prefix	Select any one prefix from the existing list of prefixes. This populates the pre-configured information in the Service Rule and Guest Web Login sections. The Name Prefix field is not editable.
Name Prefix	Enter a prefix that you want to append to services using this template. Use this to identify services that use templates.
Service Rule	
Page name	Enter the name of the Guest Web Login page.
Add new Guest Web Login page	Click this link to launch a new Web UI session for the Guest Web Login page.
Guest Access Restrictions	
Days allowed for access	Select the duration in number of days to enable on which the guest users are allowed network access.

Guest Authentication with MAC Caching

This template is designed for authenticating guest accounts based on the cached MAC addresses used during authentication.

A guest can belong to a specific role such as Contractor, Guest, or Employee, and each role can have different lifetime for the cached MAC address.

The following figure displays the **Guest MAC Authentication** service template:

Figure 27: *Guest MAC Authentication Service Template*

Service Templates - Guest MAC Authentication

The screenshot displays the configuration page for a 'Guest MAC Authentication' service template. At the top, there are five tabs: 'General' (selected), 'Wireless Network Settings', 'MAC Caching Settings', 'Posture Settings', and 'Guest Access Restrictions'. Below the tabs, the 'Name Prefix' field is populated with 'Guest_MAC'. A 'Description' section contains the following text: 'Guest users first login via captive portal and their MAC addresses are cached. Subsequent logins will use MAC authentication and bypass the captive portal. Network access can be restricted based on day of the week, bandwidth limit or number of unique devices used by the guest. The cache lifetime of the MAC address can vary according to the guest's role (Guest, Employee or Contractor) and after that the guest will have to re-authenticate via captive portal. Posture checks can be enabled, optionally, to validate the client device for AntiVirus, AntiSpyware, Firewall status. These results will determine the enforcement for the device.' At the bottom of the form, there is a 'Back to Start Here' button on the left and a row of four buttons on the right: 'Delete', 'Next >', 'Add Service', and 'Cancel'.

The following table describes the **Guest MAC Authentication** service template parameters:

Table 17: Guest MAC Authentication Service Template Parameters

Parameter	Description
General	
Select Prefix	Select a prefix from the existing list of prefixes. This populates the pre-configured information in the Wireless Network Settings , MAC Caching Settings , and Guest Access restrictions tabs. The Name Prefix field is not editable.
Name Prefix	Enter a prefix that you want to append to services using this template. Use this to identify services that use templates.
Wireless Network Settings	
Wireless SSID for Guest access	Enter the SSID name of your network.
Select wireless controller	Select the wireless controller from the drop-down list if you already configured.
Wireless controller name	Enter the name of the wireless controller.
Controller IP Address	Enter the wireless controller's IP address.
Vendor Name	Select the manufacturer of the wireless controller.
RADIUS Shared Secret	Enter the shared secret that is configured on the controller and inside W-Policy Manager to send and receive RADIUS requests.
Enable RADIUS CoA	Select to enable RADIUS initiated CoA on the network device.
RADIUS CoA Port	Specifies the default port 3799 if RADIUS CoA is enabled. Change this value only if you defined a custom port on the network device.
MAC Caching Settings	
Cache duration for Guest Role	Enter the duration in number of days the MAC account will remain valid for the Guest role. After this the guest must re-authenticate using captive portal. NOTE: You must enter cache duration for at least one role.
Cache duration for Employee role	Enter the duration in number of days the MAC account will remain valid for the Employee role. After this the guest must re-authenticate using captive portal.
Cache duration for Contractor role	Enter the duration in number of days the MAC account will remain valid for the Contractor role. After this the guest must re-authenticate using captive portal.
Posture Settings	
Enable Posture	Select the check box to perform health checks post authentication. This enables the Host

Table 17: *Guest MAC Authentication Service Template Parameters (Continued)*

Parameter	Description
Checks	Operating System and Quarantine Message fields.
Host Operating System	Select the operating system: Windows, Linux, or Mac OS X.
Quarantine Message	Specify the quarantine message that will appear on the client.
Initial Role/VLAN	Enter the initial role of the client before posture checks are performed.
Quarantine Role/VLAN	Enter the role of clients that fail posture checks.
Guest Access Restrictions	
Days allowed for access	Select the duration in number of days to enable on which the guest users are allowed network access.
Maximum number of devices allowed per user	Enter a number to define how many devices users can connect to the network.
Maximum bandwidth allowed per user	Enter a number to set an upper limit for the amount of data in megabytes to which a user is allowed per day. A value of 0 (zero), the default, means no limit is set.

Guest Social Media Authentication

This template is designed for authenticating guest users logging in through captive portal with their social media accounts such as Google, Facebook, LinkedIn, and Twitter. Guests must re-authenticate after the session ends.

The following figure displays the **Guest Social Media Authentication** service template:

Figure 28: *Guest Social Media Authentication Service Template*

Service Templates - Guest Social Media Authentication

General Wireless Network Settings Guest Access Restrictions

Name Prefix*: Social_Media_Auth

Description

For authenticating guest users who login via captive portal with their social media accounts. Guests must re-authenticate after their session ends. Network access can be restricted based on day of the week or bandwidth limit used by the guest user. Posture checks can be enabled, optionally, to validate the client device for AntiVirus, AntiSpyware, Firewall status. These results will determine the enforcement for the device.

[Back to Start Here](#) [Delete](#) [Next >](#) [Add Service](#) [Cancel](#)

The following table describes the **Guest Social Media Authentication** service template parameters:

Table 18: *Guest Social Media Service Template Parameters*

Parameter	Description
General	
Select Prefix	Select a prefix from the existing list of prefixes. This populates the pre-configured information in the Wireless Network Settings , MAC Caching Settings , and Guest Access restrictions tabs. The Name Prefix field is not editable.
Name Prefix	Enter a prefix that you want to append to services using this template. Use this to identify services that use templates.
Wireless Network Settings	
Select wireless controller	Select the wireless controller from the drop-down list if you already configured.
Wireless controller name	Enter the name of the wireless controller.
Controller IP Address	Enter the wireless controller's IP address.
Vendor Name	Select the manufacturer of the wireless controller.
RADIUS Shared Secret	Enter the shared secret that is configured on the controller and inside W-Policy Manager to send and receive RADIUS requests.
Enable RADIUS CoA	Select to enable RADIUS initiated CoA on the network device.
RADIUS CoA Port	Specifies the default port 3799 if RADIUS CoA is enabled. Change this value only if you defined a custom port on the network device.
Guest Access Restrictions	

Table 18: *Guest Social Media Service Template Parameters (Continued)*

Parameter	Description
Social login Provider	Select the social media network options: Google, Facebook, LinkedIn, and Twitter.
Days allowed for access	Select the duration in number of days to enable on which the guest users are allowed network access.
Maximum bandwidth allowed per user	Enter a number to set an upper limit for the amount of data in megabytes to which a user is allowed per day. A value of 0 (zero), the default, means no limit is set.

OAuth2 API User Access

This template is designed for configuration that supports W-ClearPass Policy Manager to authenticate API clients with username and OAuth2 grant type password. The **OAuth2 API User Access** service template uses the **Guest Operator Logins** as the default enforcement policy. The **Local User Repository** and **Admin User Repository** repositories are used as the default authentication sources.

The following figure displays the **OAuth2 API User Access** service template:

Figure 29: *OAuth2 API User Access Service Template*

Service Templates - OAuth2 API User Access

General

Name Prefix*: OAuth2_API

Description

Service template for API clients authenticating with username and password (OAuth2 grant type "password")

[Back to Start Here](#) [Delete](#) [Next >](#) [Add Service](#) [Cancel](#)

The following table describes the **OAuth2 API User Access** service template parameters:

Table 19: *OAuth2 API User Access Service Template Parameters*

Parameter	Description
General	
Select Prefix	Select a prefix from the existing list of prefixes.
Name Prefix	Enter a prefix that is appended to services using this template. You can use this prefix to identify the services that use templates.

Onboard

This template is designed for configuration that allows to perform checks before allowing Onboard provisioning for Bring Your Own Device (BYOD) use-cases. This service creates an Onboard Pre-Auth service to check the user's credentials before starting the device provisioning process. This also creates an authorization service that checks whether a user's device can be provisioned using Onboard. Use an **802.1X Wireless** service to authenticate users prior to device provisioning with Onboard and after device provisioning is completed.



You cannot view the **Onboard** service template if the **High Capacity Guest** mode is enabled in the cluster.

The following figure displays the **Onboard Authorization** service template:

Figure 30: *Onboard Authorization Service Template*

Service Templates - Onboard

The following table describes the **Onboard Authorization** service template parameters:

Table 20: *Onboard Authorization Service Template Parameters*

Parameter	Description
General	
Select Prefix	Select a prefix from the existing list of prefixes. This populates the pre-configured information in the Wireless Network Settings , Device Access Restrictions , and Provisioning Wireless Network Settings sections. The Name Prefix field is not editable.
Name Prefix	Enter a prefix that you want to append to services using this template. Use this to identify services that use templates.
Wireless Network Settings	
Select wireless controller	Select the wireless controller from the drop-down list if you already configured.
Wireless controller name	Enter the name given to the wireless controller.
Controller IP Address	Enter the wireless controller's IP address.
Vendor Name	Select the manufacturer of the wireless controller.
RADIUS Shared Secret	Enter the shared secret that is configured on the controller and inside W-Policy Manager to send and receive RADIUS requests.
Enable RADIUS CoA	Select to enable RADIUS initiated CoA on the network device.
RADIUS CoA Port	Specifies the default port 3799 if RADIUS CoA is enabled. Change this value only if you defined a custom port on the network device.

Table 20: Onboard Authorization Service Template Parameters (Continued)

Parameter	Description
Device Access Restrictions	
Days allowed for access	Select the duration in number of days to enable on which the guest users are allowed network access.
Provisioning Wireless Network Settings	
Wireless SSID for Onboard Provisioning	Enter the SSID of your network.
Add new Onboard Network settings	Click the Add new Onboard Network settings link to launch the Web UI to modify the Onboard Network settings.

Policy Manager Service Types

The following service types are available in Policy Manager:

- [Dell 802.1X Wireless on page 83](#)
- [802.1X Wireless - Identity Only on page 82](#)
- [802.1X Wired on page 70](#)
- [802.1X Wired - Identity Only on page 71](#)
- [Cisco Web Authentication Proxy on page 94](#)
- [MAC Authentication on page 95](#)
- [RADIUS Authorization on page 96](#)
- [RADIUS Enforcement \(Generic\) on page 97](#)
- [RADIUS Proxy on page 97](#)
- [Dell W-Series Application Authentication on page 98](#)
- [Dell W-Series Application Authorization on page 99](#)
- [W-ClearPass OnConnect Enforcement on page 99](#)
- [Event-Based Enforcement on page 101](#)
- [TACACS+ Enforcement on page 103](#)
- [Web-based Authentication on page 104](#)
- [Web-based Health Check Only on page 104](#)
- [Web-based Open Network Access on page 105](#)

802.1X Wired

Configure this service for clients connecting through an Ethernet LAN with authentication using IEEE 802.1X. Except for the NAS-Port-Type service rule value (which is Ethernet for 802.1X Wired and Wireless 802.11 for 802.1X Wireless), configuration for the rest of the tabs is similar to the Dell 802.1X Wireless service. For more information, see [Dell 802.1X Wireless on page 83](#). The following figure displays the **802.1X Wired** service page:

Figure 31: 802.1X Wired Service

Configuration » Services » Add

Services

Service	Authentication	Roles	Enforcement	Accounting Proxy	Summary
Type:	802.1X Wired				
Name:	WiredAccess Service				
Description:	802.1X Wired Access Service				
Monitor Mode:	☐ Enable to monitor network access without enforcement				
More Options:	☐ Authorization ☐ Posture Compliance ☐ Audit End-hosts ☐ Profile Endpoints ☒ Accounting Proxy				
Service Rule					
Matches ☐ ANY or ☒ 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)		
3. Click to add...					

802.1X Wired - Identity Only

Configure this service for clients connecting through an Ethernet LAN with authentication using IEEE 802.1X. Configuration for the **802.1X Wired - Identity Only** service is same as the **802.1X Wired** service except that **Posture** and **Audit** policies are not configurable, when you use this template. For more information, see [802.1X Wired on page 70](#). The following figure displays the **802.1X Wired - Identity Only** service:

Figure 32: 802.1X Wired - Identity Only Service

Services

Service	Authentication	Roles	Enforcement	Summary	
Type:	802.1X Wired - Identity Only				
Name:	Dot1X_Wired				
Description:	802.1X Wired Access Service - Identity Only				
Monitor Mode:	☐ Enable to monitor network access without enforcement				
More Options:	☐ Authorization ☐ Profile Endpoints ☐ Accounting Proxy				
Service Rule					
Matches ☐ ANY or ☒ 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)		
3. Click to add...					

Dell 802.1X Wireless

Configure this service for wireless hosts by connecting through a Dell 802.1X wireless access device or controller with authentication using IEEE 802.1X. Service rules are customized for a typical Dell W-Series Controller deployment.

By default, the Dell W-Series 802.1X service includes a rule that specifies that a Dell ESSID exists.

The following are the default configuration tabs available in the **Configuration > Services > Add** page:

- [Service Tab on page 72](#)
- [Authentication Tab on page 74](#)
- [Roles Tab on page 76](#)
- [Enforcement Tab on page 78](#)
- [Summary Tab on page 82](#)

You can also enable the following additional tabs by checking the **More Options** field to access these configuration tabs:

- [Authorization Tab on page 75](#)
- [Posture Tab on page 77](#)

- [Audit Tab on page 79](#)
- [Profiler Tab on page 80](#)
- [Accounting Proxy Tab on page 81](#)

The following figure displays the **Dell 802.1X Wireless** service configuration fields:

Figure 33: *Dell 802.1X Wireless Service*

The screenshot shows the 'Service' tab of the configuration dialog. It includes fields for Type (DELL W-Series Wireless), Name, and Description (DELL 802.1X Wireless Access Service). There are checkboxes for Monitor Mode and More Options (Authorization, Posture Compliance, Audit End-hosts, Profile Endpoints). Below is a 'Service Rule' section with a table of 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:Aruba	Aruba-Essid-Name	EXISTS	
4. Click to add...			

At the bottom, there is a 'Back to Start Here' link and 'Next >', 'Save', and 'Cancel' buttons.

Service Tab

The **Service** tab includes basic information about the service. The **Service Rules** section defines a set of criteria that supplicants must match to trigger the service. Some service templates have one or more rules predefined.

You can click on a service rule to modify any of its options.

The following figure displays the **Service** tab:

Figure 34: *Dell 802.1X Wireless Service > Service Dialog*

This screenshot is identical to Figure 33, showing the 'Service' tab of the configuration dialog. It includes fields for Type (DELL W-Series Wireless), Name, and Description (DELL 802.1X Wireless Access Service). There are checkboxes for Monitor Mode and More Options (Authorization, Posture Compliance, Audit End-hosts, Profile Endpoints). Below is a 'Service Rule' section with a table of 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:Aruba	Aruba-Essid-Name	EXISTS	
4. Click to add...			

At the bottom, there is a 'Back to Start Here' link and 'Next >', 'Save', and 'Cancel' buttons.

1. Specify the **Service** tab parameters as described in the following table:

Table 21: Dell 802.1X Wireless Service > Service Tab Parameters

Parameter	Action/Description
Type	Select a service from the drop-down list that defines what type of service can be configured.
Name	Enter the name of the service.
Description	Provide additional information that helps to identify the service.
Monitor Mode	Check this box to monitor network access activity without enforcement.
More Options	Check these boxes to access the additional configuration tabs: • Authorization • Posture Compliance • Audit End-hosts • Profile Endpoints • Accounting Proxy
Service Rule	
Type	Select the service rule type from the drop-down list.
Name	Select the name of the service rule from the drop-down list.
Operator	Select an appropriate operator from the list of operators for the data type of the attribute. For example, you can select from BELONGS_TO, NOT_BELONGS_TO, CONTAINS, or EQUALS.
Value	Select the value from the drop-down list depends on the operator selected.

Service rules define a set of criteria that supplicants must match to trigger the service. Some service templates have one or more rules predefined.

2. Click on a service rule to modify its options.



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 reuse the policy components (authentication methods, authentication source, authorization source, role mapping policies, posture policies, and enforcement policies) in both services.

Authentication Tab

The **Authentication** tab contains options for configuring authentication methods and authentication sources. The following figure displays the **Authentication** tab:

Figure 35: Dell 802.1X Wireless Service > Authentication Tab

The screenshot shows the 'Authentication' tab of the 'Add Services' configuration page. The page has a breadcrumb 'Configuration » Services » Add' and a title 'Services'. Below the title are tabs for 'Service', 'Authentication' (selected), 'Roles', 'Enforcement', and 'Summary'. The 'Authentication' section is divided into three main areas: 'Authentication Methods', 'Authentication Sources', and 'Strip Username Rules'. Each area has a list of items, a 'Select to Add' dropdown, and a set of action buttons (Move Up, Move Down, Remove, View Details, Modify). The 'Strip Username Rules' dropdown is currently open, showing a list of rules. At the bottom, there are buttons for 'Back to Services', 'Next >', 'Save', and 'Cancel'.

Service	Authentication	Roles	Enforcement	Summary
Authentication Methods:				
[EAP PEAP] [EAP FAST] [EAP TLS] [EAP TTLS] [EAP MSCHAPV2] --Select to Add--				
Add new Authentication Method				
Authentication Sources:				
--Select to Add--				
Add new Authentication Source				
Strip Username Rules:				
of rules to strip username prefixes or suffixes				
AD [Active Directory] [Admin User Repository] [Local SQL DB] [Blacklist User Repository] [Local SQL DB] [Endpoints Repository] [Local SQL DB] [Guest Device Repository] [Local SQL DB] [Guest User Repository] [Local SQL DB] [Insight Repository] [Local SQL DB] [Local User Repository] [Local SQL DB] [Onboard Devices Repository] [Local SQL DB] [Social Login Repository] [Local SQL DB] [Time Source] [Local SQL DB]				
Back to Services Next > Save Cancel				

1. Specify the **Authentication** tab parameters as described in the following table:

Table 22: Dell 802.1X Wireless Service > Authentication Parameters

Parameter	Action/Description
Authentication Methods	Select authentication methods using the Select to Add field used for this service depend on the 802.1X supplicants and the type of authentication methods you choose to deploy. W-Policy Manager automatically selects the appropriate method for authentication, when a user attempts to connect. The common types, which are automatically selected include the following examples: • EAP PEAP • EAP FAST • EAP TLS • EAP TTLS • EAP MSCHAPV2 The EAP-MD5 authentication type is not supported if you use W-ClearPass Policy Manager in FIPS mode. The order of authentication is significant, when a client tries to perform an 802.1X authentication. W-Policy Manager proposes the first authentication method configured. However, the client can accept the authentication method proposed by W-Policy Manager and continue authentication or send a Negative-Acknowledgment (NAK) and propose a different authentication method. If the newly proposed authentication method is also configured, then the authentication proceeds, otherwise authentication fails. If most of the clients in the network use a specific authentication method, that authentication method should be configured first in the list. This would reduce the number of RADIUS packets exchanged. For more information, see the following: • Adding and Modifying Authentication Methods on page 169 • Adding and Modifying Authentication Sources on page 193.
Authentication Sources	Specify the authentication sources using the Select to Add field. This can be one or more instances of the following list of authentication sources: • Active Directory • Admin User Repository • Blacklist User Repository • Endpoints Repository • Guest Device Repository • Guest User Repository • Insight Repository • Local User Repository • Onboard Devices Repository • Social Login Repository • Time Sources NOTE: When you attempt to specify more than 23 Services authentication sources, the following error message is displayed: No. of Authentication Sources cannot exceed 23.
Strip Username Rules	Select the check box to preprocess the user name (to remove prefixes and suffixes) before authenticating and authorizing against the authentication source.

Authorization Tab

Use the **Authorization** tab to select the authorization sources for this service. The **Authorization** tab is not displayed by default.

To access this tab, select the **Authorization** check box from **More Options** on the **Services** tab.

1. W-ClearPass fetches role-mapping attributes from the authorization sources associated with the 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:

- Authorization sources associated with the authentication source
- Authorization sources associated with the service

The following figure displays the **Authorization** tab:

Figure 36: Dell 802.1X Wireless Service > Authorization Dialog

Services

Service Authentication **Authorization** Roles Posture Enforcement Audit Profiler Summary

Authorization Details:

Authorization sources from which role mapping attributes are fetched (for each Authentication Source)

Authentication Source	Attributes Fetched From
1. [Blacklist User Repository] [Local SQL DB]	[Blacklist User Repository] [Local SQL DB]
2. [Admin User Repository] [Local SQL DB]	[Admin User Repository] [Local SQL DB]

Additional authorization sources from which to fetch role-mapping attributes -

[Admin User Repository] [Local SQL DB] Remove
 [Blacklist User Repository] [Local SQL DB] View Details
 [Local User Repository] [Local SQL DB] Modify
 [Onboard Devices Repository] [Local SQL DB]
 --Select to Add--

[Add new Authentication Source](#)

2. Specify the **Authorization** parameters as described in the following table:

Table 23: Dell 802.1X Wireless Service > Authorization Parameters

Parameter	Action/Description
Authentication Source	Displays the authorization sources from which role mapping attributes are fetched for each authentication source.
Attributes Fetched From	Displays the source of attributes.
Additional authorization sources from which to fetch role-mapping attributes	Select the additional authorization sources using the Select to Add drop-down list.

For more information on configuring authorization sources, see [Adding and Modifying Authentication Methods on page 169](#).

Roles Tab

Use the **Roles** tab to associate a role mapping policy with this service. The following figure displays the **Dell 802.1X Wireless Service > Roles** tab:

Figure 37: Dell 802.1X Wireless Service > Roles Tab

Services

Service Authentication Roles **Enforcement** Summary

Role Mapping Policy: ClearPass admin roles - AD Modify [Add new Role Mapping Policy](#)

Role Mapping Policy Details

Description: Policy to allow specific access to the ClearPass server for AD accounts

Default Role: Deny

Rules Evaluation Algorithm: evaluate-all

Conditions	Role
1. (Authorization:Clearpass lab AD:memberOf CONTAINS Network)	[TACACS Super Admin]
2. (Authorization:Clearpass lab AD:memberOf CONTAINS Help Desk)	[TACACS Help Desk]
3. (Authorization:Clearpass lab AD:memberOf CONTAINS Staff)	[TACACS Receptionist]
4. (Authorization:Clearpass lab AD:memberOf CONTAINS Student)	User Type 2
5. (Authorization:Clearpass lab AD:memberOf CONTAINS Faculty)	User Type 1
6. (Authorization:Clearpass lab AD:UserDN EXISTS)	[TACACS Read-only Admin]

1. Specify the **Roles** parameters as described in the following table:

Table 24: Dell 802.1X Wireless Service > Roles Tab Parameters

Parameter	Action/Description
Role Mapping Policy	Select a role mapping policy from the drop-down list. W-Policy Manager ships a number of preconfigured roles. NOTE: A service can be configured without a role-mapping policy, but only one role-mapping policy can be configured for each service.
Role Mapping Policy Details	
Description	Provide additional information about the selected role-mapping policy.
Default Role	Specify the role to which W-Policy Manager defaults when the role-mapping policy does not produce a match.
Rules Evaluation Algorithm	Shows the first matched rule and returns the role or Select all matched rules and returns a set of roles.

For information on configuring role-mapping policies, see [Configuring a Role and Role Mapping Policy](#) on page 257.

Posture Tab

The **Posture** tab is not enabled by default.

1. To enable posture checking for this service, select the **Posture Compliance** check box from the **More Options** field on the **Service** tab.

You can enable the posture checking for this kind of service, if you deploy any of the following:

- W-Policy Manager in a Microsoft Network Access Protection (NAP)
- Cisco Network Admission Control (NAC) Framework environment
- Dell hosted captive portal that performs posture checks through a dissolvable agent



You cannot view the **Posture** tab if you enable the **High Capacity Guest** mode in the cluster.

The following figure displays the **Posture** dialog:

Figure 38: Dell 802.1X Wireless Service > Posture Dialog

Configuration » Services » Add

Services

Service Authentication Roles **Posture** Enforcement Summary

Posture Policies:

Posture Policies: Only NAP agent type Posture Policies are applicable for this service

--Select to Add--

Remove View Details Modify

[Add new Posture Policy](#)

Default Posture Token: UNKNOWN (100)

Remediate End-Hosts: ☐ Enable auto-remediation of non-compliant end-hosts

Remediation URL:

- Specify the Wireless Service **Posture** parameters as described in [Table 25](#):

Table 25: *Dell 802.1X Wireless Service > Posture Parameters*

Parameter	Action/Description
Posture Policies	
Posture Policies	Select the posture policy from the Select to Add drop-down list. If you do not have any preconfigured posture policies, click Add new Posture Policy to create a new posture policy. NOTE: Only NAP agent-type posture policies are applicable for this service.
Default Posture Token	Select the default posture token from the drop-down list.
Remediate End-Hosts	To perform remediation action, when a client is quarantined, select the Enable auto-remediation of non-compliant end-hosts check box.
Remediation URL	To perform the remediation, enter the web link of a server resource.

For more information on configuring posture policies, see [Configuring Posture Policy Agents and Hosts on page 269](#).

Enforcement Tab

Use this tab to select an enforcement policy for a service. The following figure displays the **Enforcement** dialog:

Figure 39: *Dell 802.1X Wireless Service > Enforcement Dialog*

Services

Service	Authentication	Roles	Enforcement	Summary
Use Cached Results: ☐ Use cached Roles and Posture attributes from previous sessions Enforcement Policy: Onboard Authorization Policy Modify Add new Enforcement Policy				
Enforcement Policy Details				
Description: Sample policy controlling authorization during Onboard provisioning				
Default Profile: [Deny Access Profile]				
Rules Evaluation Algorithm: evaluate-all				
Conditions		Enforcement Profiles		
1. (Authentication:Source EQUALS [Guest User Repository])		Guest Session Timeout		
2. (Date:Day-of-Week BELONGS_TO Monday,Tuesday,Wednesday,Thursday,Friday,Saturday,Sunday)		[Allow Access Profile]		

- Specify the **Enforcement** parameters as described in the following table:

Table 26: Dell 802.1X Wireless Service > Enforcement Parameters

Parameter	Action/Description
Use Cached Results	Select this check box to use cached roles and posture attributes from previous sessions.
Enforcement Policy	Select the preconfigured enforcement policy from the drop-down list. This is mandatory. If you do not have any preconfigured enforcement policies, click Add new Enforcement Policy to create a new enforcement policy.
Enforcement Policy Details	
Description	Displays additional information about the selected enforcement policy.
Default Profile	Displays a default profile applied by Policy Manager .
Rules Evaluation Algorithm	Shows first matched rule and return the role or select all matched rules and return a set of roles.

For more information, see [Configuring Enforcement Policies on page 343](#).

Audit Tab

Use the **Audit** tab to enable the Audit checking for this service.

1. To enable the **Audit** tab, select the **Audit End-hosts** check box from the **More Options** field on the **Service** tab.

The **Audit** dialog opens.

Figure 40: Dell 8021X Wireless Service - Audit Tab

Services

Service	Authentication	Authorization	Roles	Posture	Enforcement	Audit	Profiler	Summary

Audit Server:

[Nessus Server]

View Details

Modify

Add new Audit Server

Audit Trigger Conditions:

☐ Always

☐ When posture is not available

☒ For MAC authentication request

☐ For known end-hosts only

☐ For unknown end-hosts only

☐ For all end-hosts

Action after audit:

☐ No Action

☐ Do SNMP bounce

☒ Trigger RADIUS CoA action

Aruba Terminate Session-

View Details

Modify

Add new RADIUS CoA Action

2. Specify the **Audit End-Hosts** parameters as described in the following table:

Table 27: Dell 802.1X Wireless Service > Audit End-Hosts Parameters

Parameter	Action/Description
Audit Server	Select the audit server from the following options: ● Nessus Server: Interfaces with W-Policy Manager primarily to perform vulnerability scanning ● Nmap Audit: Performs specific audit functions You can click the View Details button to view the Policy Manager Entity Details dialog with the summary of audit server details. To view the Summary tab with audit server details, click the Modify button.
Audit Trigger Conditions	Select an audit trigger condition: ● Always: Always perform an audit. ● When posture is not available: Perform audit only when posture credentials are not available in the request. ● For MAC Authentication Request: If you select this option, W-Policy Manager presents the following three additional settings: ■ For known end-hosts only: Select this option when you want to reject unknown end-hosts and to audit known clients. Known end-hosts are defined as clients that are found in the authentication source(s) associated with this service. ■ For unknown end-hosts only: Select this option when known end-hosts are assumed to be healthy, but you want to establish the identity of unknown end-hosts and assign roles. Unknown end-hosts are end-hosts that are not found in any of the authentication sources associated with this service. ■ For all end-hosts: For both known and unknown end-hosts.
Action after audit	Specify the audit that can be performed only after the MAC authentication request is completed and the client has acquired an IP address through DHCP. Once the audit results are available, W-Policy Manager reapplies policies on the network device in one of the following ways: ● No Action: The audit does not apply policies on the network device after completing this audit. ● Do SNMP bounce: This option bounces the switch port or forces an 802.1X reauthentication (both done using SNMP). Bouncing the port triggers a new 802.1X or 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 W-ClearPass. ● Trigger RADIUS CoA action: This option sends a RADIUS CoA command from W-ClearPass to the network device.

Profiler Tab

The **Profiler** tab is not displayed by default.

1. To access this tab, select the **More Options > Profile Endpoints** check box.

The following figure displays the **Profile Endpoints** dialog:

Figure 41: Dell 802.1X Wireless Service > Profile Endpoints Dialog

Services

Service Authentication Authorization Roles Posture Enforcement Audit Profiler Summary

Endpoint Classification: Select the classification(s) after which an action must be triggered -

Embedded
Game Console
Power
-- Select --

Remove

RADIUS CoA Action: [Cisco - Bounce-Host-Port] View Details Modify [Add new RADIUS CoA Action](#)

2. Specify the **Profile Endpoints** parameters as described in the following table:

Table 28: Dell 802.1X Wireless Service > Profile Endpoints Parameters

Parameter	Action/Description
Endpoint Classification	Select one or more endpoint classification items from the drop-down list.
RADIUS CoA Action	Select the RADIUS CoA action from the drop-down list. - To view the Policy Manager Entity Details page with the summary of enforcement profile details, click the View Details button. - To view the Summary tab with profile details, click the Modify button. - To create a new RADIUS CoA action, click the Add new RADIUS CoA Action link.

Accounting Proxy Tab

Use the **Accounting Proxy** tab to broadcast the RADIUS accounting packets to all the proxy targets.

You can configure the proxy targets to which RADIUS server should be forwarded and the attributes to be added in the accounting. This enables the external security solutions to use the RADIUS account event to detect when a user connects and disconnects to the server.

1. To enable the **Accounting Proxy** tab, select the **More Options > Accounting Proxy** check box.

The following figure displays the **Accounting Proxy** dialog:

Figure 42: 802.1X Wireless > Accounting Proxy Dialog

Services

Service Authentication Roles Enforcement Accounting Proxy Summary

Accounting Proxy Targets : [Accounting-Proxy] Remove View Details Modify [Add new Accounting Proxy Target](#)

--Select to Add--

RADIUS attributes to be added for Accounting proxy

Type	Name	=	Value	
1. Radius:Aruba	Aruba-Admin-Role	=	%{Authorization:172.31.1.11:UserDN}	
2. Radius:Aruba	Auth-Simulation-Id	=	%{Authorization:172.31.1.11:Email}	
3. Radius:Aruba	Aruba-AS-Username	=	%{Authorization:172.31.1.11:company}	
4. Click to add...				

2. Specify the **Accounting Proxy** parameters as described in the following table:

Table 29: Dell 802.1X Wireless Service > Accounting Proxy Tab Parameters

Parameter	Action/Description
Accounting Proxy Targets	Specify the proxy targets to which the RADIUS server should be forwarded and the attributes to be added in the accounting. Select the accounting proxy target from the Select to Add drop-down list.
Add New Accounting Proxy Target	Click this link to add a new accounting proxy target.
RADIUS attributes to be added for Accounting proxy	
Type	Select the RADIUS attribute type from the drop-down list.
Name	Select the name of the RADIUS attribute from the drop-down list.
Value	Select the value from the Value drop-down list. The values displayed here depend on the RADIUS attribute Type selected.

Summary Tab

The **Summary** page presents the summary of parameters defined when you created a new service. The following figure displays the **Summary** tab:

Figure 43: Dell 802.1X Wireless Service > Summary Page

Services

Service	Authentication	Roles	Enforcement	Summary

Service:

Type:	802.1X Wired
Name:	
Description:	802.1X Wired Access Service
Monitor Mode:	Disabled
More Options:	-

Service 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:

Authentication Methods:	1. [EAP PEAP] 2. [EAP FAST] 3. [EAP TLS] 4. [EAP TTLS] 5. [EAP MSCHAPv2]
Authentication Sources:	-
Strip Username Rules:	-

Roles:

Role Mapping Policy:	-

Enforcement:

Use Cached Results:	Disabled
Enforcement Policy:	[Sample Allow Access Policy]

802.1X Wireless - Identity Only

Configuration for this type of service is the same as the **Dell 802.1X Wireless** service except that **Posture** and **Audit** policies are not configurable, when you use this template. For more information, see [Dell 802.1X Wireless on page 83](#). The following figure displays the **802.1X Wireless - Identity Only** service:

Figure 44: 802.1X Wireless - Identity Only Service

Services

Service Authentication Roles Enforcement Summary

Type: 802.1X Wireless - Identity Only

Name: Dot1x_Wireless_Identity_Only

Description: 802.1X Wireless Access Service - Identity Only

Monitor Mode: ☐ Enable to monitor network access without enforcement

More Options: ☐ Authorization ☐ Profile Endpoints ☐ Accounting Proxy

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...			

Dell 802.1X Wireless

Configure this service for wireless hosts by connecting through a Dell 802.1X wireless access device or controller with authentication using IEEE 802.1X. Service rules are customized for a typical Dell W-Series Controller deployment.

By default, the Dell W-Series 802.1X service includes a rule that specifies that a Dell ESSID exists.

The following are the default configuration tabs available in the **Configuration > Services > Add** page:

- [Service Tab on page 84](#)
- [Authentication Tab on page 86](#)
- [Roles Tab on page 88](#)
- [Enforcement Tab on page 90](#)
- [Summary Tab on page 94](#)

You can also enable the following additional tabs by checking the **More Options** field to access these configuration tabs:

- [Authorization Tab on page 87](#)
- [Posture Tab on page 89](#)
- [Audit Tab on page 91](#)
- [Profiler Tab on page 92](#)
- [Accounting Proxy Tab on page 93](#)

The following figure displays the **Dell 802.1X Wireless** service configuration fields:

Figure 45: *Dell 802.1X Wireless Service*

The screenshot shows the 'Service Rule' tab of the 'Dell 802.1X Wireless Service' configuration. The 'Type' is set to 'DELL W-Series Wireless'. The 'Name' field is empty. The 'Description' is 'DELL 802.1X Wireless Access Service'. Under 'Monitor Mode', the checkbox 'Enable to monitor network access without enforcement' is unchecked. Under 'More Options', the checkboxes for 'Authorization', 'Posture Compliance', 'Audit End-hosts', and 'Profile Endpoints' are all unchecked. The 'Service Rule' section shows a table with 3 conditions, all of which must be matched (ALL conditions). The conditions are:

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:Aruba	Aruba-Essid-Name	EXISTS	

At the bottom, there is a 'Back to Start Here' link and buttons for 'Next >', 'Save', and 'Cancel'.

Service Tab

The **Service** tab includes basic information about the service. The **Service Rules** section defines a set of criteria that supplicants must match to trigger the service. Some service templates have one or more rules predefined.

You can click on a service rule to modify any of its options.

The following figure displays the **Service** tab:

Figure 46: *Dell 802.1X Wireless Service > Service Dialog*

The screenshot shows the 'Service' tab of the 'Dell 802.1X Wireless Service' configuration. The 'Type' is set to 'DELL W-Series Wireless'. The 'Name' field is empty. The 'Description' is 'DELL 802.1X Wireless Access Service'. Under 'Monitor Mode', the checkbox 'Enable to monitor network access without enforcement' is unchecked. Under 'More Options', the checkboxes for 'Authorization', 'Posture Compliance', 'Audit End-hosts', and 'Profile Endpoints' are all unchecked. The 'Service Rule' section shows a table with 3 conditions, all of which must be matched (ALL conditions). The conditions are:

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:Aruba	Aruba-Essid-Name	EXISTS	

At the bottom, there is a 'Back to Start Here' link and buttons for 'Next >', 'Save', and 'Cancel'.

1. Specify the **Service** tab parameters as described in the following table:

Table 30: Dell 802.1X Wireless Service > Service Tab Parameters

Parameter	Action/Description
Type	Select a service from the drop-down list that defines what type of service can be configured.
Name	Enter the name of the service.
Description	Provide additional information that helps to identify the service.
Monitor Mode	Check this box to monitor network access activity without enforcement.
More Options	Check these boxes to access the additional configuration tabs: • Authorization • Posture Compliance • Audit End-hosts • Profile Endpoints • Accounting Proxy
Service Rule	
Type	Select the service rule type from the drop-down list.
Name	Select the name of the service rule from the drop-down list.
Operator	Select an appropriate operator from the list of operators for the data type of the attribute. For example, you can select from BELONGS_TO, NOT_BELONGS_TO, CONTAINS, or EQUALS.
Value	Select the value from the drop-down list depends on the operator selected.

Service rules define a set of criteria that supplicants must match to trigger the service. Some service templates have one or more rules predefined.

- Click on a service rule to modify its options.



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 reuse the policy components (authentication methods, authentication source, authorization source, role mapping policies, posture policies, and enforcement policies) in both services.

Authentication Tab

The **Authentication** tab contains options for configuring authentication methods and authentication sources. The following figure displays the **Authentication** tab:

Figure 47: Dell 802.1X Wireless Service > Authentication Tab

The screenshot shows the 'Authentication' tab in the Dell 802.1X Wireless Service configuration. The breadcrumb trail is 'Configuration » Services » Add'. The page title is 'Services'. There are five tabs: 'Service', 'Authentication' (selected), 'Roles', 'Enforcement', and 'Summary'. The 'Authentication' section is divided into three main areas: 'Authentication Methods', 'Authentication Sources', and 'Strip Username Rules'. Each area has a list of items, a 'Select to Add' dropdown, and a set of action buttons (Move Up, Move Down, Remove, View Details, Modify). The 'Strip Username Rules' section has a dropdown menu open, showing a list of rules. At the bottom, there are buttons for 'Back to Services', 'Next >', 'Save', and 'Cancel'.

Service	Authentication	Roles	Enforcement	Summary
Authentication Methods:				
[EAP PEAP] [EAP FAST] [EAP TLS] [EAP TTLS] [EAP MSCHAPV2]				
--Select to Add--				
Add new Authentication Method				
Authentication Sources:				
--Select to Add--				
Add new Authentication Source				
Strip Username Rules:				
of rules to strip username prefixes or suffixes				
AD [Active Directory] [Admin User Repository] [Local SQL DB] [Blacklist User Repository] [Local SQL DB] [Endpoints Repository] [Local SQL DB] [Guest Device Repository] [Local SQL DB] [Guest User Repository] [Local SQL DB] [Insight Repository] [Local SQL DB] [Local User Repository] [Local SQL DB] [Onboard Devices Repository] [Local SQL DB] [Social Login Repository] [Local SQL DB] [Time Source] [Local SQL DB]				
Back to Services				
Next > Save Cancel				

1. Specify the **Authentication** tab parameters as described in the following table:

Table 31: Dell 802.1X Wireless Service > Authentication Parameters

Parameter	Action/Description
Authentication Methods	Select authentication methods using the Select to Add field used for this service depend on the 802.1X supplicants and the type of authentication methods you choose to deploy. W-Policy Manager automatically selects the appropriate method for authentication, when a user attempts to connect. The common types, which are automatically selected include the following examples: • EAP PEAP • EAP FAST • EAP TLS • EAP TTLS • EAP MSCHAPV2 The EAP-MD5 authentication type is not supported if you use W-ClearPass Policy Manager in FIPS mode. The order of authentication is significant, when a client tries to perform an 802.1X authentication. W-Policy Manager proposes the first authentication method configured. However, the client can accept the authentication method proposed by W-Policy Manager and continue authentication or send a Negative-Acknowledgment (NAK) and propose a different authentication method. If the newly proposed authentication method is also configured, then the authentication proceeds, otherwise authentication fails. If most of the clients in the network use a specific authentication method, that authentication method should be configured first in the list. This would reduce the number of RADIUS packets exchanged. For more information, see the following: • Adding and Modifying Authentication Methods on page 169 • Adding and Modifying Authentication Sources on page 193.
Authentication Sources	Specify the authentication sources using the Select to Add field. This can be one or more instances of the following list of authentication sources: • Active Directory • Admin User Repository • Blacklist User Repository • Endpoints Repository • Guest Device Repository • Guest User Repository • Insight Repository • Local User Repository • Onboard Devices Repository • Social Login Repository • Time Sources NOTE: When you attempt to specify more than 23 Services authentication sources, the following error message is displayed: No. of Authentication Sources cannot exceed 23.
Strip Username Rules	Select the check box to preprocess the user name (to remove prefixes and suffixes) before authenticating and authorizing against the authentication source.

Authorization Tab

Use the **Authorization** tab to select the authorization sources for this service. The **Authorization** tab is not displayed by default.

To access this tab, select the **Authorization** check box from **More Options** on the **Services** tab.

1. W-ClearPass fetches role-mapping attributes from the authorization sources associated with the 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:

- Authorization sources associated with the authentication source
- Authorization sources associated with the service

The following figure displays the **Authorization** tab:

Figure 48: Dell 802.1X Wireless Service > Authorization Dialog

Services

Service Authentication **Authorization** Roles Posture Enforcement Audit Profiler Summary

Authorization Details:

Authorization sources from which role mapping attributes are fetched (for each Authentication Source)

Authentication Source	Attributes Fetched From
1. [Blacklist User Repository] [Local SQL DB]	[Blacklist User Repository] [Local SQL DB]
2. [Admin User Repository] [Local SQL DB]	[Admin User Repository] [Local SQL DB]

Additional authorization sources from which to fetch role-mapping attributes -

[Admin User Repository] [Local SQL DB] Remove
 [Blacklist User Repository] [Local SQL DB] View Details
 [Local User Repository] [Local SQL DB] Modify
 [Onboard Devices Repository] [Local SQL DB]
 --Select to Add--

[Add new Authentication Source](#)

2. Specify the **Authorization** parameters as described in the following table:

Table 32: Dell 802.1X Wireless Service > Authorization Parameters

Parameter	Action/Description
Authentication Source	Displays the authorization sources from which role mapping attributes are fetched for each authentication source.
Attributes Fetched From	Displays the source of attributes.
Additional authorization sources from which to fetch role-mapping attributes	Select the additional authorization sources using the Select to Add drop-down list.

For more information on configuring authorization sources, see [Adding and Modifying Authentication Methods on page 169](#).

Roles Tab

Use the **Roles** tab to associate a role mapping policy with this service. The following figure displays the **Dell 802.1X Wireless Service > Roles** tab:

Figure 49: Dell 802.1X Wireless Service > Roles Tab

Services

Service Authentication Roles **Enforcement** Summary

Role Mapping Policy: ClearPass admin roles - AD [Modify](#) [Add new Role Mapping Policy](#)

Role Mapping Policy Details

Description: Policy to allow specific access to the ClearPass server for AD accounts

Default Role: Deny

Rules Evaluation Algorithm: evaluate-all

Conditions	Role
1. (Authorization:Clearpass lab AD:memberOf CONTAINS Network)	[TACACS Super Admin]
2. (Authorization:Clearpass lab AD:memberOf CONTAINS Help Desk)	[TACACS Help Desk]
3. (Authorization:Clearpass lab AD:memberOf CONTAINS Staff)	[TACACS Receptionist]
4. (Authorization:Clearpass lab AD:memberOf CONTAINS Student)	User Type 2
5. (Authorization:Clearpass lab AD:memberOf CONTAINS Faculty)	User Type 1
6. (Authorization:Clearpass lab AD:UserDN EXISTS)	[TACACS Read-only Admin]

1. Specify the **Roles** parameters as described in the following table:

Table 33: *Dell 802.1X Wireless Service > Roles Tab Parameters*

Parameter	Action/Description
Role Mapping Policy	Select a role mapping policy from the drop-down list. W-Policy Manager ships a number of preconfigured roles. NOTE: A service can be configured without a role-mapping policy, but only one role-mapping policy can be configured for each service.
Role Mapping Policy Details	
Description	Provide additional information about the selected role-mapping policy.
Default Role	Specify the role to which W-Policy Manager defaults when the role-mapping policy does not produce a match.
Rules Evaluation Algorithm	Shows the first matched rule and returns the role or Select all matched rules and returns a set of roles.

For information on configuring role-mapping policies, see [Configuring a Role and Role Mapping Policy on page 257](#).

Posture Tab

The **Posture** tab is not enabled by default.

1. To enable posture checking for this service, select the **Posture Compliance** check box from the **More Options** field on the **Service** tab.

You can enable the posture checking for this kind of service, if you deploy any of the following:

- W-Policy Manager in a Microsoft Network Access Protection (NAP)
- Cisco Network Admission Control (NAC) Framework environment
- Dell hosted captive portal that performs posture checks through a dissolvable agent



You cannot view the **Posture** tab if you enable the **High Capacity Guest** mode in the cluster.

The following figure displays the **Posture** dialog:

Figure 50: *Dell 802.1X Wireless Service > Posture Dialog*

Configuration » Services » Add

Services

Service Authentication Roles **Posture** Enforcement Summary

Posture Policies:

Posture Policies: Only NAP agent type Posture Policies are applicable for this service

--Select to Add--

Remove View Details Modify

[Add new Posture Policy](#)

Default Posture Token: UNKNOWN (100)

Remediate End-Hosts: ☐ Enable auto-remediation of non-compliant end-hosts

Remediation URL:

- Specify the Wireless Service **Posture** parameters as described in [Table 34](#):

Table 34: *Dell 802.1X Wireless Service > Posture Parameters*

Parameter	Action/Description
Posture Policies	
Posture Policies	Select the posture policy from the Select to Add drop-down list. If you do not have any preconfigured posture policies, click Add new Posture Policy to create a new posture policy. NOTE: Only NAP agent-type posture policies are applicable for this service.
Default Posture Token	Select the default posture token from the drop-down list.
Remediate End-Hosts	To perform remediation action, when a client is quarantined, select the Enable auto-remediation of non-compliant end-hosts check box.
Remediation URL	To perform the remediation, enter the web link of a server resource.

For more information on configuring posture policies, see [Configuring Posture Policy Agents and Hosts on page 269](#).

Enforcement Tab

Use this tab to select an enforcement policy for a service. The following figure displays the **Enforcement** dialog:

Figure 51: *Dell 802.1X Wireless Service > Enforcement Dialog*

Services

Service	Authentication	Roles	Enforcement	Summary
Use Cached Results: ☐ Use cached Roles and Posture attributes from previous sessions Enforcement Policy: Onboard Authorization Policy Modify Add new Enforcement Policy				
Enforcement Policy Details				
Description: Sample policy controlling authorization during Onboard provisioning				
Default Profile: [Deny Access Profile]				
Rules Evaluation Algorithm: evaluate-all				
Conditions		Enforcement Profiles		
1. (Authentication:Source EQUALS [Guest User Repository])		Guest Session Timeout		
2. (Date:Day-of-Week BELONGS_TO Monday,Tuesday,Wednesday,Thursday,Friday,Saturday,Sunday)		[Allow Access Profile]		

- Specify the **Enforcement** parameters as described in the following table:

Table 35: Dell 802.1X Wireless Service > Enforcement Parameters

Parameter	Action/Description
Use Cached Results	Select this check box to use cached roles and posture attributes from previous sessions.
Enforcement Policy	Select the preconfigured enforcement policy from the drop-down list. This is mandatory. If you do not have any preconfigured enforcement policies, click Add new Enforcement Policy to create a new enforcement policy.
Enforcement Policy Details	
Description	Displays additional information about the selected enforcement policy.
Default Profile	Displays a default profile applied by Policy Manager .
Rules Evaluation Algorithm	Shows first matched rule and return the role or select all matched rules and return a set of roles.

For more information, see [Configuring Enforcement Policies on page 343](#).

Audit Tab

Use the **Audit** tab to enable the Audit checking for this service.

1. To enable the **Audit** tab, select the **Audit End-hosts** check box from the **More Options** field on the **Service** tab.

The **Audit** dialog opens.

Figure 52: Dell 8021X Wireless Service - Audit Tab

Services

Service	Authentication	Authorization	Roles	Posture	Enforcement	Audit	Profiler	Summary

Audit Server: [Nessus Server] [View Details](#) [Modify](#) [Add new Audit Server](#)

Audit Trigger Conditions:

- ☐ Always
- ☐ When posture is not available
- ☒ For MAC authentication request
 - ☐ For known end-hosts only
 - ☐ For unknown end-hosts only
 - ☐ For all end-hosts

Action after audit:

- ☐ No Action
- ☐ Do SNMP bounce
- ☒ Trigger RADIUS CoA action
 - Aruba Terminate Session- [View Details](#) [Modify](#) [Add new RADIUS CoA Action](#)

2. Specify the **Audit End-Hosts** parameters as described in the following table:

Table 36: Dell 802.1X Wireless Service > Audit End-Hosts Parameters

Parameter	Action/Description
Audit Server	Select the audit server from the following options: ● Nessus Server: Interfaces with W-Policy Manager primarily to perform vulnerability scanning ● Nmap Audit: Performs specific audit functions You can click the View Details button to view the Policy Manager Entity Details dialog with the summary of audit server details. To view the Summary tab with audit server details, click the Modify button.
Audit Trigger Conditions	Select an audit trigger condition: ● Always: Always perform an audit. ● When posture is not available: Perform audit only when posture credentials are not available in the request. ● For MAC Authentication Request: If you select this option, W-Policy Manager presents the following three additional settings: ■ For known end-hosts only: Select this option when you want to reject unknown end-hosts and to audit known clients. Known end-hosts are defined as clients that are found in the authentication source(s) associated with this service. ■ For unknown end-hosts only: Select this option when known end-hosts are assumed to be healthy, but you want to establish the identity of unknown end-hosts and assign roles. Unknown end-hosts are end-hosts that are not found in any of the authentication sources associated with this service. ■ For all end-hosts: For both known and unknown end-hosts.
Action after audit	Specify the audit that can be performed only after the MAC authentication request is completed and the client has acquired an IP address through DHCP. Once the audit results are available, W-Policy Manager reapplies policies on the network device in one of the following ways: ● No Action: The audit does not apply policies on the network device after completing this audit. ● Do SNMP bounce: This option bounces the switch port or forces an 802.1X reauthentication (both done using SNMP). Bouncing the port triggers a new 802.1X or 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 W-ClearPass. ● Trigger RADIUS CoA action: This option sends a RADIUS CoA command from W-ClearPass to the network device.

Profiler Tab

The **Profiler** tab is not displayed by default.

1. To access this tab, select the **More Options > Profile Endpoints** check box.

The following figure displays the **Profile Endpoints** dialog:

Figure 53: Dell 802.1X Wireless Service > Profile Endpoints Dialog

Services

Service	Authentication	Authorization	Roles	Posture	Enforcement	Audit	Profiler	Summary
Endpoint Classification: Select the classification(s) after which an action must be triggered - Embedded Game Console Power -- Select -- Remove								
RADIUS CoA Action: [Cisco - Bounce-Host-Port] View Details Modify Add new RADIUS CoA Action								

2. Specify the **Profile Endpoints** parameters as described in the following table:

Table 37: Dell 802.1X Wireless Service > Profile Endpoints Parameters

Parameter	Action/Description
Endpoint Classification	Select one or more endpoint classification items from the drop-down list.
RADIUS CoA Action	Select the RADIUS CoA action from the drop-down list. - To view the Policy Manager Entity Details page with the summary of enforcement profile details, click the View Details button. - To view the Summary tab with profile details, click the Modify button. - To create a new RADIUS CoA action, click the Add new RADIUS CoA Action link.

Accounting Proxy Tab

Use the **Accounting Proxy** tab to broadcast the RADIUS accounting packets to all the proxy targets.

You can configure the proxy targets to which RADIUS server should be forwarded and the attributes to be added in the accounting. This enables the external security solutions to use the RADIUS account event to detect when a user connects and disconnects to the server.

1. To enable the **Accounting Proxy** tab, select the **More Options > Accounting Proxy** check box.

The following figure displays the **Accounting Proxy** dialog:

Figure 54: 802.1X Wireless > Accounting Proxy Dialog

Services

Service	Authentication	Roles	Enforcement	Accounting Proxy	Summary																														
Accounting Proxy Targets : [Accounting_Proxy] Remove View Details Modify Add new Accounting Proxy Target --Select to Add--																																			
RADIUS attributes to be added for Accounting proxy <table border="1"> <thead> <tr> <th>Type</th> <th>Name</th> <th>=</th> <th>Value</th> <th></th> <th></th> </tr> </thead> <tbody> <tr> <td>1. Radius:Aruba</td> <td>Aruba-Admin-Role</td> <td>=</td> <td>%{Authorization:172.31.1.11:UserDN}</td> <td></td> <td></td> </tr> <tr> <td>2. Radius:Aruba</td> <td>Auth-Simulation-Id</td> <td>=</td> <td>%{Authorization:172.31.1.11:Email}</td> <td></td> <td></td> </tr> <tr> <td>3. Radius:Aruba</td> <td>Aruba-AS-Username</td> <td>=</td> <td>%{Authorization:172.31.1.11:company}</td> <td></td> <td></td> </tr> <tr> <td>4. Click to add...</td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> </tbody> </table>						Type	Name	=	Value			1. Radius:Aruba	Aruba-Admin-Role	=	%{Authorization:172.31.1.11:UserDN}			2. Radius:Aruba	Auth-Simulation-Id	=	%{Authorization:172.31.1.11:Email}			3. Radius:Aruba	Aruba-AS-Username	=	%{Authorization:172.31.1.11:company}			4. Click to add...					
Type	Name	=	Value																																
1. Radius:Aruba	Aruba-Admin-Role	=	%{Authorization:172.31.1.11:UserDN}																																
2. Radius:Aruba	Auth-Simulation-Id	=	%{Authorization:172.31.1.11:Email}																																
3. Radius:Aruba	Aruba-AS-Username	=	%{Authorization:172.31.1.11:company}																																
4. Click to add...																																			

2. Specify the **Accounting Proxy** parameters as described in the following table:

Table 38: Dell 802.1X Wireless Service > Accounting Proxy Tab Parameters

Parameter	Action/Description
Accounting Proxy Targets	Specify the proxy targets to which the RADIUS server should be forwarded and the attributes to be added in the accounting. Select the accounting proxy target from the Select to Add drop-down list.
Add New Accounting Proxy Target	Click this link to add a new accounting proxy target.
RADIUS attributes to be added for Accounting proxy	
Type	Select the RADIUS attribute type from the drop-down list.
Name	Select the name of the RADIUS attribute from the drop-down list.
Value	Select the value from the Value drop-down list. The values displayed here depend on the RADIUS attribute Type selected.

Summary Tab

The **Summary** page presents the summary of parameters defined when you created a new service. The following figure displays the **Summary** tab:

Figure 55: Dell 802.1X Wireless Service > Summary Page

Services

Service	Authentication	Roles	Enforcement	Summary
Service:				
Type:	802.1X Wired			
Name:				
Description:	802.1X Wired Access Service			
Monitor Mode:	Disabled			
More Options:	-			
Service 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:				
Authentication Methods:	1. [EAP PEAP] 2. [EAP FAST] 3. [EAP TLS] 4. [EAP TTLS] 5. [EAP MSCHAPv2]			
Authentication Sources:	-			
Strip Username Rules:	-			
Roles:				
Role Mapping Policy:	-			
Enforcement:				
Use Cached Results:	Disabled			
Enforcement Policy:	[Sample Allow Access Policy]			

Cisco Web Authentication Proxy

This service is a web-based authentication service for guests or agent-less hosts. The Cisco switch hosts a captive portal and the portal web page that collects username and password information. Subsequently, the switch sends a RADIUS request in the form of a password authentication protocol (PAP) authentication request to Policy Manager. By default, this service uses the **PAP** authentication method. You can click on the **Authorization** and **Audit End-hosts** options to enable additional tabs.

The following figure displays the **Cisco Web Authentication Proxy** service:

Figure 56: Cisco Web Authentication Proxy Service

The screenshot shows the configuration page for the Cisco Web Authentication Proxy service. The 'Service' tab is selected. The 'Type' is set to 'Cisco Web Authentication Proxy'. The 'Name' and 'Description' fields are empty. The 'Monitor Mode' checkbox is unchecked. The 'More Options' section has 'Authorization' and 'Audit End-hosts' checked. The 'Service Rule' section shows a table with conditions for Radius:IETF, NAS-Port-Type, and Service-Type.

Type	Name	Operator
1. Radius:IETF	NAS-Port-Type	BELONGS_TO
2. Radius:IETF	Service-Type	EQUALS
3. Click to add...		

Configuring the **Cisco Web Authentication Proxy** service is similar to configuring the **Dell 802.1X Wireless** service except that the **Posture Compliance** and **Profile Endpoints** options are not available. For more information on configuration tabs, see [Dell 802.1X Wireless on page 83](#).

MAC Authentication

MAC-based authentication service is used 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 W-Policy Manager. W-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.



You cannot configure posture for this type of service.

The following figure displays the **MAC Authentication** service:

Figure 57: MAC Authentication Service

Type	Name	Operator	Value
1. Radius:IETF	NAS-Port-Type	BELONGS_TO	Etherne
2. Radius:IETF	Service-Type	BELONGS_TO	Login-Us
3. Connection	Client-Mac-Address	EQUALS	%{Radiu
4. Click to add...			

The **Posture** tab is not available for the MAC-based authentication service. Configuration for the rest of the tabs is similar to the **Dell 802.1X Wireless** service. For more information on configuration tabs, See [Dell 802.1X Wireless on page 83](#) for details.

RADIUS Authorization

Configure the **RADIUS Authorization** service type for services that perform authorization using RADIUS. When this service is selected, the **Authorization** tab is enabled by default. The following figure displays the **RADIUS Authorization** service:

Figure 58: RADIUS Authorization Service

Type	Name	Operator	Value
1. Radius:IETF	Service-Type	EQUALS	Authorize-Only (17)
2. Click to add...			

Configuration for this service is the same as the **RADIUS Enforcement (Generic)** service except that you do not configure authentication or posture with this service type. Refer to [RADIUS Enforcement \(Generic\) on page 97](#) for more information.

RADIUS Enforcement (Generic)

Configure the **RADIUS Enforcement (Generic)** service for any kind of RADIUS request.



The **[AirGroup Authorization Service]** service is the only **RADIUS Enforcement (Generic)** service that is available by default.

The default configuration tabs include **Service**, **Authentication**, **Roles**, and **Enforcement**. You can also select **Authorization**, **Posture Compliance**, **Audit End Hosts**, and **Profile Endpoints** in the **More Options** field on the **Service** tab.

There are no default rules 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). The following figure displays the **RADIUS Enforcement (Generic)** service:

Figure 59: *RADIUS Enforcement (Generic) Service*

The screenshot shows the configuration interface for the 'RADIUS Enforcement (Generic)' service. It features a tabbed interface with 'Service', 'Authentication', 'Roles', 'Enforcement', and 'Summary' tabs. The 'Service' tab is active, displaying fields for 'Type' (set to 'RADIUS Enforcement (Generic)'), 'Name', and 'Description'. Below these are checkboxes for 'Monitor Mode' (labeled 'Enable to monitor network access without enforcement') and 'More Options' (including 'Authorization', 'Posture Compliance', 'Audit End-hosts', and 'Profile Endpoints'). A 'Service Rule' section is also visible, showing a table with columns 'Type', 'Name', 'Operator', and 'Value'. The table currently contains one row with the text '1. Click to add...'. The 'Matches' section is set to 'ALL of the following conditions'.

Configuring a service for RADIUS requests is similar to configuring the **Dell 802.1X Wireless** service. For more information on configuration tabs, see [Dell 802.1X Wireless on page 83](#).

RADIUS Proxy

Configure the **RADIUS Proxy** service for any kind of RADIUS request that needs to be proxied to another RADIUS server (a Proxy Target). There are no default rules 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 the domain of the user trying to access the network.

Configuration of this service is the same as the **RADIUS Enforcement (Generic)** service except that you do not configure **Authentication** or **Posture** policies with this service type. However, you need to configure proxy targets (the servers to which requests are proxied). Requests can be dispatched to the proxy targets randomly, and are load balanced. However, in the **Failover** mode, requests can be dispatched to the first proxy target in the ordered list of targets and subsequently to the other proxy targets if the prior requests failed. When you select the **Enable proxy for accounting requests** accounting requests are also sent to the proxy targets.

The following figure displays the **RADIUS Proxy** service:

Figure 60: *RADIUS Proxy Service*

The screenshot shows the configuration page for the 'RADIUS Proxy' service. The interface has tabs for 'Service', 'Roles', 'Proxy Targets', 'Enforcement', and 'Summary'. The 'Service' tab is active. Fields include 'Type' (set to 'RADIUS Proxy'), 'Name' (empty), and 'Description' (empty). 'Monitor Mode' has a checkbox 'Enable to monitor network access without enforcement' which is unchecked. 'More Options' includes checkboxes for 'Authorization' (checked), 'Audit End-hosts' (unchecked), and 'Profile Endpoints' (unchecked). Below these is the 'Service Rule' section with a 'Matches' dropdown set to 'ALL of the following conditions:'. A table with columns 'Type', 'Name', 'Operator', and 'Value' contains one row: '1. Click to add...'. At the bottom are buttons for 'Back to Start Here', 'Next >', 'Save', and 'Cancel'.

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

For more information, see [RADIUS Enforcement \(Generic\)](#) on page 97.

Dell W-Series Application Authentication

This type of service provides authentication and authorization to users of Dell applications: W-Series W-ClearPass Guest and W-Series W-ClearPass Insight.

You can send [Generic Application Enforcement on page 372](#) to these or other generic applications for authenticating and authorizing the users.

The following figure displays the Dell **W-Series Application Authentication** service:

Figure 61: *Dell W-Series Application Authentication*

The screenshot shows the configuration page for the 'DELL W-Series Application Authentication' service. The interface has tabs for 'Service', 'Authentication', 'Roles', 'Enforcement', and 'Summary'. The 'Service' tab is active. Fields include 'Type' (set to 'DELL W-Series Application Authentication'), 'Name' (empty), and 'Description' (set to 'Authentication Service for Applications'). 'Monitor Mode' has a checkbox 'Enable to monitor network access without enforcement' which is unchecked. 'More Options' includes a checkbox for 'Authorization' which is checked. Below these is the 'Service Rule' section with a 'Matches' dropdown set to 'ALL of the following conditions:'. A table with columns 'Type', 'Name', 'Operator', and 'Value' contains two rows: '1. Application' with 'Name' as the value, 'EQUALS' as the operator, and 'Enter App Name' as the value; and '2. Click to add...'. At the bottom are buttons for 'Back to Start Here', 'Next >', 'Save', and 'Cancel'.

Type	Name	Operator	Value
1. Application	Name	EQUALS	Enter App Name
2. Click to add...			

Configuring the Dell **W-Series Application Authentication** service is similar to configuring the **Dell 802.1X Wireless** service except that the **Posture Compliance**, **Audit End-hosts**, and **Profile Endpoints** options are not available. For more information on configuration tabs, see [Dell 802.1X Wireless on page 83](#).

Dell W-Series Application Authorization

This type of service provides authorization for users of Dell applications: W-Series W-ClearPass Guest and W-Series W-ClearPass Insight. [Generic Application Enforcement on page 372](#) can be sent to these or other generic applications for authorizing the users. The following figure displays the **Dell W-Series Application Authorization** service:

Figure 62: Dell W-Series Application Authorization

The screenshot shows the configuration page for the Dell W-Series Application Authorization service. The 'Authorization' tab is selected. The 'Type' is set to 'DELL W-Series Application Authorization'. The 'Name' field is empty. The 'Description' is 'Authorization Service for Applications'. The 'Monitor Mode' checkbox is checked, with the label 'Enable to monitor network access without enforcement'. The 'More Options' section has the 'Authorization' checkbox checked. Below this is the 'Service Rule' section, which shows a table with columns 'Type', 'Name', 'Operator', and 'Value'. The table contains two rows: '1. Application' with 'Name' as the value, 'EQUALS' as the operator, and 'Enter App Name' as the value; and '2. Click to add...'. At the bottom, there are buttons for 'Back to Start Here', 'Next >', 'Save', and 'Cancel'.

Type	Name	Operator	Value
1. Application	Name	EQUALS	Enter App Name
2. Click to add...			

Configuring the Dell W-Series Application Authorization service is similar to configuring the Dell 802.1X Wireless service except that the **Posture Compliance**, **Audit End-hosts**, and **Profile Endpoints** options are not available. For more information on configuration tabs, see [Dell 802.1X Wireless on page 83](#).

W-ClearPass OnConnect Enforcement

This section provides the following information:

- [Adding a W-ClearPass OnConnect Enforcement Service](#)
- [Associating the W-ClearPass OnConnect Service with an Enforcement Policy](#)

W-ClearPass OnConnect Enforcement is an enforcement model that allows you to use non-802.1X methods for device scans, VLAN placement, and so on. W-ClearPass OnConnect Enforcement allows enforcement in non-802.1X environments without the need for an agent, such as OnGuard, on the endpoint.

For related information, see [Enabling W-ClearPass OnConnect Enforcement on a Network Device on page 436](#).

When W-ClearPass OnConnect Enforcement is enabled, W-ClearPass performs the following actions:

- Detects when a new endpoint connects to the network.
- Scans the endpoint to identify the logged-in user and other device-specific information.
- Triggers a Web-based authentication (WebAuth) for the device.
- Performs SNMP-based enforcement to change the network access profile for the device.

Adding a W-ClearPass OnConnect Enforcement Service

To add an OnConnect Enforcement service:

1. Navigate to **Configuration > Services**.

The **Services** page opens.

2. To add the service, click **Add**.

The **Add Services** dialog opens.

3. From the **Type** drop-down list, select **W-ClearPass OnConnect Enforcement** (see [Figure 63](#)).

Figure 63: Specifying W-ClearPass OnConnect Enforcement

Configuration » Services » Add

Services

Service | Authentication | Authorization | Roles | Enforcement | Summary

Type: ClearPass OnConnect Enforcement

Name: Non-Dot1X Enforcement

Description: Service for ClearPass OnConnect non-802.1X enforcement

Monitor Mode: ☒ Enable to monitor network access without enforcement

More Options: ☒ Authorization

Service Rule

Matches ☐ ANY or ☒ ALL of the following conditions:

Type	Name	Operator	Value	
1. Host	CheckType	EQUALS	None	
2. Click to add...				

4. Enter the name or label of the OnConnect Enforcement service.

5. Enter the values for any other parameters, including service rules, required for this service.

For a description of all the parameters in the **Service** page, see [Adding Services on page 1](#).

Associating the W-ClearPass OnConnect Service with an Enforcement Policy

After you create the W-ClearPass OnConnect Enforcement service, you must associate the service with an enforcement policy.

WMI (Windows Management Instrumentation) configuration is used to retrieve the Loggedin User information.

Whenever a domain-joined Windows client connects to an OnConnect-enabled port with the domain user logged in, Authorization attributes for this user are fetched from authorization sources to determine the role of the user; this information is then used in configuring Policy Enforcement. For details on configuring WMI credentials, see [WMI Credentials Configuration on page 144](#).

To associate a W-ClearPass OnConnect Enforcement service with an enforcement policy:

1. When finished with the parameter settings on the **Add Services > Service** page, click **Next**.

The **Services > Enforcement** page appears.

Figure 64: *Selecting the W-ClearPass OnConnect Enforcement Policy*

Enforcement Policy Details	
Description:	
Default Profile:	snmp-port-bounce
Rules Evaluation Algorithm:	first-applicable
Conditions	Enforcement Profiles
1. (Connection:Src-IP-Address <i>NOT_EXISTS</i>)	snmp-port-bounce
2. (Authentication:Full-Username <i>NOT_EXISTS</i>)	snmp-port-bounce
3. <i>AND</i> (Authorization:AD-UserDN <i>EXISTS</i>) (Connection:NAD-Port-Name <i>EQUALS</i> Fa1/0/7)	vlan6
4. <i>AND</i> (Authorization:AD-UserDN <i>EXISTS</i>) (Connection:NAD-Port-Name <i>EQUALS</i> Fa1/0/3)	vlan4
5. (Connection:NAD-Port-Name <i>EQUALS</i> Fa1/0/5)	vlan5
6. (Connection:NAD-Port-Name <i>EQUALS</i> Fa1/0/8)	vlan4

From the **Services > Add > Enforcement** page, you can either select an existing enforcement policy or create a new one.

- From the **Enforcement Policy** drop-down list, select the appropriate OnConnect Enforcement policy.
 - If you have not configured an OnConnect-type Enforcement policy, click **Add New Enforcement Policy** to create a new enforcement policy.
- Specify the values for the remaining parameters as described in [Table 39](#), then click **Save**.

Table 39: *Service Enforcement Page Parameters*

Parameter	Description
Use Cached Results	1. Select this check box to use cached roles and posture attributes from previous sessions.
Enforcement Policy	2. From the drop-down list, select the preconfigured enforcement policy. This is a mandatory step.
Enforcement Policy Details	
Description	Displays additional information about the selected enforcement policy.
Default Profile	Displays a default profile applied by .
Rules Evaluation Algorithm	Shows first matched rule and return the role or select all matched rules and return a set of roles.

Event-Based Enforcement

The **Event-Based Enforcement** service manages enforcement actions in response to threat-event processing.

When there is a suspicious user, this user could represent a common DOS attack or some other threat. When a threat is detected, W-ClearPass performs enforcement operations as configured; for example, executing a change of authorization (COA) to disconnect a suspicious user from the network.

To add an event-based enforcement service:

- Navigate to **Configuration > Services**.

- The **Services** page appears. The **Services** page provides options to add, modify, and remove a service.
- To add the service, click **Add**.
The **Add Services** dialog appears.
 - From the **Type** drop-down list, select **Event-based Enforcement** (see [Figure 65](#)).

Figure 65: Specifying Event -Based Enforcement

Configuration » Services » Add

Services

Enforcement policy "Event-based enforcement policy" has been added

Service | Enforcement | Summary

Type: Event-based Enforcement

Name: Event-based Enforcement Service

Description: Service for ingress events based enforcement

Monitor Mode: ☒ Enable to monitor network access without enforcement

More Options:

Service Rule

Matches ☐ ANY or ☒ ALL of the following conditions:

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

- Enter the name or label of the event-based enforcement service.
- Enter the values for any other parameters, including service rules, required for this service.
For a description of all the parameters in the **Service** page, see [Adding Services on page 1](#).

Associating the Service with an Enforcement Policy

After you create the event-based enforcement service, you must associate the service with an enforcement policy. You can do this from the **Services > Add > Enforcement** page.

- When finished with the parameter settings on the **Add Services > Service** page, click **Next**.
The **Services > Enforcement** page appears.

Figure 66: Selecting the Ingress Events Enforcement Policy

Dashboard | Monitoring | Configuration

Configuration » Services » Edit - Juniper-Event-Service

Services - Juniper-Event-Service

Summary | Service | **Enforcement**

Use Cached Results: ☐ Use cached Roles and Posture attributes from previous sessions

Enforcement Policy: Test-Event-Enf-Policy Modify Add new Enforcement Policy

Enforcement Policy Details

Description: [Aruba Terminate Session]

Default Profile: [Aruba Terminate Session]

Rules Evaluation Algorithm: first-applicable

Conditions	Enforcement Profiles
1. {Event:Juniper-SRX-TS:attack-name EXISTS }	[Aruba Terminate Session], Update-Endpoint-Threat-Tags-TS
2. {Event:Juniper-SRX-SS:attack-name EXISTS }	[Aruba Terminate Session], Update-Endpoint-Threat-Tags-SS

- From the **Services > Add > Enforcement** page, you can either select an existing enforcement policy or create a new one.
- From the **Enforcement Policy** drop-down list, select the appropriate Event Enforcement policy.
 - If you have not configured Event-type Enforcement policies, click **Add New Enforcement Policy** to create a new enforcement policy.
 - Specify the values for the remaining parameters as described in [Table 40](#), then click **Save**.

Table 40: Service Enforcement Page Parameters

Parameter	Description
Use Cached Results	1. Select this check box to use cached roles and posture attributes from previous sessions.
Enforcement Policy	2. From the drop-down list, select the preconfigured enforcement policy. This is mandatory.
Enforcement Policy Details	
Description	Displays additional information about the selected enforcement policy.
Default Profile	Displays a default profile applied by .
Rules Evaluation Algorithm	Shows first matched rule and return the role or select all matched rules and return a set of roles.

TACACS+ Enforcement

Configure the **TACACS+ Enforcement** service for any kind of TACACS+ request. 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. Note that this tab is not enabled by default. Select the **Authorization** check box from **More Options** on the **Service** tab to enable this 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 [TACACS+ Based Enforcement on page 387](#) for more information. The following figure displays the **TACACS+ Enforcement** service:

Figure 67: TACACS+ Enforcement Service

The screenshot shows the configuration interface for the TACACS+ Enforcement service. The 'Service' tab is selected. The 'Type' is set to 'TACACS+ Enforcement'. The 'Name' and 'Description' fields are empty. The 'Monitor Mode' checkbox is unchecked, and the 'More Options' checkbox for 'Authorization' is checked. Below this is the 'Service Rule' section, which includes a radio button to select 'ANY' or 'ALL' of the following conditions. A table with columns 'Type', 'Name', 'Operator', and 'Value' is shown, with a single row containing the text '1. Click to add...'.

Configuring the **TACACS+ Enforcement** service is similar to configuring the **Dell 802.1X Wireless** service except that the **Posture Compliance**, **Audit End-hosts**, and **Profile Endpoints** options are not available. For more information on configuration tabs, see [Dell 802.1X Wireless on page 83](#).

Web-based Authentication

Configure this service for guests or agent-less hosts that connect through the Dell built-in Portal. The user is redirected to the Dell 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 the following operating systems:

- Windows 7
- Windows Vista
- Windows XP
- Windows Server 2008
- Windows Server 2003
- Linux

An internal service rule **Connection:Protocol EQUALS WebAuth** categorizes requests into this type of service. You can add additional rules if needed. The following figure displays the **Web-based Authentication** service:

Figure 68: *Web-based Authentication Service*

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



The **Audit End-hosts** and **Profile Endpoints** options are not available for the **Web-based Authentication** service.

Configuring the **Web-based Authentication** service for guests or agentless hosts is similar to configuring the **Dell 802.1X Wireless** service. For more information on configuration tabs, see [Dell 802.1X Wireless on page 83](#).

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 check is done. The internal service rule **Connection:Protocol EQUALS WebAuth** categorizes requests into this type of service. The external service rule **Host:CheckType EQUALS Health** is automatically added when you select this type of service. For more information, see [Web-based Authentication on page 104](#).



This service does not include authentication options. This service performs health checks only.

The following figure displays the **Web-Based Health Check Only** service:

Figure 69: *Web-Based Health Check Only Service*

The screenshot shows the configuration page for the 'Web-based Health Check Only' service. The 'Service' tab is selected. The 'Type' dropdown is set to 'Web-based Health Check Only'. The 'Name' and 'Description' fields are empty. The 'Monitor Mode' checkbox is checked, with the label 'Enable to monitor network access without enforcement'. The 'More Options' section has two checkboxes: 'Authorization' (checked) and 'Posture Compliance' (unchecked). The 'Service Rule' section is expanded, showing a table with the following data:

Type	Name	Operator	Value
1. Host	CheckType	MATCHES_ALL	Health
2. Click to add...			

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

For more information on configuration tabs, see [Dell 802.1X Wireless on page 83](#)

Web-based Open Network Access

Configuration for this service is the same as **Web-based Authentication** service except that a health check is not performed on the endpoints. A **Terms of Service** page (as configured on the **W-ClearPass Policy Manager Guest Portal** page) is presented to the user. Network access is granted, when you click **Submit Action**. The **Posture** option is not available for the **Web-based Authentication** service. For more information, see [Web-based Authentication on page 104](#). The following figure displays the **Web-based Open Network** service page:

Figure 70: *Web-based Open Network Access Service*

The screenshot shows the configuration page for the 'Web-based Open Network Access' service. The 'Service' tab is selected. The 'Type' dropdown is set to 'Web-based Open Network Access'. The 'Name' and 'Description' fields are empty. The 'Monitor Mode' checkbox is checked, with the label 'Enable to monitor network access without enforcement'. The 'More Options' section has one checkbox: 'Authorization' (checked). The 'Service Rule' section is expanded, showing a table with the following data:

Type	Name	Operator	Value
1. Host	CheckType	EQUALS	None
2. Click to add...			

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

For more information on configuration tabs, see [Dell 802.1X Wireless on page 83](#).

The Monitoring features in W-Policy Manager provide access to live monitoring of components and other functions. W-ClearPass Policy Manager includes the following Monitoring features:

- Network Discovery
 - [Profiler and Discovery: Network Discovery on page 140](#)
- Live Monitoring
 - [Live Monitoring: Access Tracker on page 107](#)
 - [Live Monitoring: Accounting on page 116](#)
 - [Live Monitoring: Analysis and Trending on page 133](#)
 - [Profiler and Discovery: Endpoint Profiler on page 139](#)
 - [Live Monitoring: OnGuard Activity on page 1](#)
 - [Live Monitoring: System Monitor on page 134](#)
- Audit Viewer
 - [Audit Viewer on page 152](#)
- Event Viewer
 - [Event Viewer on page 155](#)
- Data Filters
 - [Data Filters on page 158](#)
- Blacklisted Users
 - [Restoring Blacklisted Users to the Network on page 162](#)

Live Monitoring: Access Tracker

This section provides the following information:

- [About the Access Tracker](#)
- [Customizing the Access Tracker](#)
- [Viewing Access Tracker Session Details](#)

About the Access Tracker

The **Access Tracker** provides a real-time display of per-session access activity on the selected server or domain.

1. To view this page, navigate to **Monitoring > Live Monitoring > Access Tracker**.
The **Access Tracker** page opens.

Figure 71: Access Tracker Page

Monitoring » Live Monitoring » Access Tracker

Access Tracker Jul 20, 2016 03:40:25 IST Auto Refresh

[All Requests] VM-5-109 (10.) Last 1 week before Today Edit

Filter: Request ID contains Go Clear Filter Show 100 records

#	Server	Source	Username	Host MAC Address	Service	Login Status	Enforcement Profiles	Request Timestamp
1.	10.	WEBAUTH		f0761cb5efab	Srini-OnConnect	ACCEPT	wmi-lookup-failed-snmpport-bounce	2016/07/15 15:48:45
2.	10.	WEBAUTH		0015c57b1c7d	Srini-OnConnect	ACCEPT	wmi-lookup-failed-snmpport-bounce	2016/07/15 15:36:23
3.	10.	WEBAUTH		f0761cb5efab	Srini-OnConnect	ACCEPT	wmi-lookup-failed-snmpport-bounce	2016/07/15 15:34:59
4.	10.	WEBAUTH		f0761cb5efab	Srini-OnConnect	ACCEPT	wmi-lookup-failed-snmpport-bounce	2016/07/15 15:34:49

Table 41 describes the information in the **Access Tracker** page:

Table 41: Access Tracker Page Columns

Column	Description
Server	Displays the IP address of the server.
Source	Displays the authentication source for the session. For example, TACACS or web authentication (WEBAUTH).
Username	Displays the username or MAC address of the user.
Service	Displays the name of the service.
Login Status	Displays the status of the request, such as Accept , Reject , or Timeout .
Enforcement Profiles	Displays the names of the enforcement profiles associated with the Service.
Request Timestamp	Displays the date and time when the status was last updated.

Customizing the Access Tracker

To customize the **Access Tracker** parameters:

1. Click the **Edit** button.

The **Access Tracker Edit** page opens.

Figure 72: Access Tracker Edit Page

Monitoring » Live Monitoring » Access Tracker

Access Tracker Jul 20, 2016 03:50:34 IST Auto Refresh

Select Server/Domain: VM-5-109 (10...)

Select Filter: [All Requests] + Add

Select Date Range: Last 1 week before Show Latest

Select Columns:

Available Columns: Auth Type, NAS IP Address, Monitor Mode, NAS Port, Request ID, Alerts Present

Selected Columns: Server, Source, Username, Host MAC Address, Service, Login Status Up Down

Save Cancel

Filter: Request ID contains Go Clear Filter Show 100 records

#	Server	Source	Username	Host MAC Address	Service	Login Status	Enforcement Profiles	Request Timestamp
1.	10...	WEBAUTH		f0761cb5efab	Srini-OnConnect	ACCEPT	wmi-lookup-failed-snmpport-bounce	2016/07/15 15:48:45
2.	10...	WEBAUTH		0015c57b1c7d	Srini-OnConnect	ACCEPT	wmi-lookup-failed-snmpport-bounce	2016/07/15 15:36:23

2. Modify the **Access Tracker Edit** page parameters as described in the following table, then click **Save**:

Table 42: Access Tracker Edit Page Parameters

Parameter	Action Description
Select Server/Domain	Displays information for the selected server or domain on the Access Tracker page. To display transactions from all nodes in the W-Policy Manager cluster, select all the servers.
Select Filter	Select a filter category to filter the displayed data. For a description of available filters, see Data Filters on page 158 .
Modify Filter	To modify the current data filter, click the icon. For more information, see Data Filters on page 158 .
Add Filter	To add a data filter, click the + Add icon. The Data Filters page opens. For more information, see Data Filters on page 158 .
Select Date Range	To select the start of the range of dates for which the Access Tracker table displays data, click the Last drop-down list. Available options are one to six days, or one week.

Table 42: Access Tracker Edit Page Parameters (Continued)

Parameter	Action Description
Select Date	To select a date, click the  icon.
Show Latest	To set the date in the before field to the current date, click Show Latest .
Select Columns	This section displays the following two fields: • Available Columns: Displays the data column available to be displayed in an Access Tracker table. • Selected Columns: Displays the data columns currently selected for display. To move a column name from one field to another: • Select the column name and click the left or right arrows. To change the order in which the columns are displayed: • Click a column name in the Selected Columns field, then click the Up or Down buttons.

Viewing Access Tracker Session Details

This section provides the following information:

- [Summary Tab on page 110](#)
- [Input Tab on page 111](#)
- [Output Tab on page 112](#)
- [Alerts Tab on page 113](#)
- [Viewing Access Tracker Session Details on page 110](#)
- [Access Control Capabilities on page 114](#)

To view details about a selected session:

1. Navigate to the **Monitoring > Live Monitoring > Access Tracker** page.
2. Click any session in the **Access Tracker** table.
The information in this page varies, depending upon the session selected.
3. Refer to the following sections for details about the specific types of information that can appear on each tab of the **Request Details** page:

Summary Tab

The **Request Details > Summary** page shows a summary view of the transaction, including policies that are applied and protocol-specific attributes.

Click any table row in the **Monitoring > Live Monitoring > Access Tracker** page to view the **Summary** tab.

The following figure displays the **Summary** tab:

Figure 73: *Request Details > Summary Tab*

The screenshot shows a web interface titled "Request Details" with a tabbed menu at the top containing "Summary", "Input", "Output", and "Alerts". The "Summary" tab is active, displaying a table of request details. Below the table is a section titled "Policies Used -" which contains another table of policy-related information. At the bottom of the interface, there is a status bar showing "Showing 3 of 1-56 records" and several action buttons: "Change Status", "Show Configuration", "Export", "Show Logs", and "Close".

Login Status:	ACCEPT
Session Identifier:	agentless-enforce-00000001-01-5788b52d
Date and Time:	Jul 15, 2016 15:34:59 IST
End-Host Identifier:	f0761cb5efab (Computer / Windows / Windows 8/10)
Username:	-
Access Device IP/Port:	10. :Fa1/0/7 (Cisco-Switch / Cisco)
System Posture Status:	UNKNOWN (100)

Policies Used -	
Service:	Srini-OnConnect
Authentication Method:	Not applicable
Authentication Source:	-
Authorization Source:	AD
Roles:	[BYOD Operator], [User Authenticated]
Enforcement Profiles:	wmi-lookup-failed-snmp-port-bounce
Service Monitor Mode:	Disabled
Online Status:	Not Available

Showing 3 of 1-56 records

Change Status Show Configuration Export Show Logs Close

Input Tab

The **Input** tab shows protocol-specific attributes that W-Policy Manager received in a transaction request, including authentication and posture details (if available).

The **Input** tab also shows computed attributes that W-Policy Manager derived from the request attributes. All of these attributes can be used in role mapping rules.

1. To view the **Input** tab, click any table row in the **Monitoring > Live Monitoring > Access Tracker** page, then select the **Input** tab.

The **Request Details > Input** page opens.

Figure 74: Request Details > Input Page

The screenshot shows the 'Request Details' window with the 'Input' tab selected. The window has a title bar 'Request Details' and a close button. Below the title bar are four tabs: 'Summary', 'Input', 'Output', and 'Alerts'. The 'Input' tab is active, displaying a form with the following fields:

Username:	BANGALORE\k
End-Host Identifier:	f0761cb5efab (Computer / Windows / Windows 8/10)
Access Device IP/Port:	10. :Fa1/0/7 (Cisco-Switch / Cisco)

Below these fields is a section titled 'Authorization Attributes' with a scrollable list of attributes:

Authorization:AD:Account Expires	9223372036854775807 [30828-09-14 08:18:05 IST]
Authorization:AD:company	Aruba
Authorization:AD:Department	Network Services
Authorization:AD:Email	k.com
Authorization:AD:memberOf	CN=Administrators,CN=Builtin,DC=bangalore,DC=avendasys,DC=com, CN=employee,DC=bangalore,DC=avendasys,DC=com
Authorization:AD:Name	k
Authorization:AD:Phone	123456789
Authorization:AD:Title	QA
Authorization:AD:UserDN	CN=,CN=Users,DC=bangalore,DC=avendasys,DC=com

Below the 'Authorization Attributes' section is a section titled 'Computed Attributes' which is currently empty. At the bottom of the window, there is a status bar showing 'Showing 20 of 1-56 records' and several action buttons: 'Change Status', 'Show Configuration', 'Export', 'Show Logs', and 'Close'.

Output Tab

The **Request Details > Output** tab shows the attributes that were sent to the network device (switch or controller) and the posture-capable endpoint (for example, MAC devices).

You can view the posture response and posture evaluation with accurate results. For example, you can view details such as missing registry keys and the reasons for a failed registry key check.

To view the **Request Details > Output** page:

1. Navigate to the **Monitoring > Live Monitoring > Access Tracker** page.
2. Click any table row in the **Access Tracker** page.
3. Select the **Output** tab.

The **Request Details > Output** page opens:

Figure 75: *Request Details > Output Page*

The screenshot shows the 'Request Details' window with the 'Output' tab selected. The 'Summary' tab is also visible. The 'Output' tab displays the following information:

Enforcement Profiles:	wmi-lookup-failed-snmp-port-bounce
System Posture Status:	UNKNOWN (100)
Audit Posture Status:	UNKNOWN (100)

Below this, there is a section titled 'SNMP Response' with a dropdown arrow. It contains the following data:

ResetConnection	true
SessionTimeout	180

At the bottom of the window, there is a status bar showing 'Showing 4 of 1-56 records' and several action buttons: 'Change Status', 'Show Configuration', 'Export', 'Show Logs', and 'Close'.



Access Tracker shows an alert if more than two anti-malware products are installed on a client.

Alerts Tab

The **Request Details > Alerts** page shows information about a session that has an error.

To view the **Request Details > Alerts** page:

1. Navigate to the **Monitoring > Live Monitoring > Access Tracker** page.
2. Click a table row for a session that has an error.

The **Request Details > Alerts** page opens:

Figure 76: *Request Details > Alerts Page*

The screenshot shows the 'Request Details' window with the 'Alerts' tab selected. The 'Summary' tab is also visible. The 'Alerts' tab displays the following information:

Error Code:	-
Error Category:	Success
Error Message:	Success

Below this, there is a section titled 'Alerts for this Request' with a dropdown arrow. It contains the following data:

WebAuthService	wmi: Query with configured credentials failed for host 10. . Username is empty in the request

At the bottom of the window, there is a status bar showing 'Showing 4 of 1-56 records' and several action buttons: 'Change Status', 'Show Configuration', 'Export', 'Show Logs', and 'Close'.

Configuration Tab

The **Request Details > Configuration** page shows the attributes that W-Policy Manager received in a transaction request, including service rules, role mapping policies used, authorization sources, and enforcement policies used (if available).

To view the **Configuration** page:

1. Click any table row in the **Monitoring > Live Monitoring > Access Tracker** page.
The **Request Details** page opens.
2. Click the **Show Configuration** button.
The **Configuration** tab appears and the **Request Details > Configuration** page opens:

Figure 77: Request Details > Configuration Page

Request Details

Summary Input Output Alerts **Configuration**

Service Details

Name:	Srini-OnConnect
Description:	Service for ClearPass OnConnect enforcement
Type:	ClearPass OnConnect Enforcement
Status:	Enabled
Monitor Mode:	Disabled

Type	Name	Operator	Value
1. Host	CheckType	EQUALS	None

Role Mapping Policy Details

Enforcement Policy Details

Name:	srini-snmp-test
Description:	
Default Profile:	default-snmp-port-bounce
Rules Evaluation Algorithm:	first-applicable

Showing 4 of 1-56 records

Change Status **Show Configuration** Export Show Logs Close

Access Control Capabilities

The **Access Control Capabilities** page shows a summary view of the transaction, including policies that are applied and protocol-specific attributes. You can use the **Access Control Capabilities** page to view or change the access control type.



The **Change Status** button is enabled only if you use the RADIUS and WebAuth authentication types.

To view the **Access Control Capabilities** page:

1. Click any table row in the **Monitoring > Live Monitoring > Access Tracker** page.
The **Request Details** page opens.
2. Click the **Change Status** button.
The **Request Details > Access Control Capabilities** page opens:

Figure 78: *Request Details > Access Control Capabilities Dialog*

Access Control Capabilities -	
Select Access Control Type : ☐ Agent ☐ SNMP ☐ RADIUS CoA ☒ Server Action	
Server Action:	Handle AirGroup Time Sharing
Context Server:	localhost
Server Type:	Generic HTTP
Action Description:	Sends time-based sharing policy to the AirGroup notification service

Submit Cancel

3. Specify the **Request Details > Access Control Capabilities** page parameters as described in the following table:

Table 43: Request Details > Access Control Capabilities Page Parameters

Parameter	Action/Description
Change Status	You can view or change to any of the following access control types: . ● Agent: This control is available for a session where the endpoint has the OnGuard Agent installed. The following actions are allowed: ■ Bouncing ■ Sending Messages ■ Tagging the status of the endpoint as Disabled or Known. ● SNMP: This control is available for any session for which W-Policy Manager has the switch and port-level information associated with the MAC address of the endpoint. W-Policy Manager uses SNMP to bounce the switch port with which the endpoint is associated. NOTE: For this type of control, SNMP read and write community strings must be configured for the network device. You must configure W-Policy Manager as an SNMP trap receiver to receive link up/down traps. For more information, see SNMP Trap Receivers on page 533. ● RADIUS CoA: This control is available for any session where access was previously controlled by a RADIUS transaction. NOTE: The network device must be RADIUS CoA-capable and RADIUS CoA-enabled when you configure the network device in W-Policy Manager (see Adding a Network Device on page 430). The actions available depend on the type of device. The Disconnect or Terminate Section action is supported by all devices. Some devices support setting a session timeout, changing the VLAN for the session, and applying an ACL. ● Server Action: This control is available by default for any session. Select the server action from the Server Action drop-down list.
Server Action	Select the server action that is performed on endpoints. You can select from the following options: ● Check Point Login - AD User ● Check Point Login - Guest User ● Check Point Logout ● Fortinet Login ● Fortinet Logout ● Handle AirGroup Time Sharing ● Infoblox Login ● Nmap scan: Appears only if the server action contains a valid IP address. ● SNMP Scan: Appears only if the server action contains a valid IP address.
Context Server	Select a Context Server from the drop-down list.
Server Type	Displays the server type configured when the server action was configured.
Action Description	Provides the description of the server action; for example, "Inform Check Point that user logged in."

Live Monitoring: Accounting

This section provides the following information:

- [Modifying the Accounting Page Parameters](#)

- [RADIUS Accounting Details > Summary Tab](#)
- [RADIUS Accounting Record Details > Auth Sessions Tab](#)
- [RADIUS Accounting Record Details > Utilization Tab](#)
- [RADIUS Accounting Record Details > Details Tab](#)
- [TACACS+ Accounting Record Details > Request Tab](#)
- [TACACS+ Accounting Record Details > Auth Sessions Tab](#)
- [TACACS+ Accounting Record Details > Details Tab](#)

The **Monitoring > Live Monitoring > Accounting** page provides a dynamic report that describes session access, as reported by the network access device by means of RADIUS or TACACS+ accounting records.

The following figure displays the **Live Monitoring > Accounting** page:

Figure 79: *Live Monitoring > Accounting Page*

#	Server	Protocol	User	Access Device	Start Time
1.	10.10.10.10	TACACS	mahesh	10.10.10.10	Jul 26, 2016 10:43:39 PDT
2.	10.10.10.10	TACACS	mahesh	10.10.10.10	Jul 26, 2016 10:33:30 PDT
3.	10.10.10.10	TACACS	mahesh	10.10.10.10	Jul 25, 2016 17:07:29 PDT
4.	10.10.10.10	TACACS	mahesh	10.10.10.10	Jul 25, 2016 16:52:06 PDT
5.	10.10.10.10	TACACS	mahesh	10.10.10.10	Jul 25, 2016 15:51:25 PDT
6.	10.10.10.10	TACACS	mahesh	10.10.10.10	Jul 25, 2016 15:38:27 PDT
7.	10.10.10.10	TACACS	mahesh	10.10.10.10	Jul 25, 2016 15:07:51 PDT
8.	10.10.10.10	TACACS	mahesh	10.10.10.10	Jul 25, 2016 14:50:11 PDT
9.	10.10.10.10	TACACS	tim	10.10.10.10	Jul 25, 2016 13:10:06 PDT
10.	10.10.10.10	TACACS	tim	10.10.10.10	Jul 25, 2016 12:59:15 PDT

The following table describes the **Accounting** parameters:

Table 44: *Accounting Page Parameters*

Parameter	Description
Server	Specifies the IP address of the host name.
Protocol	Specifies the protocol used.
User	Displays the user name.
Access Device	Displays the IP address of the device.
Start Time	Displays the date and time.



You can click any row in the Accounting page to drill down and display the corresponding **Accounting Record Details** page for the selected session. For details, see [RADIUS Accounting Details > Summary Tab](#) on page 119 and [TACACS+ Accounting Record Details > Auth Sessions Tab](#) on page 125.

Modifying the Accounting Page Parameters

You can filter or modify the information displayed in this table by creating a filter, or selecting a different server, domain, or time range.

To filter the data currently displayed in the **Accounting** page:

1. Navigate to the **Monitoring > Live Monitoring > Accounting** page.
2. Click **Edit**.

The **Edit Accounting Page** dialog opens.

Figure 80: Edit Accounting Page Dialog

Monitoring > Live Monitoring > Accounting

Accounting

Select Server/Domain: clearpass-a (10.)

Select Filter: [All Requests] + Add

Select Date Range: Last 1 day before

Show Latest

Save Cancel

Filter: Protocol contains Go Clear Filter

Show 10 records

#	Server	Protocol	User	Access Device	Start Time
1.	10.	TACACS	mahesh	10.	Jul 26, 2016 10:43:39 PDT
2.	10.	TACACS	mahesh	10.	Jul 26, 2016 10:33:30 PDT

3. Specify the **Edit Accounting Page** parameters as described in [Table 45](#):

Table 45: Edit Accounting Page Parameters

Parameter	Action/Description
Select Server/ Domain	Select the W-ClearPass server for the dashboard data to be displayed.
Select Filter	To constrain the data display, select a filter from the drop-down list. You can select one of the following filters: • Protocol • User • Access Device
Modify	To modify a data filter, click the Modify Data Filter icon  (as shown in Figure 80).
Add	To create a new data filter, click the  Add icon.
Select Date Range	Select the number of days prior to the configured date for which the accounting data to be displayed. You can specify the number from one day to a week.
Show Latest	To view the latest information, set the date to Today .
Select Columns	• To move data between Available Columns and Selected Columns, click the right or left arrows. • To rearrange columns, click the Up or Down buttons.

RADIUS Accounting Details > Summary Tab

To drill down and display the corresponding **Accounting Record Details** page for the session, click any row in the **Accounting** page.

The **Accounting Record Details > Summary** tab shows a summary view of the transaction including session IDs, timestamp, and network details for the RADIUS protocol.

The following figure displays the **RADIUS Accounting Record Details > Summary** page:

Figure 81: RADIUS Accounting Record Details Summary Page

Accounting Record Details			
Summary	Auth Sessions	Utilization	Details
Session ID:	R0004ec01-01-578cf14		
Account Session ID:	cptest-1469042341-197@example.com1700000000c5-197		
Start Timestamp:	Jul 20, 2016 12:20:52 PDT		
End Timestamp:	Jul 20, 2016 12:22:32 PDT		
Status:	Inactive		
Username:	cptest-1469042341-197@example.com		
Termination Cause:	User-Request		
Service Type:	-		
Network Details -			
NAS IP Address:	10.0.0.0		
NAS Port Type:	Ethernet		
Calling Station ID:	1700000000c5		
Called Station ID:	000c292f177f		
Framed IP Address:	10.0.0.197		
Account Auth:	-		
<button>Close</button>			

The following table describes the configuration parameters on the **RADIUS Accounting Record Details > Summary** page:

Table 46: RADIUS Accounting Record Details Summary Tab Parameters

Parameter	Description
Session ID	Specifies the W-Policy Manager session identifier. You can correlate this record with a record in Access Tracker .
Account Session ID	Specifies a unique ID for this accounting record.
Start Timestamp End Timestamp	Shows the start time and end time of the session.

Table 46: RADIUS Accounting Record Details Summary Tab Parameters (Continued)

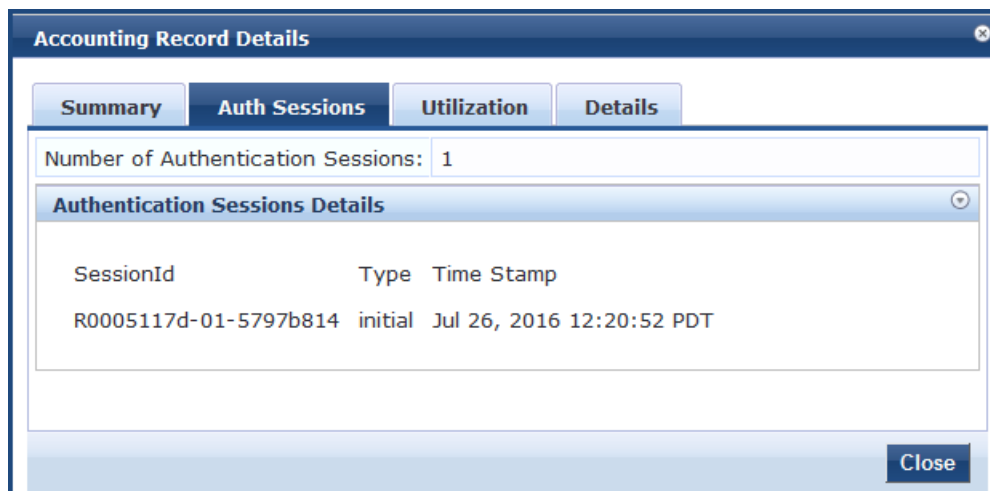
Parameter	Description
Status	Shows the current connection status of the session.
Username	Username associated with this record.
Termination Cause	Specifies the reason for termination of this session.
Service Type	Shows the value of the standard RADIUS attribute service type.
Network Details	
NAS IP Address	Shows the IP address of the network device.
NAS Port Type	Shows the access methods. For example, Ethernet, or 802.11 Wireless.
Calling Station ID	Specifies the MAC address of the client that is supported by W-Policy Manager.
Called Station ID	Shows the MAC address of the network device.
Framed IP Address	Shows the IP address of the client (if available).
Account Auth	Specifies the type of authentication; for example, RADIUS authentication.

RADIUS Accounting Record Details > Auth Sessions Tab

This section describes the parameters of the **Accounting Record Details > Auth Sessions** tab for the RADIUS protocol.

The following figure displays the the **Accounting Record Details > Auth Sessions** page:

Figure 82: RADIUS Accounting Record Details > Auth Sessions Page



The following table describes the **RADIUS Accounting Record Details >Auth Sessions** parameters:

Table 47: RADIUS Accounting Record Details Auth Sessions Tab Parameters

Parameter	Description
Number of Authentication Sessions	Specifies the total number of authentications (always 1) and authorizations in this session.
Authentication Sessions Details	
Session ID	Displays the W-Policy Manager session ID.
Type	Specifies the type of authentication: Initial authentication or reauthentication.
Time Stamp	Specifies the time when the event occurred.

RADIUS Accounting Record Details > Utilization Tab

This section describes the parameters of the **Accounting Record Details > Utilization** tab for the RADIUS protocol.

The following figure displays the **RADIUS Accounting Record Details > Utilization** page:

Figure 83: RADIUS Accounting Record Details > Utilization Page

The screenshot shows a web interface titled "Accounting Record Details" with a close button in the top right corner. Below the title bar are four tabs: "Summary", "Auth Sessions", "Utilization" (which is selected and highlighted with a dashed border), and "Details". The "Utilization" tab displays a table with the following data:

Active Time:	9027 Sec
Account Delay Time:	-
Account Input Octets :	2647001
Account Output Octets :	11540248
Account Input Packets :	14200
Account Output Packets :	37866

At the bottom right of the page, there is a "Close" button.

The following table describes the configuration parameters on the **RADIUS Accounting Record Details - Utilization** tab:

Table 48: *RADIUS Accounting Record Details > Utilization Tab Parameters*

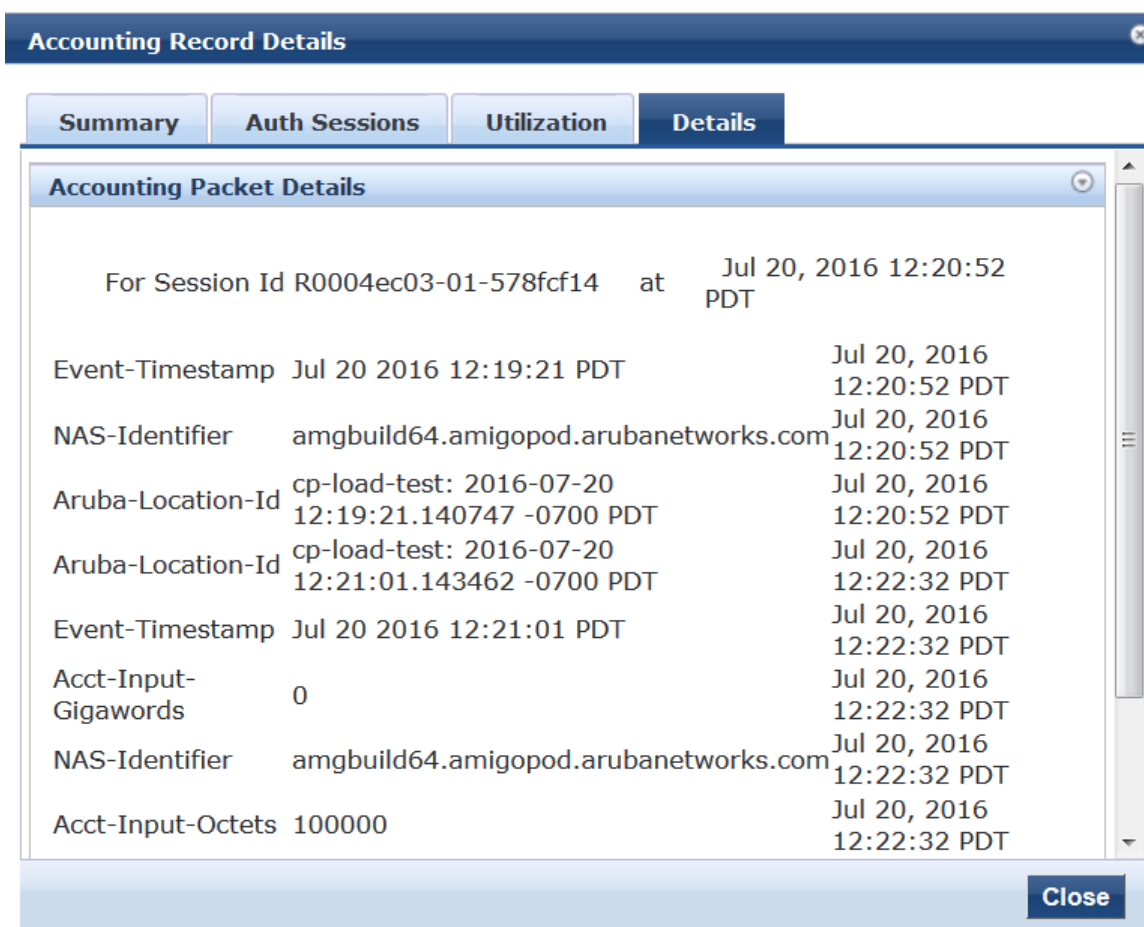
Parameter	Description
Active Time	Displays the duration of the session that was active.
Account Delay Time	Displays how many seconds the network device has been trying to send this record for (subtract from record time stamp to determine the time this record was actually generated by the device).
Account Input Octets	Specifies the quantity of octets sent to and received from the device port during the session.
Account Output Octets	
Account Input Packets	Specifies the packets sent and received from the device port during the session.
Account Output Packets	

RADIUS Accounting Record Details > Details Tab

This section describes the parameters of the **Accounting Record Details > Details** tab for the RADIUS protocol.

The following figure displays the example of the **RADIUS Accounting Record Details > Details** page:

Figure 84: RADIUS Accounting > Details Page



The following table summarizes the configuration information provided on the **RADIUS Accounting Record Details > Details** page:

Table 49: RADIUS Accounting Record > Details Page Summary

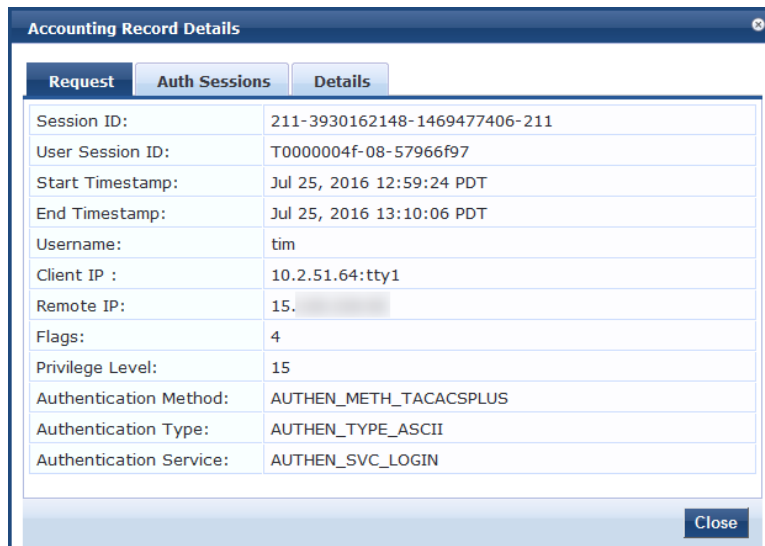
Parameter	Description
Accounting Packet Details	Shows the details of RADIUS attributes sent and received from the network device during an initial authentication and subsequent reauthentications. Each section in the Details page corresponds to a session in W-Policy Manager.

TACACS+ Accounting Record Details > Request Tab

When you navigate to the **Monitoring > Live Monitoring > Accounting** page and select a TACACS+ Accounting record, the **Accounting Record Details** page opens to the **Request** page.

The following figure displays the **TACACS+ Accounting Record Details > Request** page:

Figure 85: TACACS+ Accounting Record Details > Request Page



Accounting Record Details		
Request	Auth Sessions	Details
Session ID:	211-3930162148-1469477406-211	
User Session ID:	T0000004F-08-57966f97	
Start Timestamp:	Jul 25, 2016 12:59:24 PDT	
End Timestamp:	Jul 25, 2016 13:10:06 PDT	
Username:	tim	
Client IP :	10.2.51.64:tty1	
Remote IP:	15. [REDACTED]	
Flags:	4	
Privilege Level:	15	
Authentication Method:	AUTHEN_METH_TACACSPLUS	
Authentication Type:	AUTHEN_TYPE_ASCII	
Authentication Service:	AUTHEN_SVC_LOGIN	

Close

The following table describes the configuration parameters on the **TACACS+ Accounting Record > Request** page:

Table 50: TACACS+ Accounting Record Request Page Parameters

Parameter	Description
Session ID	Specifies the Session ID , which is a unique ID associated with a request.
User Session ID	Specifies a session ID that correlates authentication, authorization, and accounting records.
Start and End Timestamp	Shows the start and end times of the session.
Username	Shows the username associated with this record.
Client IP	Shows the IP address and tty (text terminal) of the device interface.
Remote IP	Shows the IP address from which the Administrator is logged in.
Flags	Shows the identifier corresponding to starting, stopping, or updating the accounting record.
Privilege Level	Specifies the privilege level of the Administrator. The range is from 1 (lowest) to 15 (highest).

Table 50: TACACS+ Accounting Record Request Page Parameters (Continued)

Parameter	Description
Authentication Method	Identifies the authentication method used for network access.
Authentication Type	Identifies the authentication type used for network access.
Authentication Service	Identifies the authentication service used for network access.

TACACS+ Accounting Record Details > Auth Sessions Tab

This section describes the parameters of the **Accounting Record Details > Auth Sessions** tab for the TACACS+ protocol.

You can click any row in the **Accounting** page to display the corresponding **Accounting Record Details** page for the session.

1. Navigate to the **Monitoring > Live Monitoring > Accounting** page.

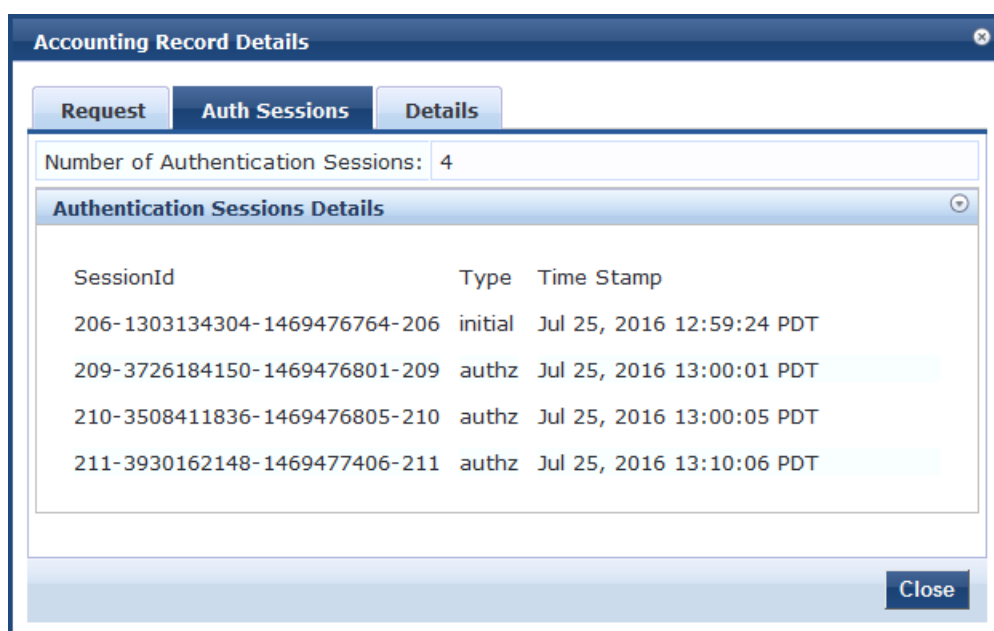
2. Select a TACACS+ Accounting record.

The **Accounting Record Details** page opens.

3. To view the Authentication Sessions details, click the **Auth Sessions** tab.

The following figure displays the **TACACS+ Accounting Record Details > Auth Sessions** page:

Figure 86: TACACS+ Accounting Record Details > Auth Sessions Page



The following table summarizes the information available on the **TACACS+ Accounting Record Details > Auth Sessions** page:

Table 51: TACACS+ Accounting Record Details > Authentication Sessions Page Parameters

Parameter	Description
Number of Authentication Sessions	Specifies the total number of authentications (always 1) and authorizations in this session.
Authentication Sessions Details	Denotes whether the request is an authentication or authorization request, and the time at which the request was sent for each request ID.

TACACS+ Accounting Record Details > Details Tab

This section describes the parameters of the **Accounting Record Details > Details** page for the TACACS+ protocol.

You can click any row in the **Accounting** page to display the corresponding **Accounting Record Details** page for the session.

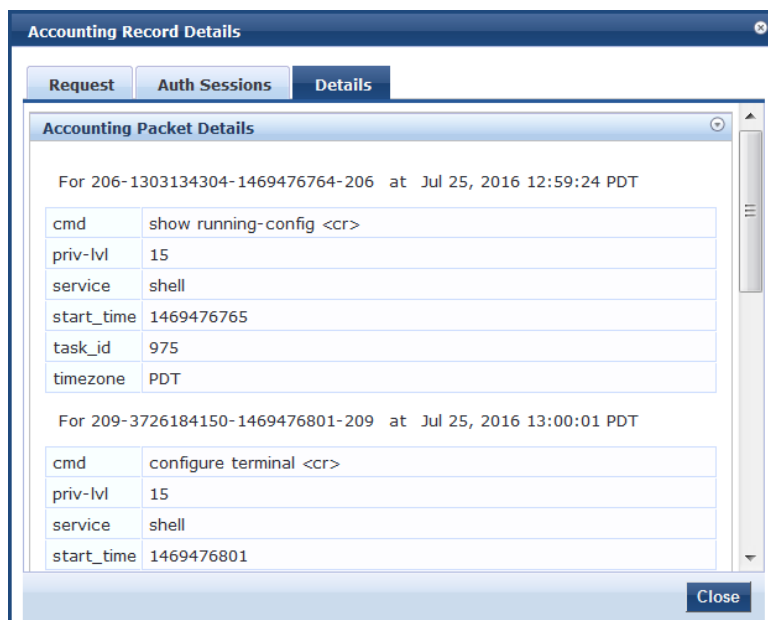
1. Navigate to the **Monitoring > Live Monitoring > Accounting** page.
2. Select a TACACS+ Accounting record.

The **Accounting Record Details** page opens.

3. To view the sessions details, click the **Details** tab.

The following figure displays the **TACACS+ Accounting Record Details > Details** page:

Figure 87: TACACS+ Accounting Record Details > Details Page



The following table summarizes the configuration parameters provided on the **TACACS+ Accounting Record > Details** tab:

Table 52: TACACS+ Accounting Record > Details Page Parameters

Parameter	Description
Accounting Packet Details	Shows command typed (cmd), privilege level of the administrator executing the command (priv-lvl) and service (shell) for each authorization request, as well as the start time, task ID, and the time zone.

Live Monitoring: OnGuard Activity

This section provides the following information:

- [About OnGuard Activity](#)
- [Bouncing an Agent Using Non-SNMP](#)
- [Bouncing a Client Using SNMP](#)
- [Broadcasting a Message to Active Endpoints](#)
- [Sending a Message to Selected Endpoints](#)

About OnGuard Activity

The **OnGuard Activity** page shows the real-time status of all endpoints that have W-ClearPass W-OnGuard persistent agent.

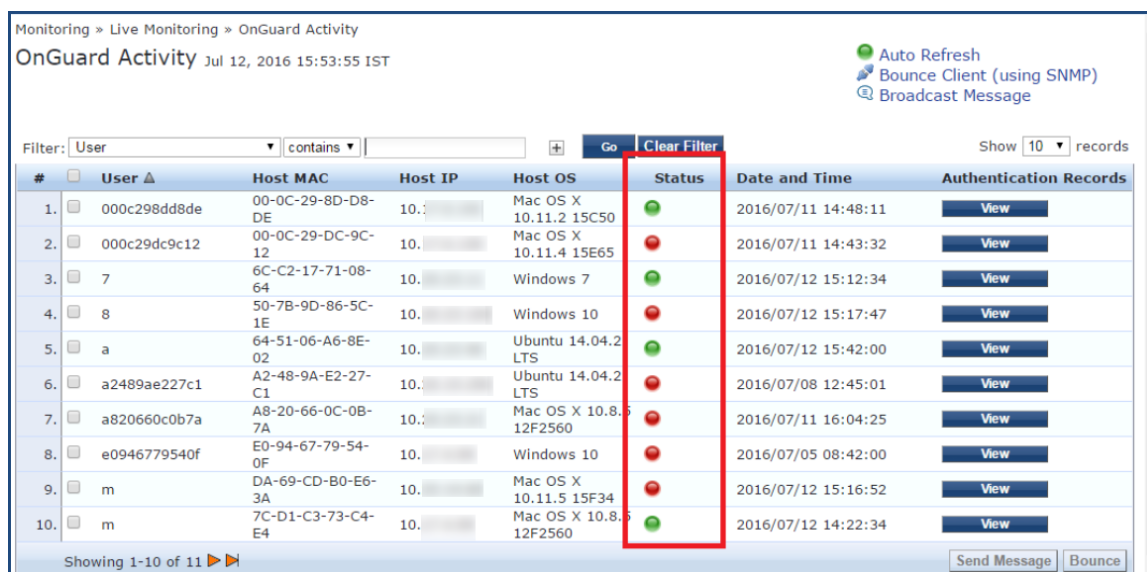
This page also presents configuration tools to bounce an endpoint and to send unicast or broadcast messages to all endpoints running the W-OnGuard agent.

To access the **OnGuard Activity** page:

1. Navigate to **Monitoring > Live Monitoring > OnGuard Activity**.

The **OnGuard Activity** page opens:

Figure 88: OnGuard Activity Page



Monitoring » Live Monitoring » OnGuard Activity
OnGuard Activity Jul 12, 2016 15:53:55 IST

Auto Refresh
Bounce Client (using SNMP)
Broadcast Message

Filter: User contains [] Go Clear Filter Show 10 records

#	User	Host MAC	Host IP	Host OS	Status	Date and Time	Authentication Records
1.	000c298dd8de	00-0C-29-8D-D8-DE	10.11.2.15C50	Mac OS X 10.11.2 15C50	●	2016/07/11 14:48:11	View
2.	000c29dc9c12	00-0C-29-DC-9C-12	10.11.4.15E65	Mac OS X 10.11.4 15E65	●	2016/07/11 14:43:32	View
3.	7	6C-C2-17-71-08-64	10.11.2.15C50	Windows 7	●	2016/07/12 15:12:34	View
4.	8	50-7B-9D-86-5C-1E	10.11.2.15C50	Windows 10	●	2016/07/12 15:17:47	View
5.	a	64-51-06-A6-8E-02	10.11.2.15C50	Ubuntu 14.04.2 LTS	●	2016/07/12 15:42:00	View
6.	a2489ae227c1	A2-48-9A-E2-27-C1	10.11.2.15C50	Ubuntu 14.04.2 LTS	●	2016/07/08 12:45:01	View
7.	a820660c0b7a	A8-20-66-0C-0B-7A	10.11.2.15C50	Mac OS X 10.8.5 12F2560	●	2016/07/11 16:04:25	View
8.	e0946779540f	E0-94-67-79-54-0F	10.11.2.15C50	Windows 10	●	2016/07/05 08:42:00	View
9.	m	DA-69-CD-B0-E6-3A	10.11.2.15C50	Mac OS X 10.11.5 15F34	●	2016/07/12 15:16:52	View
10.	m	7C-D1-C3-73-C4-E4	10.11.2.15C50	Mac OS X 10.8.5 12F2560	●	2016/07/12 14:22:34	View

Showing 1-10 of 11 records

[Send Message](#) [Bounce](#)

The following table describes the configuration parameters on the **OnGuard Activity** page:

Table 53: *OnGuard Activity Parameters*

Parameter	Description
User	Displays the name of the user.
Host MAC	Displays the MAC address of the host.
Host IP	Displays the IP address of the host.
Host OS	Displays the operating system that runs on the host.
Status	Displays the online status of the host. Green indicates online and red indicates offline.
Date and Time	Displays the date and time at which the user was created.
Authentication Records	Click the Authentication Records > View button to see the Endpoint Authentication Details page with the authentication records.

Bouncing an Agent Using Non-SNMP

This page is used to initiate a bounce on an endpoint's managed interface.



Endpoint bounce only works with endpoints that run the W-OnGuard persistent agent.

Initiating a bounce on the managed interface on the endpoint results in creating tags for the specified endpoint in the **Endpoints** page (navigate to **Configuration > Identity > Endpoints**).

One or more of the following tags are created:

- Disabled by
- Disabled Reason
- Enabled by
- Enabled Reason
- Info URL

To bounce an agent:

1. Navigate to **Monitoring > OnGuard Activity**.
The **OnGuard Activity** page opens.
2. Click a device listed on the **OnGuard Activity** page.
The **Agent and Endpoint Details** page opens.

Figure 89: Agent and Endpoint Details

Agent and Endpoint details			
EndPoint		Attributes	
Host MAC:	000c298dd8de	Static IP	TRUE
Description:		Hostname	arubabuilds-Mac-3.local
Status:	Unknown	Device Category	Computer
Added by:	Policy Manager	Device OS Family	Apple Mac
MAC Vendor	VMware, Inc.	Device Name	Mac OS X
OnGuard Details			
User:	000c298dd8de		
Host IP:	10.		
Status:	Online		
Agent Type:	OnGuard		
Host OS:	Mac OS X 10.11.2 15C50		
Registered Policy Manager Server:	Garuda-146 [10.]		
Registered at:	2016/07/11 14:48:11		
Last Unregistered at:	-		
Last Seen Health Status:	-		
Unhealthy Health Classes:	-		
Send Message Bounce Close			

The following table describes the configuration parameters on the **Agent and Endpoint Details** page:

Table 54: Agent and Endpoint Details Parameters

Parameter	Description
Host MAC	Displays the MAC address of the user.
Description	Optional description of the endpoint.
Status	Displays the status of the endpoint.
Added by	Displays the server name.
MAC Vendor	Vendor name and OS of the endpoint device.
OnGuard Details	
User	Displays the name of the user.
Host IP	Displays the IP address of the host.
Status	Shows the online or offline status of the agent.
Agent Type	Specifies the type of the OnGuard agent.
Host OS	Displays the operating system that runs on the endpoint.

Table 54: Agent and Endpoint Details Parameters (Continued)

Parameter	Description
Registered W-Policy Manager Server	Displays the name and IP address of the W-Policy Manager server.
Registered at	Displays the date and time at which the W-Policy Manager installation was registered.
Last Unregistered at	Displays the date and time at which the W-Policy Manager installation was last unregistered.
Last Seen Health Status	Displays the health status of the endpoint. For example, QUARANTINED or HEALTHY.
Unhealthy Health Classes	Displays the health classes that are unhealthy.

3. Click **Bounce**.

The **Bounce Agents** page opens.

Figure 90: Bounce Agents Page

The following table describes the configuration parameters on the **Bounce Agents** page:

Table 55: Bounce Agents Page Parameters

Parameter	Action/Description
Display Message (Optional)	An optional message to display on the endpoint using the OnGuard interface.
Web link for more details (Optional)	An optional clickable URL that is displayed along with the Display Message.
Endpoint Status	No change in status: 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 existing status of an endpoint. Allow network access: Allow network access by white-listing this endpoint. Clicking Allow network access sets the status of the endpoint as Known.

Table 55: *Bounce Agents Page Parameters (Continued)*

Parameter	Action/Description
	NOTE: You must configure Enforcement Policy Rules to allow access to the endpoints with the status Known. • Block network access: Block network access by blacklisting this endpoint. Clicking Block network access sets the status of the endpoint to Disabled. NOTE: You must configure Enforcement Policy Rules to allow access to the endpoints with the status Disabled.

Bouncing a Client Using SNMP

The **Bounce Client (using SNMP)** dialog is used to initiate a bounce operation using SNMP with wired Ethernet switches.



Endpoint bounce only works with endpoints that run the W-OnGuard persistent agent.

Requirements

To successfully bounce a client using SNMP, the following conditions are required:

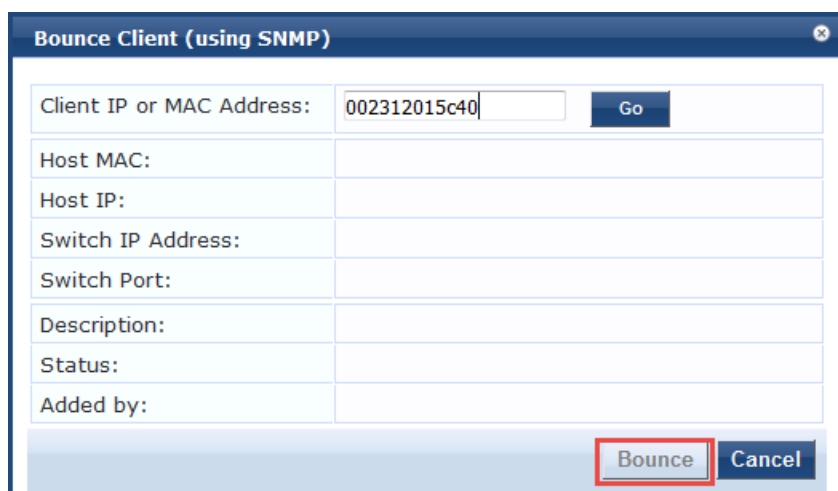
- The network device must be added to W-Policy Manager and SNMP read and write parameters must be configured.
 - For information about adding a network device to W-ClearPass Policy Manager, see [Adding a Network Device on page 430](#).
 - For details about configuring SNMP settings, see [SNMP Read Settings Parameters on page 432](#) and [SNMP Write Settings Parameters on page 434](#).
- SNMP traps (link up and/or MAC notification) must be enabled on the switch port (see [W-ClearPass SNMP Traps and OIDs on page 784](#) and [SNMP Trap Details on page 786](#)).
- The DHCP snooper service on a W-ClearPass server must receive DHCP packets from the endpoint to specify the IP address of the endpoint to bounce.
 - For information about configuring the **DhcpSnooper** service, see [W-ClearPass Network Services Options on page 472](#).
 - For information about configuring the IP helper address, see [DHCP Collector on page 421](#).

Bouncing a Client

To bounce a client using SNMP:

1. Navigate to **Monitoring > OnGuard Activity**.
The **OnGuard Activity** page opens.
2. Click the **Bounce Client (using SNMP)** link on the top-right of the **OnGuard Activity** page.
The **Bounce Client (using SNMP)** dialog opens.

Figure 91: *Bounce Client (Using SNMP) Dialog*



3. Enter the client IP or MAC Address.
4. Click **Go**, then click **Bounce**.

The following table describes the configuration parameters on the **Bounce Client (Using SNMP)** page:

Table 56: *Bounce Client (Using SNMP) Page Parameters*

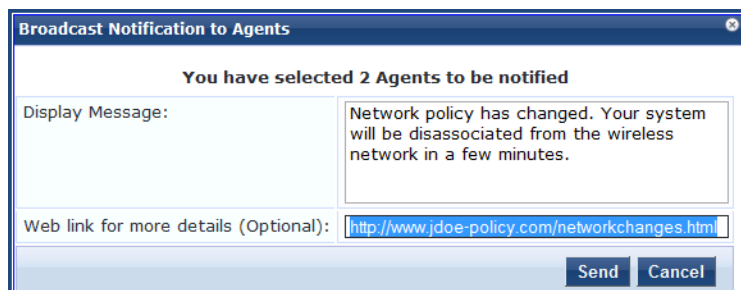
Parameter	Action/Description
Client IP or MAC address	Enter the client IP address or MAC address of the bounce client.
Host MAC	Displays the MAC address of the host.
Host IP	Displays the IP address of the host.
Switch IP Address	Displays the IP address of the switch.
Switch Port	Displays the port number of the switch.
Description	Displays the description of the client.
Status	Displays the status of the client.
Added by	Displays the name of the user who added the client.

Broadcasting a Message to Active Endpoints

To broadcast a message to selected active endpoints:

1. Navigate to **Monitoring > OnGuard Activity**.
The **OnGuard Activity** page opens.
2. Select the endpoint(s) that you want to broadcast to.
3. Click the **Broadcast Message** link on the top-right of the **OnGuard Activity** page.
The **Broadcast Notification to Agents** dialog opens.

Figure 92: *Broadcast Notification to Agents Dialog*



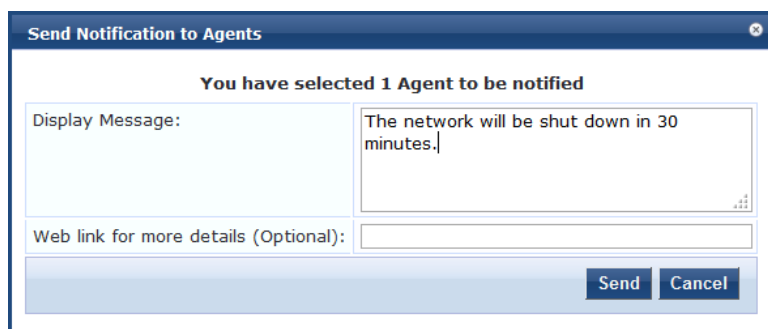
4. **Display Message:** Enter the text of the message you want to send to the selected active endpoints.
5. **Web link:** Optionally, enter a URL to be included with the **Display Message**.
6. Click **Send**.

Sending a Message to Selected Endpoints

To send a message to selected endpoints:

1. Navigate to **Monitoring > OnGuard Activity**.
The **OnGuard Activity** page opens.
2. Select one or more devices listed on the **OnGuard Activity** page.
3. Click the **Send Message** button.
The **Send Notification to Agents** dialog opens.

Figure 93: *Send Notifications to Agents*



4. **Display Message:** Enter a message to be sent to the selected endpoints
5. **Web link:** Optionally, enter a URL to be included with the message.
6. Click **Send**.

Live Monitoring: Analysis and Trending

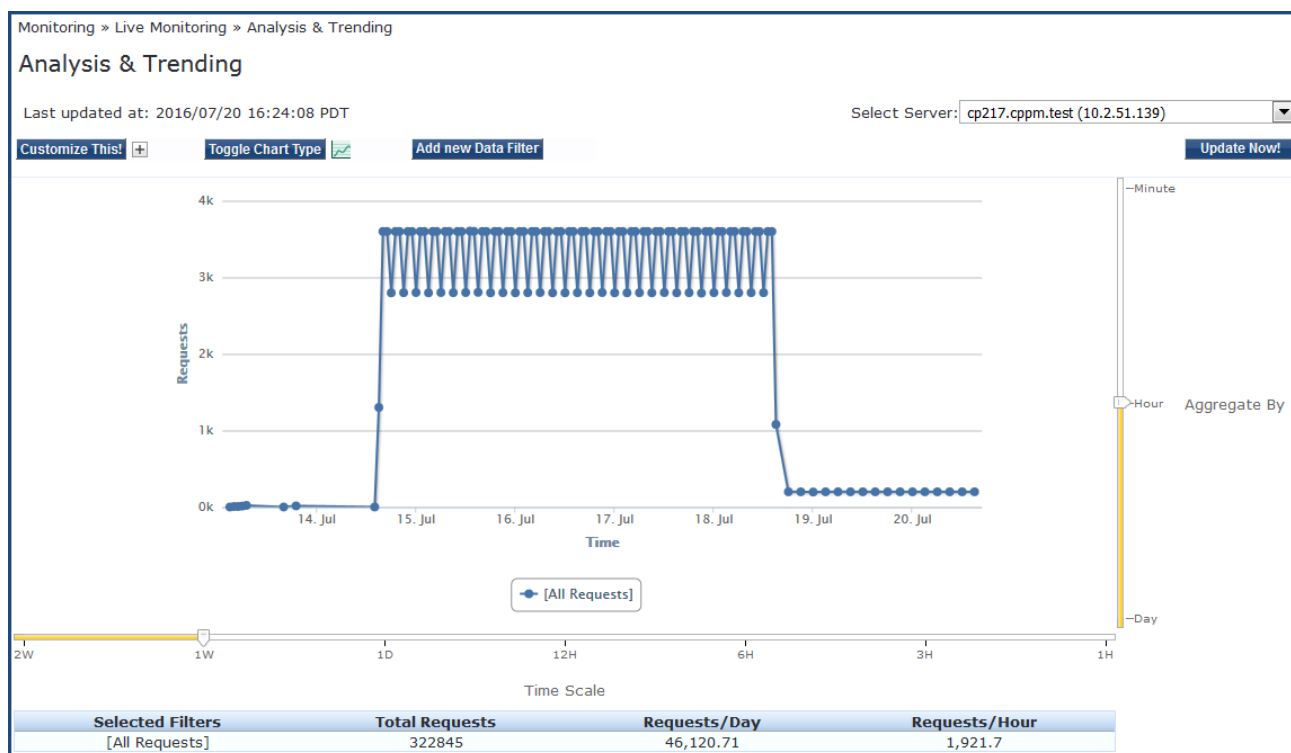
The **Analysis and Trending** page displays requests for the subset of components included in the selected filters over a selected time period: one month, two weeks, one week, one day, 12 hours, 6 hours, 3 hours, or one hour.

The data can be aggregated by **minute**, **hour**, **day**, or **week**. The list at the end of this section shows the per-filter count for the aggregated data.

Each bar corresponding to each filter in the bar graph is clickable. Clicking a bar drills down into the Access Tracker (see [Live Monitoring: Access Tracker on page 107](#)) that shows session data for the specific time-slice and for the specific requests.

To access this page, navigate to **Monitoring > Live Monitoring > Analysis and Trending**.

Figure 94: Analysis and Trending



Use the following components in the WebUI to customize and filter the **Analysis and Trending** page:

Component	Action/Description
Select Server	Select a node from the cluster for which data will be displayed.
Update Now!	Click to update the display with the latest available data.
Customize This!	Click to customize the display by adding filters. You can add a maximum of four filters.
Toggle Chart Type	Click to toggle the chart display between line and bar type.
Add New Data Filter	Click to add a data filter in the global filter list. For more information on adding filters, refer to Data Filters on page 158 .

Live Monitoring: System Monitor

The **System Monitor** page has four tabs. Each tab provides one or more charts or graphs that give real-time information about various components.



Auto refresh ensures that the **System Monitor** page is updated for every two minutes. You can see the last updated time in the **Last updated at** field in the **System Monitor** page.

- [System Monitor Page](#)

- [Process Monitor Page](#)
- [Network Monitor Page](#)
- [ClearPass Monitor Page](#)

System Monitor Page

The **System Monitor** page displays charts and graphs that display information about CPU load, CPU usage, memory usage, and disk usage for the selected W-ClearPass server.

To access the **System Monitor** page for the selected W-ClearPass server:

1. Navigate to **Monitoring > Live Monitoring > System Monitor**.
2. From the **Select Server** drop-down, select the desired W-ClearPass server.

Figure 95: System Monitor Page

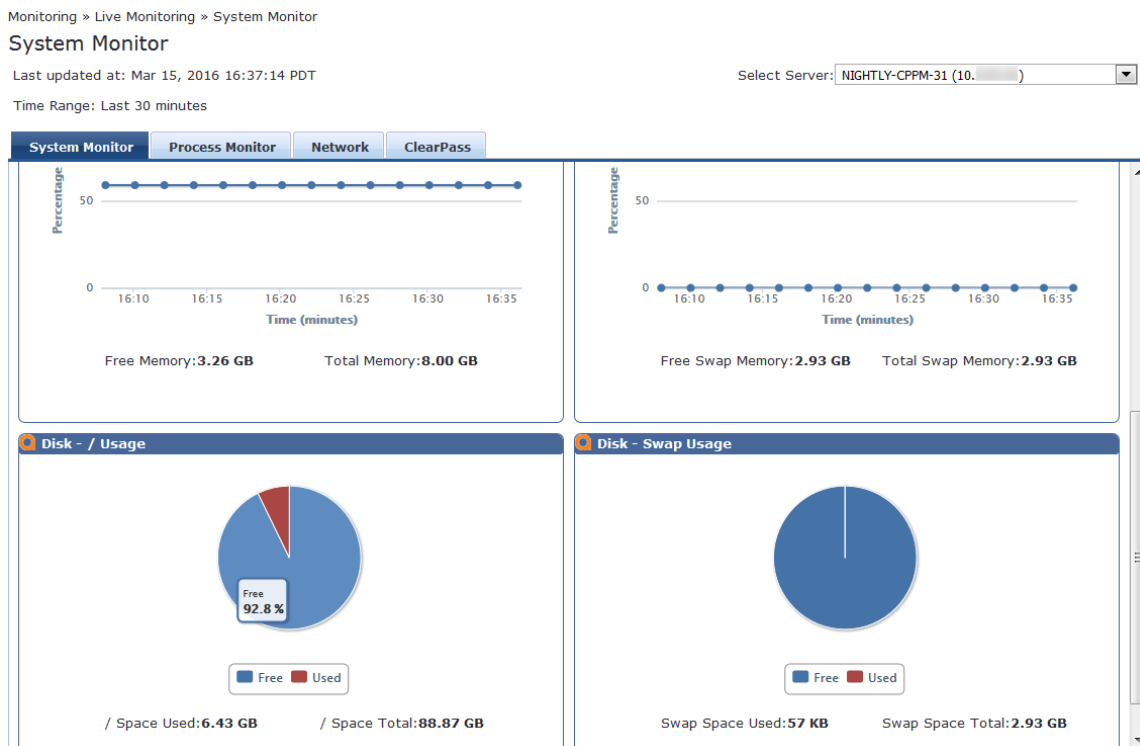


Table 57: System Monitor Page Report Widgets

Widget	Description
CPU Usage	Percentage of CPU usage for the following: System , User , I/O Wait , and Idle time.
CPU Load	Percentage of CPU load averages in increments of 1, 5, and 15 minutes.
Memory Usage	Percentage of free and total memory in Gigabytes.
Swap Memory Usage	Percentage of free and total swap memory in Gigabytes.
Disk - Usage	Percentage of used and free disk space.
Disk - Swap Usage	Percentage of used and total swap space.

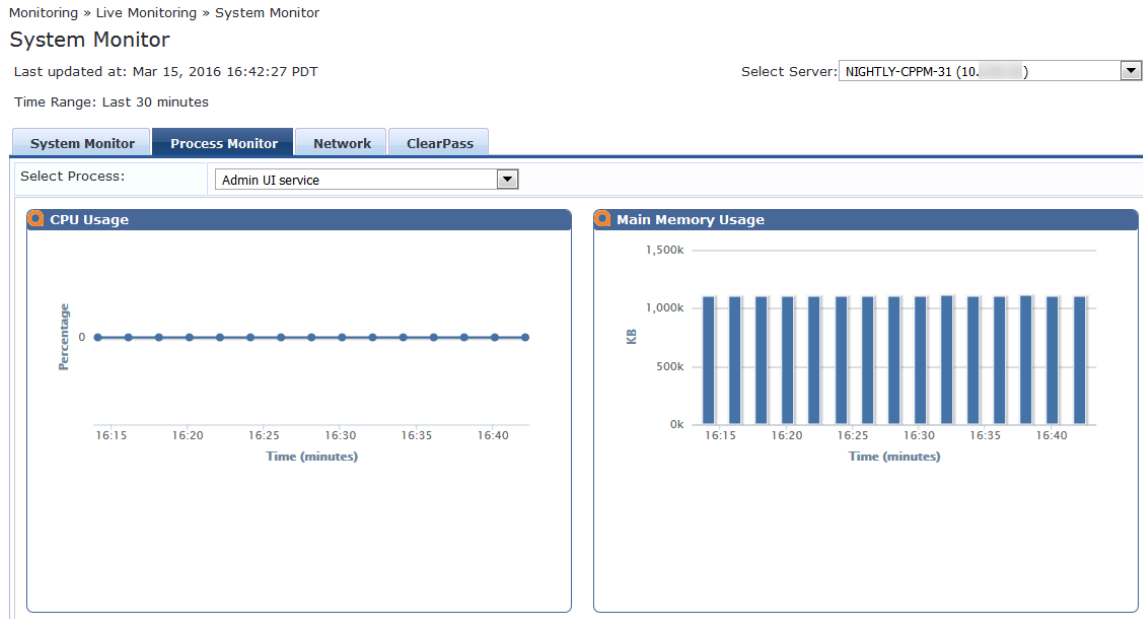
Process Monitor Page

The **Process Monitor** page displays CPU Usage and Main Memory Usage for a selected process or service.

To access the Process Monitor page:

1. Navigate to **Monitoring > Live Monitoring > System Monitor > Process Monitor**.

Figure 96: System Monitoring: Process Monitor Page



2. To view CPU Usage and Main Memory usage for the selected process or service, click the **Select Process** drop-down list.
3. Select one of the following options :
 - Admin UI service
 - AirGroup notification service
 - Apache web server
 - Async DB write service
 - Async network services
 - W-ClearPass IPsec service
 - DB change notification server
 - DB replication service
 - Domain service
 - Extensions service
 - Ingress logger service
 - Ingress logrepo service
 - Micros Fidelio FIAS
 - Multi-master cache
 - Policy server
 - Radius server
 - Stats aggregation service
 - Stats collection service

- System auxiliary services
- System monitor service
- Tacacs server
- Virtual IP service

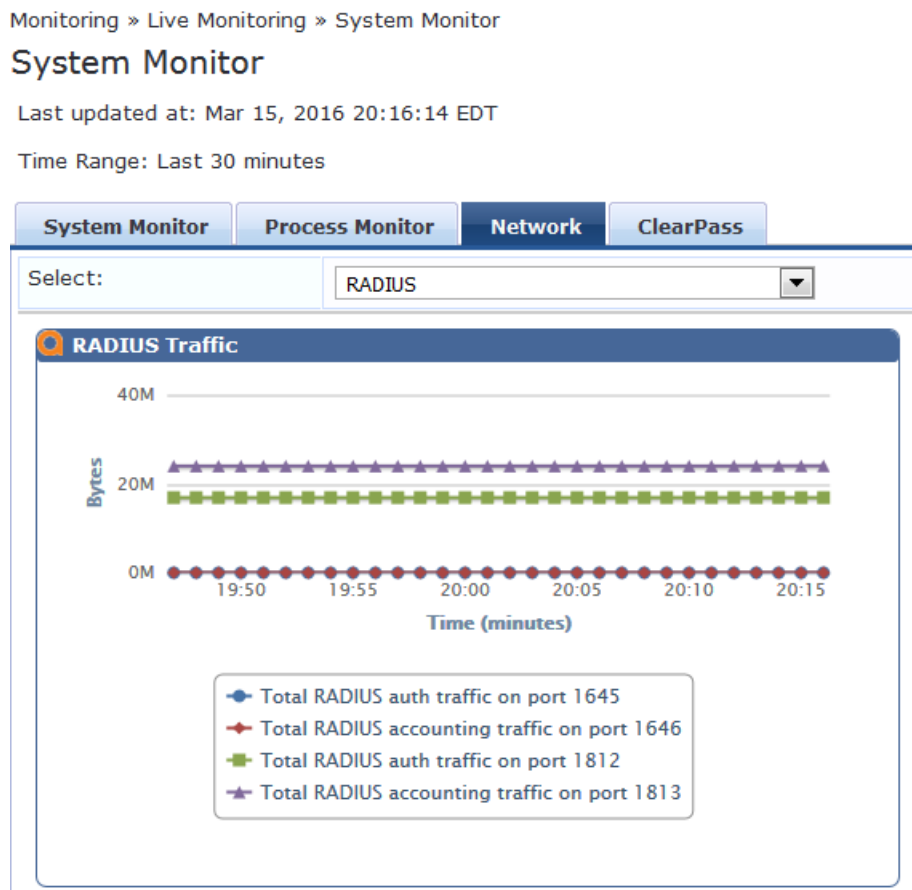
Network Monitor Page

The **Network Monitor** page displays information about the selected network traffic type.

To access the **Network Monitor** page:

1. Navigate to **Monitoring > Live Monitoring > System Monitor > Network** tab.
2. From the **Select** drop-down, select the desired traffic type.

Figure 97: Network Monitor Page



The **Network Monitor** page displays network activity (in bytes) for the following traffic types:

- OnGuard
- Database
- Web Traffic
- RADIUS
- TACACS
- SSH
- NTP

ClearPass Monitor Page

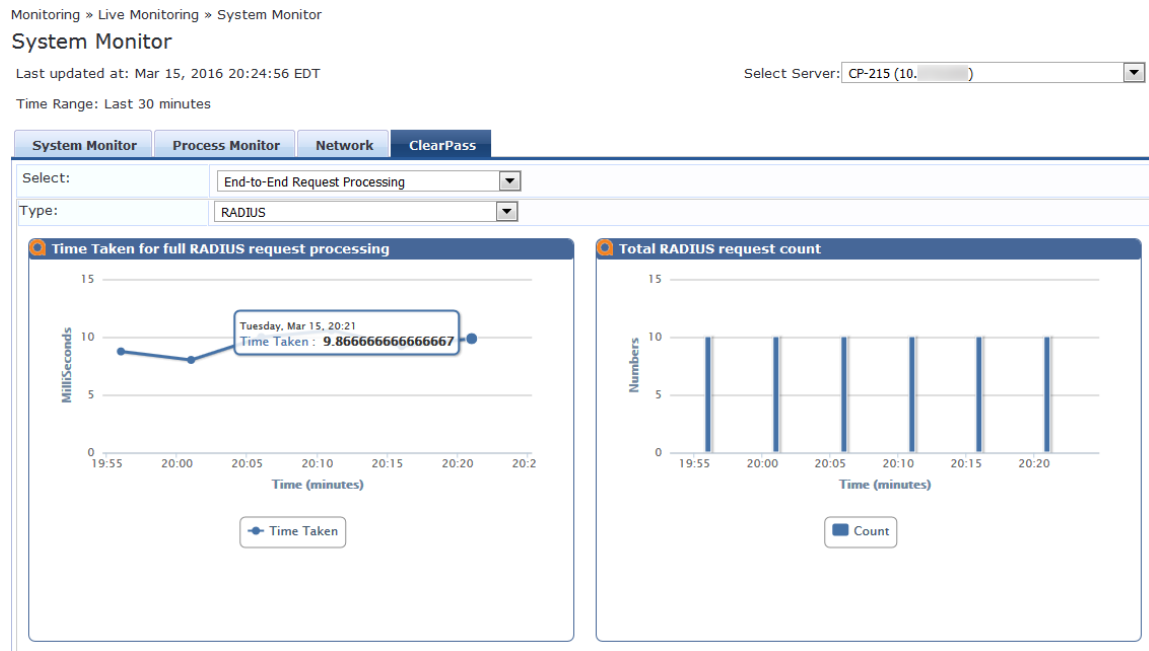
The **ClearPass** Monitoring page displays performance monitoring counters and timers for the last 30 minutes of activity for the following W-ClearPass components:

- Service Categorization
- Authentication (RADIUS, TACACS, or WebAuth)
- Authorization
- Role Mapping
- Posture Evaluation
- Audit Scan
- Enforcement
- End-to-End Request Processing (RADIUS, TACACS, or WebAuth)
- Advanced

To access the **ClearPass Monitor** page:

1. Navigate to **Monitoring > Live Monitoring > System Monitor > ClearPass** tab.
2. Click the **Select** drop-down.
3. Select the desired W-ClearPass performance monitoring counter.

Figure 98: System Monitoring: ClearPass Monitor Page



Profiler and Discovery

This section provides the following information:

- [Profiler and Discovery: Endpoint Profiler](#)
- [Profiler and Discovery: Network Discovery](#)

Profiler and Discovery: Endpoint Profiler

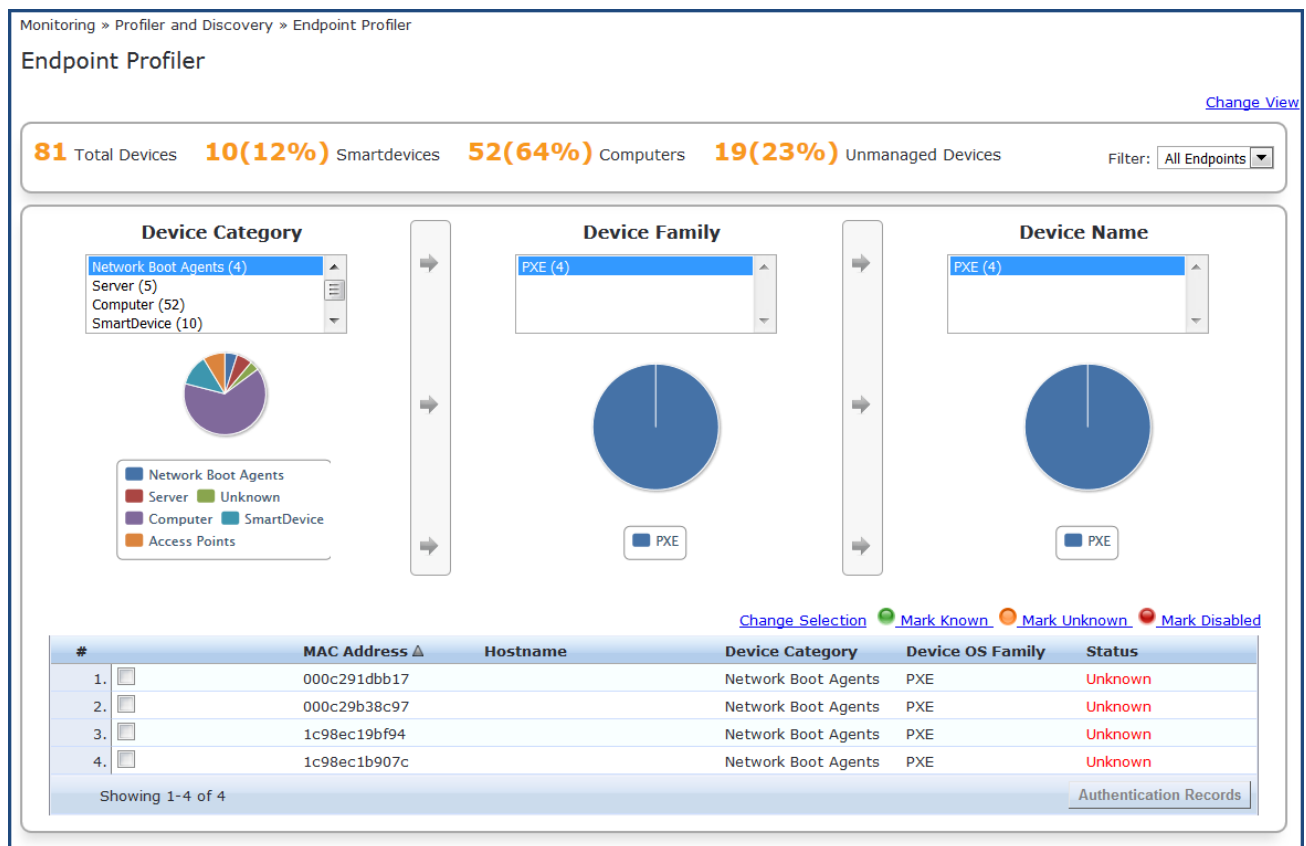
If the Profile license is enabled, a list of the profiled endpoints are visible in the **Endpoints Profiler** page.

1. To access the Endpoint Profiler, navigate to the **Monitoring > Profiler and Discovery > Endpoint Profiler** page.

The list of endpoints you view is based on the **Device Category**, **Device Family**, and **Device Name** items that you selected.

Figure 99 shows an example of the graphs available on the **Endpoint Profiler** page:

Figure 99: Endpoint Profiler Page



2. To modify the selection criteria used to list the devices, click **Change Selection**.
3. To see graphs that show information about distribution and update frequency for devices and computers, click **Change View**.
4. To view endpoint details about a specific device, click a device in the table below the graphs.

The **Endpoint Profiler Details > Endpoint** page opens:

Figure 100: *Endpoint Profiler Details*

Monitoring » Profiler and Discovery » Endpoint Profiler

Endpoint Profiler

View Endpoint

EndPoint	Attributes		
MAC Address	000c291dbb17	IP Address	10.
Description		Static IP	FALSE
Status	Unknown	Hostname	-
MAC Vendor	VMware, Inc.	Device Category	Network Boot Agents
Added by	Policy Manager	Device OS Family	PXE
		Device Name	PXE
		Added At	Jun 14, 2016 15:15:30 PDT
		Updated At	Jun 14, 2016 15:15:30 PDT
		Show Fingerprint	☐

Cancel

5. To return to the **Endpoint Profiler** page, select the **Cancel** button.

Profiler and Discovery: Network Discovery

This section provides the following information:

- [About Network Discovery](#)
- [Adding the Configurations to Query Seed Devices](#)
- [Initiating a Network Discovery Scan](#)
- [About Auto-Refresh](#)
- [Importing and Viewing Discovered Network Devices](#)
- [Viewing Discovered Endpoints](#)

About Network Discovery

Network Discovery uses a configured *seed network device* (typically a switch, router, or controller) to discover endpoints and network devices.

The following information is read from the seed device:

- SNMP information
An SNMP description is necessary for discovering and profiling the network devices. For more information, see [SNMP Credentials Configuration on page 141](#).
- SSH credentials
For Linux server or network device discovery, specify SSH configuration credentials. For more information, see [SSH Credentials Configuration on page 142](#).
- WMI credentials
For Windows device discovery, specify WMI (Windows Management Instrumentation) credentials. For more information, see [WMI Credentials Configuration on page 144](#).
- Connected endpoints

Information about endpoints connected to the network device (typically MAC addresses of endpoints connected to switch ports). These are added as discovered endpoints. For more information, see [Viewing Discovered Endpoints on page 151](#).

- ARP table

The ARP table provides information about MAC address > IP associations for endpoints that were recently seen by this device. These endpoints are probed further in an attempt to profile them. For more information, see [Viewing Discovered Endpoints on page 151](#).

- Neighbor network devices

Other network devices connected to the seed device as determined by neighbor discovery protocols such as Cisco Discovery Protocol (CDP) and Link Layer Discovery Protocol (LLDP) (if enabled in your network).

Each of the discovered neighbor network devices are further queried as seed devices; this is repeated for multiple levels in your network up to a specified scan depth. For more information, see [Viewing Details on a Discovered Device on page 151](#).

Network Discovery High-Level Tasks

Configuring Network Discovery consists of these major tasks:

1. Add the configurations (SNMP, SSH, or WMI) needed to query all the devices in the target network.
2. Initiate a network discovery scan.
3. Import the discovered network devices into W-ClearPass.
4. Review the set of discovered devices and view the connected endpoints and neighbors.

Adding the Configurations to Query Seed Devices

You must configure SNMP, SSH, and WMI credentials for the devices that you want to discover as part of the network scan. These credentials are used during Network Discovery or an On-Demand subnet scan to profile Linux servers and machines (SSH credentials), Windows servers and machines (WMI credentials), and network devices (SNMP).

SNMP Credentials Configuration

For network device discovery, specify SNMP Read credentials. An SNMP-based scan sends an SNMP request to retrieve the network device information.

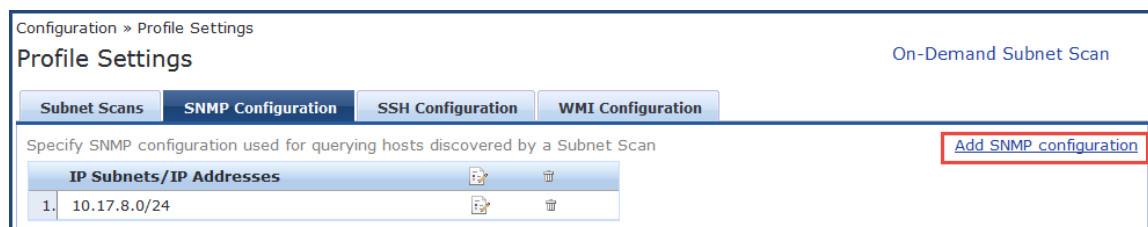
To add the SNMP configuration:

1. Navigate to **Configuration > Profile Settings**, then select the **SNMP Configuration** tab.

The **Profile Settings > SNMP Configuration** page opens.

2. Click the **SNMP Configuration** tab.

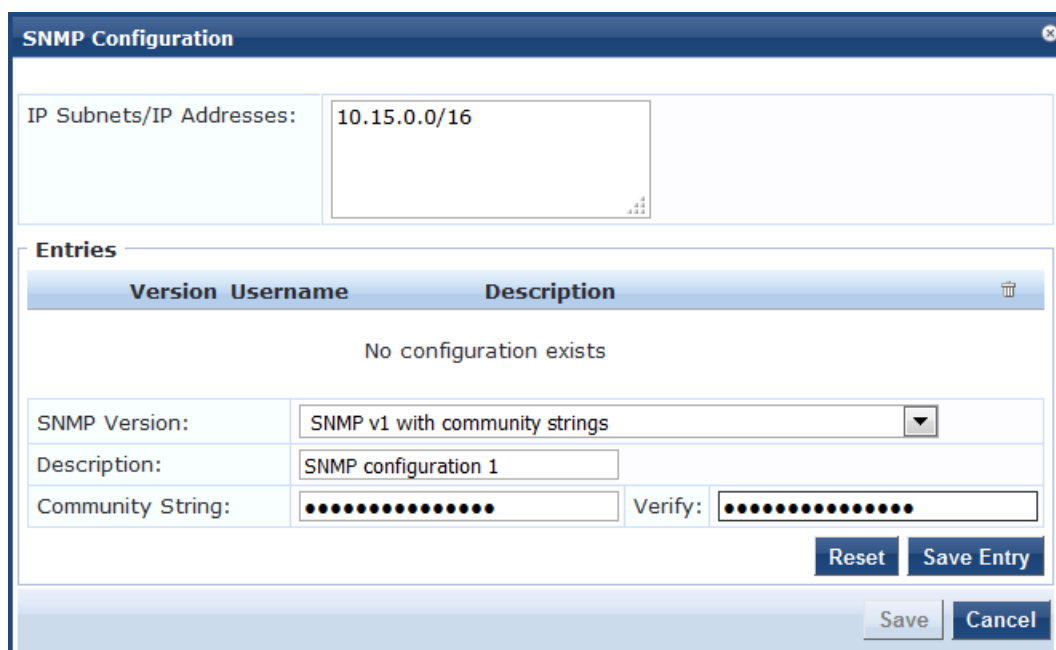
Figure 101: Adding an SNMP Configuration



3. Click **Add SNMP Configuration**.

The SNMP Configuration dialog opens.

Figure 102: *SNMP Configuration Dialog*

The image shows a 'SNMP Configuration' dialog box. At the top, there's a title bar with a close button. Below it, a section labeled 'IP Subnets/IP Addresses:' contains a text field with '10.15.0.0/16'. Below this is a section titled 'Entries' which contains a table with columns 'Version', 'Username', and 'Description'. The table is currently empty, with the text 'No configuration exists' centered below the header. Below the table, there are three input fields: 'SNMP Version:' with a dropdown menu showing 'SNMP v1 with community strings', 'Description:' with a text field containing 'SNMP configuration 1', and 'Community String:' with a masked text field. To the right of the 'Community String' field is a 'Verify:' field, also masked. At the bottom right, there are four buttons: 'Reset', 'Save Entry', 'Save', and 'Cancel'.

4. Specify the **SNMP Configuration** parameters as described in Table 58. When finished, click **Save Entry**, then click **Save**.

Table 58: *SNMP Configuration Parameters*

Field	Action/Description
IP Subnets/ IP Addresses	1. Enter either one or more IP subnets or one or more IP addresses. For multiple entries, separate multiple IP addresses with commas. When you initiate the network discovery scan, W-ClearPass will use the SNMP configuration to fetch the network device information for discovered devices.
SNMP Version	2. From the drop-down, select the appropriate SNMP version.
Description	3. Optionally, enter a description of this SNMP configuration (recommended).
Community String	4. Enter the community string, then reenter the community string in the Verify field.

SSH Credentials Configuration

For Linux server or network device discovery, specify SSH (Secure Shell) configuration credentials. When SSH is found for an IP address or subnet, Network Discovery looks for any Linux server or machine associated with that IP address or subnet.

You can configure multiple user names and passwords. These credentials are organized in the order in which they were created.

To configure SSH credentials for a network discovery scan:



The SSH configuration can be for a single IP address or a subnet. These credentials are used when an SSH scan is initiated.

1. Navigate to **Configuration > Profile Settings**.

The **Profile Settings** page opens.

Figure 103: Profile Settings Page

The screenshot shows the 'Profile Settings' page with the 'Subnet Scans' tab selected. The page title is 'Configuration » Profile Settings'. On the right, there is a link 'On-Demand Subnet Scan'. Below the tabs, there is a section titled 'Specify the IP subnets to be scanned for discovering hosts and their capabilities -'. It contains a table with two columns: 'Policy Manager Zone' and 'IP Subnet to Scan'. The first row has a value '1. Click to add...' in the 'IP Subnet to Scan' column.

2. Select the **SSH Configuration** tab.

Figure 104: SSH Configuration Tab

The screenshot shows the 'Profile Settings' page with the 'SSH Configuration' tab selected. The page title is 'Configuration » Profile Settings'. On the right, there is a link 'On-Demand Subnet Scan'. Below the tabs, there is a section titled 'Specify settings required for performing SSH netscan -'. It contains a table with two columns: 'IP Subnets/IP Addresses' and an empty column. There is a red box around the 'Add Configuration' link on the right.

3. Click **Add Configuration**.

The **SSH Configuration** page opens.

Figure 105: SSH Configuration Page

The screenshot shows the 'SSH Configuration' dialog box. It has a title bar 'Configuration'. Inside, there is a section 'IP Subnets/IP Addresses' with a text box containing '10.x.x.x/24'. Below this is a section 'Entries' with a table. The table has two columns: 'Username' and 'Description'. The table is empty, and the text 'No Configuration present' is displayed. Below the table, there are input fields for 'Username' (root), 'Password' (masked), 'Verify Password' (masked), 'Enable Password' (masked), and 'Enable Password Verify' (masked). The 'Description' field contains 'SSH configuration to discover Linux devices'. At the bottom right, there are buttons 'Reset', 'Save Entry', 'Save', and 'Cancel'.

4. Specify the parameters in the **SSH Configuration** dialog as described in the following table, then click **Save Entry**.

Table 59: SSH Configuration Parameters

Field	Action/Description
IP Subnets/ IP Addresses	1. Enter either one or more IP subnets or one or more IP addresses. For multiple entries, separate multiple IP addresses with commas.
Username	2. Enter the username for the device or subnet specified.
Password	3. Enter the password for the device or subnet specified.
Enable Password	4. Enter the Enable password, then reenter the password in the Enable Password Verify field.
Description	5. Optionally, enter a description of this SNMP configuration (recommended).

6. Repeat this procedure for additional entries if needed.

7. When finished, click **Save**.

You return to the **Profile Settings** page, where you can see that the SSH configuration has been added successfully (see [Figure 106](#)).

Figure 106: SSH Configuration Added Successfully

The screenshot shows the 'Profile Settings' page in a web interface. At the top, there's a breadcrumb 'Configuration » Profile Settings' and the title 'Profile Settings'. Below this is a 'Configuration' section with a close button. It contains a text input for 'IP Subnets/IP Addresses:' with the value '10.x.x.x/24'. Below that is an 'Entries' table with two columns: 'Username' and 'Description'. The first entry is highlighted with a red box and has a radio button selected next to it. The entry is: '1. root' with the description 'SSH configuration to discover Linux devices'. There is a trash icon to the right of the entry.

Configuration	
Profile Settings	
Configuration	
IP Subnets/IP Addresses:	10.x.x.x/24
Entries	
Username	Description
1. ☒ root	SSH configuration to discover Linux devices

WMI Credentials Configuration

For Windows device discovery, specify WMI (Windows Management Instrumentation) configuration credentials. WMI configuration is necessary to discover Windows systems and device fingerprint details.

WMI is a key part of the Windows operating system. It is used to gather system statistics, monitor system health, and manage system components. To work properly, WMI relies on the WMI service. This service must be running and properly configured for your environment.

For WMI, the login format for **username** is usually **domain\username**. Whatever domain you provide, it will be prepended to the username before logging into that machine.

Suppose you have provided an IP subnet address:

- W-ClearPass first checks to see if WMI is configured for that subnet/IP address.
- If WMI is configured, W-ClearPass checks to see if port 135 is open.
- If port 135 is open, W-ClearPass attempts the WMI login with those credentials.

If you provide just one IP address, the WMI login is performed for that particular IP address only.
To configure WMI credentials for a network discovery scan:

1. Navigate to **Configuration > Profile Settings**.

The **Profile Settings** page opens.

Figure 107: Profile Settings Page

Configuration » Profile Settings

Profile Settings On-Demand Subnet Scan

Subnet Scans | SNMP Configuration | SSH Configuration | WMI Configuration

Specify the IP subnets to be scanned for discovering hosts and their capabilities -

Policy Manager Zone	IP Subnet to Scan	
1. Click to add...		

2. Select the **WMI Configuration** tab.

Figure 108: WMI Configuration Tab

Configuration » Profile Settings

Profile Settings On-Demand Subnet Scan

Subnet Scans | SNMP Configuration | SSH Configuration | **WMI Configuration**

Specify settings required for performing WMI netscan -

IP Subnets/IP Addresses + - 🗑️

[Add Configuration](#)

3. Click **Add Configuration**.

The **WMI Configuration** page opens.

Figure 109: WMI Configuration Page

Configuration

IP Subnets/IP Addresses:

Entries

Username	Description	
No Configuration present		

Domain:

Username:

Password: Verify Password:

Description:

Reset **Save Entry**

Save **Cancel**

4. Specify the **WMI Configuration** parameters as described in [Table 60](#), then click **Save Entry**.

Table 60: WMI Configuration Parameters

Field	Action/Description
IP Subnets/ IP Addresses	1. Enter either one or more IP subnets or one or more IP addresses. For multiple entries, separate multiple IP addresses with commas. NOTE: The WMI configuration can be for a single IP address or a subnet. These credentials are used when a WMI scan is initiated.
Domain	2. Enter the name of the Windows domain for logging into the device(s) that you are scanning.
Username	3. Enter the username for the device or subnet specified.
Password	4. Enter the password for the device or subnet specified.
Description	5. Optionally, enter a description of this SNMP configuration (recommended).

6. Repeat this procedure for additional entries if needed.

7. When finished, click **Save**.

You return to the **Profile Settings** page, where you can see that the WMI configuration has been added successfully (see [Figure 110](#)).

Figure 110: WMI Configuration Added Successfully

The screenshot shows the 'Profile Settings' page with a 'Configuration' tab selected. Under 'Configuration', there is a text input field for 'IP Subnets/IP Addresses' containing '10.x.x.x'. Below this is an 'Entries' table with two columns: 'Username' and 'Description'. The table contains one entry: 'UOFCAL.EDU/root' with the description 'WMI configuration to discover Windows devices'. There are also icons for adding and deleting entries.

Configuration	
IP Subnets/IP Addresses:	10.x.x.x
Entries	
Username	Description
1. UOFCAL.EDU/root	WMI configuration to discover Windows devices

Initiating a Network Discovery Scan

Seed devices are the initial IP addresses provided by the network administrator to start the network scan. When you initiate a network discovery scan and specify the seed devices, network discovery uses SNMP to:

- Find any other devices connected to the seed devices.
- Profile the connected devices.
- W-ClearPass uses that information to detect more devices in the network. The network discovery scan will proceed to the network depth specified by the **Scan Depth** parameter (described in [Table 61](#) below).
- You can go to those devices and see their neighbor devices.



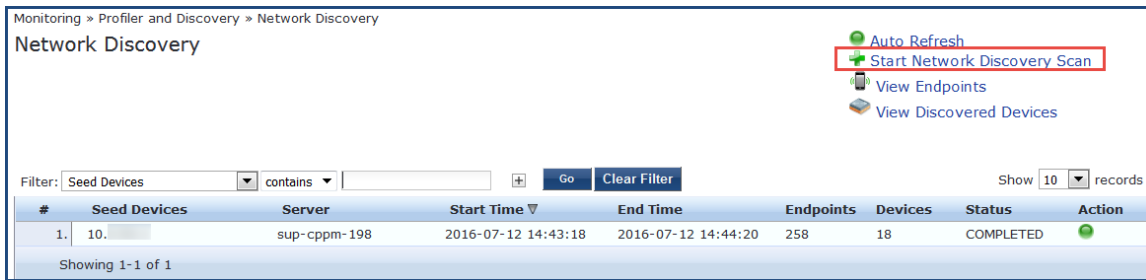
Running a network discovery scan on seed devices is a time- and resource-consuming operation. Depending on the number of devices associated with the seed device, a complete scan can take more than an hour. It is recommended that the network scan should be done outside of normal business hours or performed on a W-ClearPass node that is not servicing core authentications.

To initiate a Network Discovery Scan:

1. Navigate to **Monitoring > Profiler and Discovery > Network Discovery**.

The **Network Discovery** page opens.

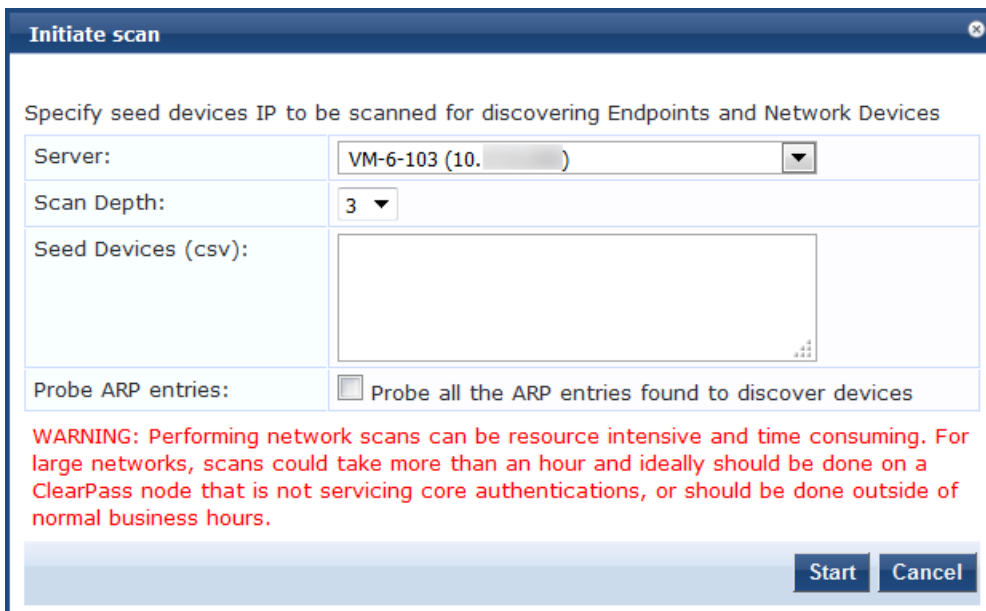
Figure 111: *Network Discovery Page*



2. Click **Start Network Discovery Scan**.

The **Initiate Scan** dialog opens.

Figure 112: *Initiating the Seed Devices Scan*



3. Enter the appropriate information in the **Initiate Scan** dialog as described in Table 61.

Table 61: *Initiating Network Discovery Scan Parameters*

Field	Action/Description
Server	From the drop-down list, select the W-ClearPass W-Policy Manager server. If the W-ClearPass server is in a cluster, the list will display the cluster node IP addresses that you can choose. NOTE: Once you select the node, the network discovery scan starts with that node.
Scan Depth	Specify the Scan Depth by selecting the desired number from 1 to 5. The Scan Depth numbers indicate the levels of the network you want to scan. The default is Scan Depth 3. The seed devices are, by default, at Scan Depth 1. Starting from the seed device, the next device level is Scan Depth 2, and so on, until the scan reaches the scan depth specified here.
Seed Devices	Enter the IP addresses of one or more seed devices from which the network scan should proceed. Separate multiple device IP addresses with commas.

4. Click **Start**.

You return to the **Network Discovery** page, which now indicates the following:

- The **Start Time** and **End Time** for the seed device scan.
- The number of **Endpoints** and **Devices** connected to the seed device.
- The **Status** of the scan operation, which shows initially as "**Scheduled**," then "**In Progress**," and finally, "**Completed**."

Figure 113: *Seed Device Successfully Scanned*

Monitoring » Profiler and Discovery » Network Discovery

Network Discovery

[Auto Refresh](#)
[Start Network Discovery Scan](#)
[View Endpoints](#)
[View Discovered Devices](#)

Filter: Seed Devices contains [] + Go Clear Filter Show 10 records

#	Seed Devices	Server	Start Time	End Time	Endpoints	Devices	Status	Action
1.	10.	sup-cppm-198	2016-07-12 14:43:18	2016-07-12 14:44:20	258	18	COMPLETED	

Showing 1-1 of 1

5. You can stop a scheduled seed device scan or restart a completed scan:

- a. To stop the scan operation, click the **Red Action** button, then click **Yes** to confirm the stop operation.
- b. To restart a completed scan, click the **Green Action** button.

About Auto-Refresh

When **Auto-Refresh** is enabled (it is enabled by default), W-ClearPass fetches fresh data every few seconds to ensure that the network discovery scan status is always current.

When **Auto-Refresh** is enabled, the button is green. You can disable **Auto-Refresh** by clicking the button, which will then turn red to indicate this feature is disabled.

To enable or disable Auto Refresh:

- Navigate to **Monitoring > Profiler and Discovery > Network Discovery**.

Figure 114: Network Discovery > Auto Refresh

Monitoring » Profiler and Discovery » Network Discovery

Network Discovery

Filter: Seed Devices contains [] Go Clear Filter Show 10 records

Auto Refresh
Start Network Discovery Scan
View Endpoints
View Discovered Devices

#	Seed Devices	Server	Start Time	End Time	Endpoints	Devices	Status	Action
1.	10.2.51.1	sup-cppm-198	2016-07-12 14:43:18	2016-07-12 14:44:20	258	18	COMPLETED	

Showing 1-1 of 1

- Click the **Auto Refresh** link.

Every **Auto-Refresh** operation accesses the database and reads the data. When there is no network scan occurring, you can disable **Auto-Refresh** as there is no need to access the database every time.

Importing and Viewing Discovered Network Devices

To import and view discovered network devices:

- Navigate to **Monitoring > Profiler and Discovery > Discovered Devices**.

The **Discovered Devices** page opens.

Figure 115: Discovered Devices Page

Monitoring » Profiler and Discovery » Discovered Devices

Discovered Devices

Vendor: ALL (16), Aruba (8), Cisco (7), Hewlett-Packard-Enterprise (1)

Status: ALL (16), Imported (1), New (15)

Filter: Name contains [] Go Clear Filter Show 10 records

#	Name	IP Address	Vendor	Status	Update Time
11.	Cisco-switch-51.202	10.2.51.1	Cisco	New	2016-01-12 00:04:30
12.	Cisco-Switch-51.64	10.2.51.1	Cisco	New	2016-01-12 00:04:30
13.	cppm7240	192.168.1.1	Aruba	New	2016-01-12 00:04:30
14.	CPPM-HP-2920-I	10.2.51.1	Hewlett-Packard-Enterprise	New	2016-01-12 00:04:30
15.	sw1.lab1.arubathena.com	10.2.51.1	Aruba	New	2016-01-12 00:04:30
16.	testlabcorvina2	10.2.51.1	Aruba	New	2016-01-12 00:04:30

Back to Network Discovery Showing 11-16 of 16 Import Ignore

Importing Network Devices

The devices that you import are added to the set of network devices known to W-ClearPass.



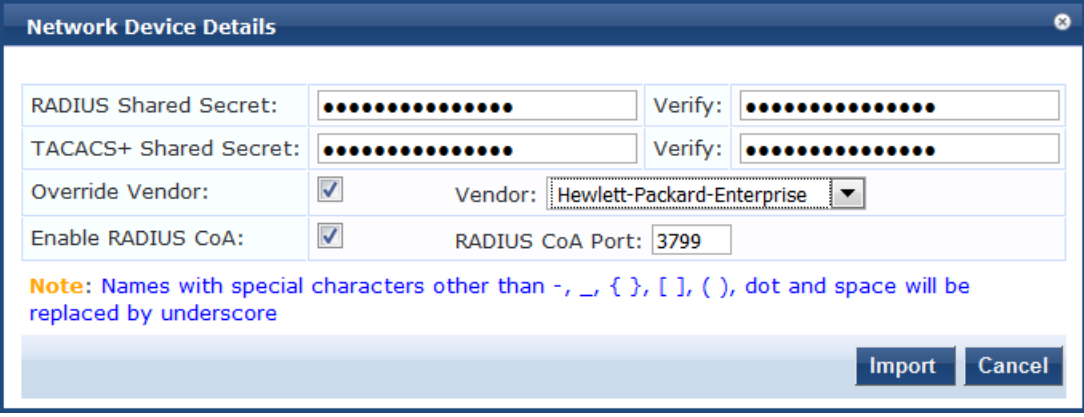
You can import devices from the Publisher node only.

To import and add discovered devices to the set of W-ClearPass Network Devices:

- From the list of discovered devices, select a device you wish to import (as shown in [Figure 115](#)). You can select all of the discovered devices at once by clicking the **Name** check box.
- Click the **Import** button.

The **Network Device Details** dialog opens.

Figure 116: Importing a Network Device



The **Network Device Details** dialog box contains the following fields and controls:

- RADIUS Shared Secret:** A text field with masked characters (dots).
- Verify:** A text field with masked characters (dots).
- TACACS+ Shared Secret:** A text field with masked characters (dots).
- Verify:** A text field with masked characters (dots).
- Override Vendor:** A checked checkbox.
- Vendor:** A dropdown menu currently showing **Hewlett-Packard-Enterprise**.
- Enable RADIUS CoA:** A checked checkbox.
- RADIUS CoA Port:** A text field containing the value **3799**.

Note: Names with special characters other than -, _, { }, [], (), dot and space will be replaced by underscore

Buttons: **Import** and **Cancel**

3. Enter the appropriate information in the **Network Device Details** dialog as described in Table 62.

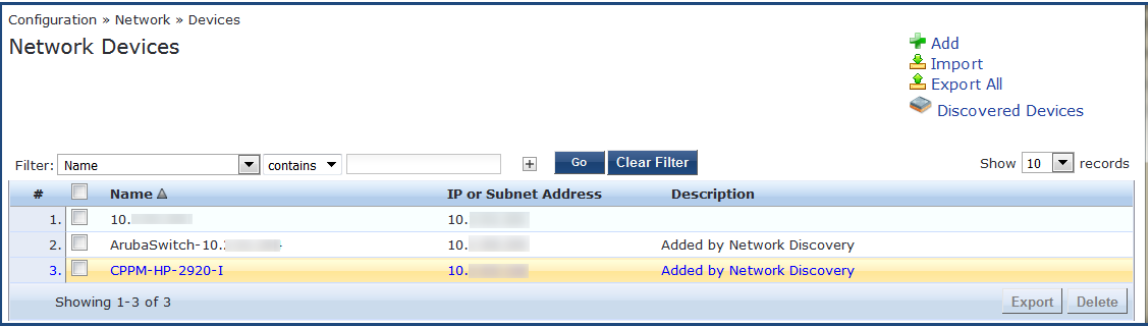
Table 62: Specifying Network Device Details for Importing Devices

Field	Action/Description
RADIUS Shared Secret	1. If using RADIUS, enter the RADIUS Shared Secret for the selected discovered device.
TACACS+ Shared Secret	2. If using TACACS+, enter the TACACS+ Shared Secret for the selected discovered device.
Override Vendor	3. Optionally, to override the discovered vendor type, select this check box.
Vendor	This field is displayed when you select Override Vendor . 4. From the Vendor drop-down, select the name of the vendor type to override the discovered vendor type.
Enable RADIUS CoA	5. Select this check box to enable RADIUS CoA (Change of Authorization).
RADIUS CoA Port	The default RADIUS CoA port is 3799 . 6. To change the RADIUS CoA port number, enter the new port number.

7. Click **Import**.

The selected network device has been added to W-ClearPass. To see the network device listed, navigate to **Configuration > Network > Devices**.

Figure 117: Network Device Added to W-ClearPass



The **Network Devices** page shows a list of discovered devices. The interface includes a filter bar and a table of results.

Filter: Name contains [] Go Clear Filter Show 10 records

#	Name	IP or Subnet Address	Description
1.	10.	10.	
2.	ArubaSwitch-10.	10.	Added by Network Discovery
3.	CPPM-HP-2920-I	10.	Added by Network Discovery

Showing 1-3 of 3 Export Delete

Viewing Details on a Discovered Device

To view detailed information about a discovered network devices, including a list of its neighbors in the network:

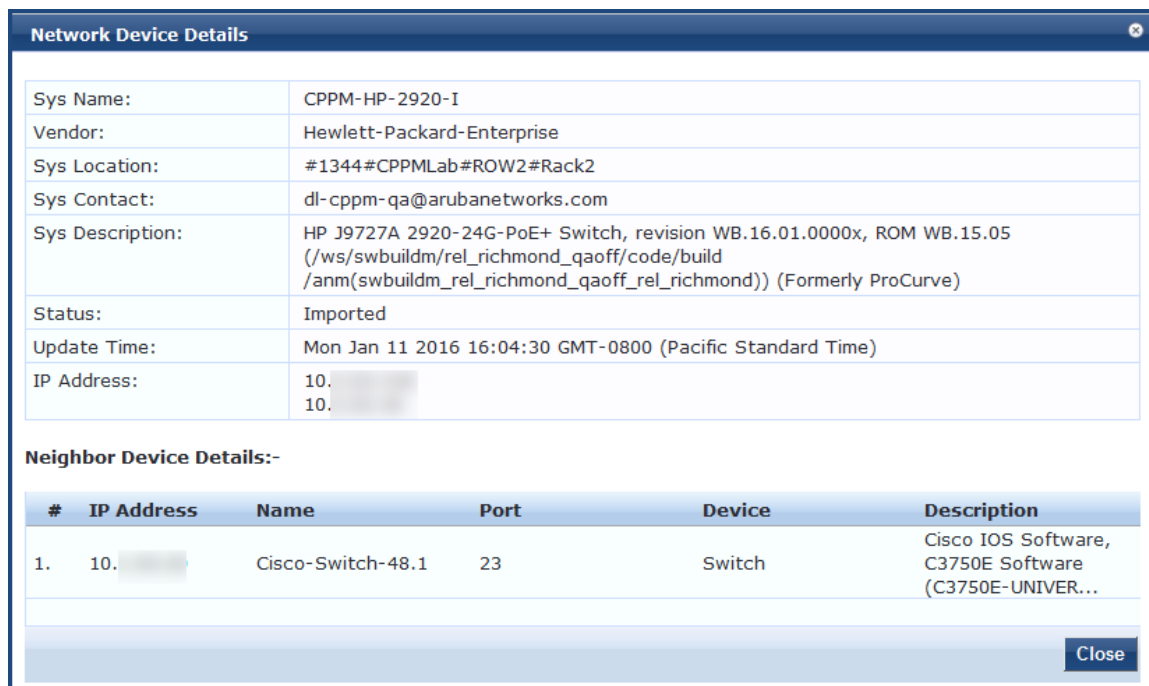
1. Navigate to **Monitoring > Profiler and Discovery > Discovered Devices**.

The **Discovered Devices** page opens.

2. Click the name of the device of interest.

The **Network Device Details** page opens.

Figure 118: Viewing Details for a Discovered Device



The screenshot shows a window titled "Network Device Details" with a close button in the top right corner. The window contains two main sections. The first section is a table with device details. The second section is titled "Neighbor Device Details:-" and contains a table with neighbor information. At the bottom right of the window is a "Close" button.

Sys Name:	CPPM-HP-2920-I
Vendor:	Hewlett-Packard-Enterprise
Sys Location:	#1344#CPPMLab#ROW2#Rack2
Sys Contact:	dl-cppm-qa@arubanetworks.com
Sys Description:	HP J9727A 2920-24G-PoE+ Switch, revision WB.16.01.0000x, ROM WB.15.05 (/ws/swbuildm/rel_richmond_qaoff/code/build/anm(swbuildm_rel_richmond_qaoff_rel_richmond)) (Formerly ProCurve)
Status:	Imported
Update Time:	Mon Jan 11 2016 16:04:30 GMT-0800 (Pacific Standard Time)
IP Address:	10. [redacted] 10. [redacted]

Neighbor Device Details:-

#	IP Address	Name	Port	Device	Description
1.	10. [redacted]	Cisco-Switch-48.1	23	Switch	Cisco IOS Software, C3750E Software (C3750E-UNIVER...

Close

3. When finished, click **Close**.

Viewing Discovered Endpoints

To view all the discovered endpoints that are connected to the network:

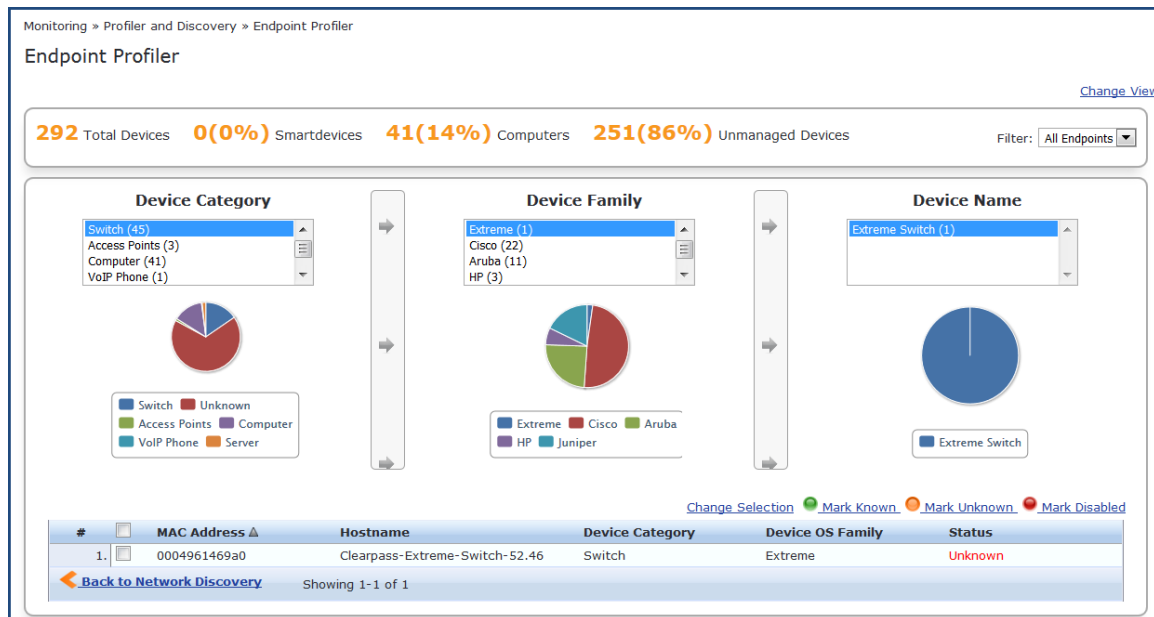
1. Navigate to **Monitoring > Profiler and Discovery > Network Discovery**.

The **Network Discovery** page opens.

2. Click **View Endpoints**.

The Endpoint Profiler opens.

Figure 119: Viewing the Discovered Endpoints Information



3. When finished, click **Back to Network Discovery**.

Audit Viewer

This section provides the following information:

- [Introduction](#)
- [Audit Viewer](#)
- [Audit Viewer](#)
- [Audit Viewer](#)

Introduction

The **Audit Viewer** page provides a dynamic report on actions, device name, category of W-Policy Manager component, user, and timestamp. To access the Audit Viewer:

1. Navigate to **Monitoring > Audit Viewer**.

The **Audit Viewer** page opens.

Figure 120: Audit Viewer Page

Monitoring » Audit Viewer

Audit Viewer

Filter: Action contains Show 10 records

#	Action	Name	Category	User	Timestamp
1.	ADD	10.2.51.12	SNMP Trap Config	admin	Mar 16, 2016 00:51:45 PDT
2.	MODIFY	CPATS LDAP FO service	Radius Enforcement Service	admin	Mar 16, 2016 00:51:20 PDT
3.	MODIFY	CPATS MYSQL FO service	Radius Enforcement Service	admin	Mar 16, 2016 00:51:20 PDT
4.	MODIFY	CPATS Oracle FO service	Radius Enforcement Service	admin	Mar 16, 2016 00:51:20 PDT
5.	MODIFY	CPATS AD FO service	Radius Enforcement Service	admin	Mar 16, 2016 00:51:20 PDT
6.	MODIFY	CPATS MSSQL FO service	Radius Enforcement Service	admin	Mar 16, 2016 00:51:20 PDT
7.	MODIFY	CPATS MySQL with FO	Authentication Source	admin	Mar 16, 2016 00:51:19 PDT
8.	MODIFY	CPATS LDAP with FO	Authentication Source	admin	Mar 16, 2016 00:51:19 PDT
9.	MODIFY	CPATS AD with FO	Authentication Source	admin	Mar 16, 2016 00:51:19 PDT
10.	MODIFY	CPATS MSSQL with FO	Authentication Source	admin	Mar 16, 2016 00:51:19 PDT

Showing 1-10 of 3411

- To display detailed information about the selected event, click any row in the audit viewer.
The **Audit Row Details** page opens (see).
The content in the **Audit Row Details** page varies, depending upon type of event you select.

Add Events

To display additional details that are specific to the new policy component, click a row with the **Add** action type.
The **Audit Row Details** page opens.

Figure 121: Audit Row Details for Add Event

Audit Row Details

Guest User - **cptest-1469117941-200@example.com**

Guest User	
User ID	cptest-1469117941-200@example.com
Guest Type	USER
Start Time	Jul 21, 2016 09:20:53 PDT
Expiry Time	Jul 22, 2016 09:20:53 PDT
Sponsor Name	cptest-1469117941-200@example.com
Enabled	true
Approval Status	Approved
Email Guest User	No
SMS Guest User	No

Attributes	
Name	Value

For example, if a TACACS enforcement profile is added, the **Audit Row Details** page displays detailed information about that profile.

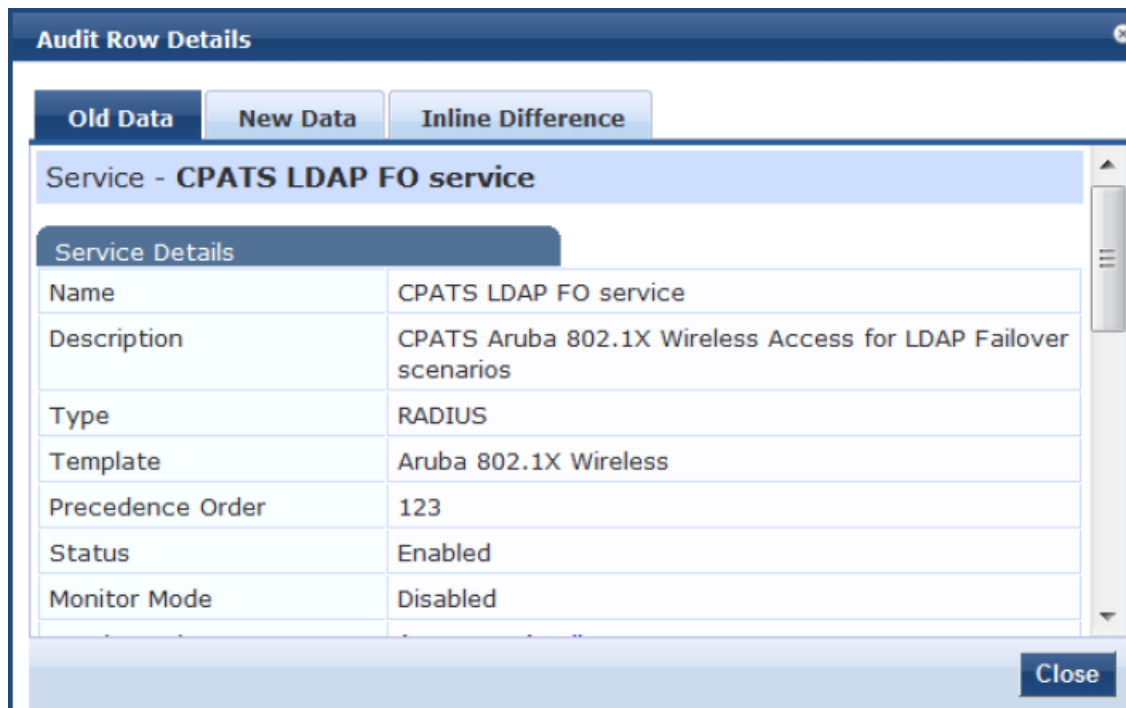
If a policy is created, the **Audit Row Details** page displays information about the policy.

Modify Events

To display additional details information about the change, including the previous values, the latest, updated values, and the differences between the two, click a row with the **Modify** action type.

Figure 122 shows the **Audit Row Details** page for a **Modify Event**.

Figure 122: Audit Row Details for Modify Event



When you view a modify event, the **Audit Row Details** window contains the following three tabs:

Table 63: Audit Row Details > Modify Event Page

Parameter	Description
Old Data	Displays a summary of details about the original data values. - The Profile section shows a summary of the profile values. - The Attributes section shows data about the original attributes and values.
New Data	Displays a summary of details about the new data values. - The Profile section shows a summary of the profile values. - The Attributes section shows data about the original attributes and values.
Inline Difference	Displays information about what changed. The information is color-coded to indicate the following types of changes: - Modified - Added - Deleted

Table 63: Audit Row Details > Modify Event Page (Continued)

Parameter	Description
	- Moved up - Moved down

Remove Events

To display details about attributes that were removed, click a row with the **Remove** action type.

Event Viewer

This section provides the following information:

- About the Event Viewer
- Creating an Event Viewer Report Using Default Values
- Creating an Event Viewer Report Using Custom Values
- Viewing Report Details

About the Event Viewer

The **Event Viewer** page provides reports about system-level events.

To access the Event Viewer:

- Navigate to **Monitoring > Event Viewer**.

The **Event Viewer** page opens.

Figure 123: Event Viewer Page

The screenshot shows the 'Event Viewer' page in a web application. At the top, there's a breadcrumb 'Monitoring > Event Viewer' and the page title 'Event Viewer'. On the right, there's a 'Select Server' dropdown menu with 'eighty84 (10...)' selected. Below this is a filter section with a 'Filter:' label, a dropdown set to 'Source', a 'contains' dropdown, and a text input field. To the right of the filter are 'Go' and 'Clear Filter' buttons, and a 'Show 10 records' dropdown. The main part of the page is a table with the following columns: #, Source, Level, Category, Action, and Timestamp. The table contains 10 rows of event data. The first row is highlighted in red, indicating an error. The last row is also highlighted in red. The bottom of the page shows 'Showing 1-10 of 1580' with a pagination icon.

#	Source	Level	Category	Action	Timestamp
1.	Sysmon	ERROR	System	None	Nov 20, 2013 14:05:01 PST
2.	Admin UI	INFO	Logged in	None	Nov 20, 2013 13:47:31 PST
3.	Admin UI	INFO	Logged in	None	Nov 20, 2013 13:33:35 PST
4.	Endpoint Context Server	INFO	MobileIron: Profile details updated	None	Nov 20, 2013 13:22:17 PST
5.	Endpoint Context Server	INFO	MobileIron: Endpoint details updated	None	Nov 20, 2013 13:22:12 PST
6.	Endpoint Context Server	INFO	airwatch: Profile details updated	None	Nov 20, 2013 13:21:52 PST
7.	Endpoint Context Server	INFO	airwatch: Endpoint details updated	None	Nov 20, 2013 13:21:46 PST
8.	Sysmon	ERROR	System	None	Nov 20, 2013 13:05:02 PST
9.	Endpoint Context Server	INFO	MobileIron: Profile details updated	None	Nov 20, 2013 12:22:19 PST
10.	Endpoint Context Server	INFO	MobileIron: Endpoint details updated	None	Nov 20, 2013 12:22:14 PST

The following table describes the **Event Viewer** parameters:

Table 64: *Event Viewer Page Parameters*

Parameter	Description
Source	Displays the source of the event. For example, AdminUI or W-ClearPass Updater.
Level	Displays the level of the event from the following options: • INFO • WARN • ERROR
Category	Displays the category of the event. For example, Logged in, System, or AV/AS Updates.
Action	Displays the status of the event action. For example, Success, Failed, Unknown, and None.
Timestamp	Displays the date and time when the event occurred.

Creating an Event Viewer Report Using Default Values

1. In the **Filter** field, select **Source** as the filter parameter.
2. Click **Go**.
W-ClearPass returns all event records.

Creating an Event Viewer Report Using Custom Values

1. Click the  icon.
A new filter is added. You can add up to four filters.
2. Click **Select ANY match**.
3. In the first **Filter** field, select **Level**.
4. Leave the search term set to **contains**.
5. Enter **ERROR** in the text field.
6. In the second **Filter** field, select **Source**.
7. Change the search field to **equals**.
8. Enter **SYSMON** in the text field.
9. Change the **Show records** value to **20**.
10. Click **Go**.

The following figure displays the **Event Viewer** report with custom values:

Figure 124: Event Viewer Report with Customized Filter

Monitoring » Event Viewer

Event Viewer

Select Server: cp217.cppm.test (10.)

Select ALL matches Select ANY match

Filter: Level contains ERROR

Filter: Source equals SYSMON

Go Clear Filter

Show 10 records

#	Source	Level	Category	Action	Timestamp
1.	Monitor	ERROR	battery		Jul 19, 2016 13:34:41 PDT
2.	Cluster	ERROR	Replication	Failed	Jul 19, 2016 13:30:03 PDT
3.	Monitor	ERROR	Insight(Sync)		Jul 19, 2016 13:28:52 PDT
4.	Monitor	ERROR	battery		Jul 19, 2016 13:19:41 PDT
5.	Monitor	ERROR	Insight(Sync)		Jul 19, 2016 13:13:51 PDT
6.	Monitor	ERROR	battery		Jul 19, 2016 13:04:41 PDT
7.	Cluster	ERROR	Replication	Failed	Jul 19, 2016 13:00:03 PDT
8.	Monitor	ERROR	Insight(Sync)		Jul 19, 2016 12:58:50 PDT
9.	Monitor	ERROR	battery		Jul 19, 2016 12:49:41 PDT
10.	Monitor	ERROR	Insight(Sync)		Jul 19, 2016 12:43:49 PDT

Showing 1-10 of 29

Viewing Report Details

To display the **System Event Details** page, click a row in the **Event Viewer** page.

Figure 125: System Event Details Page

System Event Details	
Source	Cluster
Level	ERROR
Category	Replication
Action	Failed
Timestamp	Jul 19, 2016 13:30:03 PDT
Description	Node with IP=10.2.51.249 out of sync by 114 minutes
Close	

The following table describes the **System Event Details** parameters:

Table 65: System Event Details Page Parameters

Parameter	Description
Source	Displays the source of the event. For example, AdminUI, RADIUS, and SnmpService.
Level	Displays the level of the event from the following options: - INFO - WARN - ERROR
Category	Displays the category of the event. For example, Request, Authentication, and System.

Table 65: System Event Details Page Parameters (Continued)

Parameter	Description
Action	Displays the action of the events. For example, Success, Failed, Unknown, and None.
Timestamp	Displays the date and time when the event occurred.
Description	Displays additional information about the event, including the node's IP address when pertinent.

Data Filters

This section provides the following information:

- [About Data Filters](#)
- [Adding a Data Filter](#)

About Data Filters

The **Data Filters** page provides a way to limit the number of rows of data shown by defining custom criteria or rules in the following components in W-Policy Manager:

- [Live Monitoring: Access Tracker on page 107](#)
- [Syslog Export Filters on page 541](#)
- [Live Monitoring: Analysis and Trending on page 133](#)
- [Live Monitoring: Accounting on page 116](#)

Preconfigured Data Filters

W-Policy Manager is preconfigured with the following data filters:

- **All Requests:** Shows all requests (without any rows filtered).
- **W-ClearPass Application Requests:** Shows all Application session log requests.
- **Failed Requests:** Shows all authentication requests that were rejected or failed.
- **Guest Access Requests:** Shows all requests—RADIUS or Web Authentication—where the user was assigned the built-in role **Guest**.
- **Healthy Requests:** Shows all requests that were deemed healthy by W-Policy Manager.
- **RADIUS Requests:** Shows all RADIUS requests.
- **Successful Requests:** Shows all authentication requests that were successful.
- **TACACS Requests:** Shows all TACACS requests.
- **Unhealthy Requests:** Shows all requests that were not deemed healthy by W-Policy Manager.
- **WebAuth Requests:** Shows all Web Authentication requests (requests originated from the Guest Portal).

Accessing the Data Filters Page

To access the **Data Filters** page:

1. Navigate to **Monitoring > Data Filters**.
The **Data Filters** page opens.

Figure 126: Data Filters Page

Monitoring » Data Filters

Data Filters

Filter: Name contains [] + Go Clear Filter

Show 10 records

#	☐	Name ▲	Description
1.	☒	[Active sessions]	All Active sessions
2.	☐	[All Requests]	All session log requests
3.	☐	[Application Authentication]	All Application Authentications
4.	☐	[ClearPass Application Requests]	All Application session log requests
5.	☐	[ClearPass Configuration Audit]	All ClearPass Configuration Audit
6.	☐	[ClearPass Guest]	All ClearPass Guest
7.	☐	[ClearPass System Events]	All ClearPass System Events
8.	☐	[Endpoints]	All Endpoints
9.	☐	[Event Requests]	All Event requests
10.	☐	[Failed Application Authentication]	All Failed Application Authentication

Showing 1-10 of 34 ▶▶

Copy Export Delete

Top right actions: Add, Import, Export All

Adding a Data Filter

To add a data filter:

1. Click the **Add** link in the top-right corner of the page.

The **Add Data Filters** page opens to the **Filter** tab.

Figure 127 shows the **Filter** dialog when you choose **Select Attributes**.

Figure 127: Add Data Filter > Filter Tab > Select Attributes

Monitoring » Data Filters » Add

Data Filters

Filter Rules Summary

Name: All RADIUS Requests

Description: Filter for all RADIUS requests

Configuration Type: ☐ Specify Custom SQL ☒ Select Attributes

Custom SQL:

Back to Data Filters

Next > Save Cancel

Figure 128 shows the **Filter** dialog when you choose **Specify Custom SQL**.

Figure 128: Add Data Filter > Filter Tab > Specify Custom SQL

The screenshot shows the 'Add Data Filters' dialog with the 'Filter' tab selected. The 'Configuration Type' is set to 'Specify Custom SQL'. The 'Custom SQL' field contains the following query:

```
LEFT OUTER JOIN tips_session_log_details T2 ON T2.session_id = T1.id WHERE T2.type = " and T2.attr_name = " and T2.attr_value = "
```

Below the query field, it states: 'The complete Access Tracker query with custom SQL specified is -'

```
SELECT T1.id as "Common.Request-Id", T1.source as "Common.Source", T1.user_name as "Common.Username", T1.nas_ip as "Common.NAS-IP-Address", T1.nas_port as "Common.NAS-Port", T1.host_mac as "Common.Host-MAC-Address", T1.service_name as "Common.Service", T1.alerts_present as "Common.Alerts-Present", T1.conn_status as "Common.Connection-Status", T1.login_status as "Common.Login-Status", T1.error_code as "Common.Error-Code", T1.timestamp as "Common.Request-Timestamp" FROM tips_dashboard_summary T1 LEFT OUTER JOIN tips_session_log_details T2 ON T2.session_id = T1.id WHERE T2.type = " and T2.attr_name = " and T2.attr_value = " AND ((T1.timestamp >= --START-TIME--) AND (T1.timestamp <= --END-TIME--));
```

2. Specify the **Add Data Filters** parameters as described in the following table.

Table 66: Add Data Filters Page > Filter Tab Parameters

Parameter	Action/Description
Name	Enter a name for the data filter.
Description	Optionally, enter a description of this data filter (recommended).
Configuration Type	Choose one of the following configuration types: Select Attributes Specify Custom SQL
Select Attributes	This option is selected by default. When you specify Select Attributes , the Rules tab appears. Use the Rules tab to configure rules for this filter.
Specify Custom SQL	When you choose Specify Custom SQL , a default SQL template is displayed. In the text entry field, enter the attributes for the type, attribute name, and attribute value. NOTE: Dell does not recommend that you enable this option without first consulting Support (navigate to Administration > Support > Contact Support).

Rules Tab

The **Rules** tab displays when you choose the **Select Attributes** configuration type on the **Filter** dialog.

Figure 129: Add Data Filter > Rules Dialog

Table 67 describes the **Add Filter > Rules** tab parameters:

Table 67: Add Filter > Rules Tab

Parameter	Action/Description
Rule Evaluation Algorithm	Select ANY 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.
Edit Rule	Edit an existing rule.
Remove Rule	When you select an existing rule and click Remove Rule , the selected Rule is deleted immediately (no confirmation prompt appears).

When you click **Add Rule** or **Edit Rule**, the **Dashboard Filter Rules Editor** dialog opens.

Figure 130: Dashboard Filters > Rules Editor

Table 68 describes the **Dashboard Filters > Rules Editor** parameters:

Table 68: *Dashboard Filters > Rules Editor Configuration Parameters*

Parameter	Action/Description
Matches	Specify the match conditions: • ANY matches one of the configured conditions. • ALL specifies to match all of the configured conditions.
Type	Select the type of data filter. • Common: Attributes common to RADIUS, TACACS, and WebAuth requests and responses. • RADIUS: Attributes associated with RADIUS authentication, accounting requests, and responses. • TACACS: Attributes associated with TACACS authentication, accounting, policy requests, and responses. • Web Authentication Policy: W-Policy Manager policy objects assigned after the evaluation of policies associated with Web Authentication requests. For example, Auth Method, Auth Source, and Enforcement Profiles.
Name	Select the name of the attribute from the Name drop-down list. The Name list varies according to which Type you selected.
Operator	Select any subset of string data type operators from the following list: • EQUALS • NOT_EQUALS • LESS_THAN • LESS_THAN_OR_EQUALS • GREATER_THAN • GREATER_THAN_OR_EQUALS • CONTAINS • NOT_CONTAINS • EXISTS • NOT_EXISTS
Value	The value of the attribute.

Restoring Blacklisted Users to the Network

The **Blacklisted Users** page lists the MAC address and user name of all blacklisted users, the authentication source for that user, and indicates whether the bandwidth limit or session duration limits were exceeded by each blacklisted user.

After a user entry is removed from the blacklisted users list, the user is eligible to access the network.

To access the **Blacklisted Users** page:

1. Navigate to **Monitoring > Blacklisted Users**.

Figure 131: Blacklisted Users Page

Filter: MAC Address contains Go Clear Filter							Show 20 records
#	☐	MAC Address	User Name	Authentication Source	Bandwidth Limit	Session Duration	Timestamp ▲
1.	☐	FB6755E2BDC0	user1	[Local User Repository]	Exceeded	Exceeded	Aug 19, 2013 19:20:23 IST
2.	☐	7871E5B3793D	user2	[Guest User Repository]	Exceeded	Not Exceeded	Aug 19, 2013 19:20:23 IST
3.	☐	06507A6574F8	user3	[Guest Device Repository]	Exceeded	Exceeded	Aug 19, 2013 19:20:23 IST
4.	☐	5F39EA4CCF35	user4	[Endpoints Repository]	Not Exceeded	Exceeded	Aug 19, 2013 19:20:23 IST
5.	☐	BD2813331857	user5	[Onboard Devices Repository]	Exceeded	Not Exceeded	Aug 19, 2013 19:20:23 IST
6.	☐	FE1AFE26D551	user6	[Admin User Repository]	Not Exceeded	Exceeded	Aug 19, 2013 19:20:23 IST
7.	☐	C8CB61D93511	user7	[Blacklist User Repository]	Exceeded	Exceeded	Aug 19, 2013 19:20:23 IST
8.	☐	E17C3B06FF82	user8	[Insight Repository]	Exceeded	Not Exceeded	Aug 19, 2013 19:20:23 IST
9.	☐	F5F920B10173	user9	[Local User Repository]	Not Exceeded	Not Exceeded	Aug 19, 2013 19:20:23 IST
10.	☐	A6D394659CF3	user10	[Guest User Repository]	Not Exceeded	Exceeded	Aug 19, 2013 19:20:23 IST
11.	☐	8249A5FC722A	user11	[Guest Device Repository]	Exceeded	Exceeded	Aug 19, 2013 19:20:23 IST
Showing 1-11 of 11							Delete

- To delete a user from this blacklist, select the user row and click **Delete**.
The deleted Blacklisted user is now eligible to access the network.

As a first step in the service-based processing, W-Policy Manager uses an authentication method to authenticate the user or device against an authentication source. After the user or device is authenticated, Policy Manager fetches attributes for role mapping policies from the authorization sources associated with this authentication source. For a general overview of W-Policy Manager authentication and authorization, see [Authentication and Authorization Architecture and Flow on page 165](#)

For more information, see:

- [Supported Authentication Methods on page 165](#)
- [Adding and Modifying Authentication Methods on page 169](#)
- [Adding and Modifying Authentication Sources on page 193](#)
- [Configuring Authentication Components on page 167](#)

Supported Authentication Methods

Policy Manager supports the following authentication methods:

- Tunneled EAP authentication
 - 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 authentication
 - EAP Message Digest 5 (EAP-MD5) - W-ClearPass Policy Manager does not support EAP-MD5 in the **FIPS** mode
 - EAP Microsoft Challenge Handshake Authentication Protocol version 2 (EAP-MSCHAPv2)
 - EAP Generic Token Card (EAP-GTC)
 - Challenge Handshake Authentication Protocol (CHAP)
 - Password Authentication Protocol (PAP)
 - Microsoft CHAP version 1 and 2
 - MAC authentication method (MAC-AUTH)
- Authorize authentication

The MAC_AUTH authentication type must be used exclusively in a MAC-based authentication service. When the MAC_AUTH method is selected, W-Policy Manager makes internal checks to verify that the request is a **MAC_Authentication** request and not a spoofed request. In tunneled EAP methods, authentication and posture credential exchanges occur inside a protected outer tunnel.

Authentication and Authorization Architecture and Flow

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

- Authentication method
- Authentication source
- Authorization source

Authentication Method

W-Policy Manager initiates the authentication handshake by sending available methods in a priority order until the client accepts a method or until the client rejects the last method (with NAKs) with the following possible outcomes:

- Successful negotiation returns a method, which is used to authenticate 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.
- W-Policy Manager rejects the connection.



An authentication method is configurable only for some service types. For more information, see [Policy Manager Service Types on page 70](#). All 802.1X wired and wireless services have an associated authentication method. For example, the MAC_AUTH authentication method can be associated with the MAC authentication service type.

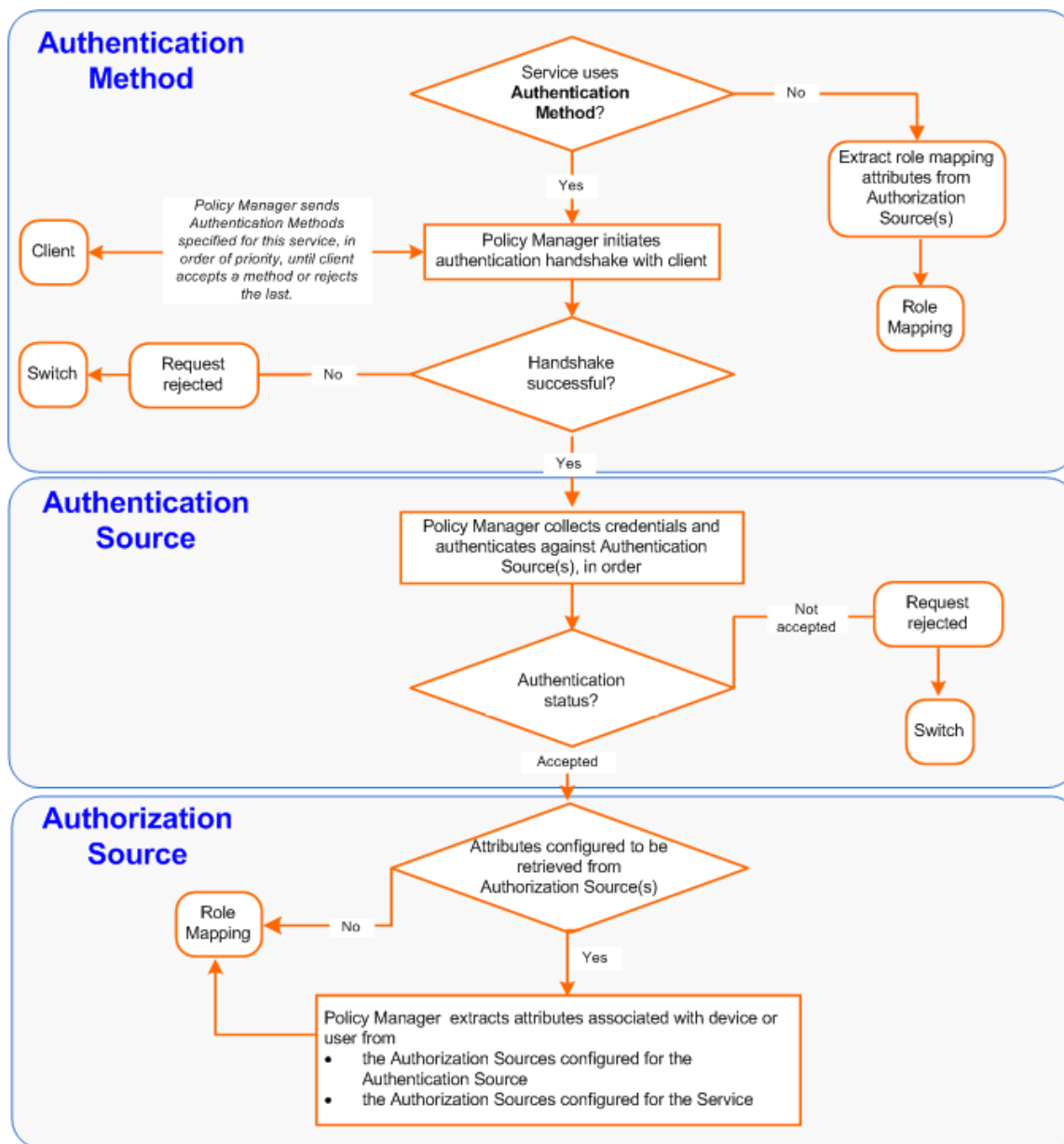
Authentication Source

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 (the 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. After 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 collects 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.

After 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 132: Authentication and Authorization Flow of Control



Configuring Authentication Components

To add or modify an authentication method or source for an existing service, navigate to the **Services** (**Configuration > Services > Add**) page and click the **Authentication** tab). For a new service, the **Policy Manager** wizard automatically opens the **Authentication** tab for configuration. You can open an authentication method or source from the **Configuration > Authentication > Methods** or **Configuration > Authentication > Sources** page. The following figure is an example of the **Authentication** tab:

Figure 133: Authentication Components

Services - [AirGroup Authorization Service]

Table 69: Authentication Options at the Service Level

Component	Configuration Steps
Sequence of Authentication Methods	• Select a method, then select 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 displays a popup with the edit widgets for the select authentication method. ■ To add a previously configured authentication method, select from the Select to Add drop-down list. ■ To configure a new method, click the Add new Authentication Method link. For more information about authentication methods, see Adding and Modifying Authentication Methods on page 169. NOTE: An authentication method is only configurable for some service types. For more information, refer to Policy Manager Service Types on page 70.
Sequence of Authentication Sources	• Select a 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 displays the Authentication Source Configuration wizard for the selected authentication source. • To add a previously configured authentication source, select from the Select to Add drop-down list. • To configure a new authentication source, click the Add new Authentication Source link. For more information about authentication sources, see Adding and Modifying Authentication Sources on page 193.
Whether to standardize the form in which usernames are present	Select the Enable to specify a comma-separated list of rules to strip usernames check box to pre-process the user name and to remove prefixes and suffixes before authenticating it to the authentication source.

Adding and Modifying Authentication Methods

This section provides the following information:

- [Adding a New Authentication Service](#)
- [Modifying an Existing Authentication Service](#)

Adding a New Authentication Service

To add a new authentication service:

1. Navigate to **Configuration > Authentication > Methods**.

The **Authentication Methods** page opens.

Figure 134: *Authentication Methods Page*

Configuration » Authentication » Methods

Authentication Methods

Filter: Name contains Go Clear Filter Show 10 records

#	Name	Type	Description
1.	[Allow All MAC AUTH]	MAC-AUTH	Default settings for Allow All MAC-AUTH
2.	[Aruba EAP GTC]	EAP-GTC	EAP-GTC method to use with Aruba EAP-GTC plugin for Windows
3.	[Authorize]	Authorize	Default settings for Authorize
4.	[CHAP]	CHAP	Default settings for CHAP
5.	[EAP FAST]	EAP-FAST	Default settings for EAP-FAST
6.	[EAP GTC]	EAP-GTC	Default settings for EAP-GTC
7.	[EAP MD5]	EAP-MD5	Default settings for EAP-MD5
8.	[EAP MSCHAPv2]	EAP-MSCHAPv2	Default settings for EAP-MSCHAPv2
9.	[EAP PEAP]	EAP-PEAP	Default settings for EAP-PEAP
10.	[EAP PEAP Public]	EAP-PEAP-Public	Default settings for EAP-PEAP-Public

Showing 1-10 of 19 Export Delete

Add Import Export All

2. Click **Add Authentication Method** page opens.

Figure 135: *Add Authentication Method Page*

Add Authentication Method

General

Name:

Description:

Type:

Select Authentication type...

- Authorize
- CHAP
- EAP-FAST
- EAP-GTC
- EAP-MD5
- EAP-MSCHAPv2
- EAP-PEAP
- EAP-PEAP-Public
- EAP-PWD
- EAP-TLS
- EAP-TTLS
- MAC-AUTH
- MSCHAP
- PAP

ve Cancel

3. Enter the name and description of the new service.

4. From the **Type** drop-down, select the type of service you want to add.

Modifying an Existing Authentication Service

To modify an existing authentication service:

1. Navigate to **Configuration > Authentication > Methods**.
2. Click any row in the **Authentication Methods** page.

The Edit Authentication Method page opens.

Figure 136: *Edit Authentication Method Page*

Edit Authentication Method	
General Inner Methods PACs PAC Provisioning	
Name:	[EAP FAST]
Description:	Default settings for EAP-FAST
Type:	EAP-FAST
Method Details	
Session Resumption:	☒ Enable
Session Timeout:	6 hours
End-Host Authentication:	Using PACs
Certificate Comparison:	Do not compare
Copy Save Cancel	

3. Configure the Authentication Method of interest as described in the following sections:

- [Authorize Authentication Method on page 171](#)
- [CHAP and EAP-MD5 on page 171](#)
- [EAP-FAST on page 172](#)
- [EAP-GTC on page 177](#)
- [EAP-MSCHAPv2 on page 179](#)
- [EAP-PEAP on page 179](#)
- [EAP-PEAP-Public on page 182](#)
- [EAP-PWD on page 185](#)
- [EAP-TLS on page 186](#)
- [EAP-TTLS on page 188](#)
- [MAC-AUTH on page 191](#)
- [MSCHAP on page 191](#)
- [PAP on page 192](#)

Authorize Authentication Method

This is an authorization-only method that you can add with a custom name. The **General** tab labels the authentication method and defines session details. The following figure displays the **Authorization - General** tab:

Figure 137: Add Authentication - General Tab

The screenshot shows a window titled "Add Authentication Method". Inside, there is a "General" tab. The form has three main sections: "Name:" with a text box, "Description:" with a text area, and "Type:" with a dropdown menu currently set to "Authorize". At the bottom right of the window are "Save" and "Cancel" buttons.

The following table describes the **Authorize General** parameters:

Table 70: Authorize General Tab Parameters

Parameter	Description
Name	Specify the label of the authentication method.
Description	Provide additional information that helps to identify the authentication method.
Type	Select the type of authentication. In this context, select Authorize .

CHAP and EAP-MD5

Policy Manager is packaged with **CHAP** and **EAP-MD5** authentication methods. You can create one or more instances of CHAP and EAP-MD5 authentication methods by assigning a customized name to each one. These methods can also be associated to a service as authentication methods.



The EAP-MD5 authentication type is not supported if you use W-ClearPass Policy Manager in the FIPS (**Administration > Server Manager > Server Configuration > FIPS** tab) mode.

The following figure is an example of the **General** tab for the **CHAP** authentication method:

Figure 138: *General Tab (CHAP)*

The following table describes the **CHAP and EAP-MD5 - General** parameters:

Table 71: *CHAP and EAP-MD5 - General Tab Parameters*

Parameter	Description
Name	Specify the name of the authentication method.
Description	Provide the additional information that helps to identify the authentication method.
Type	Select the type of authentication. In this context, always CHAP or EAP-MD5 .

EAP-FAST

EAP-Flexible Authentication through Secure Tunneling (EAP-FAST) is an authentication method that encrypts EAP transactions within a TLS tunnel.

This section describes how to configure the following four EAP-FAST authentication method tabs:

- [General Tab on page 172](#)
- [Inner Methods Tab on page 174](#)
- [PACs Tab on page 175](#)
- [PAC Provisioning Tab on page 175](#)

General Tab

The **General** tab labels the authentication method and defines session details.



The **PACs** and **PAC Provisioning** tabs are available only when **Using PACs** is specified in the **End-Host Authentication** field on the **General** tab.

1. Navigate to **Configuration > Authentication > Methods**.
The **Authentication Methods** page appears.
2. Create a new EAP-FAST authentication service or edit an existing one.
The following figure displays the **EAP-FAST - General** tab:

Figure 139: *EAP-FAST - General Tab*

The screenshot shows the 'Add Authentication Method' dialog box with the 'General' tab selected. The 'Name' and 'Description' fields are empty. The 'Type' dropdown is set to 'EAP-FAST'. The 'Method Details' section includes: 'Session Resumption' checked, 'Session Timeout' set to 6 hours, 'End-Host Authentication' set to 'Using PACs', and 'Certificate Comparison' set to 'Do not compare'. 'Save' and 'Cancel' buttons are at the bottom right.

3. Configure the EAP-FAST authentication service as described in [Table 72](#).

Table 72: *EAP_FAST - General Tab Parameters*

Parameter	Action/Description
Name	1. Specify the name of the authentication method.
Description	2. Provide the additional information that helps to identify the authentication method.
Type	3. Select EAP_FAST .
Session Resumption	4. Caches EAP-FAST sessions on W-Policy Manager for reuse if the user/end-host reconnects to the W-ClearPass server within the session-timeout interval. By default, this option is enabled.
Session Timeout	Caches EAP-FAST sessions on Policy Manager for reuse if the user/end-host reconnects to W-Policy Manager within the session-timeout interval. 5. Specify the Session Timeout in the number of hours. The default is 6 hours. If the Session Timeout value is set to 0 , the cached sessions are not purged.
End-Host Authentication	6. Specify one of the following end-host authentication methods: ■ Using PACS (Protected Access Credentials)

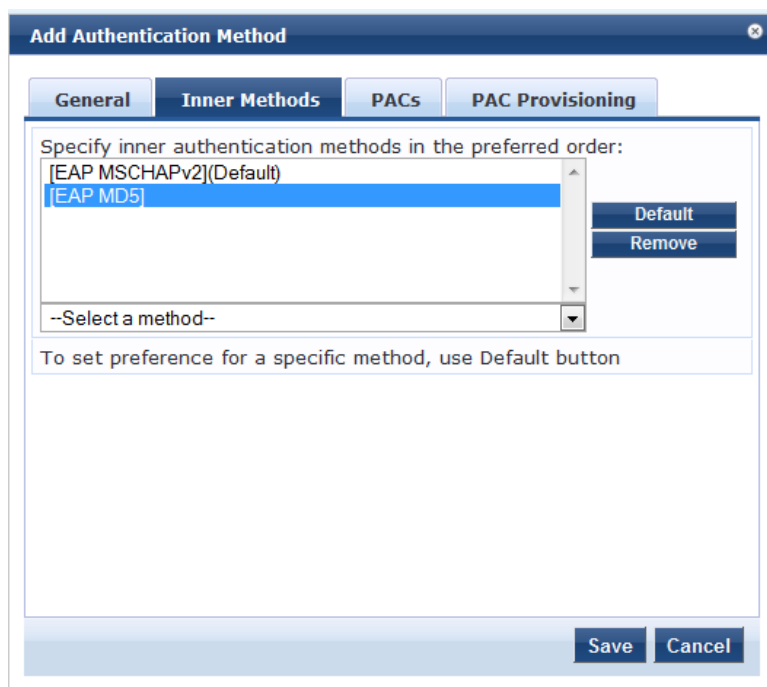
Table 72: *EAP_FAST - General Tab Parameters (Continued)*

Parameter	Action/Description
	■ Using Client Certificate
Certificate Comparison	7. Specify one of the following Certificate Comparison actions: ■ Do not compare ■ Compare Distinguished Name (DN) ■ Compare Common Name (CN) ■ Compare Subject Altname Subject Name (SAN) ■ Compare CN or SAN ■ Compare Binary
	8. When finished, click the Inner Methods tab.

Inner Methods Tab

The **Inner Methods** tab controls the inner methods for the **EAP-FAST** method. The following figure displays the **EAP-FAST - Inner Methods** tab:

Figure 140: *EAP-FAST Add Authentication Method - Inner Methods Tab*



The EAP-MD5 authentication method is not supported if you use W-ClearPass Policy Manager in FIPS mode (**Administration > Server Manager > Server Configuration > FIPS** tab).

Table 73: EAP-FAST - Inner Methods Tab Parameters

Parameter	Description
Specify inner authentication methods in the preferred order	- 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 from the Select a method drop-down list. The list can contain multiple inner methods, which W-Policy Manager sends 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 inner method (the method tried first), select a method and click Default. - When finished, click the PACs tab.

PACs Tab

The **PACs** tab enables or disables Protected Access Credential (PAC) types. The following figure displays the **EAP-FAST - PACs** dialog:

Figure 141: EAP_FAST PACs Dialog

The screenshot shows the 'Add Authentication Method' dialog box with the 'PACs' tab selected. The dialog contains four sections for configuring Protected Access Credentials (PACs):

- Tunnel PAC:** Checked checkbox, expiration time set to 1 days.
- Machine PAC:** Checked checkbox, expiration time set to 1 days.
- Authorization PAC:** Checked checkbox, expiration time set to 1 days.
- Posture PAC:** Checked checkbox, expiration time set to 1 days.

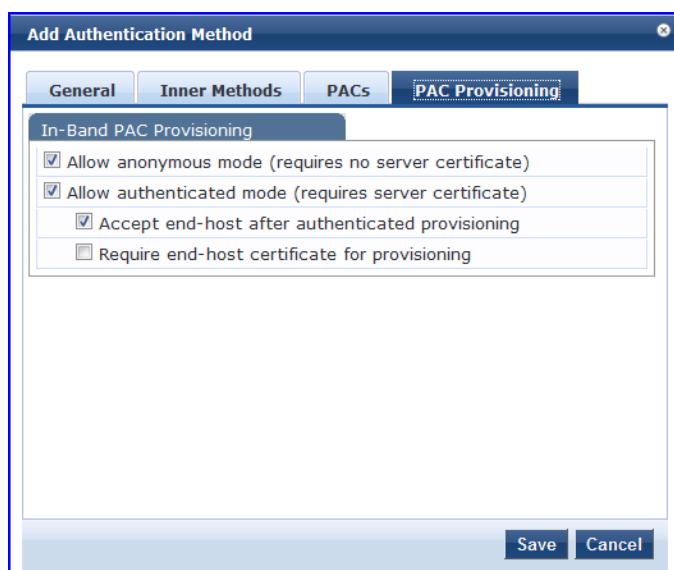
At the bottom of the dialog are 'Save' and 'Cancel' buttons.

- Specify the **Expiration Time** (number of **hours, days, weeks, months, or years**) for each of the Protected Access Credentials:
 - Tunnel PAC Expiration Time
 - Machine PAC Expiration Time
 - Authorization PAC Expiration Time
 - Posture PAC Expiration Time
- Select the **PAC Provisioning** tab.

PAC Provisioning Tab

The **PAC Provisioning** tab controls anonymous and authenticated modes. The following figure displays the **EAP-FAST PAC - Provisioning** dialog:

Figure 142: *EAP_FAST PAC Provisioning Dialog*



1. Configure the PAC Provisioning parameters as described in [Table 74](#).
2. When finished, click **Save**.

Table 74: *EAP_FAST PAC Provisioning Tab Parameters*

Parameter	Description	Considerations
In-Band PAC Provisioning		
Allow anonymous mode	When in anonymous mode, phase 0 of EAP_FAST provisioning establishes an outer tunnel without end-host/W-Policy Manager authentication. NOTE: This mode is not as secure as the authenticated mode. After an outer tunnel is established, the end-host and W-Policy Manager perform mutual authentication using MSCHAPv2, then W-Policy Manager provisions the end-host with an appropriate PAC (tunnel or machine).	Authenticated mode is more secure than anonymous provisioning mode. After the server is authenticated, the phase 0 tunnel is established. The end-host and W-Policy Manager perform mutual authentication and provision on the end-host with an appropriate PAC (tunnel or machine): • If both anonymous and authenticated provisioning modes are enabled and the end-host sends a cipher suite that supports server authentication, W-Policy Manager picks the authenticated provisioning mode. • If the appropriate cipher suite is supported by the end-host, W-Policy Manager performs anonymous provisioning.
Allow authenticated mode	Enable to allow authenticated mode provisioning. When Allow authenticated mode is in phase 0, Policy Manager establishes the outer tunnel inside a server-authenticated tunnel. The end-host authenticates the server by validating the Policy Manager certificate.	
Accept end-host after authenticated provisioning	After the authenticated provisioning mode is complete and the end-host is provisioned with a PAC, W-Policy Manager rejects the end-host	None.

Table 74: *EAP_FAST PAC Provisioning Tab Parameters (Continued)*

Parameter	Description	Considerations
	authentication. The end-host subsequently re-authenticates using the newly provisioned PAC. When this field is enabled, W-Policy Manager accepts the end-host authentication in the provisioning mode itself. The end-host does not have to re-authenticate.	
Required end-host certificate for provisioning	In authenticated provisioning mode, the end-host authenticates the server by validating the server certificate, which results in a protected outer tunnel. The end-host is authenticated by the server inside this tunnel. When this field is enabled, the server can require the end-host to send a certificate inside the tunnel for the purpose of authenticating the end-host.	None.

EAP-GTC

EAP-Generic Token Card (GTC) enables the exchange of clear-text authentication credentials across the network. EAP-GTC is used inside a TLS tunnel created by TTLS or PEAP to provide server authentication in wireless environments. The EAP-GTC method contains the **General** tab that labels the authentication method and defines session details.

The following figure displays the **EAP-GTC - General** tab:

Figure 143: *EAP-GTC - General Tab*

The screenshot shows a window titled "Edit Authentication Method" with a close button in the top right corner. The "General" tab is selected. It contains the following fields:

- Name:** A text input field.
- Description:** A text area with a small icon in the bottom right corner.
- Type:** A dropdown menu currently showing "EAP-GTC".
- Method Details:** A sub-section containing:
 - Challenge:** A text input field.
 - Password:** A text input field.

At the bottom right of the dialog are "Save" and "Cancel" buttons.

The following figure displays the **EAP-GTC General** parameters:

Table 75: *EAP-GTC General Tab Parameters*

Parameter	Description
Name	Specify the name of the authentication method.
Description	Provide the additional information that helps to identify the authentication method.
Type	Select the type of authentication. In this context, select EAP-GTC .
Method Details	
Challenge	Specify an optional password.

EAP-MSCHAPv2

The **EAP-MSCHAPv2** method contains the **General** tab that labels the method and defines session details. The following figure is an example of the **EAP-MSCHAPv2 - General** tab:

Figure 144: *EAP-MSCHAPv2 - General Tab*

The screenshot shows a window titled "Add Authentication Method" with a close button in the top right corner. Inside the window, there is a tab labeled "General". Below the tab, there are three input fields: "Name:" with the text "aaaa", "Description:" with the text "default settings for", and "Type:" with a dropdown menu showing "EAP-MSCHAPv2". At the bottom right of the window, there are two buttons: "Save" and "Cancel".

The following table describes the **EAP-MSCHAPv2 - General** parameters:

Table 76: *EAP-MSCHAPv2 - General Tab Parameters*

Parameter	Description
Name	Specify the name of the authentication method.
Description	Provide the additional information that helps to identify the authentication method.
Type	Select the type of authentication. In this context, select EAP-MSCHAPv2 .

EAP-PEAP

EAP-Protected Extensible Authentication Protocol (EAP-PEAP) is a protocol that creates an encrypted (and more secure) channel before the password-based authentication occurs. PEAP is an 802.1X authentication method that uses server-side public key certificate to establish a secure tunnel in which the client authenticates with server. The PEAP authentication creates an encrypted SSL/TLS tunnel between client and authentication server.

The exchange of information is encrypted and stored in the tunnel ensuring that the user credentials are kept secure.

The **EAP-PEAP** authentication method contains the following two tabs:

- [General Tab on page 180](#)
- [Inner Methods Tab on page 181](#)

General Tab

The **General** tab labels the authentication method and defines session details. The following figure is an example of the **EAP-PEAP General** tab:

Figure 145: *EAP-PEAP - General Tab*

The screenshot shows the 'Add Authentication Method' dialog box with the 'General' tab selected. The 'Name' and 'Description' fields are empty. The 'Type' dropdown is set to 'EAP-PEAP'. The 'Method Details' section includes 'Session Resumption' (checked), 'Session Timeout' (6 hours), 'Fast Reconnect' (checked), 'Microsoft NAP Support' (checked), and 'Cryptobinding' (None). 'Save' and 'Cancel' buttons are at the bottom right.

The following table describes the **EAP-PEAP - General** parameters:

Table 77: *EAP-PEAP - General Tab Parameters*

Parameter	Description
Name	Specify the name of the authentication method.
Description	Provide the additional information that helps to identify the authentication method.
Type	Specify the type of authentication. In this context, select EAP-PEAP .
Method Details	

Table 77: EAP-PEAP - General Tab Parameters (Continued)

Parameter	Description
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 check box 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 the fast reconnect to work, session resumption must be enabled.

Inner Methods Tab

The **Inner Methods** tab controls the inner methods for the **EAP-PEAP** authentication method. The following figure is an example of the **EAP-PEAP - Inner Methods** tab:

Figure 146: EAP-PEAP - Inner Methods Tab

Add Authentication Method

General **Inner Methods**

Specify inner authentication methods in the preferred order:

- [EAP MD5](Default)
- [EAP TLS]

--Select a method--

To set preference for a specific method, use Default button

Save **Cancel**



The EAP-MD5 authentication method is not supported if you use W-ClearPass Policy Manager in the FIPS (**Administration > Server Manager > Server Configuration > FIPS**) mode.

The following table describes the **EAP-PEAP Inner Methods** parameters:

Table 78: *EAP-PEAP Inner Methods Tab Parameters*

Parameter	Description
Specify inner authentication methods in the preferred order	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 Select a method drop-down list. The list can contain multiple inner methods, which Policy Manager sends 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-PEAP-Public

The **EAP-PEAP-Public** method is used for authenticating and providing a secured wireless guest access to the endpoints. To provide a secured wireless guest access, the Wi-Fi Protected Access (WPA) is provided for publicly known username and password. This ensures that every device gets a unique wireless session key that is used to encrypt the traffic and provide secured wireless access without intruding the privacy of others though the same username and password is shared to all devices.

The **EAP-PEAP-Public** method contains the following two tabs:

- [General on page 183](#)
- [Inner Methods on page 184](#)

General

The **General** tab labels the authentication method and defines session details. The following figure is an example of the **EAP-PEAP-Public - General** tab:

Figure 147: *EAP-PEAP-Public - General Tab*

The screenshot shows a window titled "Add Authentication Method". It has two tabs: "General" and "Inner Methods". The "General" tab is selected. The form contains the following fields:

- Name:** A text input field.
- Description:** A text input field.
- Type:** A dropdown menu with "EAP-PEAP-Public" selected.
- Method Details:** A section containing:
 - Session Resumption:** A checkbox labeled "Enable" which is checked.
 - Session Timeout:** A text input field with "6" and the unit "hours".
 - Fast Reconnect:** A checkbox labeled "Enable" which is checked.
 - Public Username:** A text input field.
 - Public Password:** A text input field.

At the bottom right of the window are "Save" and "Cancel" buttons.

The following table describes the **EAP-PEAP-Public - General** parameters:

Table 79: *EAP-PEAP-Public - General Tab Parameters*

Parameter	Description
Name	Specify the name of the authentication method.
Description	Provide the additional information that helps to identify the authentication method.
Type	Specify the type of authentication. In this context, select EAP-PEAP-Public .
Session Resumption	Caches EAP-PEAP-Public sessions on Policy Manager for reuse if the user/client reconnects to Policy Manager within the session timeout interval. By default, this option is enabled.
Session Timeout	Caches EAP-PEAP-Public sessions on Policy Manager for reuse if the user/client reconnects to Policy Manager within the session timeout interval in hours. If session timeout value is set to 0, the cached sessions are not purged. The default session timeout is 6 hours.

Table 79: EAP-PEAP-Public - General Tab Parameters (Continued)

Parameter	Description
Fast Reconnect	Enable this check box 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 the fast reconnect to work, session resumption must be enabled.
Public Username	Enter the Guest username. In this context, enter 'public'.
Public Password	Enter the Guest password. In this context, enter 'public'.

Inner Methods

The **Inner Methods** tab controls the inner methods for the **EAP-PEAP-Public** authentication method. The following figure is an example of the **EAP-PEAP-Public - Inner Methods** tab:

Figure 148: EAP-PEAP-Public - Inner Methods Tab

Add Authentication Method

General **Inner Methods**

Specify inner Authentication Methods in the preferred order:

[EAP MSCHAPv2](Default)

Default
Remove

--Select a method--

To set preference for a specific method, use Default button

Save Cancel



The EAP-MD5 authentication method is not supported if you use W-ClearPass Policy Manager in the FIPS (**Administration > Server Manager > Server Configuration > FIPS** tab) mode.

Table 80: EAP-PEAP-Public Inner Methods Tab Parameters

Parameter	Description
Specify inner authentication methods in the preferred order	Select the inner authentication method available from the drop-down list. In this context, only the EAP-MSCHAPv2 method is available. The following functions are available in this tab: • To append an inner method to the displayed list, select it from the drop-down list. The list can contain multiple inner methods, which Policy Manager sends 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-PWD

EAP-PWD is an EAP authentication method, which uses a shared password for authentication. EAP-PWD addresses the problem of password-based authenticated key exchange using a possibly weak password for authentication to derive an authenticated and cryptographically strong shared secret. The **EAP-PWD** method contains the **General** tab that labels the authentication method and defines session details.

The following figure displays the **EAP-PWD - General** tab:

Figure 149: EAP-PWD - General Tab

The screenshot shows a window titled "Add Authentication Method". Inside, the "General" tab is active. It contains the following fields:

- Name:** EAP-PWD auth
- Description:** Specifies the EAP-PWD authentication method.
- Type:** EAP-PWD (selected from a dropdown menu)

Below the "General" tab is a section titled "Method Details" which contains:

- Group:** 256-bit random ECP group (selected from a dropdown menu)
- Server Id:** CPPM

At the bottom right of the window are "Save" and "Cancel" buttons.

The following table describes the **EAP-PWD - General** parameters:

Table 81: *EAP-PWD - General Tab Parameters*

Parameter	Description
Name	Specify the name of the authentication method.
Description	Provide the additional information that helps to identify the authentication method.
Type	Specify the type of authentication. In this context, select EAP-PWD .
Method Details	
Group	Select the group from the drop-down list. Each party to the exchange derives ephemeral keys with respect to a particular set of domain parameters, that is a 'group'. A group can be based on Finite Field Cryptography (FFC) or Elliptic Curve Cryptography (ECC).
Server Id	Specify the string that identifies the server to the peer.

EAP-TLS

EAP-Transport Layer Security (EAP-TLS) requires an exchange of proof of identities through public key cryptography (such as digital certificates). EAP-TLS secures this exchange with an encrypted TLS tunnel which helps to resist dictionary or other attacks. The **EAP-TLS** authentication method contains the **General** tab that labels and defines session details.

The following figure displays the **EAP-TLS - General** tab:

Figure 150: EAP-TLS - General Tab

Add Authentication Method

General

Name: EAP-TLS 4-hour session timeout

Description: session times out after 4 hours

Type: EAP-TLS

Method Details

Session Resumption: ☒ Enable

Session Timeout: 4 hours

Authorization Required: ☒ Enable

Certificate Comparison: Do not compare

Verify Certificate using OCSP: None

Override OCSP URL from Client: ☒ Enable

OCSP URL:

Save Cancel

The following table describes the **EAP_TLS - General** parameters:

Table 82: EAP_TLS - General Tab Parameters

Parameter	Description
Name	Specify the name of the authentication method.
Description	Provide the additional information that helps to identify the authentication method.
Type	Specify the type of authentication. In this context, select EAP_TLS .
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	Specifies the duration in hours for the cached EAP-TLS sessions to be retained.
Authorization Required	Check Enable to specify whether to perform an authorization check.
Certificate Comparison	Specify the type of certificate comparison (identity matching) upon presenting Policy Manager with a client certificate:

Table 82: *EAP_TLS - General Tab Parameters (Continued)*

Parameter	Description
	• To skip the certificate comparison, choose Do not compare. • To compare specific attributes, choose Compare Common Name (CN), Compare Subject Alternate Name (SAN), or Compare CN or SAN. • To perform a binary comparison of the stored (in the client record in Active Directory or another LDAP-compliant directory) and presented certificates, choose Compare Binary.
Verify Certificate using OCSP	Select Optional or Required if the certificate to be verified by the Online Certificate Status Protocol (OCSP). Select None to not to verify the certificate.
Override OCSP URL from the Client	Select this option to use a different URL for OCSP. After this option is enabled, you can enter a new URL in the OCSP URL field.
OCSP URL	If the Override OCSP URL from the Client field is enabled, then enter the replacement URL.

EAP-TTLS

EAP-Tunneled Transport Layer Security (EAP-TTLS) is designed to provide authentication that is similar to EAP-TLS, but each user does not require a certificate be issued. The certificates are issued only to authentication servers.

The **EAP-TTLS** method contains the following two tabs:

- [General Tab on page 189](#)
- [Inner Methods Tab on page 190](#)

General Tab

The **General** tab labels the method and defines session details. The following figure is an example of the **EAP-TTLS - General** tab:

Figure 151: EAP-TTLS - General Tab

The screenshot shows a window titled "Add Authentication Method". It has two tabs: "General" and "Inner Methods". The "General" tab is selected. Inside the "General" tab, there are three input fields: "Name:", "Description:", and "Type:". The "Type:" dropdown menu is set to "EAP-TTLS". Below these fields is a section titled "Method Details". Inside this section, there are two settings: "Session Resumption:" with a checked checkbox and the word "Enable", and "Session Timeout:" with a text box containing "6" and the word "hours". At the bottom right of the window are two buttons: "Save" and "Cancel".

The following table describes the **EAP-TTLS - General** parameters:

Table 83: EAP-TTLS - General Tab Parameters

Parameter	Description
Name	Specify the name of the authentication method.
Description	Provide the additional information that helps to identify the authentication method.
Type	Select the type of authentication. In this context, select EAP-TTLS . NOTE: The EAP-MD5 authentication type is not supported if you use W-ClearPass Policy Manager in the FIPS (Administration > Server Manager > Server Configuration > FIPS tab) mode.
Method Details	
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	Specify the duration in hours for the EAP-TTLS sessions to be cached.

Inner Methods Tab

The **Inner Methods** tab controls the inner methods for the **EAP-TTLS** method. The following figure is an example of the **EAP-TTLS - Inner Methods** tab:

Figure 152: *EAP_TTLS - Inner Methods Tab*

Edit Authentication Method

General **Inner Methods**

Specify inner authentication methods in the preferred order:

- [EAP MSCHAPv2]
- [EAP TLS]
- [EAP GTC]
- [PAP]

Default
Remove

Select a method...

To set preference for a specific method, use Default button

Save Cancel

The following table describes the **EAP-TTLS - Inner Methods** parameters:

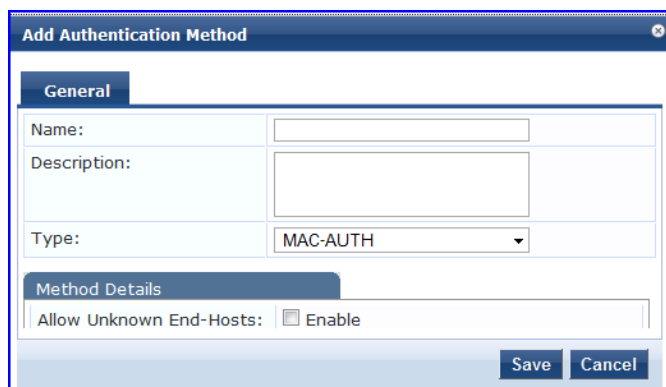
Table 84: *EAP-TTLS - Inner Methods Tab Parameters*

Parameter	Description
Specify inner authentication methods in the preferred order	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. The list can contain multiple inner methods, which Policy Manager sends 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 that tried first), select it and click Default. NOTE: The EAP-MD5 authentication type is not supported if you use W-ClearPass Policy Manager in the FIPS (Administration > Server Manager > Server Configuration > FIPS tab) mode.

MAC-AUTH

The MAC-AUTH method contains the **General** tab that labels the authentication method and defines session details. The following figure is an example of the **MAC-AUTH - General** tab:

Figure 153: MAC-AUTH - General Tab



The following table describes the **MAC-Auth - General** parameters:

Table 85: MAC-Auth - General Tab Parameters

Parameter	Description
General	
Name	Specify the name of the authentication method.
Description	Provide the additional information that helps to identify the authentication method.
Type	Select the type of authentication. In this context, select MAC-AUTH .
Method Details	
Allow Unknown End-Hosts	Enables further policy processing of MAC authentication requests of unknown clients. If this is not enabled, 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 selecting this check box and enabling audit (See Configuring Audit Servers on page 327), you can trigger an audit of an unknown client.

MSCHAP

The MS-CHAP authentication method authenticates remote Windows-based workstations, integrating the functionality to which LAN-based users are accustomed with the hashing algorithms used on Windows networks. MS-CHAP uses a challenge-response mechanism to authenticate connections without sending any passwords. The MSCHAP method contains the **General** tab that labels the authentication method and defines session details.

The following figure is an example of the **MSCHAP - General** tab:

Figure 154: *MSCHAP - General Tab*

The screenshot shows a dialog box titled "Add Authentication Method" with a close button in the top right corner. The "General" tab is selected. It contains three input fields: "Name:" (a text box), "Description:" (a larger text box), and "Type:" (a dropdown menu with "MSCHAP" selected). At the bottom right are "Save" and "Cancel" buttons.

The following table describes the **MSCHAP - General** parameters:

Table 86: *MSCHAP - General Tab Parameters*

Parameter	Description
Name	Specify the name of the authentication method.
Description	Provide the additional information that helps to identify the authentication method.
Type	Select the type of authentication. In this context, select MSCHAP .

PAP

The Password Authentication Protocol (PAP) is an authentication protocol in which the user name and password are sent to the remote access server in unencrypted form.

The **Add Authentication Method** dialog identifies the authentication method—in this example, PAP—and defines the method details.

displays the **Add Authentication Method > PAP** dialog.

Figure 155: *Adding the PAP Authentication Method*

The screenshot shows the "Add Authentication Method" dialog box with the "General" tab selected. The "Name:" and "Description:" fields are empty. The "Type:" dropdown menu is set to "PAP". Below the "General" tab is a "Method Details" section with a sub-tab. Under "Method Details", the "Enable Aruba-SSO:" checkbox is unchecked, and the dropdown menu next to it is set to "False". "Save" and "Cancel" buttons are at the bottom right.

Table 87 describes the **PAP** parameters:

Table 87: PAP Authentication Method Parameters

Parameter	Action/Description
Name	1. Specify the name of the authentication method.
Description	2. Provide the additional information that helps to identify the authentication method.
Type	3. Select PAP as the Type of authentication.
Method Details	
Enable Aruba-SSO	4. Enable or disable Aruba-SSO (Single Sign-On) by specifying True or False . The default is False .

Adding and Modifying Authentication Sources

Refer to the following sections to configure these authentication sources:

- [Generic LDAP and Active Directory](#)
- [Generic SQL DB](#)
- [HTTP](#)
- [Kerberos](#)
- [Okta](#)
- [RADIUS Server](#)
- [Static Host Lists](#)
- [Token Server](#)

To configure an authentication source for a new service:

1. Navigate to **Configuration > Authentication > Sources**.

Figure 156: Authentication Sources Page

Configuration > Authentication > Sources

Authentication Sources

Filter: Name contains [] Go Clear Filter

Show 10 records

#	Name	Type	Description
1.	[Admin User Repository]	Local SQL DB	Authenticate users against Policy Manager admin user database
2.	Automation_SHL_SOURCE	Static Host List	
3.	Bangalore-AD	Active Directory	
4.	[Blacklist User Repository]	Local SQL DB	Blacklist database with users who have exceeded bandwidth or session related limits
5.	[Endpoints Repository]	Local SQL DB	Authenticate endpoints against Policy Manager local database
6.	[Guest Device Repository]	Local SQL DB	Authenticate guest devices against Policy Manager local database
7.	[Guest User Repository]	Local SQL DB	Authenticate guest users against eTIPS local database
8.	India_AD	Active Directory	
9.	[Insight Repository]	Local SQL DB	Insight database with session information for users and devices
10.	[Local User Repository]	Local SQL DB	Authenticate users against eTIPS local user database

Showing 1-10 of 20

Copy Export Delete

2. After clicking **Add** and specifying the type of authentication source, W-Policy Manager displays the **Add** page for the selected authentication source.

Different tabs and fields appear, depending on the authentication source selected.

Figure 157: Add Authentication Source Page

Authentication Sources

General

Name:	
Description:	
Type:	-- Select -- Active Directory Generic LDAP Generic SQL DB HTTP Kerberos Okta RADIUS Server SIM File Static Host List Token Server
Use for Authorization:	☐ Enable to use this Authentication Source to also fetch role mapping attributes
Authorization Sources:	Remove View Details

Generic LDAP and Active Directory

Policy Manager can perform NTLM/MSCHAPv2, PAP/GTC, and certificate-based authentications against Microsoft Active Directory and against any LDAP-compliant directory. For example, Novell eDirectory, OpenLDAP, or Sun Directory Server. Both LDAP and Active Directory based server configurations are similar. You can retrieve role mapping attributes by using filters. For more information, see [Adding and Modifying Role Mapping Policies on page 259](#).

Use the following tabs to configure Generic LDAP and Active Directory authentication sources on the **Configuration > Authentication > Sources > Add** page:

- [General Tab on page 194](#)
- [Primary Tab on page 196](#)
- [Attributes Tab on page 198](#)
- [Summary Tab on page 207](#)

General Tab

The **General** tab labels the authentication source and defines session details. The following image is an example of the **Active Directory - General** tab:

Figure 158: *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:

Server Timeout: seconds

Cache Timeout: seconds

Backup Servers Priority:

[Back to Authentication Sources](#)

The following table describes the **Generic LDAP or Active Directory - General** parameters:

Table 88: *Generic LDAP or Active Directory - General Tab Parameters*

Parameter	Description
Name	Specify the name of the authentication source.
Description	Provide the additional information that helps to identify the authentication source.
Type	Select the type of authentication source. In this context, select Generic LDAP or Active Directory .
Use for Authorization	Enable this check box instruct 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 the Use for Authorization field is enabled. This box is checked (enabled) by default.
Authorization Sources	Specifies additional sources from which role mapping attributes to be fetched. Select a previously configured authentication source from the drop-down list and click Add to add authentication source to the list of authorization sources. Click Remove to remove the authentication source from the list. If Policy Manager authenticates the user or device from this authentication source, then also fetches role mapping attributes from these additional authorization sources NOTE: You can specify additional authorization sources at the service level. Policy Manager fetches role mapping attributes regardless of which authentication source the user or device was authenticated against.

Table 88: Generic LDAP or Active Directory - General Tab Parameters (Continued)

Parameter	Description
Server Timeout	Specifies the duration in number of seconds that W-Policy Manager waits before considering this server unreachable. If multiple backup servers are available, then this value indicates the duration in number of seconds that W-Policy Manager waits before attempting to fail over from the primary to backup servers in the order in which they are configured.
Cache Timeout	W-Policy Manager caches attributes fetched for an authenticating entity. This parameter controls the duration in number of seconds for which the attributes are cached.
Backup Servers Priority	Click Add Backup to add a backup server. If the Backup 1 tab appears, you can specify connection details for a backup server (same fields as for primary server that is specified below). To remove a backup server, select the server name and click Remove . Select 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 if the primary server is unreachable.

Primary Tab

The **Primary** tab defines the settings for the primary server. The following image is an example of the **Generic Active Directory - Primary** tab:

Figure 159: Generic LDAP or Active Directory - Primary Tab

Configuration » Authentication » Sources » Add

Authentication Sources

General	Primary	Attributes	Summary
Connection Details			
Hostname:			
Connection Security:	None		
Port:	389		
Verify Server Certificate:	☒ Enable to verify Server Certificate for secure connection		
Bind DN:			
Bind Password:			
Base DN:			Search Base Dn
Search Scope:	SubTree Search		
LDAP Referrals:	☐ Follow referrals		
Bind User:	☐ Allow bind using user password		
Password Attribute:	userPassword		
Password Type:	Cleartext		
Password Header:			
User Certificate :	userCertificate		
Back to Authentication Sources			
		Next >	Save
			Cancel

The following table describes the **Generic LDAP or Active Directory - Primary** parameters:

Table 89: *Generic LDAP or Active Directory - Primary Tab Parameters*

Parameter	Description
Hostname	Specify the hostname or the IP address of the LDAP or Active Directory server.
Connection Security	• Select None for default non-secure connection (usually port 389). • Select StartTLS for secure connection that is negotiated over the standard LDAP port. This is the preferred way to connect to an LDAP directory securely. • Select LDAP over SSL or AD over SSL to choose the legacy way of securely connecting to an LDAP directory. Port 636 must be used for this type of connection.
Port	Specifies the TCP port at which the LDAP or Active Directory server is listening for connections. The default TCP port for LDAP connections is 389 and the default port for LDAP over SSL is 636.
Verify Server Certificate	Select this checkbox to verify the server certificate as part of authentication.
Bind DN	Specify the DN of the administrator account. Policy Manager uses this account to access all other records in the directory. NOTE: For Active Directory, the bind DN can also be in the administrator@domain format (for example, administrator@acme.com).
Bind Password	Specify the password for the administrator DN entered in the Bind DN field.
NetBIOS Domain Name	Specify the Active Directory domain name for this server. Policy Manager prepends this name to the user ID to authenticate users found in this Active Directory. NOTE: This setting is available only for Active Directory.
Base DN	Enter the DN of the node in your directory tree from which to start searching for records. After entering the values for the fields described above, click Search Base DN to browse the directory hierarchy. The LDAP browser opens. You can navigate to the DN that you want to use as the base DN. 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. NOTE: This is also a method to test the connectivity to your LDAP or AD directory. If the values entered for the primary server attributes are correct, you can browse the directory hierarchy by clicking Search Base Dn.
Search Scope	Select the scope of the search you want to perform, starting at the base DN. • Base Object Search allows you to search at the level specified by the base DN. • One Level Search allows you to search up to one level lesser to the immediate children of the base DN. • Subtree Search allows you to search the entire subtree under the base DN (including at the base DN level).
LDAP Referral	Enable this check box to automatically follow referrals returned by your directory server in search results. Refer to your directory documentation for more information on referrals.

Table 89: Generic LDAP or Active Directory - Primary Tab Parameters (Continued)

Parameter	Description
Bind User	Enable this checkbox to authenticate users by performing a bind operation on the directory using the credentials (user name and password) obtained during authentication. For clients to be authenticated by using the LDAP bind method, Policy Manager must receive the password in cleartext.
Password Attribute (Available only for Generic LDAP)	Enter the name of the attribute in the user record from which user password can be retrieved. This is not available for Active Directory.
Password Type (Available only for Generic LDAP)	Specify whether the password type is Cleartext, NT Hash, or LM Hash.
Password Header (Available only for Generic LDAP)	Specifies the Oracle's LDAP implementation that prepends a header to a hashed password string. If using Oracle LDAP, enter the header in this field to correctly identify and read the password .
User Certificate	Enter the name of the attribute in the user record from which user certificate can be retrieved.
Always use NETBIOS name	Check this option to always use NETBIOS name instead of the domain part in username for authentication. NOTE: This field is available only if you select Active Directory as an authentication source.

Attributes Tab

The **Attributes** tab defines the Active Directory or LDAP Directory query filters and the attributes to be fetched by using those filters. The following images are the examples of the **Active Directory - Attributes** tab and the **Generic LDAP Directory - Attributes** tab:

Figure 160: Active Directory Attributes Tab (with Default Data)

General	Primary	Attributes	Summary
Specify filter queries used to fetch authentication and authorization attributes			
Filter Name	Attribute Name	Alias Name	Enabled As
1. Authentication	dn	UserDN	-
	department	Department	Attribute
	title	Title	Attribute
	company	company	-
	memberOf	memberOf	-
	telephoneNumber	Phone	Attribute
	mail	Email	Attribute
2. Group	displayName	Name	Attribute
	cn	Groups	Attribute
3. Machine	dNSHostName	HostName	Attribute
	operatingSystem	OperatingSystem	Attribute
	operatingSystemServicePack	OSServicePack	Attribute
4. Onboard Device Owner	memberOf	Onboard memberOf	-
5. Onboard Device Owner Group	cn	Onboard Groups	Attribute
Add More Filters			

Figure 161: Generic LDAP Directory - Attributes Tab

General	Primary	Attributes	Summary
Specify filters used to query for authentication and authorization attributes			
Filter Name	Attribute Name	Alias Name	Enable as role
1. Authentication	dn	UserDN	false
2. Group	cn	groupName	false
Add More Filters			
Back to Authentication Sources Next > Save Cancel			

The following table describes the **Active Directory/LDAP Attributes Tab - Filter Listing Screen** parameters:

Table 90: Active Directory/LDAP Attributes Tab - Filter Listing Screen Parameters

Parameter	Description
Filter Name	Specify the name of the filter.
Attribute Name	Specify the name of the LDAP/AD attributes defined for this filter.
Alias Name	Specify the alias name for each attribute name selected for the filter.
Enable As	Specify whether this value to be used directly as a role or attribute in an enforcement policy. This bypasses the step to assign a role in Policy Manager through a role mapping policy.

The following table describes the available directories:

Table 91: Active Directory/LDAP Default Filters

Directory	Default Filters
Active Directory	Authentication: This filter is used for authentication. The query searches in the objectClass of the type user. This query finds both user and machine accounts in Active Directory: <code>(&(objectClass=user)(sAMAccountName={Authentication:Username}))</code> After a request arrives, Policy Manager populates %{Authentication:Username} with the authenticating user or machine. This filter is also configured to fetch the following attributes based on this filter query: dn (alias of UserDN): This is an internal attribute that is populated with the user or machine record's DN department title company memberOf: In Active Directory, this attribute is populated with the groups that the user or machine belongs to. This is a multi-valued attribute. telephoneNumber mail displayName accountExpires Group: This is a 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 memberOf variable. The values for the memberOf attribute are fetched by the first filter (authentication) described above. The attribute fetched with this filter query is cn, 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 the name of the connecting host if available. dnsHostName, operatingSystem, and operatingSystemServicePack attributes are fetched with this filter query. Onboard Device Owner: This is the filter for retrieving the name of the owner the onboard device belongs to. This query finds the user in the Active Directory <code>(&(sAMAccountName={Onboard:Owner})(objectClass=user))</code> %{Onboard:Owner} is populated by Policy Manager with the name of the onboarded user. Onboard Device Owner Group: This filter is used for retrieving the name of the group the onboarded device owner belongs to. <code>(distinguishedName={Onboard memberOf})</code> This query fetches all group records where the DN is the value returned by the Onboard memberOf variable. The attribute fetched with this filter query is cn, which is the name of the Onboard group.
Generic LDAP Directory	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: dn (aliased to UserDN): This is an internal attribute that is populated with the user record's DN. Group: This is the filter used for retrieving the name of the groups to which a user belongs. <code>(&(objectClass=groupOfNames)(member={UserDn}))</code>

Table 91: Active Directory/LDAP Default Filters (Continued)

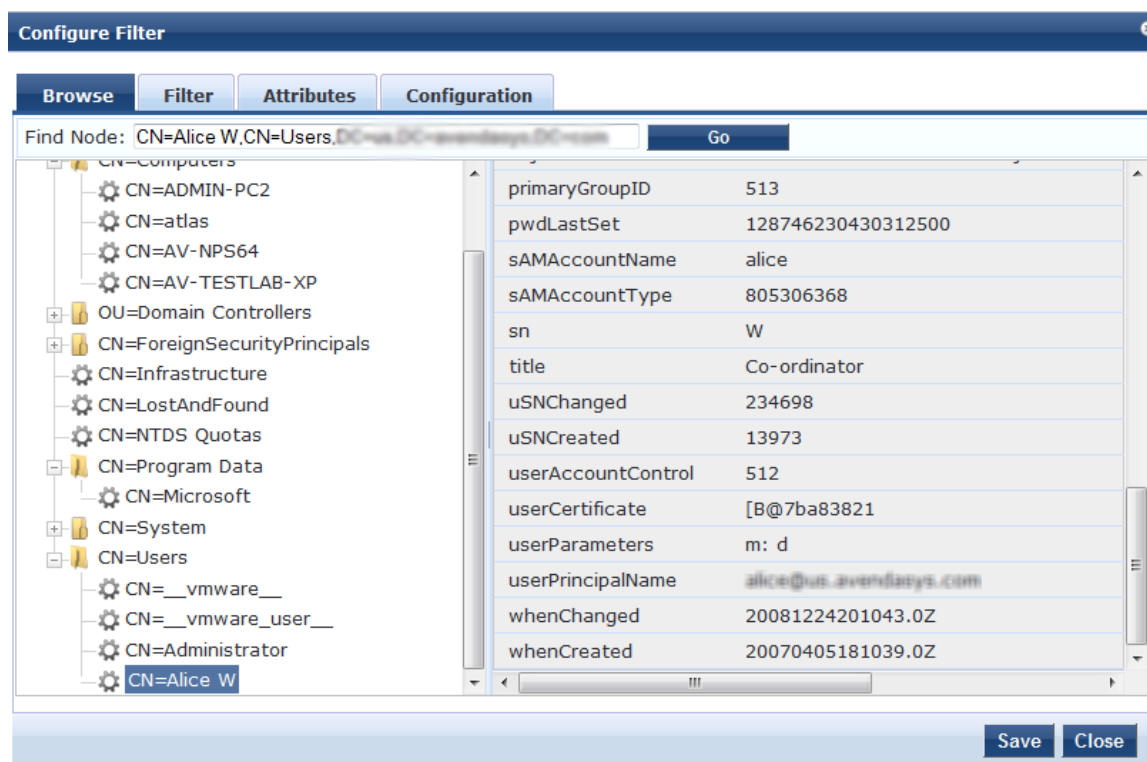
Directory	Default Filters
	This query fetches all group records (of objectClass groupOfNames), where the member field contains the DN of the user record (UserDN, which is populated after the authentication filter query is executed. The attribute fetched with this filter query is cn, which is the name of the group (this is aliased to a more readable name: groupName)).
Add More Filters	Click this button to open the Authentication Sources > Add page to open the Configure Filter page. From this page, you can define a filter query and the related attributes to be fetched.

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 the read-only mode. Selecting a leaf node (a node that has no children) displays the attributes associated with that node.

The following image is an example of the **AD/LDAP Configure Filter - Browse** tab:

Figure 162: AD/LDAP Configure Filter - Browse Tab



The following table describes the **AD/LDAP Configure Filter Page - Browse** tab parameters:

Table 92: AD/LDAP Configure Filter Page - Browse Tab Parameters

Navigation	Description
Find Node	Find the node by entering the DN and clicking the Go button.

Filter Tab

The **Filter** tab provides an LDAP browser interface to define the filter search query. You can define the attributes used in the filter query using this interface.

The following image is an example of the **AD/LDAP Create Filter Page - Filter** tab:

Figure 163: Active Directory/LDAP Create Filter Page - Filter Tab

The screenshot shows the 'Configure Filter' dialog box with the 'Filter' tab selected. The 'Find Node' field contains 'CN=Alice W,CN=Users' and the 'Go' button is visible. The tree view on the left shows the LDAP hierarchy, with 'CN=Alice W' selected. The right pane lists attributes for the selected node, including 'objectSid', 'primaryGroupID', 'pwdLastSet', 'sAMAccountName', 'sAMAccountType', 'sn', 'title', 'uSNChanged', and 'uSNCreated'. The 'Selected attributes for filter' table at the bottom shows two entries: 'sAMAccountName' with a value of 'Authentication:Username' and a second entry with a value of '%(Authentication:Username)'.

Name	Value
1. sAMAccountName	Authentication:Username
2. Click to add...	%(Authentication:Username)



Policy Manager is pre-configured with filters and selected attributes for Active Directory and generic LDAP directory. Create new filters only if you need Policy Manager to fetch role mapping attributes from a new type of record.



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

The following table describes the **Configure Filter Page - Filter** tab parameters:

Table 93: *Configure Filter Page - Filter Tab Parameters*

Parameter	Description
Find Node	Find a node by entering the DN and clicking the Go button.
Select the attributes for filter	This table has a name and value column. You can enter the attribute name in the following two ways: • By selecting a node, inspecting the attributes, and then manually entering the attribute name by clicking on Click to add... in the table row. • By selecting an attribute on the right hand side of the LDAP browser. The attribute name and value are automatically populated in the table. The attribute value can be a value that is 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.

Creating Filters

The goal of filter creation is to help W-Policy Manager to understand how to find a user or device connecting to the network in LDAP or Active Directory. Use the following steps to create a filter:

1. From the **Filter** tab, click on a node that you want to extract user or device information from. For example, browse the **Users** container in Active Directory and select the node for a user (Alice, for example). On the right hand side, you can view the attributes associated with that user.

2. Click on attributes that help W-Policy Manager to 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 with their values.

In this example, if you select **sAMAccountName**, the row in the **Filter** table shows this attribute with a value of Alice (assuming you picked Alice's record as a sample user node).

3. After Step 2, you can have values for a specific record (in this example, Alice's record). Change the value to a dynamic session attribute that helps W-Policy Manager associate a session with a specific record in LDAP/AD.

For example, if you selected the **sAMAccountName** attribute in AD, click the **Value** field and select **%{Authentication:Username}**.

When W-Policy Manager processes an authentication request, **%{Authentication:Username}** is populated with the user ID of the user connecting to the network.

4. Add more attributes from the selected node and continue with Step 2.

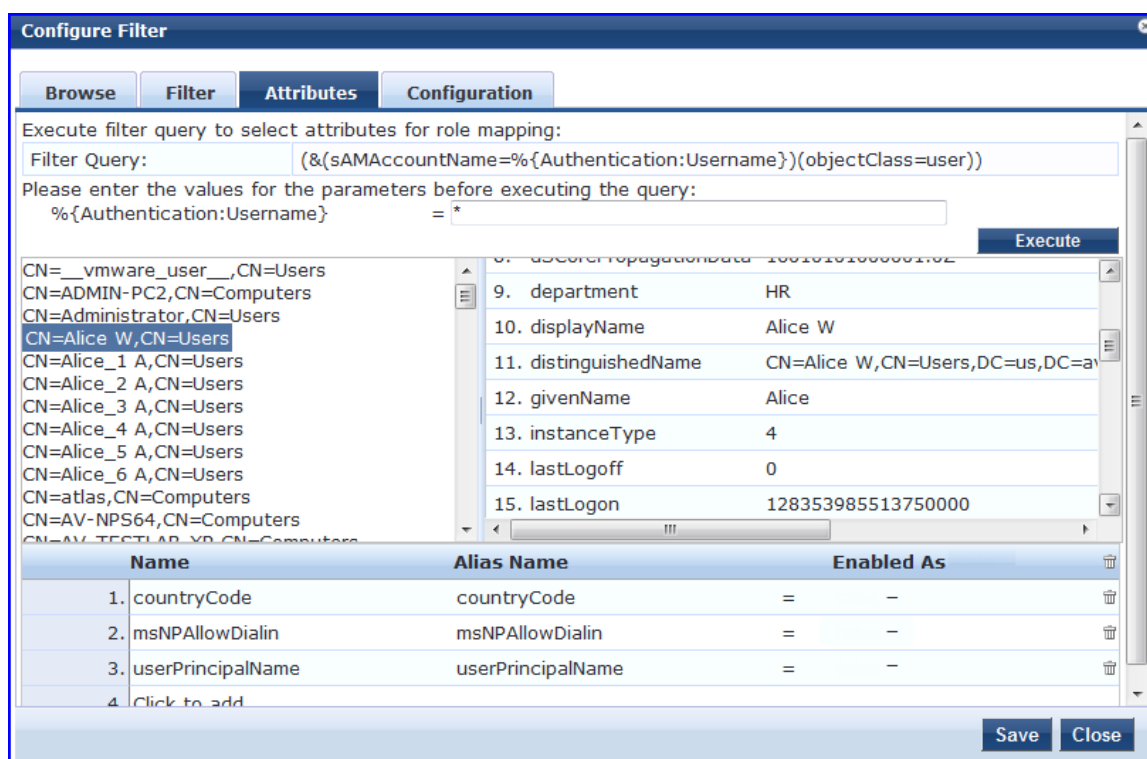
Attributes Tab

The **Attributes** tab defines the attributes to be fetched from the Active Directory or LDAP directory.

You can also enable each attribute as a role, which means the value fetched for this attribute can be used directly in enforcement policies. For more information, see [Configuring Enforcement Policies on page 343](#).

The following figure displays the **Active Directory/LDAP Configure Filter - Attributes** tab:

Figure 164: Active Directory/LDAP Configure Filter - Attributes Tab



The following table describes the **Active Directory/LDAP Configure Filter Page - Attributes** tab parameters:

Table 94: Active Directory/LDAP Configure Filter Page - Attributes Tab Parameters

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 %{Authentication:Username} 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	After entering the values for all dynamic parameters, click Execute to execute the filter query. You can see all entries that match the filter query. Click on one of the entries (nodes) to view 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	Specify the name of the attribute.
Alias Name	Specify the alternative name for the attribute. By default, this is the same as the attribute name.
Enable As	Click this to enable this attribute value to be used directly as a role in an enforcement policy. This bypasses the step of assigning a role in Policy Manager through a role mapping policy.

Configuration Tab

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.

The following figure displays the **Configure Filter - Configuration** tab:

Figure 165: Configure Filter Popup - Configuration Tab

Name	Alias Name	Data type	Enabled As	
1. countryCode	countryCode	String	-	
2. msNPAllowDialin	msNPAllowDialin	Boolean	-	
3. userPrincipalName	userPrincipalName	String	-	
4. Click to add...				

Modify Default Filters

When you add a new authentication source of type Active Directory or LDAP, a few default filters and attributes are populated. You can modify these pre-defined filters by selecting a filter on the **Authentication > Sources > Attributes** tab. This opens the **Configure Filter** page for the specified filter.



A minimum of 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 are rejected.

Figure 166: Modify Default Filters - Configuration Tab

Name	Alias Name	Data type	Enabled As	
1. dn	UserDN	String	-	
2. department	Department	String	☐ Role ☒ Attribute	
3. title	Title	String	Attribute	
4. company	company	Integer		
5. memberOf	memberOf	Date-Time	-	
6. telephoneNumber	Phone	String	Attribute	
7. mail	Email	String	Attribute	
8. displayName	Name	String	Attribute	
9. Click to add...				

The attributes that are defined for the authentication source display as attributes in role mapping policy rules editor under the authorization source namespace.

Then, on the **Role Mappings - Rules Editor** page, the operator values that display are based on the **Data type** specified here.

For example, if you modify the Active Directory **department** to be an integer rather than a string, then the list of operator values populate with values that are specific to integers.

Summary Tab

You can use the **Summary** tab to view configured parameters. The following figure is an example of the **Generic LDAP - Summary** tab:

Figure 167: *Generic LDAP - Summary Tab*

Configuration » Authentication » Sources » Add
Authentication Sources

General	Primary	Attributes	Summary
General:			
Name:	Test Auth source		
Description:	Authenticating against the Local DB.		
Type:	Ldap		
Use for Authorization:	Enabled		
Authorization Sources:	[Local User Repository] [Local]		

Generic SQL DB

Policy Manager can perform MSCHAPv2 and PAP/GTC authentication against any Open Database Connectivity (ODBC) compliant SQL database such as Microsoft SQL Server, Oracle, MySQL, or PostgreSQL. Specify a stored procedure to query the relevant tables and retrieve role mapping attributes by using filters.

Configure the primary and backup servers, session details, filter query, and role mapping attributes to fetch the Generic SQL authentication sources on the following tabs:

- [General Tab on page 208](#)
- [Primary Tab on page 209](#)
- [Attributes Tab on page 210](#)
- [Summary Tab on page 212](#)

The **Configuration > Authentication > Sources > Add** page includes two configuration options for managing existing Generic SQL DB authentication source. The **Clear Cache** option on the main page clears the attributes cached by Policy Manager for all entities that authorize against this serve, and the **Copy** option creates a copy of this authentication/authorization source.

General Tab

The **General** tab labels the authentication source and defines session details, authorization sources, and backup server details. The following figure displays the **Generic SQL DB - General** tab:

Figure 168: *Generic SQL DB - General Tab*

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:

Cache Timeout: seconds

Backup Servers Priority:

[Back to Authentication Sources](#)

The following table describes the **General SQL DB - General** parameters:

Table 95: *General SQL DB - General Tab Parameters*

Parameter	Description
Name	Specify the name of the authentication source.
Description	Provide the additional information that helps to identify the authentication source.
Type	Select the type of source. In this context, select Generic SQL DB .
Use for Authorization	Enable this option to request 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 the Use for Authorization field is enabled. This check box is enabled by default.

Table 95: General SQL DB - General Tab Parameters (Continued)

Parameter	Description
Authorization Sources	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 to the list of authorization sources. Click Remove to remove the authorization source from the list. If Policy Manager authenticates the user or device from this authentication source, then Policy Manager also fetches role mapping attributes from these additional authorization sources. NOTE: You can specify additional authorization sources at the service level. Policy Manager fetches role mapping attributes irrespective of which authentication source the user or device was authenticated against.
Backup Servers	To add a backup server, click Add Backup . From the Backup 1 tab, you can specify connection details for a backup server (same fields as for primary server that are specified below). To remove a backup server, select the server name and click Remove . Select 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.
Cache Timeout	Policy Manager caches attributes fetched for an authenticating entity. This parameter controls the time period for which the attributes are cached.

Primary Tab

The **Primary** tab defines the settings for the primary server. The following figure displays the **General SQL DB - Primary** tab:

Figure 169: General SQL DB - Primary Tab

Configuration » Authentication » Sources » Add

Authentication Sources

General	Primary	Attributes	Summary

Connection Details	
Server Name:	
Port (Optional):	(Specify only if you want to override the default value)
Database Name:	
Login Username:	
Login Password:	
Timeout:	10 seconds
ODBC Driver:	PostgreSQL
Password Type:	Cleartext

The following table describes the **Generic SQL DB - Primary** parameters:

Table 96: *Generic SQL DB - Primary Tab Parameters*

Parameter	Description
Server Name	Enter the hostname or IP address of the database server.
Port (Optional)	Specify a port value to override the default port.
Database Name	Enter the name of the database from which records can be retrieved.
Login Username	Enter the name of the user used to log into the database. This account must have read access to all the attributes that need to be retrieved by the specified filters.
Password	Enter the password for the user account entered in the Login Username field.
Timeout	Enter the duration in seconds that Policy Manager waits before attempting to fail over from primary to backup servers (in the order in which they are configured).
ODBC Driver	Select the ODBC driver (Postgres, Oracle11g, or MSSQL) to connect to the database. MySQL is supported in versions 6.0 and later. Dell does not ship MySQL drivers by default. If you require MySQL, contact Dell support at dell.com/support to get the required patch. This patch does not persist across upgrades. If you are using MySQL, you should contact support before upgrading. If you connect to a Microsoft SQL server using Integrated Authentication, the login username in the authentication source, formatted as either domain/username or UPN (User Principal Name), the backslash (\) and at-sign (@) characters in addition to the hyphen and underscore characters are supported.
Password Type	Specify how the user password is stored in the database: • Cleartext : Password is stored as clear, unencrypted text. • NT Hash: Password is stored with an NT hash using MD4. • LM Hash : Password is stored with a LAN Manager Hash using DES. • SHA: Password is stored with a Secure Hash Algorithm (SHA) hash. • SHA256: Password is stored with an SHA-256 hash function.

Attributes Tab

The **Attributes** tab defines the SQL DB query filters and the attributes to be fetched by using those filters. The following figure displays the **Generic SQL DB - Attributes** tab:

Figure 170: *Generic SQL DB - Attributes Tab*

Specify filters used to query for authentication and authorization attributes

Filter Name	Attribute Name	Alias Name	Enabled As
1. Authentication	department	department	Attribute

[Add More Filters](#)
[Back to Authentication Sources](#)
[Next >](#)
[Save](#)
[Cancel](#)

The following table describes the **Generic SQL DB - Attributes (Filter List)** parameters:

Table 97: *Generic SQL DB - Attributes Tab (Filter List) Parameters*

Tab	Parameter/Description
Filter Name	Specifies the name of the filter.
Attribute Name	Specifies the name of the SQL DB attributes defined for this filter.
Alias Name	Specifies an alias name for each attribute name selected for the filter.
Enabled As	Indicates whether the filter is enabled as a role or attribute type. This can also be blank.
Add More Filters	Click this button to open the Configure Filter page. Use this page to define a filter query and the related attributes to be fetched from the SQL DB store. Figure 171 displays the Generic SQL DB - Configure Filter page.

The following figure displays the **Generic SQL DB - Configure Filter** page:

Figure 171: *Generic SQL DB - Configure Filter Page*

Configure Filter

Configuration

Filter Name:

Filter Query:

```
SELECT user_credential(password) AS User_Password,
CASE WHEN enabled = FALSE THEN 225
      WHEN ((start_time > now()) OR ((expire_time is not null) AND
(expire_time <= now()))) THEN 226
```

Name	Alias Name	Data type	Enabled As
1. sponsor_name	Owner	String	-
2. Click to add...			

[Save](#)
[Close](#)

The following table describes the **Generic SQL DB - Configure Filter** parameters:

Table 98: *Generic SQL DB Configure Filter Page Parameters*

Parameter	Description
Filter Name	Enter the name of the filter.
Filter Query	Specify an SQL query to fetch the attributes from the user or device record in DB.
Name	Specify the name of the attribute.
Alias Name	Specify the name for the attribute. By default, this is the same as the attribute name.
Data Type	Specify the data type for this attribute such as String, Integer, or Boolean.
Enabled As	Specify whether this value to be used directly as a role or attribute in an enforcement policy. This bypasses the step of having to assign a role in Policy Manager through a role mapping policy.

Summary Tab

Use the **Summary** tab to view the parameters configured in the **General**, **Primary**, and **Attributes** tabs. The following figure displays the **Generic SQL DB - Summary** tab:

Figure 172: *Generic SQL DB - Summary Tab*

Configuration » Authentication » Sources » Add
Authentication Sources

General	Primary	Attributes	Summary
General:			
Name:	Test Repository		
Description:	Authenticate users against Policy Manager local user database.		
Type:	Sql		
Use for Authorization:	Enabled		
Authorization Sources:	[Local User Repository] [Local]		
Primary:			
Server Name:	10.17.4.200		
Port (Optional):	1333		
Database Name:	Test DB		
Login Username:	admin		
Login Password:	*****		
Timeout:	10		
ODBC Driver:	PostgreSQL		
Password Type:	Cleartext		
Attributes:			
Filters :	-		

HTTP

The HTTP authentication source relies on the GET method to retrieve information. The client submits a request, and then the server returns a response. All request parameters are included in the URL. For example, **URL:** **https://hostname/websevice/.../{Auth:Username}?param1=%{...}&param2=value2**. HTTP relies on the assumption that the connection between the client and server is secure and can be trusted.

Configure primary and backup servers, session details, filter query, and role mapping attributes to fetch HTTP authentication sources using the following tabs:

- [General Tab on page 213](#)
- [Primary Tab on page 214](#)
- [Attributes Tab on page 215](#)

- [Summary Tab on page 217](#)

General Tab

The **General** tab labels the authentication source and defines session details, authorization sources, and backup server details. The following figure displays the **HTTP - General** tab:

Figure 173: HTTP - 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 Priority:

[Back to Authentication Sources](#)

The following table describes the **HTTP - General** tab parameters:

Table 99: HTTP - General Tab Parameters

Parameter	Description
Name	Specify the name of the authentication source.
Description	Provide the additional information that helps to identify the authentication source.
Type	Select the type of source. In this context, select HTTP .

Table 99: HTTP - General Tab Parameters (Continued)

Parameter	Description
Use for Authorization	Enable this option to request W-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 the Use for Authorization field is enabled. This check box is enabled by default.
Authorization Sources	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 the selected additional resource from the list. If Policy Manager authenticates the user or device from this authentication source, then also fetches role mapping attributes from these additional authorization sources. NOTE: You can specify additional authorization sources at the service level. Policy Manager fetches role mapping attributes irrespective of which authentication source the user or device was authenticated against.
Backup Servers	To add a backup server, click Add Backup . From the Backup 1 tab, you can specify connection details for a backup server (same fields applicable for primary server specified below). To remove a backup server, select the server name and click Remove . Select 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.

Primary Tab

The **Primary** tab defines the settings for the primary server. The following figure displays the **HTTP - Primary** tab:

Figure 174: HTTP - Primary Tab

Configuration » Authentication » Sources » Add

Authentication Sources

The screenshot shows the 'HTTP - Primary' configuration tab. It includes a 'Connection Details' section with input fields for 'Base URL:', 'Login Username:', and 'Login Password:'. The interface is part of a larger configuration window titled 'Authentication Sources' with tabs for 'General', 'Primary', 'Attributes', and 'Summary'. Navigation buttons at the bottom include 'Back to Authentication Sources', 'Next >', 'Save', and 'Cancel'.

The following table describes the **HTTP - Primary** tab parameters:

Table 100: *HTTP - Primary Tab Parameters*

Parameter	Description
Base URL	Enter the base URL (host name) or IP address of the HTTP server. For example, http://<hostname> or <fully-qualified domain name>:xxxx, where xxxx is the port to access the HTTP Server.
Login Username	Enter the name of the user used to log into the database. This account must have read access to all the attributes that need to be retrieved by the specified filters.
Password	Enter the password for the user account entered in the Login Username field.

Attributes Tab

The **Attributes** tab defines the HTTP query filters and the attributes to be fetched by using those filters.

Figure 175: *HTTP - Attributes Tab*

Specify filters used to query for authentication and authorization attributes

Filter Name	Attribute Name	Alias Name	Enabled As
1. Authentication	department	department	Attribute

[Add More Filters](#)
[Back to Authentication Sources](#)
[Next >](#)
[Save](#)
[Cancel](#)

The following table describes the **HTTP - Attributes** tab parameters:

Table 101: *HTTP - Attributes tab (Filter List) Parameters*

Parameter	Description
Filter Name	Displays the name of the filter.
Attribute Name	Specifies the name of the SQL DB attributes defined for this filter.
Alias Name	Specifies the name of an alias name for each attribute name selected for the filter.
Enabled As	Indicates whether an attribute is enabled as a role.
Add More Filters	Opens the Configure Filter page. For more information, see Add More Filters on page 216 .

Add More Filters

The **Configure Filter** page defines a filter query and the related attributes to be fetched from the SQL DB store. The following figure displays the **HTTP Filter Configure** page:

Figure 176: HTTP Filter Configure Page

Name	Alias Name	Data type	Enabled As
1. department	Departent	String	Attribute
2. title	Title	String	Attribute
3. name	Name	String	☒ Role ☒ Attribute
4. Click to add...			

The following table describes the **HTTP Configure - Filter** parameters:

Table 102: HTTP Configure Filter Page Parameters

Parameter	Description
Filter Name	Displays the name of the selected filter.
Filter Query	Specifies the HTTP path (without the server name) to fetch the attributes from the HTTP server. For example, if the full path name to the filter is http server URL = http://<hostname or fqdn>:xxxx/abc/def/xyz, you enter /abc/def/xyz.
Name	Specifies the name of the attribute.
Alias Name	Specifies the alias name for the attribute. By default, this is the same as the attribute name.
Data Type	Specifies the data type for this attribute such as String, Integer, and Boolean.
Enabled As	Specify whether the value to be used directly as a role or attribute in an enforcement policy. This bypasses the step of assigning a role in Policy Manager through a role mapping policy.

Summary Tab

You can use the **Summary** tab to view configured parameters. The following figure is an example of the **HTTP - Summary** tab:

Figure 177: HTTP - Summary Tab

Configuration » Authentication » Sources » Add
Authentication Sources

General	Primary	Attributes	Summary
General:			
Name:	Test Auth Source		
Description:	Authenticating against the Local DB		
Type:	HTTP		
Use for Authorization:	Enabled		
Authorization Sources:	[Local User Repository] [Local]		
Primary:			
Base URL:	-		
Login Username:	admin		
Login Password:	*****		
Attributes:			
Filters :	-		

Kerberos

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 Microsoft Active Directory server. It is mandatory to pair this source type with an authorization source (identity store) containing user records.

You can configure Kerberos authentication sources using the following tabs:

- [General Tab on page 218](#)
- [Primary Tab on page 219](#)
- [Summary Tab on page 220](#)

General Tab

The **General** tab labels the authentication source and defines session details, authorization sources, and backup server details. The following figure displays the **Kerberos - General** tab:

Figure 178: Kerberos - General Tab

Authentication Sources

The screenshot shows the 'General' tab of the 'Authentication Sources' configuration window. The window has three tabs: 'General' (selected), 'Primary', and 'Summary'. The 'General' tab contains the following fields and controls:

- Name:** A text input field.
- Description:** A text area with a small '...' icon at the bottom right.
- Type:** A dropdown menu with 'Kerberos' selected.
- Use for Authorization:** A checkbox labeled 'Enable to use this authentication source to also fetch role mapping attributes'.
- Authorization Sources:** A list box with a '-- Select --' dropdown at the bottom. To the right are 'Remove' and 'View Details' buttons.
- Backup Servers Priority:** A list box with 'Move Up' and 'Move Down' buttons to its right.
- At the bottom of the list box area are 'Add Backup' and 'Remove' buttons.

At the bottom of the window, there is a navigation bar with a blue arrow and the text 'Back to Authentication Sources', and three buttons: 'Next >', 'Save', and 'Cancel'.

The following table describes the **Kerberos - General** parameters:

Table 103: Kerberos - General Tab Parameters

Parameter	Description
Name	Specify the name of the authentication source.
Description	Provide the additional information that helps to identify the authentication source.
Type	Select the type of source. In this context, select Kerberos .

Table 103: Kerberos - General Tab Parameters (Continued)

Parameter	Description
Use for Authorization	Disable in this context.
Authorization Sources	Specify one or more authorization sources from which role mapping attributes to be fetched. 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 the selected authentication source from the list. NOTE: You can specify additional authorization sources at the service level. Policy Manager fetches role mapping attributes irrespective of which authentication source the user or device was authenticated against.
Backup Servers	To add a backup kerberos server, click Add Backup. From the Backup 1 tab, you can specify connection details for a backup server (same fields applicable for primary server specified below). To remove a backup server, select the server name and click Remove. Select 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.

Primary Tab

The **Primary** tab defines the settings for the primary server. The following figure displays the **Kerberos - Primary** tab:

Figure 179: Kerberos - Primary Tab

Configuration » Authentication » Sources » Add

Authentication Sources

General **Primary** Summary

Connection Details

Hostname:

Port:

Realm:

Service Principal:

Service Principal Password:

[Back to Authentication Sources](#) [Next >](#) [Save](#) [Cancel](#)

The following table describes the **Kerberos - Primary** parameters:

Table 104: Kerberos - Primary Tab Parameters

Parameter	Description
Hostname	Specify the name of the host or the IP address of the kerberos server.
Port	Specify the port at which the token server listens for kerberos connections. The default port is 88.
Realm	Specify the domain of authentication. In the case, specify Kerberos domain.
Service Principal Name	Enter the identity of the service principal as configured in the Kerberos server.
Service Principal Password	Enter the password for the service principal.

Summary Tab

You can use the **Summary** tab to view configured parameters. The following figure displays the **Kerberos - Summary** tab:

Figure 180: Kerberos - Summary Tab

Configuration » Authentication » Sources » Add
Authentication Sources

General	Primary	Summary
General:		
Name:	Test Auth Source	
Description:	testing auth source against local DB.	
Type:	Kerberos	
Use for Authorization:	Disabled	
Authorization Sources:	[Local User Repository] [Local]	
Primary:		
Hostname:	10.17.4.200	
Port:	88	
Realm:	-	
Service Principal:	admin	
Service Principal Password:	*****	

Okta

You can use Okta as an authentication source only for servers of the type Dell Application Authentication. Configure Okta authentication sources on the following tabs:

- [General Tab on page 221](#)
- [Primary Tab on page 222](#)
- [Attributes Tab on page 223](#)
- [Summary Tab on page 225](#)

General Tab

The **General** tab labels the authentication source and defines session details, authorization sources, and backup server details. The following figure is an example of the **Okta - General** tab:

Figure 181: *Okta - General Tab*

Configuration » Authentication » Sources » Add

Authentication Sources

The screenshot displays the 'General' tab of the 'Authentication Sources' configuration page. It includes input fields for 'Name' and 'Description', a 'Type' dropdown menu set to 'Okta', a checked 'Use for Authorization' checkbox, an empty 'Authorization Sources' list with 'Remove' and 'View Details' buttons, 'Server Timeout' (10 seconds) and 'Cache Timeout' (36000 seconds) fields, and a 'Backup Servers Priority' list with 'Move Up', 'Move Down', 'Add Backup', and 'Remove' buttons. At the bottom, there are navigation buttons: 'Back to Authentication Sources', 'Next >', 'Save', and 'Cancel'.

The following table describes the **Okta - General** parameters:

Table 105: *Okta - General Tab Parameters*

Parameter	Description
Name	Specify the name of the authentication source.
Description	Provide the additional information that helps to identify the authentication source.
Type	Select the type of source. In this context, select Okta .
Use for Authorization	Enable this check box to request W-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 the Use for Authorization field is enabled. This check box is enabled by default.

Table 105: Okta - General Tab Parameters (Continued)

Parameter	Description
Server Timeout	Specify the duration in number of seconds that W-Policy Manager waits before considering this server unreachable. If multiple backup servers are available, then this value indicates the duration in number of seconds that W-Policy Manager waits before attempting to fail over from the primary to the backup servers in the order in which they are configured.
Cache Timeout	W-Policy Manager caches attributes fetched for an authenticating entity. This parameter controls the duration in number of seconds for which the attributes are cached.
Backup Servers Priority	Click Add Backup to add a backup server. From the Backup 1 tab, you can specify connection details for a backup server (same fields as for primary server that are specified below). To remove a backup server, select the server name and click Remove . Select 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.

Primary Tab

The **Primary** tab defines the settings for the primary server. The following figure displays the **Okta - Primary** tab:

Figure 182: Okta - Primary Tab

Configuration » Authentication » Sources » Add

Authentication Sources

The screenshot shows the 'Okta - Primary' configuration page. It has four tabs: 'General', 'Primary' (which is active), 'Attributes', and 'Summary'. Under the 'Primary' tab, there is a 'Connection Details' section with two input fields: 'URL:' and 'Authorization Token:'. At the bottom of the page, there is a navigation bar with a blue arrow pointing left and the text 'Back to Authentication Sources', followed by three buttons: 'Next >', 'Save', and 'Cancel'.

The following table describes the **Okta - Primary** parameters:

Table 106: Okta - Primary Tab Parameters

Parameter	Description
Connection Details	
URL	Enter the address of the Okta server.
Authorization Token	Enter the authorization token provided by Okta support.

Attributes Tab

The **Attributes** tab defines the Okta query filters and the attributes to be fetched by using those filters. The following figure displays the **Okta - Attributes** tab:

Figure 183: *Okta - Attributes Tab*

Configuration » Authentication » Sources » Add

Authentication Sources

The screenshot shows the 'Attributes' tab of the 'Add Authentication Sources' page. It features a table with columns: Filter Name, Attribute Name, Alias Name, and Enabled As. A single filter is listed: '1. Group' with attribute 'name' and alias 'Groups'. Below the table is an 'Add More Filters' button. At the bottom, there are navigation buttons: 'Back to Authentication Sources', 'Next >', 'Save', and 'Cancel'.

Filter Name	Attribute Name	Alias Name	Enabled As
1. Group	name	Groups	-

[Add More Filters](#)

[Back to Authentication Sources](#) [Next >](#) [Save](#) [Cancel](#)

The following table describes the **Okta - Attributes** parameters:

Table 107: *Okta - Attributes Tab Parameters*

Parameter	Description
Filter Name	Displays the name of the filter. You can configure only Group for Okta.
Attribute Name	Specifies the name of the LDAP/AD attributes defined for this filter.
Alias Name	Specifies the alias name for each attribute name selected for the filter.
Enable As	Specifies whether value to be used directly as a role or attribute in an enforcement policy. This bypasses the step of assigning a role in Policy Manager through a role mapping policy.
Add More Filters	Click this button to open the Configure Filter page. Refer to Add More Filters on page 224 .

Add More Filters

The **Configure Filter** page defines a filter query and the related attributes to be fetched from the SQL DB store. The following figure displays the **Okta - Configure Filter** page:

Figure 184: Okta - Configure Filter Page

Name	Alias Name	Data type	Enabled As	
1. name	Groups	String	-	
2. Click to add...				

The following table describes the **Okta Configure Filter** parameters:

Table 108: Okta Configure Filter Page

Parameter	Description
Filter Name	Enter the name of the filter.
Filter Query	Specifies an SQL query to fetch attributes from the user or device record in DB.
Name	Displays the name of the attribute.
Alias Name	Specifies an alias name for the attribute. By default, this is the same as the attribute name.
Data Type	Specifies the data type for this attribute such as String, Integer, and Boolean.
Enabled As	Specify whether this value is to be used directly as a role or attribute in an enforcement policy. This bypasses the step of having to assign a role in Policy Manager through a role mapping policy.

Summary Tab

You can use the **Summary** tab to view configured parameters. The following figure displays the **Okta - Summary** tab:

Figure 185: Okta - Summary Tab

Configuration » Authentication » Sources » Add
Authentication Sources

General	Primary	Attributes	Summary
General:			
Name:	Test Auth Source		
Description:	Authenticating against the Local DB.		
Type:	Okta		
Use for Authorization:	Enabled		
Authorization Sources:	[Local User Repository] [Local]		
Primary:			
URL:	-		
Authorization Token:	*****		
Attributes:			
Filters :	1. /api/v1/users/{Authentication:OktaUserId}/groups		

RADIUS Server

You can use the **RADIUS Server** as an authentication source to allow W-ClearPass to query a third-party **RADIUS Server** for authentication. Configure **RADIUS Server** authentication sources on the following tabs:

- [General Tab on page 225](#)
- [Primary Tab on page 226](#)
- [Attributes Tab on page 227](#)
- [Summary Tab on page 228](#)

General Tab

The **General** tab labels the authentication source and defines session details, authorization sources, and backup server details. The following figure displays the **RADIUS Server - General** tab:

Figure 186: RADIUS Server - General Tab

Configuration » Authentication » Sources » Add

Authentication Sources

General	Primary	Attributes	Summary
Name:			
Description:			
Type:	RADIUS Server		
Use for Authorization:	☒ Enable to use this Authentication Source to also fetch role mapping attributes		
Authorization Sources:	Remove View Details -- Select --		
Server Timeout:	10 seconds		
Backup Servers Priority:	Move Up Move Down Add Backup Remove		
Back to Authentication Sources			
Next > Save Cancel			

The following table describes the **Radius Server - General** parameters:

Table 109: *Radius Server - General Tab Parameters*

Parameter	Description
Name	Specify the name of the authentication source.
Description	Provide the additional information that helps to identify the authentication source.
Type	Select the type of source. In this context, select RADIUS Server .
Use for Authorization	Enable this check box to request W-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 the Use for Authorization field is enabled. This check box is enabled by default.
Server Timeout	Specify the duration in number of seconds that W-Policy Manager waits before considering this server unreachable. If multiple backup servers are available, then this value indicates the duration in number of seconds that W-Policy Manager waits before attempting to fail over from the primary to the backup servers in the order in which they are configured.
Backup Servers Priority	Click Add Backup to add a backup server. From the Backup 1 tab, you can specify connection details for a backup server (same fields as for primary server that are specified below). To remove a backup server, select the server name and click Remove . Select 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.

Primary Tab

The **Primary** tab defines the settings for the primary server. The following figure displays the **RADIUS Server - Primary** tab:

Figure 187: *RADIUS Server - Primary Tab*

Configuration » Authentication » Sources » Add

Authentication Sources

The screenshot shows the 'Authentication Sources' configuration window with the 'Primary' tab selected. The 'Connection Details' section contains three input fields: 'Server Name' (empty), 'Port' (set to 1812), and 'Secret' (empty). At the bottom, there are four buttons: 'Back to Authentication Sources' (with a left arrow), 'Next >', 'Save', and 'Cancel'.

The following table describes the **RADIUS Server - Primary** parameters:

Table 110: RADIUS Server - Primary Tab Parameters

Parameter	Description
Connection Details	
Server Names	Enter the name of the RADIUS Server.
Port	The default port number is 1812. You may enter a different port number if required.
Secret	Enter the secret key for authentication.

Attributes Tab

The **Attributes** tab defines the Okta query filters and the attributes to be fetched by using those filters. The following figure displays the **RADIUS Server - Attributes** tab:

Figure 188: RADIUS Server - Attributes Tab

Configuration » Authentication » Sources » Add

Authentication Sources

General Primary **Attributes** Summary

RADIUS Pre Proxy Attributes:

Type	Name	Value
1. Click to add...		

RADIUS Post Proxy Attributes:

Type	Name	Enabled as Role
1. Click to add...		

[Back to Authentication Sources](#) Next > Save Cancel

The following table describes the **RADIUS Server - Attributes** parameters:

Table 111: RADIUS Server - Attributes Tab Parameters

Parameter	Description
RADIUS Pre-Proxy attributes	The following attributes that can be set prior to the proxy authentication: Type - Select a type from the drop-down. Name - Select a name from the drop-down. Value - Enter a value in the text box. Save the changes by clicking the Save icon that appears at the end of the row.
RADIUS Post-Proxy attributes	The attributes for the post-proxy authentication are identical except that these can be set after the proxy authentication. Type - Select a type from the drop-down. Name - Select a name from the drop-down. Value - Enter a value in the text box. Save the changes by clicking the Save icon that appears at the end of the row.

Summary Tab

You can use the **Summary** tab to view configured parameters. The following figure displays the **RADIUS Server - Summary** tab:

Figure 189: RADIUS Server - Summary Tab

Configuration » Authentication » Sources » Add
Authentication Sources

General	Primary	Attributes	Summary
General:			
Name:	Test Auth Source		
Description:	Testing against the Loca DB.		
Type:	RadiusServer		
Use for Authorization:	Enabled		
Authorization Sources:	[Local User Repository] [Local]		
Primary:			
Server Name:	10.17.4.197		
Port:	1812		
Secret:	*****		
Attributes:			
RADIUS Pre Proxy Attributes:			
Type	Name	Value	
1. Radius:IETF	ARAP-Password	=	67
RADIUS Post Proxy Attributes:			
Type	Name	Enabled as Role	
1. Radius:Microsoft	MS-ARAP-PW-Change-Reason	=	true

Static Host Lists

This section provides the following information:

- [About Static Host Lists](#)
- [Adding a Static Host List to ClearPass](#)
- [Adding a Static Host List as an Authentication Source](#)
- [Static Hosts Lists Configuration Summary](#)

About Static Host Lists

You can configure primary and backup servers, session details, and the list of static hosts for **Static Host List** authentication sources.

A static host list often functions, in the context of the service, as a whitelist or a blacklist. Therefore, static host lists are configured independently at the global level.

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

- 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.



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

For more information about static host lists, see [Managing Static Host Lists on page 253](#).

Adding a Static Host List to ClearPass

To add a static host list to W-ClearPass:

1. Navigate to the **Configuration > Identity > Static Host Lists** page .

The **Static Hosts Lists** page appears.

Figure 190: *Static Host Lists Page*

2. Click **Add**.

The **Add Static Host List** dialog appears.

Figure 191: *Adding a Static Host List*

3. Enter the parameters to add a static host list as described in [Table 112](#).

Table 112: *Add Static Host List Parameters*

Parameter	Action/Description
Name	1. Enter the name of the static host list.
Description	2. Enter the description that provides additional information about the static host list.
Host Format	3. Select a format for expression of the address: • Subnet • Regular Expression • List
Host Type	4. Select a host type:

Table 112: Add Static Host List Parameters (Continued)

Parameter	Action/Description
	• IP Address • MAC Address
Subnet	5. Enter the subnet address.
	6. Click Save .

The new static host list is now available to be added as an authentication source (as described in the next section).

Adding a Static Host List as an Authentication Source

To add a Static Host List as an authentication source:

1. Navigate to **Configuration > Authentication > Sources**.

The **Authentication Sources** page appears.

Figure 192: Authentication Sources Page

Configuration » Authentication » Sources

Authentication Sources

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

Filter: Name contains

Show 10 records

#	Name	Type	Description
1.	[Admin User Repository]	Local SQL DB	Authenticate users against Policy Manager admin user database
2.	Automation_SHL_SOURCE	Static Host List	
3.	Bangalore-AD	Active Directory	
4.	[Blacklist User Repository]	Local SQL DB	Blacklist database with users who have exceeded bandwidth or session related limits
5.	[Endpoints Repository]	Local SQL DB	Authenticate endpoints against Policy Manager local database
6.	[Guest Device Repository]	Local SQL DB	Authenticate guest devices against Policy Manager local database
7.	[Guest User Repository]	Local SQL DB	Authenticate guest users against eTIPS local database
8.	India_AD	Active Directory	
9.	[Insight Repository]	Local SQL DB	Insight database with session information for users and devices
10.	[Local User Repository]	Local SQL DB	Authenticate users against eTIPS local user database

Showing 1-10 of 20 records

2. Click the **Add** link.

The **Add Authentication Sources** dialog opens.

Figure 193: Specifying a Static Host List as Authentication Source

The screenshot shows the 'Authentication Sources' configuration page with the 'Static Host Lists' tab selected. The page has three tabs: 'General', 'Static Host Lists', and 'Summary'. The 'General' tab is active, showing fields for 'Name', 'Description', 'Type' (set to 'Static Host List'), 'Use for Authorization' (unchecked), and 'Authorization Sources' (empty list). At the bottom, there are buttons for 'Back to Authentication Sources', 'Next >', 'Save', and 'Cancel'.

3. Enter the name and description of the static host list.
4. In the **Type** field, select **Static Host List**.
In this context, the **Use for Authorization** and **Authorization Sources** fields are not configurable.
5. Click **Next**.
The **Static Hosts Lists** dialog appears.
6. From the **Static Host Lists** tab, select a static host list from the drop-down list.
The selected static host list is added to the MAC Address Host Lists (see Figure 194).

Figure 194: Existing Static Host List Added

The screenshot shows the 'Static Host Lists' dialog box. It has three tabs: 'General', 'Static Host Lists', and 'Summary'. The 'Static Host Lists' tab is active, showing a list of 'MAC Address Host Lists' with one entry, 'CPATS SHL MAC List', selected. To the right of the list are buttons for 'Remove', 'View Details', and 'Modify'. At the bottom of the list is a dropdown menu with '--Select--'. To the right of the dialog is a link that says 'Add new Static Host List'.



Only static host lists of type **MAC Address Host Lists** or **MAC Address Regular Expression** can be configured as authentication sources.

- a. To remove the selected static host list, click **Remove**.
 - b. To view the contents of the selected static host list, click **View Details**.
 - c. To modify the selected static host list, click **Modify**.
7. Click **Save**.

Static Hosts Lists Configuration Summary

You can use the **Summary** tab to view the static host list's configuration information.

Figure 195: *Static Hosts Lists Configuration Summary*

Configuration » Authentication » Sources » Add - CPATS Static Host List

Authentication Sources - CPATS Static Host List

Summary	General	Static Host Lists
<u>General:</u>		
Name:	CPATS Static Host List	
Description:	CPATS Static Host List Auth Source	
Type:	SHL	
Use for Authorization:	-	
Authorization Sources:	-	
<u>Static Host Lists:</u>		
MAC Address Host Lists:	1. CPATS SHL MAC List 2. CPATS SHL MAC Regex	

Token Server

W-Policy Manager can perform GTC authentication against any token server than can authenticate users by acting as a RADIUS server (for example, RSA SecurID Token Server) and can authenticate users against a token server and fetch role mapping attributes from any other configured authorization source.

Pair this source type with an authorization source (identity store) containing user records. When using a token server as an authentication source, use the administrative interface to optionally configure a separate authorization server. W-Policy Manager can also use the RADIUS attributes returned from a token server to create role mapping policies. For more information, see [Namespaces on page 845](#).

You configure primary and backup servers, session details, and the filter query and role mapping attributes to fetch for token server authentication sources on the following tabs:

- [General Tab on page 233](#)
- [Primary Tab on page 234](#)
- [Attributes Tab on page 234](#)
- [Summary Tab on page 235](#)

General Tab

The **General** tab labels the authentication source and defines session details, authorization sources, and backup server details. The following figure displays the **Token Server - General** tab:

Figure 196: *Token Server - 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:

Server Timeout: seconds

Backup Servers Priority:

[Back to Authentication Sources](#)

The following table describes the **Token Server - General** parameters:

Table 113: *Token Server - General Tab Parameters*

Parameter	Description
Name	Specify the label of the authentication source.
Description	Provide the additional information that helps to identify the authentication source.
Type	Select the type of authentication. In this context, select Token Server .
Use for Authorization	Enable this check box to instruct W-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 the Use for Authorization field is enabled. This check box is enabled by default
Authorization Sources	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. If Policy Manager authenticates the user or device from this authentication source, then it also fetches role mapping attributes from these additional authorization sources.

Table 113: Token Server - General Tab Parameters (Continued)

Parameter	Description
	NOTE: You can specify additional authorization sources at the service level. Policy Manager fetches role mapping attributes irrespective of which authentication source the user or device was authenticated against.
Server Timeout	Specify the duration in seconds that Policy Manager waits before attempting to fail over from primary to backup servers (in the order in which they are configured).
Backup Servers Priority	To add a backup server, click Add Backup . From the Backup 1 tab, you can specify connection details for a backup server (same fields as for primary server that are specified below). To remove a backup server, select the server name and click Remove . Select 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.

Primary Tab

The **Primary** tab defines the settings for the primary server. The following figure displays the **Token Server - Primary** tab:

Figure 197: Token Server - Primary Tab

The following table describes the **Token Server - Primary** parameters:

Table 114: Token Server - Primary Tab Parameters

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

Attributes Tab

The **Attributes** tab defines the RADIUS attributes to be fetched from the token server. These attributes can be used in role mapping policies. Policy Manager loads all RADIUS vendor dictionaries in the **Type** drop-down list with attributes.

The following figure is an example of the **Token Server - Attributes** tab:

Figure 198: *Token Server - Attributes Tab*

See [Configuring a Role and Role Mapping Policy on page 257](#) for more information. The following table describes the **Token Server - Attribute** parameters:

Table 115: *Token Server - Attribute Tab Parameters*

Parameter	Description
Type	Select the type of authentication source from the drop-down list.
Name	Specifies the name of the token server attributes.
Enabled as Role	Specifies whether value is to be used directly as a role or attribute in an enforcement policy. This bypasses the step of assigning a role in Policy Manager through a role mapping policy.

Summary Tab

The **Summary** tab provides the summarized view of the parameters configured in the **General**, **Primary**, and **Attributes** tab. The following figure displays the **Summary** tab:

Figure 199: *Token Servers - Summary Tab*

Configuration » Authentication » Sources » Add
Authentication Sources

This chapter provides information on the following topics:

- [Configuring Single Sign-On](#)
- [Managing Local Users](#)
- [Adding and Modifying Endpoints](#)
- [Managing Static Host Lists](#)
- [Configuring a Role and Role Mapping Policy](#)

This chapter provides details on the settings required to configure W-ClearPass Policy Manager Identify settings.

The W-Policy Manager database supports storage of user records when a particular class of users is not present in a central user repository (for example, when there is neither Active Directory nor any other database).



To authenticate local users from a particular service, include **Local User Repository** among the authentication sources.

Configuring Single Sign-On

This section provides the following information:

- [SAML Service Provider \(SP\) Configuration](#)
- [SAML Identity Provider \(IdP\) Configuration](#)

The Single Sign-On (SSO) settings on the **Single Sign-On** page allows W-ClearPass users that have signed in to W-ClearPass Policy Manager to access the Onboard, Guest, and Insight applications and W-Policy Manager administration settings without reauthenticating. W-ClearPass provides single sign-on support using the Security Assertion Markup Language (SAML).

This feature also provides differentiated single sign-on access for Guest web login and Guest Operator login (see [Table 116](#) for details).

SAML Service Provider (SP) Configuration

To configure single sign-on service provider settings:

1. Navigate to **Configuration > Identity > Single Sign-On**.

The **Single Sign-On > SAML SP Configuration** dialog opens.

Figure 200: *Configuring Single Sign-On > SAML Service Provider Parameters*

SAML SP Configuration | SAML IdP Configuration

Identity Provider (IdP) URL:

Enable SSO for

Insight	☐	Enable access to Insight application
PolicyManager	☐	Enabled access to Policy Manager administration
Onboard	☐	Enable access to Onboard device provisioning portals
Guest	☐	Enable Guest Web Login access for Guest and Onboard applications
GuestOperators	☐	Enable Guest Operator Login access for Guest and Onboard applications

Identity Provider (IdP) Certificate

Select Certificate:

Note: IdP certificate must be enabled in Certificate Trust List first, if not listed above.

CPPM Service Provider (SP) Metadata

SP Metadata:

SP Metadata URI:

- Select the application(s) you want users to access with single sign-on.
To complete this task, specify the **SAML SP Configuration** tab parameters as described in [Table 116](#).
- Create trusted relationships between a Service Provider and Identity Provider by providing the Identity Provider (IdP) URL and IdP certificate.
To complete this task, specify the **SAML IdP Configuration** tab parameters as described in [Table 117](#).

Table 116: *Single Sign-On Service Provider Configuration Settings*

Parameter	Action/Description
Identity Provider (IdP) URL	1. Enter the URL of the identity provider.
Enable SSO For	2. Select the applications to be enabled for single sign-on: ■ Insight ■ W-Policy Manager ■ Onboard device provisioning portals ■ Guest and Onboard Web Login ■ Guest and Onboard Guest Operator Login ● If you select only the Guest Operator Login, SSO will be enabled for Operator logins only, and Web logins will use standard non-SSO authentication. ● If you select only the Guest Web Login option, SSO will be enabled for Web logins only, and Operator logins will use standard non-SSO authentication. ● If you select both the Guest Operator Login and the Guest Web Login options, Operator logins and Web logins will both use SSO authentication.
Select Certificate	3. Select the Identity Provider (IdP) certificate to use for single sign-on. When you select a certificate, the page displays the following information about the certificate: ■ Subject DN ■ Issuer DN ■ Issue Date/Time ■ Expiry Date/Time

Table 116: *Single Sign-On Service Provider Configuration Settings (Continued)*

Parameter	Action/Description
	■ Validity Status ■ Signature Algorithm ■ Public Key Format ■ Serial Number ■ Enabled This field only displays certificates that are enabled in the certificate trust list. See also Certificate Trust List on page 633.
CPPM Service Provider (SP) Metadata	SP Metadata: 4. To download and view an XML file containing metadata for the Service Provider Uniform Resource Identifier (URI), click Download. Metadata URI : 5. View the Uniform Resource Identifier (URI) for the Service Provider metadata resource.

SAML Identity Provider (IdP) Configuration

To configure single sign-on identity provider settings:

1. Navigate to **Configuration > Identity > Single Sign-On**.
2. Select the **SAML IdP Configuration** tab.

Figure 201: *Configuring Single Sign-On > Identity Provider Parameters*

3. Specify the **SAML IdP Configuration** parameters as described in the following table:

Table 117: *Single Sign-On Identity Provider Configuration Settings*

Parameter	Action/Description
IdP Portal Name	1. Enter the name of the identity provider portal. 2. To download and view an XML file containing metadata for the Identity Provider Uniform Resource Identifier (URI), click Download.
IdP Metadata URI	3. View the Uniform Resource Identifier (URI) for the IdP metadata resource.
Service Provider (SP) Metadata	4. If you upload metadata for an SAML Service Providers, W-ClearPass can upload the SP metadata for validation during the single-sign on process. a. Click Add SP Metadata. b. Enter the name of the service provider. c. Upload the service provider metadata file.

Table 117: *Single Sign-On Identity Provider Configuration Settings (Continued)*

Parameter	Action/Description
CPPM Service Provider (SP) Metadata	SP Metadata section: 5. To download and view an XML file containing metadata for the Service Provider Uniform Resource Identifier (URI), click Download . The Metadata URI: 6. View the location of this metadata file.

Managing Local Users

This section provides the following information:

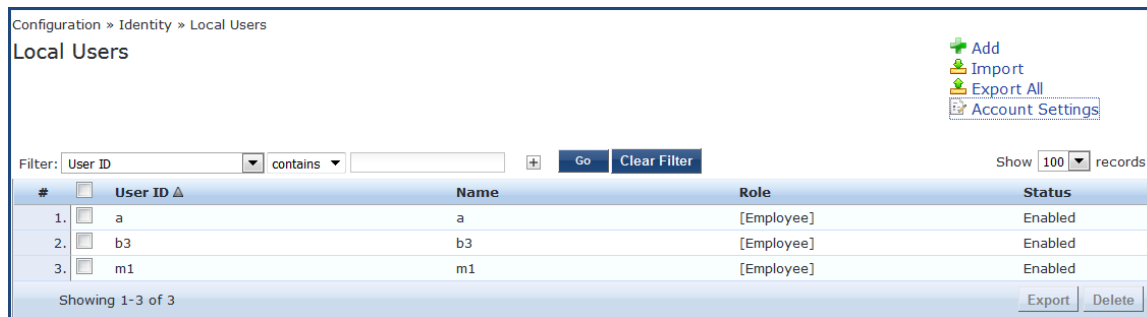
- [Adding a Local User](#)
- [Modifying a Local User Account](#)
- [Importing and Exporting Local Users](#)
- [Setting Password Policy for Local Users](#)
- [Disabling Local User Accounts](#)

W-ClearPass W-Policy Manager lists all local users in the **Local Users** page.

You can also add, import, export, set password policies, and configure the conditions for disabling accounts for the local users using the links provided at the top-right corner of the **Local Users** page.

Figure 202 displays the **Local Users** page:

Figure 202: *Local Users Page*



Configuration » Identity » Local Users				
Local Users				
Filter: User ID contains [] Go Clear Filter				
Show 100 records				
#	User ID	Name	Role	Status
1.	a	a	[Employee]	Enabled
2.	b3	b3	[Employee]	Enabled
3.	m1	m1	[Employee]	Enabled
Showing 1-3 of 3				
Export Delete				

Adding a Local User

To add a local user in the **Local Users** table:

1. Navigate to **Configuration > Identity > Local Users**.
The **Local Users** page opens.
2. Click the **Add** link at the top-right corner the page.
The **Add Local User** page opens (see [Figure 203](#)).

Figure 203: *Adding a Local User*

User ID:	edu_admin
Name:	admin
Password:	••••••••••
Verify Password:	••••••••••
Enable User:	☒ (Check to enable local user)
Change Password:	☐ (Check to force change password on next TACACS+ login)
Role:	[Aruba TACACS read-only Admin] ▼

Attributes	
Attribute	Value
1.	Click to add...

3. Specify the **Add Local User** parameters as described in the following table, then click **Add**:

Table 118: *Adding a Local User Parameters*

Parameter	Action/Description
User ID	1. Specify a user ID.
Name	2. Specify the name for the local user.
Password/ Verify Password	3. Specify a password for the local user, then verify the password.
Enable User	4. You must enable this check box to enable the local user account. Otherwise, the local user account is disabled.
Change Password	5. Enable this check box to allow the user to change the password at the next TACACS+ login (after authenticating with the old password). Once the password is changed successfully, this option is automatically disabled. NOTE: The option to change the password on the next login is applicable for network device administration logins using TACACS+ only.

Table 118: Adding a Local User Parameters (Continued)

Parameter	Action/Description
Role	6. Select a static role to be assigned to the user from the Role drop-down list.
Attributes	
	7. To add attributes for the local users, click Click to add... A new row is created with a drop-down list in the Attribute column. This field is optional. By default, the drop-down list contains the following attributes: ■ Department ■ Designation ■ Email ■ Location ■ Phone ■ Sponsor ■ Title a. To add a custom attribute in the Attribute column, select an attribute from the drop-down list or enter any string. NOTE: If you add a new custom attribute, it is available for selection in the Attribute drop-down list for all local users. b. In the Value column, enter a value for the attribute specified in the corresponding row. NOTE: All attributes entered for a local user are available in the role-mapping rules editor under the LocalUser namespace. c. Click Add. You return to the Local User page where the following message is displayed: <i>User <username> added successfully</i>

Modifying a Local User Account

To modify a local user account:

1. Navigate to the **Configuration > Identity > Local Users** page.
2. Click the **User ID** row that you want to edit.
The **Edit Local User** window opens.

Figure 204: *Modifying a Local User*

Edit Local User

User ID:

Name:

Password:

Verify Password:

Enable User: ☒ (Check to enable local user)

Change Password: ☐ (Check to force change password on next TACACS+ login)

Role:

Attributes

Attribute	Value
1. Click to add...	

Save **Cancel**

3. Modify any values as necessary in the **Edit Local User** dialog.
4. Click **Save**.

Importing and Exporting Local Users

You can import or export the admin user accounts by using the **Import** and **Export All** links at the top-right corner of the **Local Users** page.

For more information, see [Importing and Exporting Information on page 32](#).

After selecting one or more user accounts from the list, you can also export specific user accounts by clicking the **Export** button .



The passwords of the local user accounts are not stored in clear text when exported to an XML file.

Setting Password Policy for Local Users

To set password policies for the local users:

1. Navigate to the **Configuration > Identity > Local Users** page.
2. Click the **Account Settings** link.

The **Account Settings** page opens.

Figure 205: Account Settings > Password Policy Settings Dialog

Account Settings

Password Policy | **Disable Accounts**

Minimum Length: 1

Complexity: No password complexity requirement

Disallowed Characters:

Disallowed Words (CSV):

Additional checks:

- ☐ May not contain User ID or its characters in reversed order
- ☐ May not contain repeated character four or more times consecutively

Expiry Days: 0

History: Must be different from previous 1 passwords (1-99)

Reminder: Display reminder message after 1 days (1-365)

Message to be displayed:

Note:

- Password characters validation will take effect for users created or modified after changes are

Save **Cancel**

3. Specify the **Password Policy** parameters as described in [Table 119](#).

Table 119: Password Policy Parameters

Parameter	Action/Description
Minimum Length	1. Specify the minimum length required for the password.
Complexity	2. Select the complexity setting from the Complexity drop-down list. The complexity settings can be one of the following: ■ No password complexity requirement ■ At least one uppercase and one lowercase letter ■ At least one digit ■ At least one letter and one digit ■ At least one of each: uppercase letter, lowercase letter, digit ■ At least one symbol ■ At least one of each: uppercase letter, lowercase letter, digit, and symbol
Disallowed Characters	3. Specify the characters not to be allowed in the password.
Disallowed Words (CSV)	4. Specify the words not to be allowed in the password
Additional Checks	5. Select any additional checks, if required. The options are: ■ May not contain User ID or its characters in reversed order. ■ May not contain repeated character four or more times consecutively.

Table 119: Password Policy Parameters (Continued)

Parameter	Action/Description
Expiry Days	6. Set the password expiry time for the local users. The allowed range is 0 to 500 days. The default value is 0. NOTE: If the value is set to 0, the password never expires. For any other value, local users are forced to reset the expired password when they log in. W-ClearPass alerts users five days before the password expires.
History	7. Specify the number of previous passwords for this user to be compared against. This option prevents users from setting a password that was used recently. Valid options are from 1 to 99.
Reminder	8. Configure the reminder message. Setting this option displays a reminder after n days to change the password. The valid options are from 1 to 365. When set, this option only displays a reminder; it does not prompt for a new password. The message to be displayed can be set accordingly. NOTE: This option is applicable only for TACACS+ authentication.
	9. Click Save.

Disabling Local User Accounts

- The **Disable Account** check occurs every day at midnight.
- Other Local User configuration settings are applied to all local users.

To specify the conditions for disabling local user accounts:

1. Navigate to **Configuration > Identity > Local Users**.
2. Click the **Account Settings** link in the upper-right corner of the **Local Users** page.
The **Account Settings** page opens.
3. Select the **Disable Accounts** tab.
The **Disable Accounts** dialog opens.

Figure 206: *Disable Accounts Dialog*

The screenshot shows a window titled "Account Settings" with a close button in the top right corner. Inside the window, there are two tabs: "Password Policy" and "Disable Accounts". The "Disable Accounts" tab is currently selected. Below the tabs, there are five rows of settings, each with a label on the left and a text input field on the right. The first row is "Days Exceed:" followed by a text box and the text "days (1-1000)". The second row is "Date Exceeds:" followed by a text box. The third row is "Password not changed for:" followed by a text box and the text "days (1-365)". The fourth row is "Failed attempts count:" followed by a text box and the text "times (1-100)". The fifth row is "Reset failed attempts count:" followed by the text "To reset failed attempts count and enable those users, click:" and a "Reset" button. Below these settings, there is a "Note:" section with two bullet points: "• Disable Account check happens at midnight everyday." and "• Other settings will be applied to all users." At the bottom right of the window, there are "Save" and "Cancel" buttons.

Label	Value/Action
Days Exceed:	days (1-1000)
Date Exceeds:	
Password not changed for:	days (1-365)
Failed attempts count:	times (1-100)
Reset failed attempts count:	To reset failed attempts count and enable those users, click: Reset

Note:

- Disable Account check happens at midnight everyday.
- Other settings will be applied to all users.

Save **Cancel**

4. Specify the **Disable Accounts** parameters as described in [Table 120](#), then click **Save**.

Table 120: *Disable Accounts Parameters*

Parameter	Action/Description
Days Exceed	1. Specify the number of days before the account is disabled. The range is from 1 to 100 days.
Date Exceeds	2. Specify the date when local users are disabled when the current date exceeds the configured date. The configured date can either be the current system date or a future date. Entering a date prior to the current date is not supported.
Password not changed for	3. Specify the number of days allowed before the password must be changed The range is from 1 to 365 days.
Failed attempts count	4. Specify the number of failed log-in attempts are allowed before the account is disabled. The range is from 1 to 100 attempts.
Reset failed attempts count	5. To reset the failed attempts count to zero and reenable those local users who were disabled after exceeding the failed attempts count, click Reset .

Adding and Modifying Endpoints

This section provides the following information:

- [Viewing List of Authentication Endpoints](#)
- [Viewing Endpoint Authentication Details](#)
- [Triggering Actions Performed on Endpoints](#)
- [Updating Device Fingerprints From a Hosted Portal](#)

- [Manually Adding an Endpoint](#)
- [Modifying an Endpoint](#)

For related information, see:

- [Configuring Endpoint Context Server Actions on page 563](#)
- [Adding Vendor-Specific Endpoint Context Servers on page 568](#)

Viewing List of Authentication Endpoints

W-Policy Manager automatically lists all endpoints that are authenticated in the **Configuration > Identity > Endpoints** page.

The following figure shows an example of the **Endpoints** page.

Figure 207: *List of Endpoints*

Configuration > Identity > Endpoints
Endpoints

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

Filter: contains

Show records

#	MAC Address ▲	Hostname	Device Category	Device OS Family	Status	Profiled
1.	☐ 000000000000				Unknown	No
2.	☐ 000000000008	acer1smu-pc	Computer	Windows	Unknown	Yes
3.	☐ 000000000042	samantha2013-nb	Computer	Windows	Unknown	Yes
4.	☐ 000000000472	android-7ed8612406cb12ee	SmartDevice	Android	Unknown	Yes
5.	☐ 000000000c9e	epascual-acer	Computer	Windows	Unknown	Yes
6.	☐ 000000000d7a	zfpfang2013-pc	Computer	Windows	Unknown	Yes
7.	☐ 000000001a44	staciet2011-nb	Computer	Windows	Unknown	Yes
8.	☐ 000039b440ba	devpc	Computer	Windows	Unknown	Yes
9.	☐ 0000858a7f92	canon8a7f92	Printer	Canon	Unknown	Yes
10.	☐ 0000858a7fa6	canon8a7fa6	Printer	Canon	Unknown	Yes

Showing 1-10 of 78165

Table 121: *Endpoint Page Parameters*

Parameter	Description
MAC Address	Displays the MAC address of the endpoint.
Hostname	Specifies the hostname of the policy server.
Device Category	Specifies the built-in category of the profiled device belongs to. For example, Smart devices, Access Points, Computer, VOIP phone, and so on.
Device OS Family	Specifies the operating system that the device is configured with. For example, when the category is Computer, W-ClearPass shows a Device OS Family of Windows, Linux, or Mac OS X.
Status	Displays the status of the endpoint.
Profiled	Displays whether the device is profiled or not.

Viewing Endpoint Authentication Details

To view the authentication details of an endpoint, select an endpoint by clicking the check box and click the **Authentication Records** button from the **Endpoints** page.

This displays the **Endpoint Authentication Details** page.

Figure 208: *Endpoint Authentication Details*

Endpoint Authentication Details					
MAC Address	001644b19320				
	Username	Device	Authentication	Start Time	Policy Manager Server Session ID
1	[REDACTED]	10.2.50.29	ACCEPT	2012/04/25 11:23:17	10.2.50.177 R00000175-01-4f984115
2	[REDACTED]	10.2.50.29	ACCEPT	2012/04/25 11:23:03	10.2.50.177 R00000174-01-4f984107
3	[REDACTED]	10.2.50.29	ACCEPT	2012/04/25 11:17:45	10.2.50.177 R00000173-01-4f983fc9
4	[REDACTED]	10.2.50.29	ACCEPT	2012/04/25 11:17:31	10.2.50.177 R00000172-01-4f983fba
5	[REDACTED]	10.2.50.29	ACCEPT	2012/04/25 11:11:59	10.2.50.177 R00000171-01-4f983e6e
6	[REDACTED]	10.2.50.29	ACCEPT	2012/04/25 11:06:39	10.2.50.177 R00000170-01-4f983d2f
7	[REDACTED]	10.2.50.29	ACCEPT	2012/04/25 11:06:26	10.2.50.177 R0000016f-01-4f983d22
Close					

Triggering Actions Performed on Endpoints

To trigger actions that are performed on endpoints, select an endpoint by clicking the check box and click the **Trigger Server Action** button from the **Endpoints** page.

For example, locking a device, triggering a remote, enterprise wipe, and so on.

The following figure displays the **Trigger Server Action** page:

Figure 209: *Endpoints - Trigger Server Action Page*

Trigger Server Action	
4 endpoint(s) are selected for server action	
Server Action:	Handle AirGroup Time Sharing
Context Server:	localhost
Server Type:	Generic HTTP
Action Description:	Sends time-based sharing policy to the AirGroup notification service
Start Action Cancel	

The following figure displays the **Trigger Server Action** page parameters:

Table 122: *Trigger Server Action Page Parameters*

Parameter	Description
Server Action	Select the server action from the drop-down list. The list includes the following options: • Check Point Login • Check Point Logout • Fortinet Login • Fortinet Logout • Handle AirGroup Time Sharing • Nmap Scan • SNMP Scan
Context Server	Enter a valid server name. You can enter an IP address or domain name.
Server Type	Specifies the server type configured when the server action was configured.
Action Description	Specifies the description of the action. For example, the description can be "Delete all information stored" if the configured action is Remote Wipe .

Updating Device Fingerprints From a Hosted Portal

To update device fingerprints from a hosted portal, select an endpoint by clicking the check box and click the **Update Fingerprint** button from the **Endpoints** page.

The following figure displays the **Update Device Fingerprint** page:

Figure 210: *Update Device Fingerprint*

Update Device Fingerprint

Specify the device fingerprint to update 4 endpoints -

Device Category:	
Device OS Family:	
Device Name:	

Save **Cancel**

The following table describes the **Update Device Fingerprint** page:

Table 123: *Update Device Fingerprint parameters*

Parameter	Description
Device Category	Select the built-in category of the profiled device belongs to. For example, Smartdevices, Access Points, Computer, VOIP phone, and so on.
Device OS Family	Select the operating system configured on the device. For example, when the category is Computer, you can select Windows, Linux, or Mac OS X.
Device Name	Enter the name of the device. You can select the name of the device from the built-in list.

Manually Adding an Endpoint

To manually add an endpoint, click **Add** to view the **Add Endpoint** page.

The following figure displays the **Add Endpoint** page.

Figure 211: *Add Endpoint Page*

Add Endpoint

MAC Address

Description:

Status ☒ Known client ☐ Unknown client ☐ Disabled client

Attributes

Attribute	Value
1. Click to add...	

Add **Cancel**

The following table describes the **Add Endpoint** page parameters:

Table 124: *Add Endpoint Page Parameters*

Parameter	Description
MAC Address	Specifies the MAC address of the endpoint.
Description	Specifies the description that provides additional information about the endpoint.
Status	Mark the status as Known, Unknown, or Disabled client. The Known and Unknown status can be

Table 124: Add Endpoint Page Parameters (Continued)

Parameter	Description
	used in role mapping rules using the Authentication:MacAuth attribute. You can use the Disabled status 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	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 the Attribute drop-down list for all endpoints. All attributes entered for an endpoint are available in the role mapping rules editor under the Endpoint namespace.

Modifying an Endpoint

To modify an endpoint in the **Endpoints** page, click an endpoint from the list of endpoints to display the **Edit Endpoint** page.

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 212: Edit Endpoint Page

Edit Endpoint

EndPointAttributes

MAC Address	000c29e5bcd3	IP Address	10.17.5.25
Description		Static IP	FALSE
Status	☐ Known client	Hostname	localhost.localdomain
	☒ Unknown client	Device Category	Computer
	☐ Disabled client	Device OS Family	Linux
MAC Vendor	VMware, Inc.	Device Name	Linux Computer
Added by	Policy Manager	Added At	Dec 23, 2014 12:29:02 IST
Online Status	Not Available	Updated At	Dec 23, 2014 12:32:59 IST
		Show Fingerprint	☐

SaveCancel

The following table describes the **Edit Endpoint** page parameters:

Table 125: *Edit Endpoint Page Parameters*

Parameter	Description
MAC Address	Displays the MAC address of the endpoint.
Description	Specifies the description that provides additional information about the endpoint.
Status	Mark the status as Known client , Unknown client , or Disabled client . The Known and Unknown status can be used in role mapping rules using the Authentication:MacAuth attribute. You can use the Disabled client status 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).
MAC Vendor	Displays the MAC OUI (Organizationally Unique Identifier) information for all endpoints even when no other profiling information is available for an endpoint.
Added by	Displays the name of the W-ClearPass server that added the endpoint.
Online Status	Displays the online status of the endpoint.
IP Address	Displays the IP address that is associated with the endpoint.
Static IP	Specifies the static IP address of the endpoint. You can select TRUE or FALSE. The default options is FALSE.
Hostname	Enter the hostname or the IP address of the endpoint.
Device Category	Specifies the built-in category of the endpoint belongs to. For example, Smart Devices, Access Points, Computer, VOIP phone, and so on.
Device OS Family	Specifies the operating system that the endpoint is configured with. For example, when the category is Computer, ClearPass Policy Manager shows a Device OS Family of Windows, Linux, or Mac OS X.
Device Name	Enter the name of the device. You can select the name of the device from the built-in list.
Added At	Displays the time at which the endpoint was added.
Updated At	Displays the time at which the endpoint was updated.
Show Fingerprint	Select this option to view the endpoint fingerprint details.
Endpoint Fingerprint Details	

Table 125: *Edit Endpoint Page Parameters (Continued)*

Parameter	Description
Host User Agent	Displays the host user agent of the endpoint. For example, Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.2; Trident/6.0).
Host OS Type	Displays the type of the host operating system. For example, Windows 8.
Device Category	Displays the category of the device. For example, Computer.
Device Family	Displays the operating system family of the endpoint. For example, Windows.
Device Name	Displays the name of the device.

Additional Available Tasks

- To delete an endpoint, in the **Endpoints** page, select an endpoint (using check box) and click the **Delete** button.
- To export an endpoint, in the **Endpoints** page, select an endpoint (using check box) and click the **Export** button.
- To export all endpoints, in the **Endpoints** page, click the **Export All** link in the upper right corner of the page.
- To import endpoints, in the **Endpoints** page, click the **Import** link in the upper right corner of the page.

Managing Static Host Lists

This section provides the following information:

- [About Static Host Lists](#)
- [Adding a Static Host List](#)
- [Static Hosts Lists Configuration Summary](#)
- [Editing a Static Host List](#)
- [Importing and Exporting Static Host Lists](#)

About Static Host Lists

You can configure primary and backup servers, session details, and the list of static hosts for **Static Host List** authentication sources.

A static host list often functions, in the context of the service, as a whitelist or a blacklist. Therefore, static host lists are configured independently at the global level.

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

- 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.



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

Internal Relational Database

An internal relational database stores the W-ClearPass Policy Manager configuration data as well as locally configured user and device accounts.

The following predefined authentication sources represent the databases used to store local users, guest users, and registered devices respectively:

- [Local User Repository]
- [Guest User Repository]
- [Guest Device Repository]

While regular users reside in an authentication source such as Active Directory (or in other LDAP-compliant stores), you can configure the temporary users, including guest users, in the W-Policy Manager local repositories.

Role Statically Assigned

For a user account created in a local database, the role is statically assigned to that account. This means you do not need to specify a role mapping policy 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.

Preconfigured Filter

The local user database is pre-configured with a filter to retrieve the password and the expiry time for the account. W-Policy Manager can perform MSCHAPv2 and PAP/GTC authentication against the local database.

Adding a Static Host List

To add a static host list to W-ClearPass:

1. Navigate to the **Configuration > Identity > Static Host Lists** page.
The **Static Hosts Lists** page opens.

Figure 213: *Static Host Lists Page*

Configuration » Identity » Static Host Lists

Static Host Lists

Filter: Name contains [] Go Clear Filter Show 10 records

#	Name	Format	Type	Description
1.	CPATS SHL MAC List	List	MACAddress	MAC List
2.	CPATS SHL MAC Regex	Regex	MACAddress	MAC Regex

Showing 1-2 of 2

Export Delete

2. Click **Add**.
The **Add Static Host List** dialog opens.

Figure 214: *Adding a Static Host List*

Add Static Host List

Name:

Description:

Host Format: ☒ Subnet ☐ Regular Expression ☐ List

Host Type: ☒ IP Address ☐ MAC Address

Subnet:
(e.g., 192.168.1.1/24)

Save **Cancel**

3. Enter the parameters to add a static host list as described in [Table 126](#).

Table 126: *Add Static Host List Parameters*

Parameter	Action/Description
Name	1. Enter the name of the static host list.
Description	2. Enter the description that provides additional information about the static host list.
Host Format	3. Select a format for expression of the address: • Subnet • Regular Expression • List
Host Type	4. Select a host type: • IP Address • MAC Address
Subnet	5. Enter the subnet address.
	6. Click Save .

The new static host list is now available to be added as an authentication source. For details, see [Adding a Static Host List as an Authentication Source](#) on page 230.

Static Hosts Lists Configuration Summary

You can use the **Summary** tab to view the static host list's configuration information.

Figure 215: *Static Hosts Lists Configuration Summary*

Configuration » Authentication » Sources » Add
Authentication Sources

General	Static Host Lists	Summary
General:		
Name:	Test Auth source	
Description:	Authenticating against the Local DB.	
Type:	SHL	
Use for Authorization:	-	
Authorization Sources:	-	
Static Host Lists:		
MAC Address Host Lists:	-	

Editing a Static Host List

To edit a static host list:

1. Navigate to the **Configuration > Identity > Static Host Lists** page .
The **Static Hosts Lists** page opens.
2. Click on the name of the static hosts list you want to edit.
The **Edit Static Host List** dialog opens.

Figure 216: *Edit Static Host List Dialog*

Edit Static Host List

Name:	CPATS SHL MAC List	
Description:	MAC List	
Host Format:	☐ Subnet ☐ Regular Expression ☒ List	
Host Type	☐ IP Address ☒ MAC Address	
List:	78-da-6e-00-00-09 78-19-f7-00-00-03	Remove Host Add Host
SaveCancel		

3. Make any required changes, then click **Save**.

Importing and Exporting Static Host Lists

You can import static host lists into W-ClearPass or export them to a file.

1. Navigate to the **Configuration > Identity > Static Host Lists** page .
The **Static Hosts Lists** page opens.
2. Click on the name of the static hosts list you want to import or export.
3. To import a static host list into W-ClearPass, click the **Import** link.

4. To export a static host list to a file, click the **Export All** link.
For further details, see [Importing and Exporting Information on page 32](#).

Configuring a Role and Role Mapping Policy

After authenticating a request, a 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.



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 a number of preconfigured roles, including the following:

- [Contractor] - Default role for a contractor
- [Employee] - Default role for an employee
- [Guest] - Default role for guest access
- [Other] - Default role for other user or device
- [TACACS API Admin] - API administrator role for Policy Manager admin
- [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 Read-only Admin] - Read-only administrator role for Policy Manager Admin
- [TACACS Receptionist] - Policy Manager Guest provisioning role
- [TACACS Super Admin] - Policy Manager Admin role with unlimited access to all UI screens



Additional roles are available with AirGroup and Onboard licenses.

For additional tasks, see the following:

- [Adding and Modifying Role Mapping Policies on page 259](#)
- [Adding and Modifying Roles on page 259](#)

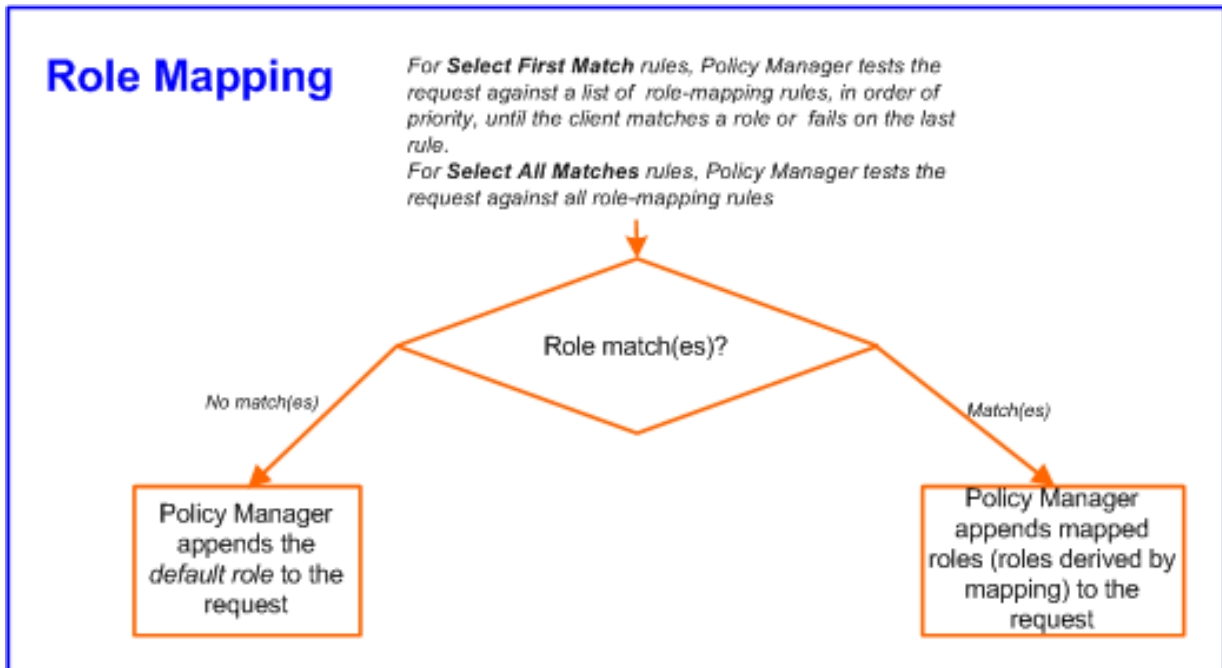
Identity Roles Architecture and Workflow

Roles can range in complexity from a simple user group (for example, Finance, Engineering, or Human Resources) to a combination of a user group with some dynamic constraints (for example, "Night Shift Worker," an employee in the Engineering department who logs in through the network device between 8:00 PM and 5:00 AM on weekdays). It can also apply to a list of users.

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.

For more information, see [Configuring a Role and Role Mapping Policy on page 257](#).

Figure 217: Role Mapping Process



A role can be:

- Authenticated through predefined Single Sign-On rules.
- Associated directly with a user in the Policy Manager *local user* database.
- Authenticated based on predefined allowed endpoints.
- Associated directly with a *static host list*, again through *role mapping*.
- Discovered by W-Policy Manager through *role mapping*.

Roles are typically discovered by W-Policy Manager by retrieving attributes from the *authentication source*. *Filter rules* associated with the authentication source tell W-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 Roles

Policy Manager lists all available roles in the **Configuration > Identity > Roles** page. The following figure displays the **Roles** page:

Figure 218: Roles Page

Configuration > Identity > Roles

Roles

Filter: Name contains Go Clear Filter

Show 10 records

#	Name	Description
1.	[AirGroup Administrator]	Operators with this role can manage multiple devices that are shared with all users
2.	[AirGroup Operator]	Operators with this role can self-provision devices within their personal WLAN
3.	[AirGroup v1]	Role for an AirGroup protocol version 1 request
4.	[AirGroup v2]	Role for an AirGroup protocol version 2 request
5.	Aruba-AP	
6.	[Aruba TACACS read-only Admin]	Default role for read-only access to Aruba device
7.	[Aruba TACACS root Admin]	Default role for root access to Aruba device
8.	[BYOD Operator]	Operators with this profile can view and manage their own provisioned devices
9.	Computer	
10.	[Contractor]	Default role for a contractor

Showing 1-10 of 99 Export Delete

You can configure a role from within a role mapping policy (**Add New Role**), or independently from the **Configuration > Identity > Roles > Add** page. 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** pop-up. The following figure displays the **Add New Role** page:

Figure 219: Add New Role Page

Add New Role

Name:

Description:

Save Cancel

The following table describes the **Add New Role** parameters:

Table 127: Add New Role Page Parameters

Parameter	Description
Name	Enter the name of the role.
Description	Enter the description that provides additional information about the new role.

Adding and Modifying Role Mapping Policies

From the **Configuration > Services** page, 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 from the **Configuration > Identity > Role Mappings** page.

The following figure displays the **Role Mappings** page:

Figure 220: Role Mappings Page

Configuration » Identity » Role Mappings

Role Mappings

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

Filter: Name contains Go Clear Filter

Show 10 records

#	Name	Description	Default Role
1.	[AirGroup Version Match]	System-defined mapping to identify the protocol version of an AirGroup request	[AirGroup v1]
2.	Automation_Rolemapping		eTIPS_Guest
3.	Auto_Rolemapping_4_UnknownClient		eTIPS_Guest
4.	AUTO_SHL_MAPPING		eTIPS_Guest
5.	Device-Type-Role-Mapping		Computer
6.	[Guest Roles]	The roles used by Guest.	[Employee]
7.	Onboard Authorization	Maps RADIUS authorization attributes to a role for the Onboard device type	[Guest]
8.	rajesh-role		Aruba-AP
9.	[SMU]AD-Account-Exist		Aruba-AP
10.	[SMU] Switch Management TACACS role mapping		[Other]

Showing 1-10 of 16

Copy Export Delete

When you click **Add** role mapping from any of these locations, Policy Manager displays the **Role Mappings** page, which contains the following three tabs:

- [Policy Tab on page 260](#)
- [Mapping Rules Tab on page 261](#)

Policy Tab

The **Policy** tab labels the method and defines the default role. The default role is the role to which Policy Manager defaults if the mapping policy does not produce a match for a given request.

The following figure displays the **Role Mappings - Policy** tab:

Figure 221: Role Mappings - Policy Tab

Configuration » Identity » Role Mappings » Add

Role Mappings

Policy Mapping Rules Summary

Policy Name:

Description:

Default Role: [Contractor] View Details Modify Add new Role

Back to Role Mappings Next > Save Cancel

The following figure displays the **Role Mappings - Policy** tab parameters:

Table 128: Role Mappings - Policy Tab Parameters

Parameter	Description
Policy Name	Enter the name of the role mapping policy.
Description	Enter the description that provides additional information about the role mapping policy.
Default Role	Select the role to which Policy Manager will default when the role mapping policy does not produce

Table 128: Role Mappings - Policy Tab Parameters (Continued)

Parameter	Description
	a match.
View Details	Click on View Details to view the details of the default role.
Modify	Click on Modify to modify the default role.
Add new Role	Click on Add new Role to add a new role.

Mapping Rules Tab

The **Mapping Rules** tab selects the evaluation algorithm to add, edit, remove, and reorder rules. On the **Mapping Rules** tab, click the **Add Rule** button to create a new rule, or select an existing rule (by clicking on the row) and then click the **Edit Rule** or **Remove Rule** button.

The following figure displays the **Role Mapping - Mapping Rules** tab:

Figure 222: Role Mapping - Mapping Rules Tab

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

Figure 223: Rules Editor Page

The following table describes the **Role Mappings Page - Rules Editor** page parameters:

Table 129: *Role Mappings Page - Rules Editor Page Parameters*

Parameter	Description
Type	The rules editor appears throughout the Policy Manager interface. It exposes different namespace dictionaries depending on context. (Refer to Namespaces on page 845.) In the role mapping context, Policy Manager allows attributes from following namespaces: • Application • Application:ClearPass • Authentication • Authorization • Authorization:<authorization_source_instance> - Policy Manager shows each instance of the authorization source for which attributes have been configured to be fetched. (See Adding and Modifying Authentication Sources on page 193). Only those attributes that have been configured to be fetched are shown in the attributes drop-down list. • Certificate • Connection • Date • Device • Endpoint • GuestUser • Host • LocalUser • Onboard • TACACS • RADIUS - All enabled RADIUS vendor dictionaries.
Name	Displays the drop-down list of attributes present in the selected namespace.
Operator	Displays the drop-down list of context-appropriate (with respect to the attribute data type) operators. Operators have the obvious meaning; for stated definitions of operator meaning, refer to Operators on page 856 .
Value	Depending on attribute data type, this may be a free-form (one or many line) edit box, a drop-down list, or a time/date widget.



The operator values that display for each type and name are based on the data type specified for the authentication source (from the **Configuration > Authentication > Sources** page). If, for example, you modify the UserDN Data type on the authentication sources page to be an integer rather than a string, then the list of operator values here will populate with values that are specific to integers.

After you save your role mapping configuration, it appears in the **Mapping Rules** list. In this interface, you can select a rule, and then use the various widgets to move up, move down, edit the rule, or remove the rule.

This chapter provides the following information:

- [Posture Architecture and Flow](#)
- [Unified Agent System Tray Status Icons](#)
- [Creating a New Posture Policy](#)
- [Configuring Posture Policy Agents and Hosts](#)
- [Configuring Posture Policy Plug-ins](#)
- [Configuring Posture Policy Rules](#)
- [Configuring Posture for Services](#)
- [Configuring Audit Servers](#)

Posture Architecture and Flow

This section provides the following information:

- [Posture Policy](#)
- [Audit Servers](#)
- [Assessing Client Consistency](#)
- [Application Token](#)
- [System Token](#)

W-Policy Manager supports two types of posture checking: posture policies and audit servers.

Posture Policy

W-Policy Manager supports four pre-configured posture plug-ins for Windows, one plug-in for Linux®, and one plug-in 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.



A service can also be configured without any posture policy.

Audit Servers

Audit servers provide posture checking for unmanageable devices, such as devices lacking adequate posture agents or supplicants. In the case of such clients, the audit server's post-audit rules map clients to roles.

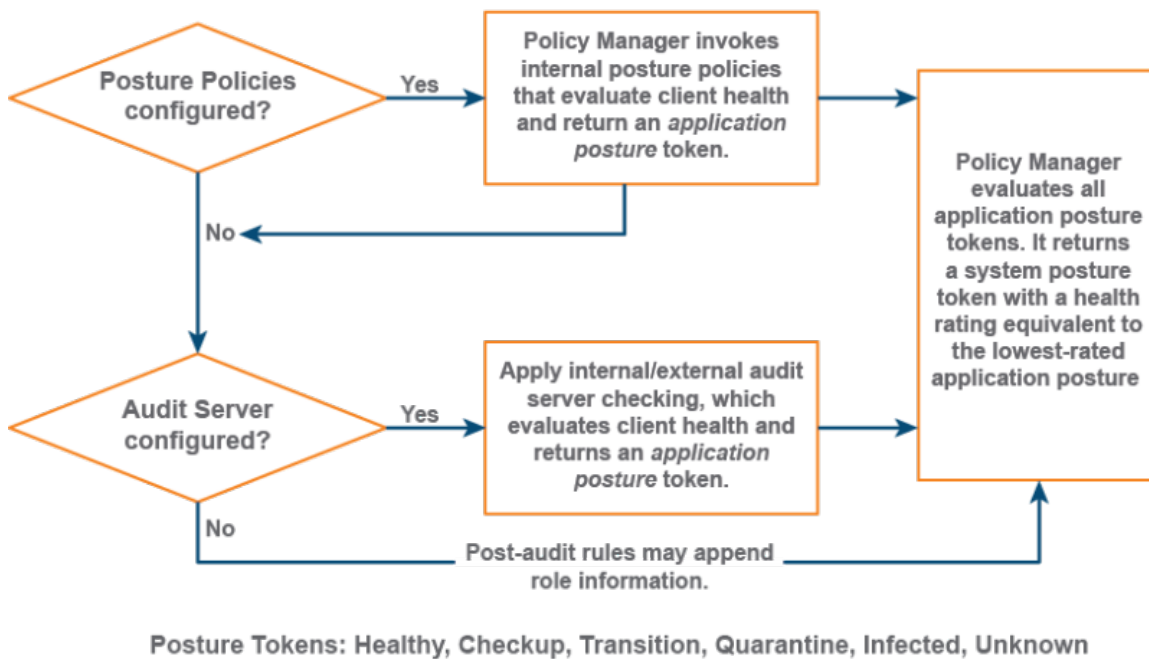
W-Policy Manager supports two types of audit servers:

- **NMAP audit server:** Primarily used to derive roles from post-audit rules.
- **NESSUS audit server:** Primarily used for vulnerability scans (and, optionally, post-audit rules).

Figure 224: Posture Evaluation Process

Posture Evaluation

ClearPass Policy Manager allows you to configure any combination of posture policies and/or audit servers. Each configured health check returns an application token that communicates the client's health status.



Assessing Client Consistency

W-ClearPass 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/antispayware/firewall configuration
- Patch level of software components
- Peer-to-Peer (P2P) application checks
- Services to be running or not running
- Processes to be running or not running

Application Token

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.

System Token

Upon completion of all configured posture checks, W-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.

Unified Agent System Tray Status Icons

This section provides the following information:

- [About the Unified Agent](#)
- [Unified Agent System Tray Icons](#)
- [OnGuard-Only System Tray Icons](#)

About the Unified Agent

W-ClearPass Onguard agent is integrated with Dell VIA (Virtual Internet Adapter) to support both VIA functionality and Onguard agent system health status collection. Thus, the integrated product is called the *Unified Agent*.

NAP (Network Access Protection) is a framework to collect system health status on Microsoft clients.

W-ClearPass supports health status collection for both NAP and OnGuard.

The Unified Agent System Tray icons display the following states of the Unified Agent status:

- OnGuard health status
- Trusted or untrusted network status
- VPN connectivity status
- Error conditions

Unified Agent System Tray Icons

[Table 130](#) describes the icons that indicate the possible states for the Unified Agent.

Table 130: *Unified Agent System Tray Icons*

OnGuard Status	Network Type	VPN Status	Icon
Healthy	Trusted	Connected	
Healthy	Trusted	Disconnected	
Unhealthy	Trusted	Connected	

Table 130: *Unified Agent System Tray Icons (Continued)*

OnGuard Status	Network Type	VPN Status	Icon
Unhealthy	Trusted	Disconnected	
Healthy	Untrusted	Connected	
Healthy	Untrusted	Disconnected	
Unhealthy	Untrusted	Connected	
Unhealthy	Untrusted	Disconnected	
Healthy	N/A	Error	
Unhealthy	N/A	Error	
Logged Out: No Health Status	N/A	Error	
Error	Trusted	Connected	
Error	Trusted	Disconnected	
Error	Untrusted	Connected	
Error	Untrusted	Disconnected	
Error	No Profile	N/A	
Error	N/A	Error	
Healthy	No Profile	N/A	
Unhealthy	No Profile	N/A	

Table 130: *Unified Agent System Tray Icons (Continued)*

OnGuard Status	Network Type	VPN Status	Icon
Logged Out: No Health Status	No Profile	N/A	
Logged Out: No Health Status	Trusted	Connected	
Logged Out: No Health Status	Untrusted	Disconnected	

OnGuard-Only System Tray Icons

Table 131 describes the icons that indicate the possible states for OnGuard-only.

Table 131: *OnGuard-Only System Tray Icons*

OnGuard Status	Network Type	VPN Status	Icon
Healthy	N/A	N/A	
Unhealthy	N/A	N/A	
Logged Out: No Health Status	N/A	N/A	
Error	N/A	N/A	

Creating a New Posture Policy

This chapter provides the following information:

- [About ClearPass Posture](#)
- [Creating a New Posture Policy](#)

About ClearPass Posture

W-ClearPass Policy Manager evaluates the health of the clients that request access using posture policies and an audit server.

All these methods return Posture Tokens (for example, Healthy and Quarantine) for use by W-Policy Manager as input into an enforcement policy. You can associate one or more posture methods with a single service.

W-ClearPass Policy Manager forwards all or part of the posture data received from the client to a posture server. Nmap (Network Mapper) or Nessus audit servers provide posture checking for unmanageable devices,

such as devices lacking adequate posture agents or supplicants. For more information on audit servers, see [Configuring Audit Servers on page 327](#).

Creating a New Posture Policy

From the **Posture Policies** page, you can create a new policy or edit an existing policy.

To create a new Posture Policy:

1. Navigate to **Configuration > Posture > Posture Policies**.

The **Posture Policies** page displays a list of all existing posture policies.

Figure 225: *Posture Policies Page*

Configuration » Posture » Posture Policies

Posture Policies

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

Filter: Name contains Show records

#	Name	Description
1.	CPATS Linux Posture - Unhealthy Client	
2.	CPATS MAC Posture - Unhealthy Client	
3.	CPATS Windows Posture - Unhealthy Client	

Showing 1-3 of 3

2. Click the **Add** link.

The **Posture Policies Add** page appears.

Figure 226: *Posture Policies Add Page*

Configuration » Posture Policies » Add

Posture Policies

Policy Name:	
Description:	
Posture Agent:	☐ NAP Agent ☒ OnGuard Agent (Persistent or Dissolvable)
Host Operating System:	☒ Windows ☐ Linux ☐ Mac OS X
Restrict by Roles:	Remove Select or type role names Add

3. Configure the information in the **Policy** page as described in [Configuring Posture Policy Agents and Hosts on page 269](#).

- For information on configuring the Posture policy plug-ins, see [Configuring Posture Policy Plug-ins on page 272](#).
- For information on configuring Posture Policy Rules, see [Configuring Posture Policy Rules on page 324](#).

Configuring Posture Policy Agents and Hosts

This section provides the following information:

- [Introduction](#)
- [NAP Agent Posture Plug-ins](#)
- [OnGuard Agent Posture Plug-ins](#)

Introduction

To configure posture policy agents and hosts:

1. Navigate to **Configuration > Posture > Posture Policies**.

The **Posture Policies** page displays a list of all existing posture policies.

Figure 227: *Posture Policies Page*

Configuration » Posture » Posture Policies

Posture Policies

 Add
 Import
 Export All

Filter: Name contains [] + Go Clear Filter Show 10 records

#	☐	Name ▲	Description
1.	☐	CPATS Linux Posture - Unhealthy Client	
2.	☐	CPATS MAC Posture - Unhealthy Client	
3.	☐	CPATS Windows Posture - Unhealthy Client	

Showing 1-3 of 3

Copy Export Delete

2. Click the **Add** link.

The **Posture Policies Add** page appears.

Figure 228: *Posture Policies Add Page*

Configuration » Posture » Posture Policies » Add

Posture Policies

Policy Posture Plugins Rules Summary

Policy Name:	
Description:	
Posture Agent:	☐ NAP Agent ☒ OnGuard Agent (Persistent or Dissolvable)
Host Operating System:	☒ Windows ☐ Linux ☐ Mac OS X
Restrict by Roles:	 Select or type role names Remove Add

3. Use the **Posture Policies > Policy** dialog to configure the policy name and description, select a posture agent and host operating system, and specify role restrictions.

The following table describes the **Add Policy** parameters:

Table 132: *Add Posture Policy Parameters*

Parameter	Action/Description
Policy Name	1. Enter the name assigned to the policy by the W-ClearPass Policy Manager administrator.
Description	2. Specify the description that provides additional information about the posture policy.
Posture Agent	3. Select the posture agent type. For information on these agents, see NAP Agent Posture Plug-ins on page 270 and OnGuard Agent Posture Plug-ins on page 270 .
Host Operating System	4. Specify whether the host is using a Window, Linux, or MAC OS X operating system.
Restrict by Roles	5. Apply the posture policy to the selected roles.

NAP Agent Posture Plug-ins

When you select **NAP Agent** as the Posture agent, you can configure the posture plug-ins as described in [Table 133](#):

Table 133: *NAP Agent: Windows OS Posture Plug-ins Support*

Plug-in	Description	Windows Support
Windows System Health Validator	The Windows System Health Validator permits or denies client computers to connect to your network. The Windows System Health Validator also restricts client access to computers that have a service pack less than service pack x.	- Windows 10: Yes - Windows 8: Yes - Windows 7: Yes - Windows Vista: Yes - Windows XP Svc Pack 3: Yes - Windows Server 2008, 2008R2: Yes
Windows Security Health Validator	The Windows Security Health Validator permits or denies client computers access to your network, subject to checks of the client's system for Firewall, Virus Protection, Spyware Protection, Automatic Updates, and Security Updates. NOTE: If you configure the Windows Security Health Validator posture plug-in for Windows XP, spyware protection is disabled.	- Windows 10: Yes - Windows 8: Yes - Windows 7: Yes - Windows Vista: Yes - Windows XP Svc Pack 3: Yes - Windows Server 2008, 2008R2: No

OnGuard Agent Posture Plug-ins

Select **OnGuard Agent (Persistent or Dissolvable)** as the **Posture Agent** for use in the following scenarios:

- An environment that does not support 802.1X-based authentication. For example, some legacy Microsoft Windows operating systems or legacy network devices.
- An environment configured with an operating system that provides support for 802.1X natively, but does not have a built-in health agent. Macintosh OS X is an example of this type of environment.

When you select the **Posture Agent: OnGuard Agent (Persistent or Dissolvable)**, you can configure the posture plug-ins for:

- Windows (see [Table 134](#))
- Macintosh OS X (see [Table 135](#))
- Linux (see [Table 136](#))

Table 134: *OnGuard Agent Validator Posture Plug-in Windows OS Support*

Plug-in	Description	Windows Support
W-ClearPassWindows Universal System Health Validator	The configurable parameter categories for this validator are Services, Processes, Registry Keys, AntiVirus, AntiSpyware, Firewall, Peer To Peer, Patch Management, Windows HotFixes, USB Devices, Virtual Machines, Network Connections, Disk Encryption, and Installed Applications.	• Windows 10: Yes • Windows 8: Yes • Windows 7: Yes • Windows Vista: Yes • Windows 2003: Yes • Windows XP Svc Pack 3: Yes • Windows Server 2008, 2008R2: Yes
Windows System Health Validator	The Windows System Health Validator allows you to configure client computers that can connect to your network, and clients that are restricted from your network. Access is determined by a check of the service pack level. You can determine the service pack level.	• Windows 10: Yes • Windows 8: Yes • Windows 7: Yes • Windows Vista: Yes • Windows 2003: Yes • Windows XP Svc Pack 3: Yes • Windows Server 2008, 2008R2: Yes
Windows Security Health Validator	The configurable parameter categories for this validator allow you to configure parameters that permit or deny client computers access to your network, subject to checks of the client's system for Firewall, Virus Protection, Spyware Protection, Automatic Updates, and Security Updates. NOTE: If you configure the posture plug-in for Windows XP, spyware protection is disabled.	• Windows 10: Yes • Windows 8: Yes • Windows 7: Yes • Windows Vista: Yes • Windows 2003: No • Windows XP Svc Pack 3: Yes • Windows Server 2008, 2008R2: No

Table 135: *OnGuard Agent (Persistent or Dissolvable) Posture Plug-ins for Mac OS X*

Plug-in	Description
W-ClearPass Macintosh OS X Universal System Health Validator	The configurable parameter categories for this validator are: ■ Services ■ Processes ■ AntiVirus ■ AntiSpyware ■ Firewall ■ Patch Management ■ Peer-to-Peer ■ USB Devices ■ Virtual Machines ■ Network Connections ■ Disk Encryption ■ Installed Applications ■ File Check

Table 136: *OnGuard Agent (Persistent or Dissolvable) Posture Plug-ins for Linux*

Name of the Plug-in	Description
W-ClearPass Linux Universal System Health Validator	The configurable parameter categories for this validator are: ■ Services ■ AntiVirus

Configuring Posture Policy Plug-ins

The **Posture Plugins** dialog of the **Posture Policies** page allows you to configure plug-ins for the posture policy. The plug-ins available on this tab vary, depending upon whether the policy is using a Network Access Protection (NAP) agent or the OnGuard Agent (Persistent or Dissolvable) plug-in.

To configure posture policy plug-ins:

1. Navigate to **Configuration > Posture > Posture Policies**.

The **Posture Policies** page appears.

Figure 229: Posture Policies Page

Configuration » Posture » Posture Policies

Posture Policies

 Add
 Import
 Export All

Filter: contains Show records

#	☐ Name ▲	Description
1.	☐ CPATS Linux Posture - Unhealthy Client	
2.	☐ CPATS MAC Posture - Unhealthy Client	
3.	☐ CPATS Windows Posture - Unhealthy Client	

Showing 1-3 of 3

2. Click **Add**.

The **Add Posture Policies** page appears.

3. In the **Policy** tab, specify the following:

- Policy Name
- Description
- Posture Agent
- Host Operating System

4. Select the **Posture Plugins** tab .

The **Add Posture Plugins** page appears.

Figure 230: Add Posture Plugins Page

Configuration » Posture » Posture Policies » Add

Posture Policies

Policy	Posture Plugins	Rules	Summary	
Select one/more plugins:				
Plugin Name		Plugin Configuration		Status
☐	ClearPass Windows Universal System Health Validator	Configure	View	-
☐	Windows System Health Validator	Configure	View	-
☐	Windows Security Health Validator	Configure	View	-

You can configure the following posture plug-ins in the **Posture Policies** page:

- [ClearPass Windows Universal System Health Validator - OnGuard Agent on page 274](#)
- [Windows System Health Validator: NAP Agent on page 321](#)
- [Windows System Health Validator: OnGuard Agent on page 302](#)
- [Windows Security Health Validator: NAP Agent on page 322](#)

5. Select the check box of the plug-in you wish to configure.

6. To view the configuration page for the selected plug-in, click **Configure**.

Configuring OnGuard Agent Plugins

If you select the **OnGuard Agent** option in the **Policy** tab of the **Posture Policies** page, the **Posture Plugins** tab allows you to configure different plugin types for hosts running Windows, Linux, and Mac OS X operating systems. Refer to the following topics for details on each plugin type:

- For Windows:
 - [ClearPass Windows Universal System Health Validator - OnGuard Agent on page 274](#)
 - [Windows System Health Validator: OnGuard Agent on page 302](#)
 - [Windows Security Health Validator: OnGuard Agent on page 303](#)

- For Linux: [W-ClearPass Linux Universal System Health Validator Plugin](#) on page 304
- For Mac OS X: [W-ClearPass Macintosh OS X Universal System Health Validator: OnGuard Agent](#) on page 307

The following figure displays the **Posture Policies - Posture Plugins** tab:

Figure 231: *OnGuard Agent Plugin Options for Mac OS X*

Configuration » Posture » Posture Policies » Add

Posture Policies

Policy	Posture Plugins	Rules	Summary
Select one/more plugins:			
Plugin Name	Plugin Configuration		Status
☐ ClearPass Mac OS X Universal System Health Validator	Configure	View	-

ClearPass Windows Universal System Health Validator - OnGuard Agent

To configure the W-ClearPass Windows Universal Health System Health Validator (OnGuard Agent):

1. Navigate to **Configuration > Posture > Posture Policies**, then click **Add**.

The **Add Posture Policies** dialog appears.

Figure 232: *Adding a Posture Policy*

Configuration » Posture » Posture Policies » Add

Posture Policies

Policy	Posture Plugins	Rules	Summary
Policy Name:			
Description:			
Posture Agent:	☐ NAP Agent ☒ OnGuard Agent (Persistent or Dissolvable)		
Host Operating System:	☒ Windows ☐ Linux ☐ Mac OS X		
Restrict by Roles:	Remove Select or type role names Add		

- a. Enter the name and a description of the posture policy.
- b. **Posture Agent:** Choose **OnGuard Agent (Persistent or Dissolvable)**.
- c. **Host Operating System:** **Windows** is selected by default.
- d. Click **Next**.

The **Posture Plugins** dialog appears.

Figure 233: *Selecting the Windows Posture Plugin*

Posture Policies

Policy	Posture Plugins	Rules	Summary
Select one/more plugins:			
Plugin Name	Plugin Configuration		Status
☒ ClearPass Windows Universal System Health Validator	Configure	View	Not Configured
☐ Windows System Health Validator	Configure	View	-
☐ Windows Security Health Validator	Configure	View	-

2. In the **Posture Plugins** page, click the check box for **ClearPass Windows Universal System Health Validator**.
3. Click **Configure**.

The **ClearPass Windows Universal System Health Validator** page is displayed:

Figure 234: *ClearPass Windows Universal System Health Validator Page*

4. Select the desired version of Windows.
5. To enable checks for the selected version, click the **Enable checks for Windows Server** check box .

The following list of configuration pages for the selected version of Windows appears:

- [Services on page 275](#)
- [Processes on page 276](#)
- [Registry Keys on page 279](#)
- [AntiVirus on page 282](#)
- [AntiSpyware on page 284](#)
- [Firewall on page 285](#)
- [Peer To Peer on page 286](#)
- [Patch Management on page 287](#)
- [Windows Hotfixes on page 291](#)
- [USB Devices on page 291](#)
- [Virtual Machines on page 292](#)
- [Network Connections on page 293](#)
- [Disk Encryption on page 295](#)
- [Installed Applications on page 296](#)
- [File Check on page 299](#)

Services

The **Services** page provides a set of widgets for specifying services to run or stop.

Figure 235: Services Page

The following table describes the **Services** parameters:

Table 137: 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).
User Notification	Enable to allow user notifications for service check 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). This list varies depending on OS types. Click the >> or << to add or remove, respectively, the services from the Service to run or Services to stop boxes.
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 .

Processes

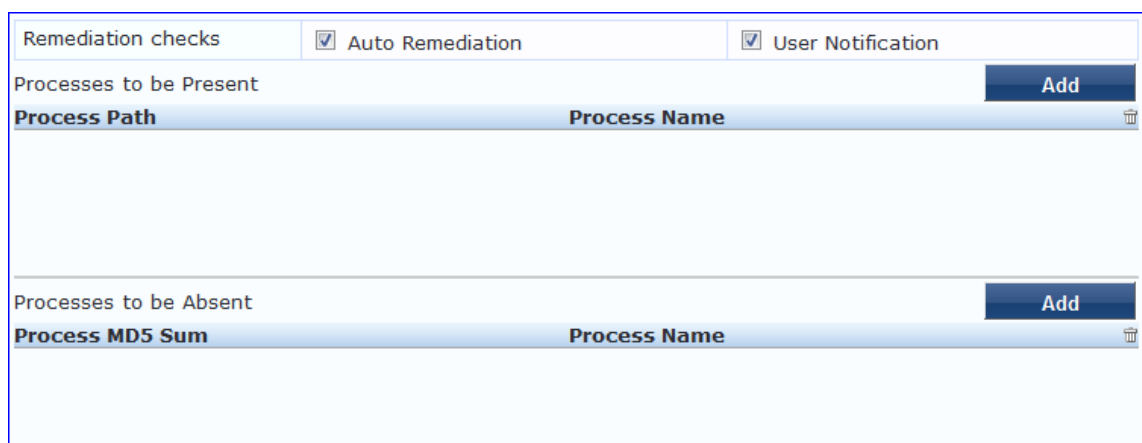
The **Processes** page provides a set of parameters to specify which processes to be explicitly present or absent on the system.

To configure Processes:

1. From the W-ClearPass Windows Universal System Health Validator page, enable checks for the selected version of Windows.
2. Select **Processes**.
3. Enable the **Network Connection Check is on** check box.

The **Processes** configuration page appears.

Figure 236: Processes Configuration Page

The screenshot shows the 'Processes Configuration Page'. At the top, there are three sections: 'Remediation checks' with a checked 'Auto Remediation' checkbox, 'User Notification' with a checked checkbox, and an 'Add' button. Below this is a section titled 'Processes to be Present' with an 'Add' button. Underneath is a table with two columns: 'Process Path' and 'Process Name'. Below this table is another section titled 'Processes to be Absent' with an 'Add' button. Underneath is another table with two columns: 'Process MD5 Sum' and 'Process Name'.

The following table describes the **Process** configuration parameters:

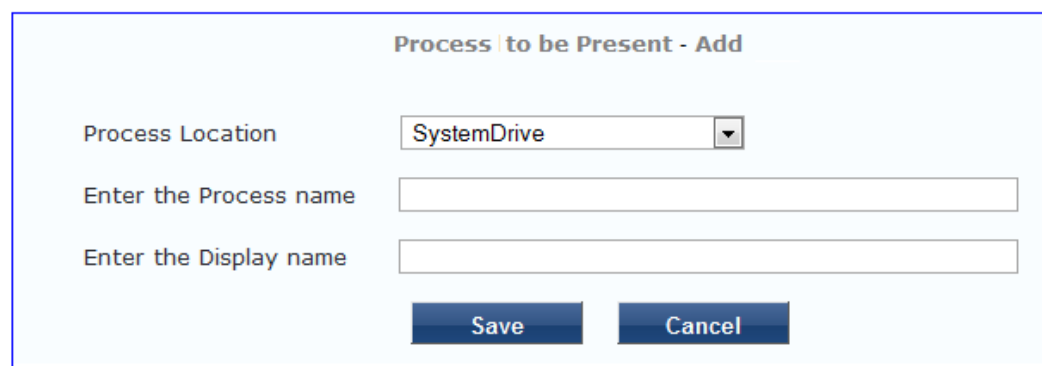
Table 138: Process Page Parameters

Parameter	Description
Auto Remediation	1. Enable to allow auto-remediation for processes.
User Notification	2. Enable to allow user notifications in the event of process policy violations.
Processes to be present/ absent	3. To specify a process to be added, either to the Processes to be present or Processes to be absent lists, click Add .

Processes to be Present Parameters

1. In the **Process to be Present** section, click **Add**.
The **Process to be Present—Add** page appears.

Figure 237: Process to be Present Page--Add Page

The screenshot shows the 'Process to be Present - Add' page. It has a title bar 'Process to be Present - Add'. Below the title bar, there are three input fields: 'Process Location' with a dropdown menu showing 'SystemDrive', 'Enter the Process name' with a text box, and 'Enter the Display name' with a text box. At the bottom, there are two buttons: 'Save' and 'Cancel'.

2. Define the parameters as described in the following table:

Table 139: *Process to be Present Page Parameters*

Parameter	Description
Process Location	1. Choose from the following locations: ■ System Drive ■ Systemroot ■ Program Files ■ HOMEDRIVE ■ HOMEPATH ■ None
Enter the Process name	2. Specify the path name containing the process executable name.
Enter the Display name	3. Enter a user-friendly name for the process. This is displayed in end-user facing messages.
	4. Click Save .

After you save the Process parameters, the information appears in the **Processes to be Present** section.

Processes to be Absent Parameters

1. In the **Process to be Absent** section, click **Add**.

The **Process to be Absent—Add** page appears.

Figure 238 shows the configuration parameters for when you select **Process Name** and when you select **MD5 Sum**.

Figure 238: *Process to be Absent Pages: Process Name and MD5 Sum*

The figure displays two screenshots of the 'Process to be Absent - Add' configuration page. The top screenshot shows the 'Process Name' tab selected, with fields for 'Enter the Process name' and 'Enter the Display name'. The bottom screenshot shows the 'MD5 Sum' tab selected, with a large text area for 'MD5 Sum' and a field for 'Enter the Display name'.

The following table describes the **Process to be Absent** parameters:

Table 140: *Process to be Absent Page Parameters*

Parameter	Action/Description
Check Type	- Select the type of process check to perform. The agent can look for: 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 display name is displayed in end-user facing messages.
	Click Save.

You return to the **Processes Configuration** page, which now shows the values for the processes that were configured:

Figure 239: *Processes Configured*

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	

Registry Keys

The **Registry Keys** page allows you to specify which registry keys are to be explicitly present or absent.

Figure 240: Registry Keys Page (Overview)

The following table describes the **Registry Keys** page parameters:

Table 141: Registry Keys Page Parameters

Parameter	Action/Description
Auto Remediation	1. Enable auto remediation for registry checks. Use this page to automatically add or remove registry keys based on the entries in Registry keys to be present and Registry keys to be absent fields.
User Notification	2. Enable user notifications for registry check policy violations.
Monitor Mode	3. Enable this to set the health status of the Registry Keys health class healthy. This allows administrators to collect information related to missing registry keys without marking the clients as unhealthy even if some registry keys are missing.
Registry keys to be present	4. To specify a registry key to be added to the Registry keys to be present list, click Add . If the specified registry key is not present, the remediation message that is added in the Registry Keys Page (Detail) window is displayed on OnGuard Agent .
Registry keys to be absent	5. To add a registry key to the Registry keys to be absent list, click Add . If the specified registry key is not absent, the remediation message that is added in the Registry Keys Page (Detail) window is displayed on OnGuard Agent .

1. To display the **Registry** page detail, click **Add**.

Figure 241: Registry Keys Page (Detail)

☒ Enable checks for Windows 10

Registry key to be Present - Add

Select the Registry Hive:

Enter the Registry key:
(eg: Software, SampleVendor, SampleApp, SampleKey)

Enter the Registry value name:

Select the Registry value data type:

Enter the Registry value data:

Enter Regex pattern for Registry value:
(To be displayed to end user if registry check fails)

Enter Remediation Message:
(To be displayed to end user if registry check fails)

2. Enter the **Registry Keys - Detail** parameters as described in [Table 142](#).

Table 142: Registry Keys Page (Detail)

Parameter	Action/Description
Select the Registry Hive	1. Specify the registry hive from the following options: ■ HKEY_CLASSES_ROOT ■ HKEY_CURRENT_USER ■ HKEY_LOCAL_MACHINE ■ HKEY_USERS ■ HKEY_CURRENT_CONFIG
Enter the Registry key	2. Specify the registry key using the examples given in the GUI.
Enter the Registry value name	3. Specify the name of the registry value.
Select the Registry value data type	4. Specify the registry value data types. The data type can be any of the following: ■ Multi String ■ String ■ DWORD ■ QWORD ■ Expandable String
Enter the Registry value data	5. Specify the registry value.

Table 142: Registry Keys Page (Detail) (Continued)

Parameter	Action/Description
Enter Regex pattern for Registry value	6. Enter the Regular Expression (Regex) pattern for the Registry value. A regular expression is a pattern that the regular expression engine attempts to match in input text. A pattern consists of one or more character literals, operators, or constructs. NOTE: Perl regular expressions are supported.
Enter Remediation Message	7. Specify the custom remediation message to be displayed to end users if the registry check fails.
	8. Click Save .

As shown in [Figure 242](#), after you save the registry configuration settings, the remediation message and Regular Expression pattern appears in the **Registry** page.

Figure 242: Registry Keys Added

☒ Enable checks for Windows 10

Remediation checks	☒ Auto Remediation	☒ User Notification
Monitor Mode	☐ (Check to enable Monitor Mode)	

Registry keys to be present Add

Key	Name	Value	Type	Remediation Message	Regex Pattern	
HKEY_CLASSES_ROOT\SampleKey	Registry3		String	Registry check failed. Install application ABC	(a.)+	

Registry keys to be absent Add

Key	Name	Value	Type	Remediation Message	Regex Pattern	

AntiVirus

In the **Antivirus** page, you can turn on an Antivirus application. Click **An anti-virus application is on** to configure the Antivirus application information.

Figure 243: Antivirus Page (Overview - Before)

☐ An antivirus application is on

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

Figure 244: Antivirus Page (Detail 1)

☒ An antivirus application is on

Remediation checks	☒ Auto Remediation	☒ User Notification	☒ Display Update URL
Add			

Antivirus	Prd Version	Eng Version	Dat Version	Dat Update	Last Scan	Rtp Check	

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

Figure 245: Antivirus Page (Detail 2)

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

Select the antivirus product Symantec AntiVirus

Product version check Is Latest

Engine version check No Check

Data file version check No Check

Data file has been updated in 2 Hour(s)

Last scan has been done before 2 Hour(s)

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

Save Cancel

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

Figure 246: Antivirus Page (Overview - After)

☒ An antivirus application is on

Remediation checks ☒ Auto Remediation ☒ User Notification ☒ Display Update URL

Add

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

Table 143: Antivirus Page

Interface	Parameter	Description
Antivirus Page	- An Antivirus Application is On - Auto Remediation - User Notification - Display Update URL	- Click Antivirus application is on to enable testing of health data for configured Antivirus application(s). - Check the Auto Remediation check box to enable auto remediation of anti-virus status. - Check the User Notification check box to enable user notification of policy violation of anti-virus status. - Check the Display Update URL check box to show the origination URL of the update.
Antivirus Page (Detail 1)	Add	To configure Antivirus application attributes for testing against health data, click Add.
Antivirus Page (Detail 2)	- Product-specific checks - Select the antivirus product	Configure the specific settings for which to test against health data. All of these checks may not

Table 143: Antivirus Page (Continued)

Interface	Parameter	Description
2)	- Product version check - Engine version check - Engine version check - Datafile version check - Data file has been updated in - Last scan has been done before - Real-time Protection Status Check	be available for some products. Where checks are not available, they are shown in disabled state on the UI. - 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. - Data file has been updated in - Specify the interval in hours, days, weeks, or months. - Last scan has been done before - Specify the interval in hours, days, weeks, or months. - Real-time Protection Status Check - No Check - W-ClearPass Policy Manager does not use RTP Status value for health evaluation. This means that the client is treated as healthy irrespective of the value of RTP. - On - Client is marked as healthy only if the value of RTP status is On. - Off - Client is marked as healthy only if the value of RTP status is Off.

AntiSpyware

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. Click **An Antipware Application is On** to configure the AntiSpyware application information.

Figure 247: AntiSpyware Page (Overview Before)

☐ An antispyware application is on

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

Figure 248: AntiSpyware Page (Detail 1)

☒ An antispyware application is on

Remediation checks
☒ Auto Remediation
☒ User Notification
☒ Display Update URL

Add

Antispyware	Prd Version	Eng Version	Dat Version	Dat Update	Last Scan	Rtp Check	

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

Figure 249: AntiSpyware Page (Detail 2)

Figure 250: AntiSpyware Page (Overview After)

Antispyware	Prd Version	Eng Version	Dat Version	Dat Update	Last Scan	Rtp Check	
AVG Anti-Malware [AntiSpyware]	isLatest	isLatest	no check	2 Hour(s)	no check	nocheck	🗑️

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

The configuration elements are the same for antivirus and antispyware products. Refer to the previous [AntiSpyware](#) configuration instructions.

Firewall

In the **Firewall** page, you can specify that a Firewall application must be on and specify information about the Firewall application.

Figure 251: Firewall Page (Overview Before)

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

Figure 252: Firewall Page (Detail 1)

Firewall Product Name	Product Version	
		🗑️

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

Figure 253: 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 254: 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	

The following table describes the **Firewall** parameters:

Table 144: Firewall Page Parameters

Interface	Parameter	Description
Firewall Page	- A Firewall Application is On - Auto Remediation - User Notification - Uncheck to allow any product	- Check the Firewall Application is On check box to enable testing of health data for configured firewall application(s). - Check the Auto Remediation check box to enable auto remediation of firewall status. - Check the User Notification check box to enable user notification of policy violation of firewall status. - Uncheck the Uncheck to allow any product check box to check whether any firewall application (any vendor) is running on the end host.
Firewall Page (Detail 1)	- Add - Trashcan icon	- To configure firewall application attributes for testing against health data, click Add. - To remove configured firewall application attributes from the list, click the trashcan icon in that row.
Firewall Page (Detail 2)	Product/Version	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. - Select the firewall product - Select a vendor from the list - Product version is at least - Enter the version of the product.

Peer To Peer

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.

The following figure displays the **Peer To Peer** health class configuration page:

Figure 255: *Peer to Peer Page*

The following table describes the **Peer to Peer** parameters:

Table 145: *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	This scrolling list contains a list of applications or networks that you can select and move to the Applications to stop panel. Click the >> or << to add or remove, respectively, the applications or networks from the Applications to stop box.

Patch Management

In the **Patch Management** page, you can specify that a patch management application must be on and allows drill-down to specify information about the patch management application. Click **A patch management application is On** to configure the patch management application information.

The following figure displays the **Patch Management** page:

Figure 256: *Patch Management Page (Overview - Before)*

When enabled, the **Patch Management** detail pop-up appears.

Figure 257: Patch Management Page (Detail 1)

☒ A patch management application is on

Remediation checks	☒ Auto Remediation	☒ User Notification

Add

PM Product Name	Product Version	Status Check	Install Level Check	

Click **Add** to specify PM Product Name, Product Version, Status Check, and Install Level Check information.

Figure 258: Patch Management Page (Detail 2)

☒ Enable checks for Windows Server 2003

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

Select Patch Management product BMC FootPrints Asset Core

Product Version is at least

Status Check Type No Check

Install Level Check Type All

Grace Period Day(s)

Scan Interval Week(s)

Save **Cancel**

When you save your patches configuration, it appears in the **Patch Management** page list.

Figure 259: Patch Management Page (Overview - After)

☒ Enable checks for Windows 7

☒ A patch management application is on

Remediation checks	☒ Auto Remediation	☒ User Notification

Add

PM Product Name	Product Version	Status Check	Install Level Check	Grace Period	Scan Interval	
Any Supported Patch Agent	no check	no check	All	2 Day(s)	1 Day(s)	

The following table describes the **Patch Management** parameters:

Table 146: Patch Management Page Parameters

Interface	Parameter	Description
Patch Management Page	• A patch management application is on • Auto Remediation • User Notification • Uncheck to allow any product	• Check the A patch management application is on to enable testing of health data for configured Antivirus application(s). • Check the Auto Remediation check box to enable auto remediation of patch management status. • Check the User Notification check box to enable user notification of policy violation of patch management status. • Clear Uncheck to allow any product check box to check whether any patch management application (any vendor) is running on the end host.
Patch Management Page (Detail 1)	• Add • Trashcan icon	• To configure patch management application attributes for testing against health data, click Add. • To remove configured patch management application attributes from the list, click the trashcan icon in that row.
Patch Management Page (Detail 2)	Product/Version	Configure settings for which to test against health data. All checks might not be available for some products. Where checks are not available, they are shown in disabled state on the UI. • Select Patch Management product: Select a vendor. This option is <i>only</i> enabled if the Product-specific checks check box is checked. • Product version is at least: Enter version number. This option is <i>only</i> enabled if the Product-specific checks check box is checked. • Status Check Type: Select this field to check whether Patch Agent is enabled or not. W-ClearPass Policy Manager server compares the Patch Agent Status sent by OnGuard Agent with the configured value. If the Patch Agent Status value is different from configured value, then client is treated as unhealthy. If Auto-remediation is enabled, then OnGuard Agent changes the Patch Agent Status on client to the configured value. Select any of the following options: ■ No Check - W-ClearPass Policy Manager server ignores Patch Agent Status value. This means it will not check status of Patch Agent application on client. ■ Enabled - Patch Agent is turned on and automatically update the client. ■ Disabled - Patch Agent is disabled and it will not check for missing patches and update the client. ■ Notify Before Download - Patch Agent is turned on and will notify user before downloading updates.

Table 146: Patch Management Page Parameters (Continued)

Interface	Parameter	Description
		■ Notify Before Install - Patch Agent is turned on and will notify user before installing updates. NOTE: The values specific to the selected product are displayed in the Status Check Type field. For example, all the 5 values are displayed for Microsoft Windows Automatic Update. For SCCM, only No Check, Disabled, and Notify Before Install are displayed. ● Install Level Check Type: Select No Check, All, Selected on Server, or Security. This option is only enabled if the Product-specific checks check box is checked. For Microsoft SCCM, selecting All, Selected on Server, or Security will return the full list of all missing patches. ■ All: Check for all missing patches, and search for all available patches. ■ Selected on Server: Check only for the patches pre-selected on the server. Some Patch Management products can push the patches to the endpoint device. This option provides the ability to check for only the pre-selected patches. ■ Security: Check only for security updates. Some of the products can install only security-related patches. NOTE: If you select the Microsoft Windows Update Agent from the Select Patch Management product list and you select an option from the Install Level Check Type list, the results are listed below: ■ All: Returns the full list of missing patches. ■ Selected on Server: Returns a list of missing patches that are pre-selected on the server site. ■ Security: Returns a list of missing patches that Microsoft classifies as Security Updates. ■ No Check - Disables the Grace Period and Scan Interval fields. ● Grace Period: Configure the time period for which OnGuard Agent should ignore missing patches. You can specify the grace period in hours, days, weeks, or months. For example, if the Grace Period is set to 3 days, then clients will be treated as 'healthy' for 3 days even if some patches are missing. After 3 days, OnGuard Agent will treat clients as 'unhealthy' if the patches are still missing. You can enable Auto-remediation to install the missing patches and to treat them as 'healthy'. This field is disabled if you selected No Check from the Install Level Check Type field.

Table 146: Patch Management Page Parameters (Continued)

Interface	Parameter	Description
		Scan Interval: Configure the time interval after which OnGuard Agent should check for missing patches. You can configure the time period in hours, days, weeks, or months. The default scan interval is 1 hour. This field is disabled if you selected No Check from the Install Level Check Type field.

Windows Hotfixes

The **Windows Hotfixes** page provides a set of widgets for checking if specific Windows hotfixes are installed on the endpoint. The following figure displays the **Windows Hotfixes** health class configuration page:

Figure 260: Windows Hotfixes Page

The following table describes the **Windows Hotfixes** parameters:

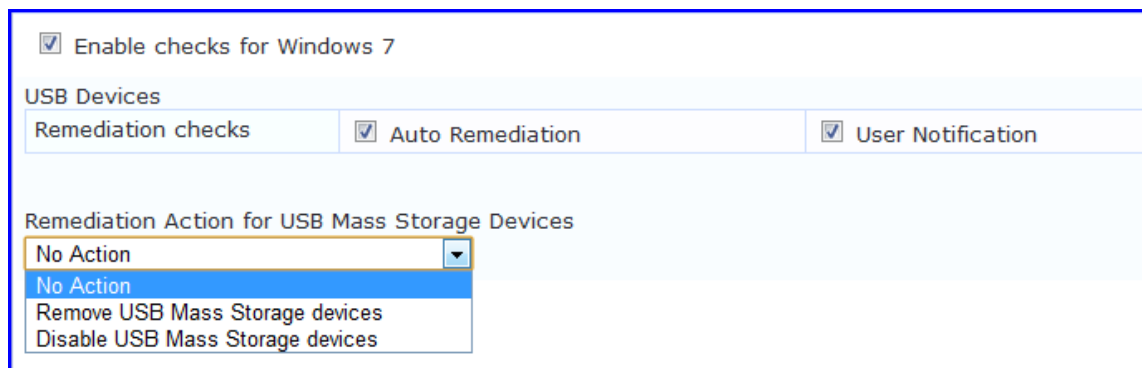
Table 147: Windows Hotfixes Page Parameters

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.
Monitor Mode	Click to enable Monitor Mode .
Available Hotfixes	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). Click the >> or << to add or remove, respectively, the hotfixes from the Hotfixes to run boxes.

USB Devices

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

Figure 261: *USB Devices*



☒ Enable checks for Windows 7

USB Devices

Remediation checks ☒ Auto Remediation ☒ User Notification

Remediation Action for USB Mass Storage Devices

No Action

No Action

Remove USB Mass Storage devices

Disable USB Mass Storage devices

The following table describes the **USB Devices** parameters:

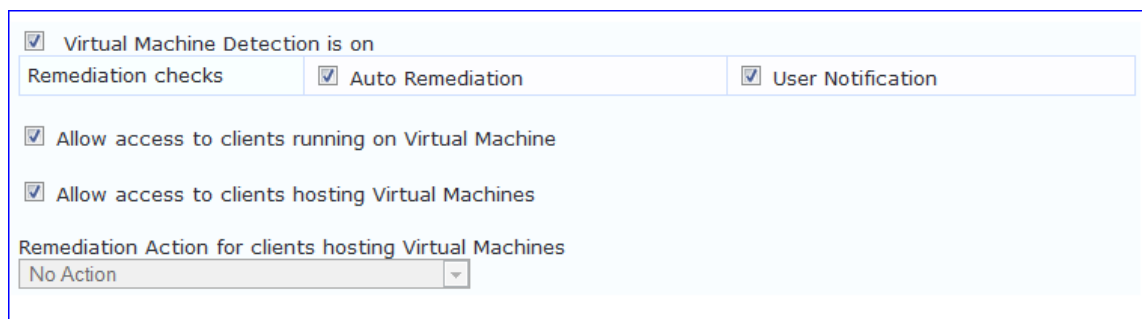
Table 148: *USB Devices*

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	• 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.

Virtual Machines

The **Virtual Machines** page provides configuration to Virtual Machines utilized by your network.

Figure 262: *Virtual Machines*



☒ Virtual Machine Detection is on

Remediation checks ☒ Auto Remediation ☒ User Notification

☒ Allow access to clients running on Virtual Machine

☒ Allow access to clients hosting Virtual Machines

Remediation Action for clients hosting Virtual Machines

No Action

The following table describes the **Virtual Machines** parameters:

Table 149: *Virtual Machines*

Parameter	Description
Auto Remediation	Enable to allow auto remediation for virtual machines connected to the endpoint.
User Notification	Enable to allow user notifications for virtual machine policy violations.
Allow access to clients running on Virtual Machine	Enable to allow clients that running a VM to be accessed and validated.
Allow access to clients hosting Virtual Machine	Enable to allow clients that hosting a VM to be accessed and validated.
Remediation Action for clients hosting Virtual Machines	• No Action - Take no action; do not stop or pause virtual machines. • Stop all Virtual Machines running on Host - Stop the VM clients that are running on Host. • Pause all Virtual Machines running on Host - Pause the VM clients that are running on Host.

Network Connections

The **Network Connections** page provides configuration to control network connections based on connection type.

To configure Network Connections:

1. From the W-ClearPass Windows Universal System Health Validator page, enable checks for the selected version of Windows.
2. Select **Network Connections**.
3. Enable the **Network Connection Check is on** check box.

The **Network Connections** configuration page appears.

Figure 263: *Network Connections Configuration Page*

☒ Enable checks for Windows 10

☒ Network Connection Check is on

Remediation checks ☒ Auto Remediation ☒ User Notification

☒ Check for Network Connection Types **Configure**

Network Connection Types	Network Connections Allowed	Remediation Action For Network Connection Types Not Allowed
-	-	-

☒ Allow Bridge Network Connection
Remediation Action for Bridge Network Connection No Action

☒ Allow Internet Connection Sharing
Remediation Action for Internet Connection Sharing No Action

☒ Allow Adhoc/Hosted Wireless Networks
Remediation Action for Adhoc/Hosted Wireless Networks No Action

4. Select the **Check for Network Connection Types** check box.
5. To specify the type of connection that you want to include, click **Configure**.
The **Network Connection Types** configuration page appears.

Figure 264: *Network Connection Types Configuration Page*

Network Connection Types

Allowed Network Connections Type Allow Only One Network Connection

Network Connections Types

Others
Wired
Wireless

Network Connections Allowed

>>
<<

Remediation Action For Network Connection Types Not Allowed No Action

Save Cancel

The following table describes the **Network Connection Types** configuration parameters:

Table 150: *Network Connection Type Configuration Parameters*

Parameter	Action/Description
Allow Network Connections Type	1. Select one of the following options: ■ Allow Only One Network Connection ■ Allow One Network Connection with VPN ■ Allow Multiple Network Connections
Network Connection Types	2. To add or remove Others , Wired , and Wireless network connection types, click >> or <<.
Remediation Action for Network Connection Types Not Allowed	3. Specify one of the following ■ No Action: Take no action. Do not eject or disable the attached devices. ■ Disable Network Connections ■ Disconnect Network Connections
	4. Click Save .

This returns you to the **Network Connections** configuration page. The following table describes the remaining fields on this page.:

Table 151: *Network Connections Configuration Parameters*

Parameter	Action/Description
Auto Remediation	1. Enable to allow auto-remediation for network connections.
User Notification	2. Enable to allow user notifications in the event of network connection policy violations.
Remediation Action for Bridge Network Connection	3. If Allow Bridge Network Connection is disabled, then specify whether to take no action when a bridge network connection exists or to disable all bridge network connections.
Remediation Action for Internet Connection Sharing	4. If Allow Internet Connection Sharing is disabled, then specify whether to take no action when Internet connection sharing exists or to disable Internet connection sharing.
Remediation Action for Adhoc/Hosted Wireless Networks	5. If Allow Adhoc/Hosted Wireless Networks is disabled, then specify whether to take no action when an adhoc wireless networks exist or to disable all adhoc/hosted wireless networks.

Disk Encryption

Disk encryption is a technology which protects information by converting it into unreadable code that cannot be deciphered easily by unauthorized people. Disk encryption uses disk encryption software or hardware to encrypt every bit of data that goes on a disk or disk volume. Disk encryption prevents unauthorized access to data storage.

The following figure displays the **Disk Encryption** health class configuration page:

Figure 265: *Disk Encryption Configuration Page*

☒ Enable checks for Windows Server 2003

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

Select Disk Encryption product

Product Version is at least

Locations to Check

The following table describes the Disk Encryption parameters:

Table 152: *Disk Encryption Parameters*

Parameter	Description
User Notification	Enable to allow user notifications for virtual machine policy violations.
Product-specific checks	Clear to allow disk encryption on any product. The Select Disk Encryption product and Product Version is at least fields are disabled after you clear the check box.
Select Disk Encryption product	Select a specific disk encryption product.
Product Version is at least	Search for the production version of the selected product.
Locations to Check	Select location to check. The options are None, System Root Drive, All Drives, or Specific Locations.

Installed Applications

The **Installed Applications** category groups classes that represent software-related objects. Access to these objects is supported by the Windows Installer. Examples of objects in this category are installed products, file specifications, and registration actions.

In the **Installed Applications Configuration** page (see [Figure 266](#)), you can turn on the installed applications check and specify information about which installed applications you want to monitor.

Figure 266: *Installed Applications for Windows Configuration Page*

The screenshot shows the 'ClearPass Windows Universal System Health Validator' window. On the left is a sidebar with a tree view containing categories like Windows Server 2003, Windows XP, Windows Vista, Windows 7, Windows Server 2008, Windows 8, and Windows 10. Under Windows 10, various system components are listed, including 'Installed Application'. The main area is titled 'Enable checks for Windows 10' and contains several configuration options: 'Installed Applications Check is on' (checked), 'Remediation checks' (checked), 'Auto Remediation' (unchecked), 'User Notification' (checked), and 'Monitor Mode' (unchecked). Below these are three tables for managing application health: 'Applications Allowed (Mandatory)', 'Applications Allowed (Optional)', and 'Applications Not Allowed'. Each table has columns for 'Application Name', 'Regular Expression Enabled', and 'Remediation Message'. At the bottom, there is a 'Quarantine Message' field and 'Reset', 'Save', and 'Cancel' buttons.

The following table describes the **Installed Applications Configuration** page parameters:

Table 153: *Installed Applications for Windows Configuration Page Parameters*

Parameter	Action/Description
Remediation checks	Auto-Remediation for the Installed Applications health class is not supported.
User Notification	1. Enable sending a remediation message with a list of applications to install or uninstall to the user.
Monitor Mode	2. Enable Monitor Mode to treat all the installed applications as always healthy.

Table 153: *Installed Applications for Windows Configuration Page Parameters (Continued)*

Parameter	Action/Description
Applications Allowed (Mandatory)	3. Specify installed applications to be monitored on a mandatory basis. NOTE: Enter the application name as they are shown in Add/Remove Programs.
Applications Allowed (Optional)	4. Specify installed applications to be monitored on an optional basis. NOTE: Enter the application name as they are shown in Add/Remove Programs.
Allow only Mandatory and Optional Applications	5. Specify that only the mandatory and optional applications are monitored. NOTE: All applications that are not either mandatory or optional must be removed or uninstalled.

Enabling Regular Expressions for a Windows Application

To enable regular expressions for an application:

1. From the **ClearPass Windows Universal System Health Validator > Configure** page (see [Windows Universal System Health Validator on page 1](#)), then select the desired version of Windows.
2. Select **Installed Applications**.
3. Click (enable) the **Installed Applications Check is on** check box.
The Installed Applications dialog appears (see [Figure 266](#)).
4. From the desired **Applications Allowed** category, click **Add**.
The **Add Mandatory Applications** dialog for the selected **Applications Allowed** category appears.

Figure 267: *Enabling Regular Expression*

☒ Enable checks for Windows 10

Applications Mandatory - Add

Enter the Application Name

Enable Regular Expression ☒ (Check to enable use of regex in Application Name)

Remediation Message

5. Configure the **Add Mandatory Applications** parameters as described in [Table 154](#).

Table 154: Mandatory Applications Parameters

Parameter	Action/Description
Enter the Application Name	1. Enter the name of the application.
Enable Regular Expression	2. Check (enable) this check box to enable the use of regular expressions in the Application Name . When this field is enabled, W-ClearPass treats the Application Name as regular expression when comparing application names.
Remediation Message	3. Optionally, enter the remediation message that will be displayed to the user in the event of an error. NOTE: Remediation messages can include reasons for remediation, links to helpful URLs and helpdesk contact information.
	4. Click Save .

You return to the **Installed Applications** dialog, where **Regular Expression Enabled** is set to **true** for the specified application (see [Figure 268](#)).

Figure 268: Regular Expression Enabled

The screenshot shows the 'Installed Applications' dialog in W-ClearPass Policy Manager. At the top, there are checkboxes for 'Enable checks for Windows 10' and 'Installed Applications Check is on', both of which are checked. Below these are sections for 'Remediation checks' (with 'Auto Remediation' unchecked and 'User Notification' checked) and 'Monitor Mode' (with '(Check to enable Monitor Mode)' unchecked). A table titled 'Applications Allowed (Mandatory)' contains one entry: 'AppABC' with 'Regular Expression Enabled' set to 'true' and 'Remediation Message' set to '-'. An 'Add' button is visible on the right side of the table.

Application Name	Regular Expression Enabled	Remediation Message
AppABC	true	-

File Check

Use the **File Check** page to verify the group of files to present or absent. In the **File Check** page, you can turn on the file check and specify information about which the files you want to check.

The following figure displays the **File Check** Health Class configuration page:

Figure 269: Windows File Check Health Class Configuration

☒ Enable checks for Windows 10

☒ File Check is On

Remediation checks ☐ Auto Remediation ☒ User Notification

Monitor Mode ☐ (Check to enable Monitor Mode)

File Groups to be Present Add

File Group Name	Evaluation Rule	Files List

File Groups to be Absent Add

File Group Name	Evaluation Rule	Files List

Save Cancel

The following table describes the **File Check Configuration** parameters:

Table 155: File Check Configuration Parameters

Parameter	Action/Description
Remediation checks	Auto-remediation for the File Check health class is not supported.
User Notification	1. When enabled, a remediation message that includes the groups of files to be present or absent is displayed to the end user.
Monitor Mode	2. To treat all the file check health classes as always healthy, enable Monitor Mode .
File Groups to be Present	3. To add the files to be present in the File Check health class, click Add .
File Groups to be Absent	4. To add the files to be absent in the File Check health class, click Add .

1. To open the **File Group to be Present > Add** page, click **Add**:

You can configure the name of the file group and specify the evaluation rule for the file group.

The following figure displays the **File Group to Be Present > Add** dialog:

☒ Enable checks for Windows 10

File Group to be Present - Add

Enter the File Group Name

File Group Evaluation Rule Pass All

Files to be Present Add

File Location	File Path	File Name	File MD5 Sum	Remediation Message

Save Cancel

The following table describes the **File Group to be Present > Add** parameters:

Table 156: *File Group to be Present - Add Parameters*

Parameter	Description
Enter the File Group Name	1. Enter the name of the file group.
File Group Evaluation Rule	2. Select the appropriate File Group Evaluation Rule: • Pass All: Select this evaluation rule if you want the File Check health class to be deemed as 'healthy' only if all the configured file groups are present. • Pass Any One: Select this evaluation rule if you want the File Check health class to be deemed as 'healthy' even if any one of the configured file groups are present.

3. To configure the name of the file group and the evaluation rule for the file group, from **File Groups to be Present**, click **Add**.

The following figure displays the **File to Be Present > Add** page:

Figure 270: *File to be Present > Add Dialog*

☒ Enable checks for Windows 10

File to be Present - Add

File Location

SystemDrive ▼

Enter the File Path

(eg: SampleVendorSampleApp, SampleFolderconfig)

Enter the File Name

(eg: SampleApp.exe, SampleFile.dll)

Enter the MD5 Sum

Remediation Message

Save

Cancel

The following table describes the **File to be Present > Add** parameters:

Table 157: *File to be Present > Add Parameters*

Parameter	Action/Description
File Location	1. Select any location of the file from the drop-down list: ■ SystemDrive ■ Systemroot ■ ProgramFiles ■ ProgramFiles (x86) ■ HOMEDRIVE ■ HOMEPATH ■ None
Enter the File Path	2. Enter the file path as described in the examples from the user interface.
Enter the File Name	3. Enter the name of the file.
Enter the MD5 Sum	Optionally, specify one or more (comma separated) MD5 checksums of the process executable file.
Remediation Message	4. Specify the custom remediation message to be displayed to end users if File check fails.

5. When finished, click **Save**.

The parameters configured in the **File to be Present > Add** dialog are reflected in the **File Groups to be Present** page as illustrated in the following figure:

Figure 271: *File Group to be Present Parameters Displayed*

☒ Enable checks for Windows 10

File Group to be Present - Add

Enter the File Group Name:

File Group Evaluation Rule:

Files to be Present

File Location	File Path	File Name	File MD5 Sum	Remediation Message
ProgramFiles (x86)	ProgramFiles (x86)/Internet Explorer	iexplore.exe	-	Internet Explorer is successfully installed on your system

Add **Save** **Cancel**

Windows System Health Validator: OnGuard Agent

This System Health Validator checks for current Windows Service Packs. The OnGuard Agent also supports legacy Windows operating systems such as Windows Server 2003.

Use the check boxes to enable support of specific operating systems and to restrict access based on the Service Pack level.

To configure the Windows System Health Validator:

1. Navigate to **Configuration > Posture > Posture Policies**.

2. Click **Add**.

The Add Posture Policies dialog appears. Specify the following:

- a. Policy Name: Enter the name of the posture policy.
- b. Posture Agent: **OnGuard Agent**
- c. Host Operating System: **Windows**

3. Click **Next**.

4. From the **Posture Plugins** tab, select **Windows System Health Validator**, then click the **Configure** button.

The **Windows System Health Validator** page appears:

Figure 272: OnGuard Agent: Windows System Health Validator

Windows System Health Validator

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

- ☒ **Windows 10**
Windows 10 clients are allowed
☐ Restrict clients which have Service Pack less than
- ☒ **Windows 8**
Windows 8 clients are allowed
☐ Restrict clients which have Service Pack less than
- ☒ **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

5. To enable support of specific operating systems, click the corresponding check box.

6. Enter the minimum Service Pack level required on the client computer to connect to your network.

7. Click **Save**.

Windows Security Health Validator: OnGuard Agent

The Windows Security Health Validator checks for the presence of specific types of security applications. You can use the options to restrict access based on the absence of the selected security application types.

To configure the Windows Security Health Validator:

1. Navigate to **Configuration > Posture > Posture Policies**.

2. Click **Add**.

The Add Posture Policies dialog appears. Specify the following:

- a. **Policy Name**: Enter the name of the posture policy.
- b. **Posture Agent**: **OnGuard Agent**
- c. **Host Operating System**: **Windows**

3. Click **Next**.

4. From the **Posture Plugins** tab, select **Windows Security Health Validator**, then click the **Configure** button.

The following screen appears:

Figure 273: *OnGuard Agent: Windows Security Health Validator Page*

5. To enable support of specific operating systems, click the corresponding check box.
6. Enter the minimum Service Pack level required on the client computer to connect to your network.
7. Click **Save**.

W-ClearPass Linux Universal System Health Validator Plugin

The **W-ClearPass Linux Universal System Health Validator** plugin appears on the **Posture Plugins (Configuration > Posture > Posture Policies > Add)** tab. Select the **Linux** host operating system and **OnGuard Agent** posture agent from the **Policy** tab in the **Posture Policy** page. Click **Configure** to configure antivirus settings and service types.

The OnGuard Dissolvable Agent version of the **ClearPass Linux Universal System Health Validator** plugin supports the following health classes:

- [Antivirus on page 304](#)
- [Services on page 306](#)

Antivirus

Use the **Antivirus** page to turn on an Antivirus application. Click **An antivirus application is on** to configure the Antivirus application information. The following figure displays the **Antivirus** health class configuration page:

Figure 274: *Antivirus Page*

AntiVirus	Prd Version	Eng Version	Dat Version	
Any Supported AntiVirus	no check	no check	isLatest	

The following table describes the **Antivirus** parameters:

Table 158: Antivirus Configuration Parameters

Parameter	Description
Remediation checks	Auto-remediation for the File Check health class is not supported.
User Notification	A remediation message having a list of files to present/absent will be displayed to end user.
Antivirus	Shows the name of the Antivirus configured. Click Add to configure the name of the Antivirus.
Prd Version	Shows the version of the Antivirus.
Eng Version	Shows the version of the engine.
Dat Version	Shows the version of the data file.

Click **Add** to configure the Antivirus product specific checks. The values configured in the **Antivirus Product configuration** pop-up will be displayed in the **Antivirus** page. The following figure is an example of the **Antivirus Product configuration** pop-up:

Figure 275: Antivirus Product configuration Pop-up

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

Select the Antivirus product avast! Antivirus ▼

Product version check No Check ▼

Engine version check No Check ▼

Data file version check No Check ▼

Save Cancel

The following table describes the **Antivirus Product configuration** parameters:

Table 159: Antivirus Product configuration Parameters

Parameter	Description
Product-specific checks	Select this check box if you want to configure a specific antivirus product. If you want to allow any antivirus product, do not select this field.
Select the Antivirus product	Select the Antivirus from the drop-down list.
Product version check	Select to check the product version from the options: No Check, Is Latest, or In Last N Updates.

Table 159: Antivirus Product configuration Parameters (Continued)

Parameter	Description
Engine version check	Select to check the engine version from the options: No Check, Is Latest, or In Last N Updates.
Data file version check	Select to check the data file version from the options: No Check, Is Latest, or In Last N Updates.

Services

The **Services** page provides a set of widgets for specifying services to run or stop. The following figure displays the **Services** page:

Figure 276: Services Page

The following table describes the **Services** page parameters:

Table 160: 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).
User Notification	Enable to allow user notifications for service check 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). This list varies depending on OS types. Click the >> or << to add or remove, respectively, the services from the Service to run or Services to stop boxes.
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 .

W-ClearPass Macintosh OS X Universal System Health Validator: OnGuard Agent

To configure the W-ClearPass Universal System Health Validator for Macintosh OS X:

1. Navigate to **Configuration > Posture > Posture Policies**, then click **Add**.

The **Add Posture Policies** dialog appears.

Figure 277: Adding a Universal System Health Validator for a Mac OS X Posture Policy

Configuration » Posture » Posture Policies » Add

Posture Policies

Policy	Posture Plugins	Rules	Summary
Policy Name:	Mac OS X Posture Policy		
Description:			
Posture Agent:	☐ NAP Agent ☒ OnGuard Agent (Persistent or Dissolvable)		
Host Operating System:	☐ Windows ☐ Linux ☒ Mac OS X		
Restrict by Roles:	 Select or type role names Remove Add		

2. Specify the following:
 - a. **Policy Name/Description:** Enter the name and a description of the posture policy.
 - b. **Posture Agent:** Select **OnGuard Agent**.
 - c. **Host Operating System:** Select **Mac OS X**.
3. Click **Next**.

The **Posture Plugins** dialog appears.

Figure 278: Selecting the Mac OS X Universal System Health Validator Posture Plug-in

Configuration » Posture » Posture Policies » Add

Posture Policies

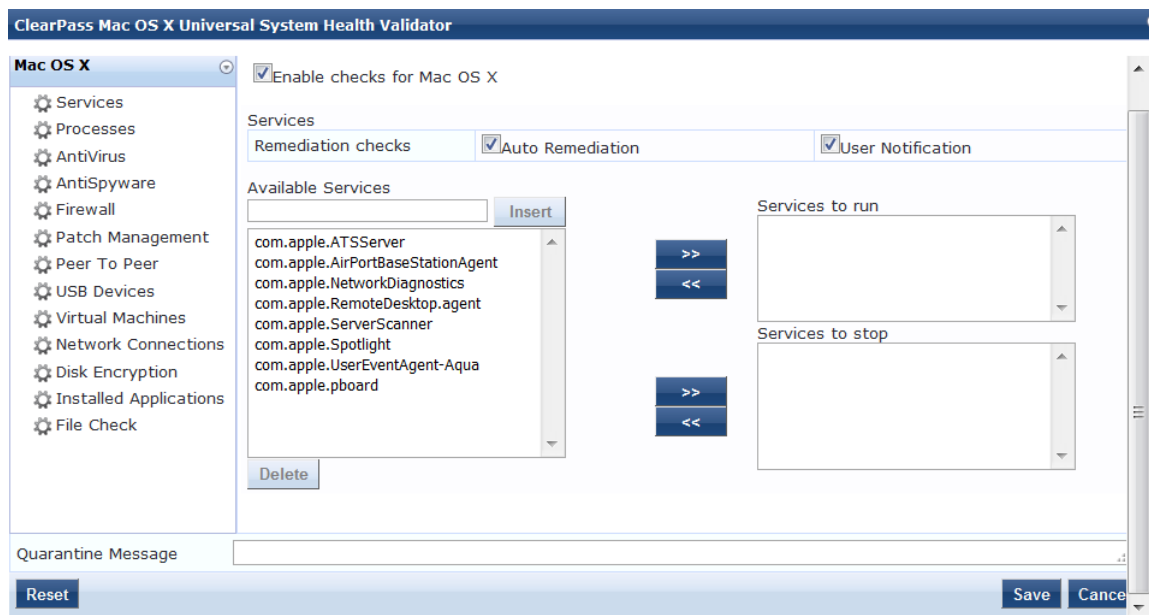
Policy	Posture Plugins	Rules	Summary
Select one/more plugins:			
☒	ClearPass Mac OS X Universal System Health Validator	Configure View	Not Configured

4. In the **Posture Plugins** page, click the check box for **ClearPass Mac OS X Universal System Health Validator**.
5. Click **Configure**.

The **ClearPass Mac OS X Universal System Health Validator** configuration page is displayed.
6. To enable checks for Mac OS X, select the **Enable checks for Mac OS X** check box.

The following configuration page appears:

Figure 279: Configuration Page: Mac OS X Universal System Health Validator



Enabling these check boxes display a corresponding set of configuration pages that are described in the following sections.

- [Services on page 308](#)
- [Processes on page 309](#)
- [Antivirus on page 310](#)
- [AntiSpyware on page 310](#)
- [Firewall on page 311](#)
- [Patch Management on page 312](#)
- [USB Devices on page 313](#)
- [Virtual Machine on page 313](#)
- [Network Connections on page 314](#)
- [Disk Encryption on page 314](#)
- [Installed Applications on page 315](#)
- [File Check on page 318](#)

Services

From the **Services** page, you can configure which services to run and which services to stop. See [ClearPass Windows Universal System Health Validator - OnGuard Agent on page 274](#) for description of the fields on this page.

The following figure displays the **Services** health class configuration page:

Figure 280: *Services Health Class Configuration Page*

☒ Enable checks for Mac OS X

Services

Remediation checks ☒ Auto Remediation ☒ User Notification

Available Services

Insert

com.apple.ATSServer
com.apple.AirPortBaseStationAgent
com.apple.NetworkDiagnostics
com.apple.RemoteDesktop.agent
com.apple.ServerScanner
com.apple.Spotlight
com.apple.UserEventAgent-Aqua
com.apple.pboard

Delete

>>
<<

Services to run

>>
<<

Services to stop

Processes

From the **Processes** page, you can view and add processes. Clicking **Enable checks for Mac OS X** provides a set of components to specify the processes that need to be explicitly present or absent on the system.

Figure 281: *Processes Page*

☒ Enable checks for Mac OS X

Remediation checks ☒ Auto Remediation ☒ User Notification

Processes to be Present **Add**

Process Path	Process Name	
Process MD5 Sum	Process Name	

Processes to be Absent **Add**

Process MD5 Sum	Process Name	

Click **Add** to open the page with options to configure the name, location, and display name of the processes. The following figure displays the **Process to be Present - Add** page:

Figure 282: *Processes to be Present - Add Page*

☒ Enable checks for Mac OS X

Process to be Present - Add

Process Location

Enter the Process name

Enter the Display name

Save **Cancel**

Antivirus

In the **Antivirus** page, you can specify information about the antivirus application. Click on **An antivirus-application is on** to configure the anti-virus application information.

The following figure displays the **Antivirus** page:

Figure 283: Antivirus Page (Detail 1)

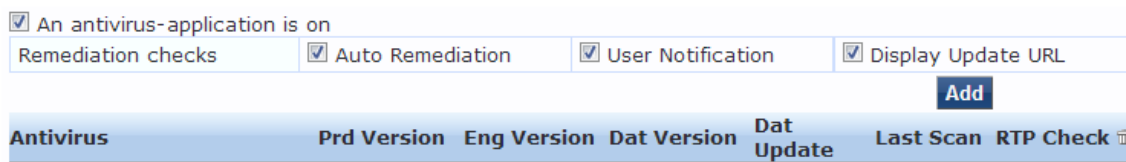


Figure 283 shows the top section of the Antivirus configuration page. It includes a header bar with the following items: 'An antivirus-application is on' (checked), 'Remediation checks', 'Auto Remediation' (checked), 'User Notification' (checked), 'Display Update URL' (checked), and an 'Add' button. Below this is a table with columns: 'Antivirus', 'Prd Version', 'Eng Version', 'Dat Version', 'Dat Update', 'Last Scan', 'RTP Check', and a trash icon.

Click **Add** to specify product and version check information in the antivirus configuration page.

Figure 284: Antivirus Configuration Page (Detail 2)

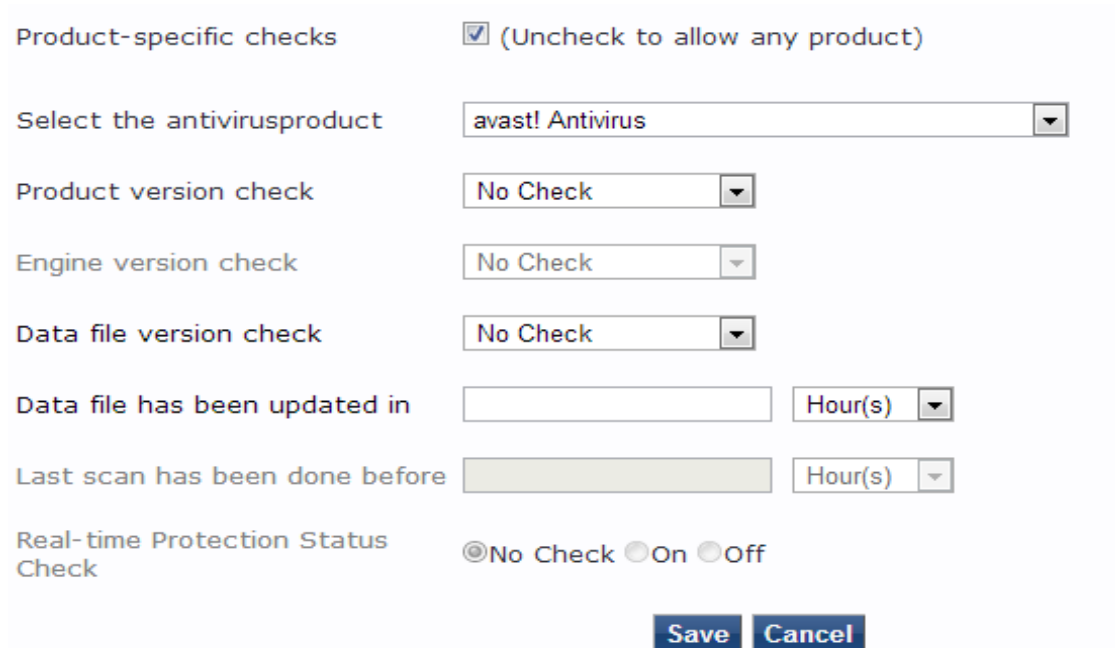


Figure 284 shows the configuration options for the antivirus application. It includes a 'Product-specific checks' section with a checkbox '(Uncheck to allow any product)' which is checked. Below this are several dropdown menus: 'Select the antivirusproduct' (set to 'avast! Antivirus'), 'Product version check' (set to 'No Check'), 'Engine version check' (set to 'No Check'), and 'Data file version check' (set to 'No Check'). There are also input fields for 'Data file has been updated in' and 'Last scan has been done before', both with 'Hour(s)' dropdown menus. At the bottom, there is a 'Real-time Protection Status Check' section with radio buttons for 'No Check' (selected), 'On', and 'Off'. 'Save' and 'Cancel' buttons are at the bottom right.

When you save your antivirus configuration, it appears in the **Antivirus** page list. See [ClearPass Windows Universal System Health Validator - OnGuard Agent on page 274](#) for antivirus page and field descriptions.

AntiSpyware

In the **AntiSpyware** page, an administrator can specify information about the antispyware application. The following figures describe the examples of the **AntiSpyware** page and the **AntiSpyware - Add** page:

Figure 285: Anti-Spyware Page

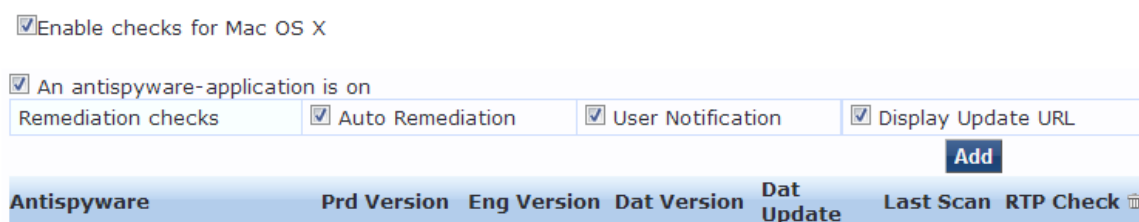


Figure 285 shows the Anti-Spyware configuration page. It includes a header bar with the following items: 'Enable checks for Mac OS X' (checked), 'An antispyware-application is on' (checked), 'Remediation checks', 'Auto Remediation' (checked), 'User Notification' (checked), 'Display Update URL' (checked), and an 'Add' button. Below this is a table with columns: 'Antispyware', 'Prd Version', 'Eng Version', 'Dat Version', 'Dat Update', 'Last Scan', 'RTP Check', and a trash icon.

In the **Antispyware** page, click **An Antispyware Application is On** to configure different configuration elements specific to the antispyware product that you select. When you save the antispyware configuration, it appears in the **Antispyware** page list.

Figure 286: *Anti-Spyware Add Page*

☒ Enable checks for Mac OS X

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

Select the antispyware product

Product version check

Engine version check

Data file version check

Data file has been updated in Hour(s)

Last scan has been done before Hour(s)

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

Save **Cancel**



The configuration elements are the same for antivirus and antispyware products.

Firewall

From the **Firewall** page, click **A Firewall Application is On** to configure the firewall application information. The following figure displays the **Firewall** page:

Figure 287: *Firewall Page*

☒ Enable checks for Mac OS X

☒ A firewall application is on

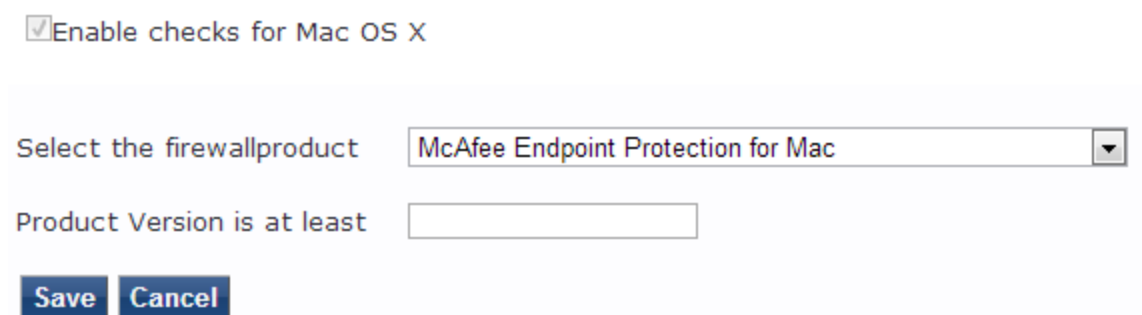
Remediation checks	☒ Auto Remediation	☒ User Notification
Product-specific checks	☒ (Uncheck to allow any product)	

Add

Firewall Product Name	Product Version	

Click **Add** from the **Firewall** page to configure different configuration elements specific to the firewall product that you select. When you save the firewall configuration, it appears in the **Firewall** page list.

Figure 288: Firewall Add Page



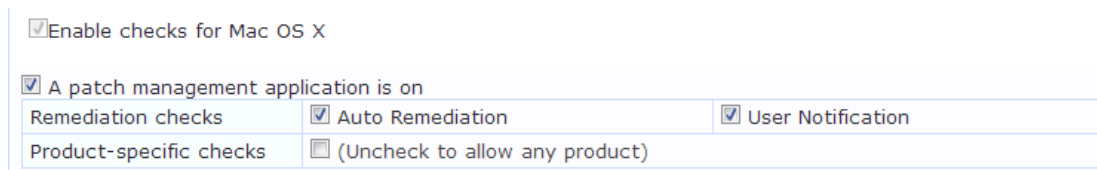
When enabled, the **Firewall** detail page appears. See [ClearPass Windows Universal System Health Validator - OnGuard Agent on page 274](#) for firewall page and field descriptions.

Patch Management

From the **Patch Management** page, you can view and add the patch management product. Select **A patch management application is on** to configure auto remediation and user notification features.

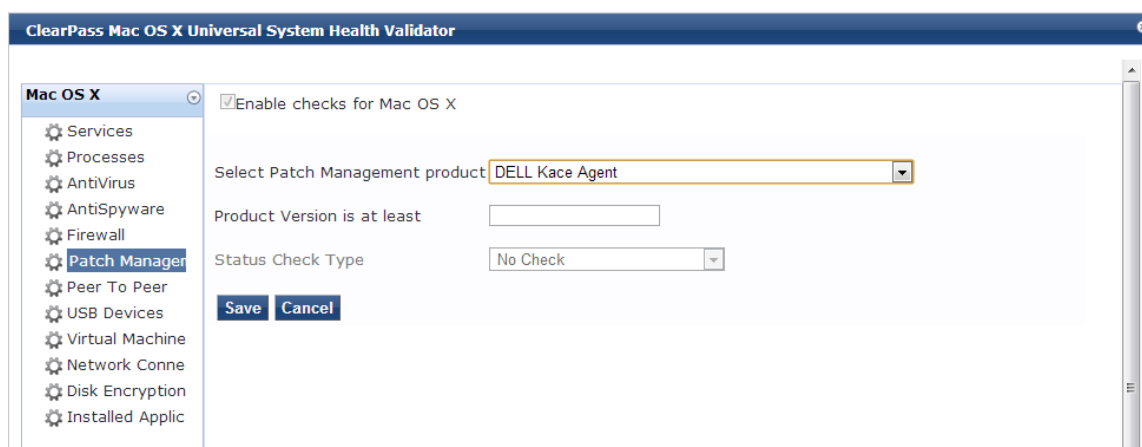
The following figure displays the **Patch Management** page:

Figure 289: Patch Management Page



Click **Add** in the **Patch Management** page to view the configuration options for the specific patch management product. The following figure displays the **Patch Management - Add** page:

Figure 290: Patch Management - Add Page



Peer To Peer

From the **Peer To Peer** page, you can view and add peer-to-peer applications. Clicking **A Peer to Peer application is on** provides configuration options to specify peer to peer applications or networks that need to be explicitly stopped. When you select a peer to peer network, all applications that make use of that network are stopped.

The following figure displays the **Peer To Peer** page:

Figure 291: *Peer To Peer Page*

The screenshot shows the 'Peer To Peer' configuration page. At the top, there are two checked checkboxes: 'Enable checks for Mac OS X' and 'A Peer to Peer application is on'. Below these, there are three tabs: 'Remediation checks', 'Auto Remediation' (which is selected), and 'User Notification' (also selected). Under the 'Auto Remediation' tab, there are two radio buttons: 'By Application' (selected) and 'By Network'. Below the 'By Application' radio button, there is a list of 'Available Applications' including Acqlite, Acquisition, Bits on Wheels, BitTorrent, Gotcha!, LimeWire, Miro, Mojo, Phex, Poisoned, and ShakesPeer. To the right of this list are two blue buttons with white arrows: '>>' and '<<'. Further right is an empty list box labeled 'Applications to stop'.

USB Devices

Use this page to configure the **Auto Remediation** and **User Notification** parameters. You can also configure the options to take remediation action for USB mass storage devices or to remove USB mass storage devices from the **Remediation Action for USB Mass Storage Devices** drop-down.

The following figure displays the **USB Devices** page:

Figure 292: *USB Devices Page*

The screenshot shows the 'USB Devices' configuration page. On the left, there is a sidebar with a 'Mac OS X' header and a list of system components: Services, Processes, AntiVirus, AntiSpyware, Firewall, and Patch Manager. The main content area has a checked checkbox for 'Enable checks for Mac OS X'. Below this, there are three tabs: 'USB Devices', 'Remediation checks', 'Auto Remediation' (selected), and 'User Notification' (selected). Under the 'Auto Remediation' tab, there is a section for 'Remediation Action for USB Mass Storage Devices' with a drop-down menu currently set to 'No Action'.

Virtual Machine

The **Virtual Machines** page provides configuration options to virtual machines utilized by the network. Select the **Virtual Machine Detection is on** option to enable the **Auto Remediation** and **User Notification** options.

The following figure displays the **Virtual Machine** page:

Figure 293: *Virtual Machine Page*

The screenshot shows the 'Virtual Machine' configuration page. At the top, there are two checked checkboxes: 'Enable checks for Mac OS X' and 'Virtual Machine Detection is on'. Below these, there are three tabs: 'Remediation checks', 'Auto Remediation' (selected), and 'User Notification' (selected). Under the 'Auto Remediation' tab, there are two checked checkboxes: 'Allow access to clients running on Virtual Machine' and 'Allow access to clients hosting Virtual Machines'. At the bottom, there is a section for 'Remediation Action for clients hosting Virtual Machines' with a drop-down menu currently set to 'No Action'.

Network Connections

The **Network Connections** page provides configuration options to control network connections based on connection type. Enabling the **Network Connection Check is on** check box provides the options to specify the remediation checks or user notification.

The following figure displays the **Network connections** page:

Figure 294: *Network Connections Page*

☒ Enable checks for Mac OS X

☒ Network Connection Check is on

Remediation checks: ☒ Auto Remediation ☒ User Notification

☐ Check for Network Connection Types **Configure**

Network Connection Types	Network Connections Allowed	Remediation Action For Network Connection Types Not Allowed
-	-	-

Select the **Check for Network Connection Types** check box from the **Network Connections** page, and then click **Configure** to specify type of network connection. You can select and allow the network connection types from the **Network Connections Configuration** page as described in the following figure:

Figure 295: *Network Connections Configuration Page*

☒ Enable checks for Mac OS X

Network Connection Types

Allowed Network Connections Type:

Network Connection Types: Others, Wired, Wireless

Network Connections Allowed:

Remediation Action For Network Connection Types Not Allowed:

Save **Cancel**

Disk Encryption

Disk encryption is a technology that protects information by converting it into unreadable code that cannot be deciphered easily by unauthorized people. Disk encryption uses disk encryption software or hardware to encrypt every bit of data that goes on a disk or disk volume. Disk encryption prevents unauthorized access to data storage.

The following figure displays the **Disk Encryption** page:

Figure 296: *Disk Encryption Page*

☒ Enable checks for Mac OS X

☒ A disk encryption application is on

Remediation checks: ☐ Auto Remediation ☒ User Notification

Add

Disk Encryption Product Name	Product Version	Locations to Check

Click **A disk encryption application is on** from the **Disk Encryption** page to configure the remediation options. Click **Add** to configure the product specific encryption checks. You can select the **Uncheck to allow any product** check box from the **Product-specific checks** field to not to allow any encryption product to check disk encryption.

The following image is an example of the **Disk Encryption - Add** page:

Figure 297: *Disk Encryption Add Page*

☒ Enable checks for Mac OS X

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

Select Disk Encryption product CREDANT Shield

Product Version is at least

Locations to Check None

Save **Cancel**

Installed Applications

The **Installed Applications** category groups classes that represent software-related objects.

From the **Installed Applications** page, you can specify information about which installed applications you want to monitor.

Figure 298: *Installed Applications Page for Macintosh OS X*

ClearPass Mac OS X Universal System Health Validator

Mac OS X

- Services
- Processes
- AntiVirus
- AntiSpyware
- Firewall
- Patch Management
- Peer To Peer
- USB Devices
- Virtual Machines
- Network Connections
- Disk Encryption
- Installed Applications**
- File Check

☒ Enable checks for Mac OS X

☒ Installed Applications Check is on

Remediation checks ☐ Auto Remediation ☒ User Notification

Monitor Mode ☐ (Check to enable Monitor Mode)

Applications Allowed (Mandatory) **Add**

Application Name	Regular Expression Enabled	Remediation Message

Applications Allowed (Optional) **Add**

Application Name	Regular Expression Enabled	Remediation Message

☐ Allow only Mandatory and Optional Applications

Applications Not Allowed **Add**

Application Name	Regular Expression Enabled	Remediation Message

Quarantine Message

Reset **Save** **Cancel**

The following table describes the **Installed Applications for Mac OSX Configuration** page parameters:

Table 161: *Installed Applications for Mac OS X Configuration Page Parameters*

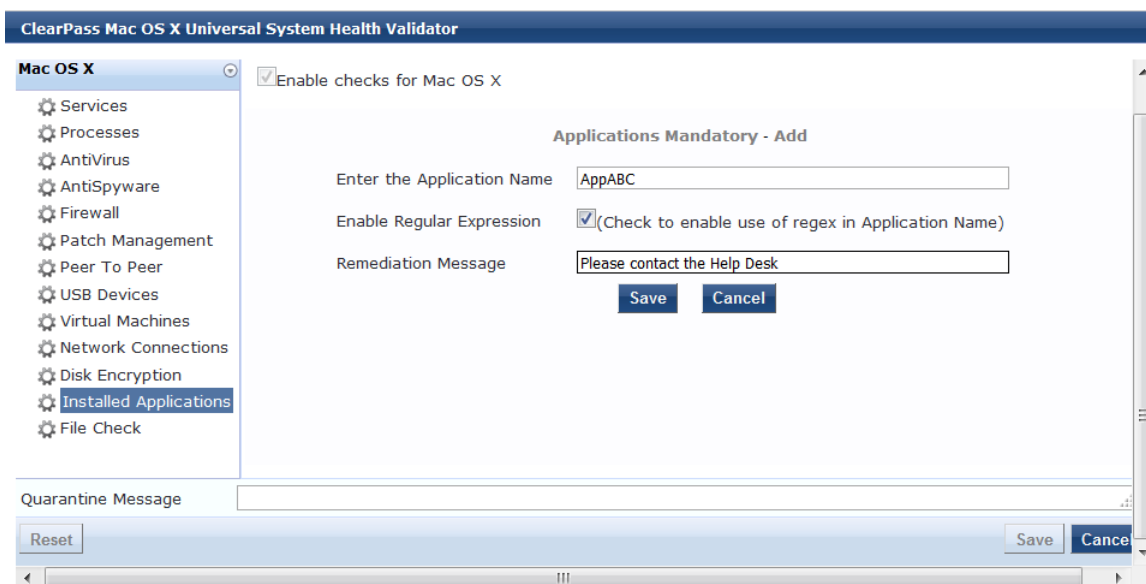
Parameter	Action/Description
Remediation checks	Auto-Remediation for the Installed Applications health class is not supported.
User Notification	1. Enable sending a remediation message with a list of applications to install or uninstall to the user.
Monitor Mode	2. Enable Monitor Mode to treat all the installed applications as always healthy.
Applications Allowed (Mandatory)	3. Specify installed applications to be monitored on a mandatory basis. NOTE: Enter the application names as they are shown in Add/Remove Programs.
Applications Allowed (Optional)	4. Specify installed applications to be monitored on an optional basis. NOTE: Enter the application name as they are shown in Add/Remove Programs.
Allow only Mandatory and Optional Applications	5. Specify that only the mandatory and optional applications are monitored. NOTE: All applications that are not either mandatory or optional must be removed or uninstalled.

Enabling Regular Expressions for a Mac OS X Application

To enable regular expressions for an application:

1. From the **ClearPass Windows Universal System Health Validator > Configure** page (see [W-ClearPass Macintosh OS X Universal System Health Validator: OnGuard Agent on page 307](#)), select **Installed Applications**.
2. Click (enable) the **Installed Applications Check is on** check box.
The Installed Applications dialog appears (see above).
3. From the desired **Applications Allowed** category, click **Add**.
The Mandatory Applications dialog appears for the selected **Applications Allowed** category (see [Figure 299](#)).

Figure 299: Enabling Regular Expression



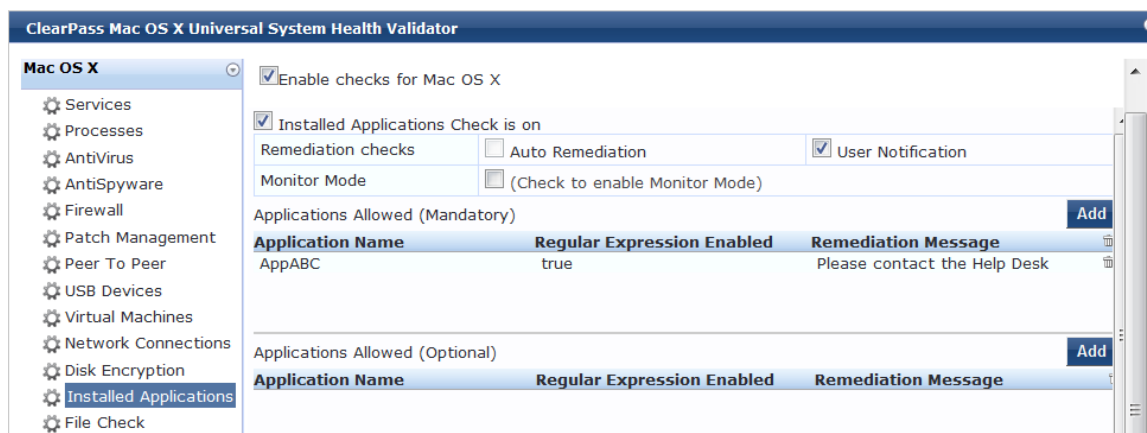
4. Configure the **Add Mandatory Applications** parameters as described in [Table 162](#).

Table 162: Add Mandatory Applications Parameters

Parameter	Action/Description
Enter the Application Name	1. Enter the name of the application.
Enable Regular Expression	2. Check (enable) this check box to enable the use of regular expressions in the Application Name . When this field is enabled, W-ClearPass treats the Application Name as regular expression when comparing application names.
Remediation Message	3. Optionally, enter the remediation message that will be displayed to the user in the event of an error. NOTE: Remediation messages can include reasons for remediation, links to helpful URLs and helpdesk contact information.
	4. Click Save .

You return to the **Installed Applications** dialog, where **Regular Expression Enabled** is set to **true** for the specified application (see [Figure 300](#)).

Figure 300: Regular Expression Enabled



File Check

From the **File Check** page, you can turn on the file check feature and specify information about which the files you want to check.

Use the **File Check** page to verify the group of files to be present or absent.

The following figure is an example of the **File Check** health class configuration dialog:

Figure 301: Mac OS X File Check Health Class Configuration

The following table describes the **File Check Configuration** parameters:

Table 163: File Check Configuration Parameters

Parameter	Action/Description
Remediation checks	Auto-remediation for the File Check health class is not supported.
User Notification	1. When enabled, a remediation message that includes the groups of files to be present or absent is displayed to the end user.
Monitor Mode	2. To treat all the file check health classes as always healthy, enable Monitor Mode .
File Groups to be Present	3. To add the files to be present in the File Check health class, click Add .
File Groups to be Absent	4. To add the files to be absent in the File Check health class, click Add .

1. To open the **File Group to be Present > Add** page, click **Add**:
You can configure the name of the file group and specify the evaluation rule for the file group.
The following figure displays the **File Group to Be Present > Add** dialog:

Figure 302: MacOSX File Group to Be Present > Add Dialog

The following table describes the **File Group to Be Present > Add** parameters:

Table 164: File Group to Be Present > Add Parameters

Parameter	Action/Description
Enter the File Group Name	1. Enter the name of the file group.
File Group Evaluation Rule	2. Select the appropriate File Group Evaluation Rule: • Pass All: Select this evaluation rule if you want the File Check health class to be deemed as 'healthy' only if all the configured file groups are present. • Pass Any One: Select this evaluation rule if you want the File Check health class to be deemed as 'healthy' even if any one of the configured file groups are present.

3. To configure the name of the file group and the evaluation rule for the file group, from **File Groups to be Present**, click **Add**.

The following figure displays the **File to Be Present > Add** page:

Figure 303: File to be Present > Add Dialog

The following table describes the **File to Be Present > Add** parameters:

Table 165: *File to Be Present > Add Parameters*

Parameter	Action/Description
File Location	1. Select any location of the file from the drop-down list: • Applications • UserBin • UserLocalBin • UserSBin • None
Enter the File Path	2. Enter the file path as described in the examples from the GUI.
Enter the File Name	3. Enter the name of the file.
Enter the MD5 Sum	Optionally, you can specify one or more (comma separated) MD5 checksums of the process executable file.
Remediation Message	4. Specify the custom remediation message to be displayed to end users if File check fails.

5. When finished, click **Save**.

The parameters configured in the **File to Be Present > Add** dialog are reflected in the **File Groups to be Present** dialog as illustrated in the following figure:

Figure 304: *File Group to Be Present Parameters Displayed*

☒ Enable checks for Mac OS X

File Group to be Present - Add

Enter the File Group Name:

File Group Evaluation Rule:

Files to be Present

File Location	File Path	File Name	File MD5 Sum	Remediation Message
Applications	Applications/Keynote	Keynote	-	Keynote is successfully installed.

Add

Save **Cancel**

Configuring NAP Agent Plugins

If your posture policy is using a NAP agent, the **Posture Plugins** tab allows you to configure the following plug-in types:

- [Windows System Health Validator: NAP Agent on page 321](#)
- [Windows Security Health Validator: NAP Agent on page 322](#)

The following figure displays the **NAP Agent - Posture Plugins** tab:

Figure 305: *NAP Agent - Posture Plugins Options*

Configuration » Posture » Posture Policies » Add

Posture Policies

Policy	Posture Plugins	Rules	Summary	
Select one/more plugins:				
Plugin Name		Plugin Configuration		Status
☐	Windows System Health Validator	Configure	View	-
☐	Windows Security Health Validator	Configure	View	-

Windows System Health Validator: NAP Agent

The Windows System Health Validator NAP (Network Access Protection) Agent checks for the level of Windows Service Packs.

To configure the minimum service pack level required, perform the following steps:

1. Navigate to **Configuration > Posture > Posture Policies**.

The Posture Policies page appears.

2. Click **Add**.

The **Add Posture Policies > Policy** dialog appears.

Figure 306: *Adding a Windows NAP Agent Posture Policy*

Configuration » Posture » Posture Policies » Add

Posture Policies

Policy		Posture Plugins		Rules		Summary	
Policy Name:							
Description:							
Posture Agent:		☐ NAP Agent ☒ OnGuard Agent (Persistent or Dissolvable)					
Host Operating System:		☒ Windows ☐ Linux ☐ Mac OS X					
Restrict by Roles:				Remove			
		Select or type role names				Add	

3. Specify the following:

- a. **Policy Name/Description:** Enter the name and description of the posture policy.
- b. **Posture Agent:** Select **NAP Agent**.
- c. **Host Operating System:** Select **Windows**.

4. Click **Next**.

The **Posture Policies > Posture Plugins** page appears.

Figure 307: Posture Plugins for Windows Health Validators

Configuration » Posture » Posture Policies » Add

Posture Policies

Policy Posture Plugins Rules Summary

Select one/more plugins:

Plugin Name	Plugin Configuration	Status
☒ Windows System Health Validator	Configure View	Not Configured
☐ Windows Security Health Validator	Configure View	-

- From the **Posture Plugins** tab, select **Windows System Health Validator**, then click the **Configure** button.

The **Windows System Health Validator** page appears:

Figure 308: Onguard NAP Agent: Windows System Health Validator

Windows System Health Validator

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

☒ **Windows 10**
Windows 10 clients are allowed
☐ Restrict clients which have Service Pack less than

☒ **Windows 8**
Windows 8 clients are allowed
☐ Restrict clients which have Service Pack less than

☒ **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

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

- To enable support of specific Windows operating systems, click the corresponding check boxes.
- Enable the **Restrict clients...** check box and specify the minimum Service Pack level required on the client computer to connect to your network.
- Click **Save**.

You return to the Posture Plugins page where the status of the plug-in is now **Configured**.

Windows Security Health Validator: NAP Agent

The Windows Security Health Validator: NAP (Network Access Protection) Agent checks for the presence of specific types of security applications. You can use the check boxes to restrict access based on the absence of the selected security application types.

To configure the minimum service pack level required, perform the following steps:

- Navigate to **Configuration > Posture > Posture Policies**.

The Posture Policies page appears.

- Click **Add**.

The Add Posture Policies dialog appears.

Figure 309: Adding Windows Security Health Validator: NAP Agent Posture Policy

Configuration » Posture » Posture Policies » Add

Posture Policies

Policy	Posture Plugins	Rules	Summary
Policy Name:	Windows Security Health Validator		
Description:	Checks for the presence of specific types of security applications		
Posture Agent:	☒ NAP Agent ☐ OnGuard Agent (Persistent or Dissolvable)		
Host Operating System:	☒ Windows ☐ Linux ☐ Mac OS X		
Restrict by Roles:	Remove Add		

3. Specify the following:
 - a. **Policy Name:** Enter the name of the posture policy.
 - b. **Posture Agent:** Select **NAP Agent**.
 - c. **Host Operating System:** Select **Windows**.

4. Click **Next**.

The **Posture Policies > Posture Plugins** page appears.

Figure 310: Selecting Posture Plugins for Windows Security Health Validator: NAP Agent

Configuration » Posture » Posture Policies » Add

Posture Policies

Policy	Posture Plugins	Rules	Summary
Select one/more plugins:			
Plugin Name	Plugin Configuration	Status	
☐ Windows System Health Validator	Configure View	-	
☒ Windows Security Health Validator	Configure View	Not Configured	

5. From the **Posture Plugins** page, select **Windows Security Health Validator**, then click **Configure**.
The **Windows System Health Validator** page appears:.
6. Click the **Enable checks for Windows 10** check box.
The Windows Security Health Validator configuration page appears as shown in [Figure 311](#).

Figure 311: *Windows Security Health Validator*

7. To enable support of specific operating systems, click the corresponding check boxes.

8. Click **Save**.

You return to the **Posture Plugins** page where the status of the Windows Security Health Validator plug-in is now **Configured**.

Configuring Posture Policy Rules

Once you have defined the posture hosts, agents, and plugins, you must configure the rules for the posture policy. To configure posture policy rules, navigate to **Configuration > Posture > Posture Policies > Add**, and click the **Rules** tab on the **Posture Policies** window.

Figure 312: Posture Policy Rules Tab and Rules Editor

Configuration » Posture » Posture Policies » Add

Posture Policies

Rules Evaluation Algorithm: First applicable

Conditions **Posture Token**

Add Rule Move Up Move Down Edit Rule Remove Rule

Rules Editor

Conditions

Select Plugin Checks: Passes all SHV checks

Select Plugins: ☐ Windows System Health Validator ☐ Windows Security Health Validator

Actions

Posture Token: HEALTHY (0)

Save Cancel

The following table describes the **Rules Editor** configuration parameters:

Table 166: Posture Policy Rules Editor Parameters

Parameter	Description
Select Plugin Checks	Click select one of the following plugin check types for System Health Validators (SHVs): • Passes all SHV checks • Passes one or more SHV checks • Fails all SHV checks • Fails one or more SHV checks
Select Plugins	Select the plug-in to which the plug-in checks should apply.
Posture Token	Select one of the following posture token types.

Configuring Posture for Services

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. To configure the posture for a service, navigate to the **Add Service (Configuration > Services > Add)** page. The **Posture** tab is not enabled by default. To enable posture checking for this service, select the **Posture Compliance** check box from the **More Options** field on the **Service** tab.

You can enable the posture checking for this kind of service, if you deploy any of the following:

- Policy Manager in a Microsoft Network Access Protection (NAP)
- Cisco Network Admission Control (NAC) Framework environment

- Dell hosted captive portal that performs posture checks through a dissolvable agent

The following figure displays an example on how to configure a posture at the service level:



The **Posture Compliance** check box must be selected on the **Service** tab in order for posture to be enabled.

Figure 313: *Posture Features at the Service Level*

You can configure the following components of a posture:

Table 167: *Posture Features at the Service Level*

Configurable Component	How to Configure
Sequence of Posture Policies	Select a policy, then select Move Up, Move Down, Remove, or View Details. • To add a previously configured policy, select from the Select drop-down list, then click Add. • To configure a new policy, click the Add link at the top-right corner of the Configuration > Posture Policies page. For more information, see Configuring Posture Policy Agents and Hosts on page 269. • To edit the selected posture policy, click Modify. For more information, see Configuring Posture Policy Agents and Hosts on page 269.
Default Posture Token	The default posture token is UNKNOWN (100). You can select the default posture token from the drop-down list.
Remediation End-Hosts	Select this check box to enable auto-remediation action on non-compliant endpoints.

Table 167: *Posture Features at the Service Level (Continued)*

Configurable Component	How to Configure
Remediation URL	This URL defines where to send additional remediation information to endpoints.
Sequence of Posture Servers	Select a posture server, then select Move Up, Move Down, Remove, or View Details. • To add a previously configured posture server, select from the Select drop-down list, then click Add. • To configure a new posture server, click Add link at the top-right corner of the Configuration > Posture Policies page. For more information, see Adding and Modifying Posture Servers. • To edit the selected posture server, click Modify. For more information, see Adding and Modifying Posture Servers.
Enable auto-remediation of non-compliant end-hosts	Select the Enable auto-remediation of non-compliant end-hosts check box to enable the specified remediation server to enable auto-remediation. Remediation server is optional. A popup appears on the client box with the URL of the remediation server.

Configuring Audit Servers

The W-ClearPass W-Policy Manager server contains default Nessus (v2.X through v6.x) and NMAP servers. For enterprises with existing audit server infrastructure, or with external audit servers, W-Policy Manager supports these servers externally.

For more information, see:

- [Default Audit Servers on page 328](#)
- [Custom Audit Servers on page 331](#)
- [Post-Audit Rules on page 340](#)

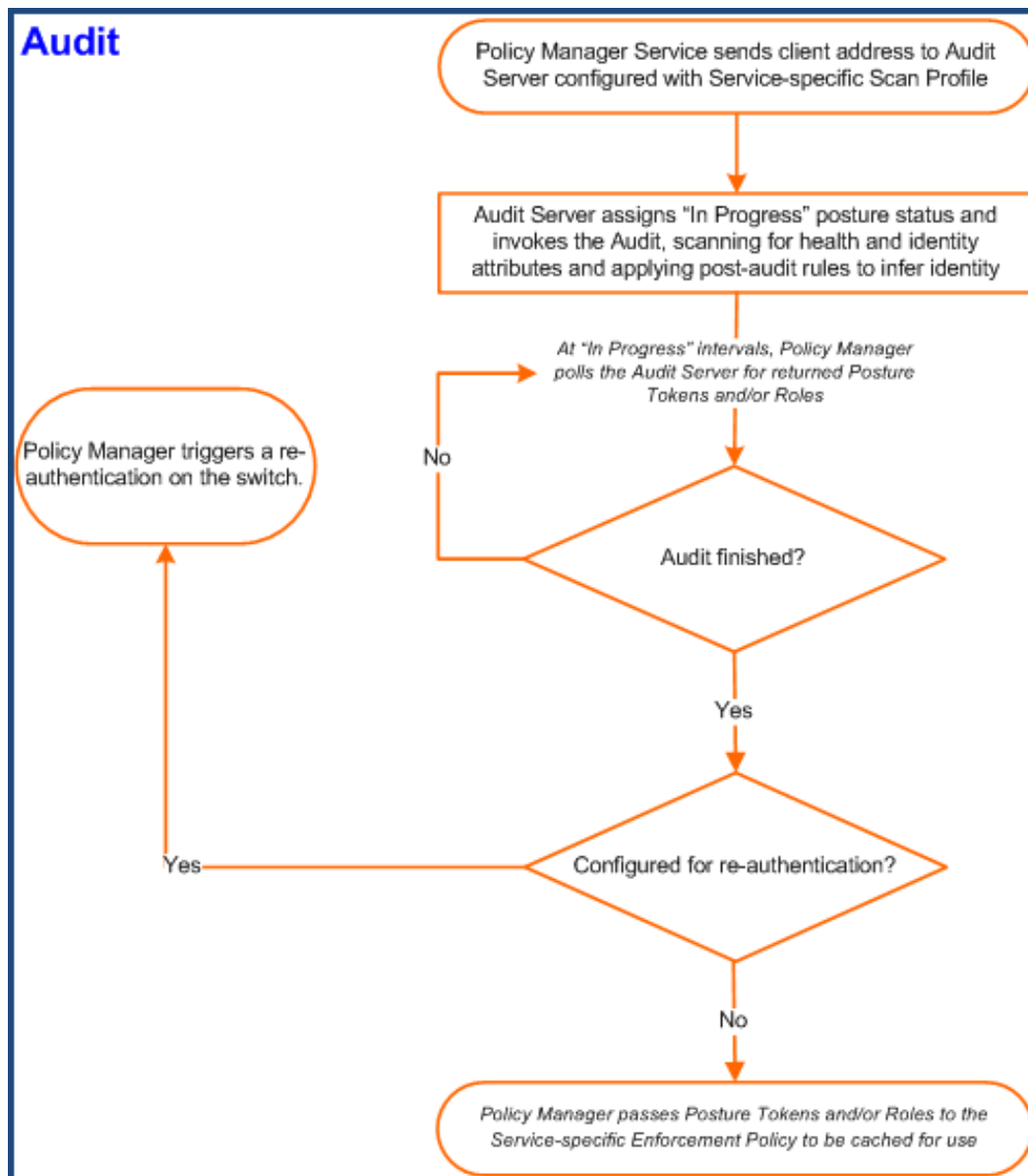
Audit Service Flow Control

Audit servers evaluate posture, role, or both for unmanaged or unmanageable clients. One example is clients that lack an adequate posture agent or an 802.1X supplicant. For example, printers, PDAs, or guest users might not be able to send posture credentials or identify themselves.

A W-Policy Manager Service can trigger an audit by sending a client ID to a pre-configured audit server, and the server returns attributes for role mapping and posture evaluation.

Audit servers are configured at a global level. Only one audit server can be associated with a service. The flow-of-control of the audit process is shown in the figure below.

Figure 314: *Flow of Policy Manager Auditing Control*



Default Audit Servers

When you configure an audit as part of a W-Policy Manager service, you can select the default Nessus (Nessus Server) or NMAP (Nmap Audit) configuration.

Adding Auditing to a Policy Manager Service

To configure an audit server for a new service:

1. Navigate to **Configuration > Services**.
The **Services** page opens.
2. Select the **Add** link in the top-right corner.
The **Add Services** dialog opens.
3. To display the **Audit** tab, select the **More Options > Audit End-Hosts** check box.
4. In the **Add Services** dialog, select the **Audit** tab.

The **Add Services > Audit** dialog opens.

Figure 315: Add Services > Audit Dialog

Configuration » Services » Add

Services

Service

Authentication

Roles

Enforcement

Audit

Summary

Audit Server:

--Select--

View Details

Modify

Add new Audit Server

Audit Trigger Conditions:

Always

When posture is not available

For MAC authentication request

Action after audit:

No Action

Do SNMP bounce

Trigger RADIUS CoA action

Back to Services

Next >

Save

Cancel

5. Complete the fields in the **Add Services > Audit** tab as described in Table 168, then click **Save**.

Table 168: Add Services > Audit Dialog Parameters

Parameter	Description
Audit Server	Select a built-in server profile from the list: ● Nessus Server: Performs vulnerability scanning and returns a Healthy/Quarantine result. ● Nmap Audit: Performs network port scans. The health evaluation always returns a Healthy result. The port scan gathers attributes that allow determination of role(s) through post-audit rules. You can click the View Details button to view the Policy Manager Entity Details dialog with the summary of audit server details. To view the Summary tab with audit server details, click the Modify button. For W-Policy Manager to trigger an audit on an end-host, it needs to get the IP address of the end-host. The IP address of the end-host is not available at the time of initial authentication for 802.1X and MAC authentication requests. W-Policy Manager's DHCP snooping service examines the DHCP request and response packets to derive the IP address of the end-host. For this to work, you need to use this service, W-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. To audit devices that have a static IP address assigned, it is recommended that you create a static binding between the MAC address and IP address of the endpoint in your DHCP server. Refer to your DHCP server documentation for configuring static bindings. NOTE: W-Policy Manager does not issue the IP address; it only examines the DHCP traffic to derive the IP address of the end-host.
Audit Trigger Conditions	Select from the following audit trigger conditions: ● Always: Always perform an audit. ● When posture is not available: Perform audit only when posture credentials are not available in the request. ● For MAC Authentication Request: If you select this option, then W-Policy Manager presents the following three additional settings: ■ For known end-hosts only: Select this option when you want to reject unknown end-hosts and to audit known clients. Known end-hosts are defined as clients that are found in the authentication source(s) associated with this service. ■ For unknown end-hosts only: Select this option when known end-hosts are assumed to be healthy, but you want to establish the identity of unknown end-hosts and assign roles. Unknown end-hosts are end-hosts that are not found in any of the authentication sources associated with this service. ■ For all end-hosts: For both known and unknown end-hosts.
Action after audit	Select an Action after audit. Performing an audit on a client is an asynchronous task, which means the audit can be performed only after the MAC authentication request is completed and the client has acquired an IP address through DHCP. Once the audit results are available, there should be a way for W-Policy Manager to re-apply policies on the network device. This can be accomplished in one of the following ways: ● No Action: The audit will not apply policies on the network device after this audit.

Table 168: Add Services > Audit Dialog Parameters (Continued)

Parameter	Description
	• Do SNMP bounce: This option will bounce the switch port or force an 802.1X reauthentication (both done using SNMP). 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. • Trigger RADIUS CoA action: This option sends a RADIUS CoA command to the network device.

Modifying Default Audit Servers

To reconfigure default W-Policy Manager audit servers:

1. Navigate to **Configuration > Posture > Audit Servers**.

Figure 316: Audit Servers Page

Configuration > Posture > Audit Servers

Audit Servers

Filter: Name contains [] Go Clear Filter

Show 10 records

#	Name	Description	Type
1.	[Nessus Server]	Nessus server running in the Policy Manager server	NESSUS
2.	[Nmap Audit]	Nmap default configuration	NMAP

Showing 1-2 of 2

Copy Export Delete

2. Select an audit server from the list of available servers.
The **Edit Audit Servers** page opens.
3. Modify the profile, plugins, and/or preferences.
 - In the **Audit** tab, you can modify the In-Progress Posture Status and Default Posture Status.
 - If you selected a Nessus Server, the **Primary Server** and **Backup Server** tabs allow you to specify a scan profile. In addition, when you add a new scan profile, you can select plugins and preferences for the profile. Refer to [Nessus Scan Profiles on page 335](#) for more information.The default W-Policy Manager Nessus audit server ships with approximately 1,000 of the most commonly used Nessus plugins.

Rules Tab

In the **Rules** tab, you can create post-audit rules for determining roles based on identity attributes discovered by the audit. For more information on creating post-audit rules, see [Post-Audit Rules on page 340](#).

Custom Audit Servers

This section provides the following information:

- [Adding a Nessus Audit Server on page 332](#)
- [Required Configuration Updates for External Nessus Servers](#)
- [Adding an Nmap Audit Server on page 338](#)

For enterprises with existing audit server infrastructure or preferring custom audit servers, W-Policy Manager supports Nessus (v2.x through v6.x) and Nmap scans using the NMAP plug-in on external Nessus servers.

Adding a Nessus Audit Server

W-ClearPass uses the Nessus audit server interface primarily to perform vulnerability scanning. It returns a result of *Healthy* or *Quarantine*.

To add a Nessus audit server:

1. Navigate to **Configuration > Posture > Audit Servers**, then click **Add**.

The **Add Audit Servers** dialog opens to the **Audit** tab.

Figure 317: Add Nessus Audit Server > Audit Tab

Configuration » Posture » Audit Servers » Add

Audit Servers

Audit Primary Server Backup Server Rules Summary

Name:

Description:

Type: ☐ NMAP ☒ NESSUS

In-Progress Posture Status:

Default Posture Status:

Back to Audit Servers

2. Specify the **Nessus Audit Server > Audit** tab parameters as described in [Table 169](#).

Table 169: Add Nessus Audit Server > Audit Tab Parameters

Parameter	Action/Description
Name	Specify the name of the audit server.
Description	Optionally (and recommended), enter the description that provides additional information about the audit server.
Type	Specify the type of audit server: Nmap (Network Mapper) or Nessus .
In-Progress Posture Status	Specify the posture status during audit.
Default Posture Status	Specify the posture status if evaluation does not return a condition/action match.

The **Primary Server** and **Backup Server** tabs specify connection information for the Nessus audit server.

Figure 318: Add Nessus Audit Server > Primary and Backup Server Tabs

The screenshot displays the 'Add Nessus Audit Server' configuration window. It features two tabs: 'Primary Server' and 'Backup Server'. The 'Primary Server' tab is active, showing fields for Nessus Server Name (extern-nessus.acme.com), Nessus Server Port (1241), Username (admin), Password (masked), and Scan Profile (default). The 'Backup Server' tab is also visible, showing a 'Backup' checkbox (checked) and the same server configuration fields. At the bottom, there are buttons for 'Back to Audit Servers', 'Next >', 'Save', and 'Cancel'.

3. Specify the **Nessus Audit Server > Primary Server** tab and **Backup Server** tab parameters as described in Table 170.

Table 170: Nessus Audit Server > Primary and Backup Server Tabs Parameters

Parameter	Action/Description
Backup	On the Backup Server dialog: For the backup server to be invoked on primary server failover, check the Enable to use backup when primary does not respond check box.
Nessus Server Name	Enter the name of the Nessus server.
Nessus Server Port	Specify the Nessus Server port. The default is 1241 .
Username	Enter the username for the primary and backup Nessus servers.
Password	Enter the password for the primary and backup Nessus servers.
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 on page 335 .
In-Progress Timeout	Specify the duration (in seconds) before polling for Nmap results. The default is 30 seconds.

4. Configure the audit server Rules.
The **Rules** tab specifies rules for post-audit evaluation of the request to assign a role. For more information, refer to [Post-Audit Rules on page 340](#).

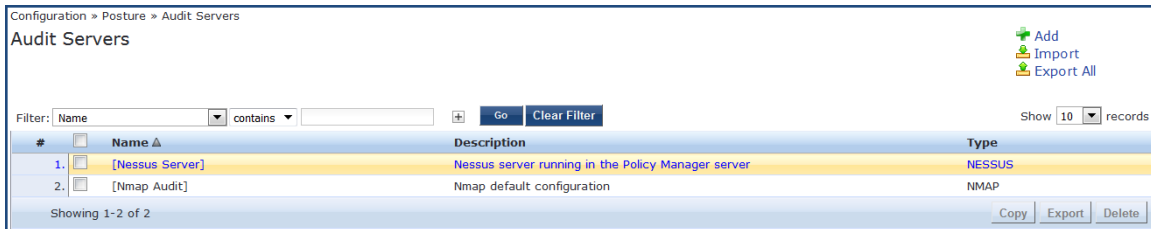
Modifying a Nessus Audit Server

To modify an existing Nessus audit server:

1. Navigate to **Configuration > Posture > Audit Server**.

The **Audit Servers** dialog opens.

Figure 319: *Selecting a Nessus Audit Server*



#	Name	Description	Type
1.	[Nessus Server]	Nessus server running in the Policy Manager server	NESSUS
2.	[Nmap Audit]	Nmap default configuration	NMAP

Showing 1-2 of 2

2. Select the Nessus audit server you wish to modify.

The **Edit Nessus Server** dialog opens to the **Summary** tab, which displays the configuration settings for the selected Nessus server.

Figure 320: *Edit Nessus Server > Summary Page*



Configuration > Posture > Audit Servers > Edit - [Nessus Server]	
Audit Servers - [Nessus Server]	
Summary Audit Primary Server Backup Server Rules	
Audit:	
Name:	[Nessus Server]
Description:	Nessus server running in the Policy Manager server
Type:	NESSUS
In-Progress Posture Status:	TRANSITION (15)
Default Posture Status:	UNKNOWN (100)
Primary Server:	
Nessus Server Name:	localhost
Nessus Server Port:	1241 (default is 1241)
Username:	aruba
Password:	*****
Scan Profile:	default
In-Progress Timeout:	60 seconds
Backup Server:	
Backup:	Disabled
Nessus Server Name:	-
Nessus Server Port:	0 (default is 1241)
Username:	-
Password:	-
Scan Profile:	-
In-Progress Timeout:	0 seconds
Rules:	
Rules Evaluation Algorithm:	Evaluate all
Conditions	Role Name

3. Make any necessary configuration changes, then click **Save**.

Required Configuration Updates for External Nessus Servers

To properly support Nessus server configuration on W-ClearPass servers, you must make the following configuration settings on the external Nessus server:

1. On the external Nessus server, set the value for the **disable_ntp** parameter to **no**.

For example, on a CENTOS/RHEL server running Nessus, you would enter the following command:

```
centos# /opt/nessus/sbin/nessuscli fix --set disable_ntp=no
```

- Restart the Nessus service.

For example:

```
centos# service nessusd restart
```

- If the external Nessus server has Transport Layer Security (TLS) enabled, add the Nessus CA Certificate to the W-ClearPass Certificate Trust List (see [Certificate Trust List on page 633](#)).

You can download the Nessus CA certificate from:

```
https://<nessus_server_name>:8834/getcert
```

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 displays.

Figure 321: Nessus Scan Profile Configuration Page

Configuration » Posture » Audit Servers » Nessus Scan Profile Configuration - default

Nessus Scan Profile Configuration - default [Refresh Plugins List](#)

Profile Selected Plugins Preferences

Select Profile: default

New Profile Name: default

Available Plugins:

☒ Filter plugins by family: - Select -

☐ Filter plugins by ID or name: Go Clear

Id	Plugin Name

[Back to Audit Servers](#) Delete Copy Save Cancel

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 check boxes (at left). Policy Manager will remember selections as you select other plugins from other plugin families.
 - When finished, click the **Selected Plugins** tab.

Figure 322: Nessus Scan Profile Configuration - Profile Tab

Profile | **Selected Plugins** | **Preferences**

Select Profile:

New Profile Name:

Available Plugins:

☒ Filter plugins by family:

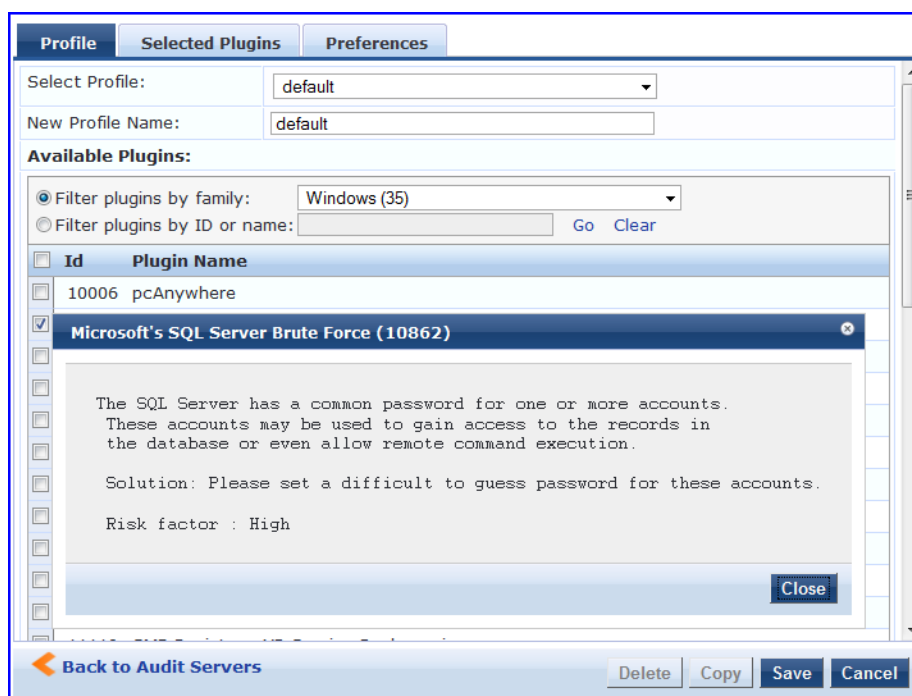
☐ Filter plugins by ID or name:

☐	Id	Plugin Name
☐	10006	pcAnywhere
☒	10144	Microsoft SQL TCP/IP listener is running
☐	10642	SMB Registry : SQL7 Patches
☐	10673	Microsoft's SQL Blank Password
☐	10674	Microsoft's SQL UDP Info Query
☐	10761	Detect CIS ports
☐	10763	Detect the HTTP RPC endpoint mapper
☐	10794	pcAnywhere TCP
☐	10829	scan for UPNP hosts
☐	10862	Microsoft's SQL Server Brute Force
☐	11067	Microsoft's SQL Hello Overflow
☐	11119	SMB Registry : XP Service Pack version
☒	11882	AOL Instant Messenger is Installed
☒	11883	Gator/GAIN Spyware Installed

[Back to Audit Servers](#)

- The **Selected Plugins** tab displays all selected plugins, plus any dependencies. To display a synopsis of any listed plugin, click on its row.

Figure 323: Nessus Scan Profile Configuration Profile Tab - Plugin Synopsis



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, or INFO. This action tells Policy Manager the vulnerability level that is considered to be assigned QUARANTINE status.

Figure 324: Nessus Scan Profile Configuration - Selected Plugins Tab

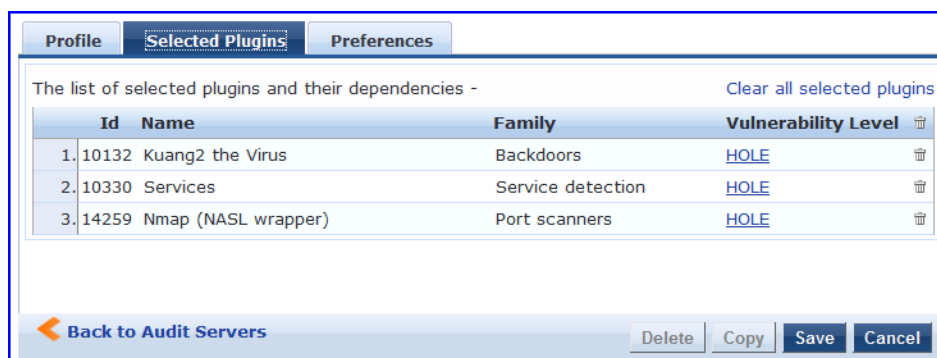
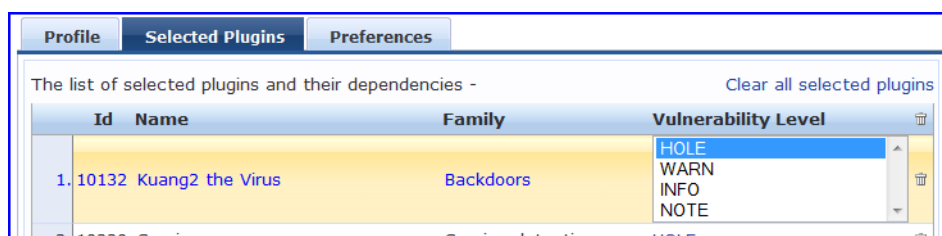


Figure 325: Nessus Scan Profile Configuration Selected Plugins Tab - Vulnerability Level



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 326: Nessus Scan Profile Configuration - Preferences Tab

After 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.

Adding an Nmap Audit Server

To create an Nmap (Network Mapping) audit server:

1. Navigate to the **Configuration > Posture > Audit Servers** page, then click **Add**.
2. From the **Audit** tab, select the **NMAP** radio button in the **Type** field.

W-Policy Manager uses the Nmap audit server interface exclusively for network port scans.

- The Health evaluation always returns a status of **Healthy**.
- The port scan gathers attributes that allow determination of role(s) through post-audit rules.

Audit Tab

You can use the **Audit** tab to identify the server and define configuration details. [Figure 327](#) shows an example of the **Audit** tab:

Figure 327: NMAP Audit Server > Audit Tab

The following table describes the parameters configured in the **Audit** tab:

Table 171: *Audit Tab Parameters*

Parameter	Action/Description
Name	Enter the name of the NMAP audit server.
Description	Optionally (and recommended), enter the description of the Nmap audit server.
Type	Select NMAP .
In-Progress Posture Status	Specify the posture status during audit.
Default Posture Status	Select the posture status if evaluation does not return a condition/action match.

NMAP Options Tab

You can use the **NMAP Options** tab to specify the type of scan configuration.

Figure 328: *Nmap Server > NMAP Options Tab*

Configuration » Posture » Audit Servers » Add

Audit Servers

Audit **NMAP Options** Rules Summary

TCP Scan: None

- None
- TCP SYN scan
- TCP Connect scan
- TCP Null scan
- TCP FIN scan
- TCP Xmas scan
- TCP ACK scan
- TCP Window scan
- TCP Maimon scan

UDP Scan: ☐ Enabled

Service Scan: ☐ Enabled

Detect Host Operating System: ☐ Enabled

Port Range:

Host Timeout: seconds

In-Progress Timeout: seconds

[Back to Audit Servers](#) Next > Save Cancel

Table 172: *NMAP Options Tab*

Parameter	Action/Description
TCP Scan	Specify the type of TCP scan: • TCP SYN scan • TCP Connect scan • TCP Null Scan • TCP FIN scan • TCP Xmas scan • TCP ACK scan • TCP Window scan • TCP Maimon scan Refer to Nmap documentation for more information on the TCP scan options. Nmap option: scanflags.
UDP Scan	To enable UDP (User Datagram Protocol) scanning, check the UDP Scan check box. Nmap option: sU.
Service Scan	To enable Service scanning, check the Service Scan check box. Nmap option: sV.
Detect Host Operating System	To enable host OS detection, check the Detect Host Operating System check box. NMAP option: A.
Port Range	Specify the range of ports to scan. NMAP option: p.
Host Timeout	Specify the time in seconds for the target host to timeout. Nmap option: host-timeout
In-Progress Timeout	Specify the duration (in seconds) before polling for Nmap results.

Rules Tab

The **Rules** tab specifies rules for post-audit evaluation of the request to assign a role. For details, refer to [Post-Audit Rules on page 340](#).

Post-Audit Rules

The **Audit Servers > Rules** dialog specifies rules for post-audit evaluation of the request to assign a role.

Figure 329: All Audit Server Configurations > Rules Dialog

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

Post-Audit Rules:

Conditions	Role Name
Add Rule	Move Up Move Down Edit Rule Remove Rule

Table 173: All Audit Server Configurations > Rules Dialog Parameters

Parameter	Action/Description
Rules Evaluation Algorithm	Select first matched rule and return the role or Select all matched rules and return a set of roles.
Add Rule	When you add a rule, the Rules Editor opens. See below for details.
Move Up/Down	Reorder the rules as necessary.
Edit Rule	Opens the selected rule in Edit mode.
Remove Rule	Removes the selected rule.

Figure 330: All Audit Server Configurations > Rules Editor

Rules Editor

Conditions

Matches ☒ ANY or ☐ ALL of the following conditions:

Name	Operator	Value
1. OS-Info	CONTAINS	Linux
2. [Dropdown]		
3. [Dropdown]		

Dropdown menu options: Audit-Status, Device-Type, Output-Msgs, Network-Apps, Mac-Vendor, OS-Info, Open-Ports

Action: [CACs Help Desk]

Table 174: *All Audit Server Configurations > Rules Editor Parameters*

Parameter	Description
Conditions	The Conditions list includes five dictionaries: • Audit-Status • Device-Type • Output-Msgs • MAC-Vendor • Network-Apps • Open-Ports • OS-Info For more information, refer to Namespaces on page 845.
Actions	The Actions list includes the names of the roles configured in W-Policy Manager.
Save	To commit a Condition/Action pairing, click Save.

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. Each enforcement policy contains a rule or set of rules for matching conditions (role, posture, and time) to actions (enforcement profiles). Commonly used enforcement profiles include attributes for VLAN, Filter ID, Downloadable ACL, and Proxy ACL. For a general overview of network access enforcement policies, see [Enforcement Architecture and Flow on page 1](#).

This chapter describes the following topics:

- [Configuring Enforcement Policies on page 343](#)
- [Configuring Enforcement Profiles on page 345](#)

Configuring Enforcement Policies

One and only one enforcement policy can be associated with each service. Enforcement policies can be added in one of two ways:

- From **Configuration > Enforcement > Enforcement Policies**.
- From the **Configuration > Services** page as part of the flow of the **Add Service** wizard.

The following figure displays the **Enforcement Policies** page:

Figure 331: *Enforcement Policies Page*

#	Name	Type	Description
1.	[Admin Network Login Policy]	TACACS	Enforcement policy controlling access to Policy Manager Admin
2.	[AirGroup Enforcement Policy]	RADIUS	Enforcement policy controlling access for AirGroup devices
3.	[Aruba Device Access Policy]	TACACS	Enforcement policy controlling access to Aruba device
4.	[Guest Operator Logins]	Application	Enforcement policy controlling access to Guest application
5.	[Insight Operator Logins]	Application	Enforcement policy controlling access to Insight application
6.	[Sample Allow Access Policy]	RADIUS	Sample policy to allow network access
7.	[Sample Deny Access Policy]	RADIUS	Sample policy to deny network access

1. To add a new enforcement policy, click **Add**.
The **Add Enforcement Policy** wizard opens:

Figure 332: Add Enforcement Policy > Enforcement tab

Configuration » Enforcement » Policies » Add

Enforcement Policies

Enforcement | Rules | Summary

Name: Employee Access Enforcement

Description: Enforcement policy for employee access

Enforcement Type: ☒ RADIUS ☐ TACACS+ ☐ WEBAUTH (SNMP/Agent/CLI/CoA) ☐ Application

Default Profile: [Allow Access Profile] [View Details](#) [Modify](#) [Add new Enforcement Profile](#)

[Back to Enforcement Policies](#) [Next >](#) [Save](#) [Cancel](#)

2. Specify the **Add Enforcement Policy > Enforcement** parameters as described in the following table:

Table 175: Add Enforcement Policy > Enforcement Tab Parameters

Parameter	Action/Description
Name	Enter the name of this enforcement policy.
Description	Enter a useful description of this enforcement policy (recommended).
Type	Select: RADIUS , TACACS+ , WebAuth (SNMP/CLI)/CoA or Application . Based on this selection, the Default Profile list shows the right type of enforcement profiles in the drop-down list (see below). NOTE: Web-based Authentication or WebAuth (HTTPS) is the mechanism used by authentications performed via a browser, and authentications performed via Dell W-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	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. Click Add new Enforcement Profile to add a new profile (This is integrated into the flow. After you create a profile, W-Policy Manager brings you back to the current tab.)

3. In the **Rules** tab, click **New Rule** to display the **Rules Editor**:

Figure 333: Add Enforcement Policy > Rules Dialog

Enforcement | **Rules** | Summary

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

Enforcement Policy Rules:

	Conditions	Actions
1.	(Tips:Role MATCHES_ANY [Employee])	[RADIUS] [Allow Access Profile]
2.	AND (Tips:Role EQUALS [Guest]) (Tips:Posture EQUALS HEALTHY (0))	[RADIUS] [Allow Access Profile]

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

[Back to Enforcement Policies](#) [Next >](#) [Save](#) [Cancel](#)

4. Specify the **Add Enforcement Policy > Rules** tab parameters as described in the following table:

Table 176: *Add Enforcement Policy (Rules tab)*

Field	Action/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 177: *Add Enforcement Policy (Rules Editor)*

Field	Description
Conditions/Enforcement Profiles	Select conditions for this rule. For each condition, select a matching action (enforcement profile). NOTE: A condition in an enforcement policy rule can contain attributes from the following namespaces: Tips:Role, Tips:Posture, and Date. NOTE: The value field for the Tips:Role attribute can be a role defined in Policy Manager, or a role fetched from the authorization source. (Refer 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. To commit the rule, click Save .
Enforcement Profiles	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. Refer to Configuring Enforcement Profiles on page 345 for a list of the default profiles.

Configuring Enforcement Profiles

This section includes the following information:

- [Adding an Enforcement Profile](#)
- [Modifying an Existing Enforcement Profile](#)

You can configure W-Policy Manager enforcement profiles globally, but they must be referenced to an enforcement policy that is associated with a service.

For information about configuring specific enforcement profiles, see:

- [Agent Enforcement on page 348](#)
- [Aruba Downloadable Role Enforcement on page 350](#)
- [Aruba RADIUS Enforcement on page 360](#)
- [Cisco Downloadable ACL Enforcement on page 362](#)
- [Cisco Web Authentication Enforcement on page 364](#)
- [ClearPass Entity Update Enforcement on page 366](#)
- [CLI Based Enforcement on page 368](#)
- [Filter ID Based Enforcement on page 370](#)
- [Generic Application Enforcement on page 372](#)

- HTTP Based Enforcement on page 374
- RADIUS Based Enforcement on page 375
- RADIUS Change of Authorization (CoA) on page 377
- Session Restrictions Enforcement on page 381
- SNMP Based Enforcement on page 386
- TACACS+ Based Enforcement on page 387
- VLAN Enforcement on page 389

Adding an Enforcement Profile

To add an enforcement profile:

1. Navigate to **Configuration > Enforcement > Profiles**.

The **Enforcement Profiles** page opens:

Figure 334: *Enforcement Profiles Page*

Configuration » Enforcement » Profiles

Enforcement Profiles

 Add
 Import
 Export All

Filter: Name contains + Go Clear Filter Show 10 records

#	☐	Name ▲	Type	Description
1.	☐	[Aerohive - Terminate Session]	RADIUS_CoA	System-defined profile to disconnect user (Aerohive)
2.	☐	[AirGroup Personal Device]	RADIUS	System-defined profile for an AirGroup personal device request
3.	☐	[AirGroup Response]	RADIUS	System-defined profile for any AirGroup request
4.	☐	[AirGroup Shared Device]	RADIUS	System-defined profile for an AirGroup shared device request
5.	☐	[Allow Access Profile]	RADIUS	System-defined profile to allow network access
6.	☐	[Allow Application Access Profile]	Application	System-defined profile to allow access to application
7.	☐	[Aruba Bounce Host-Port]	RADIUS_CoA	System-defined profile to bounce host-port (Aruba)
8.	☐	[Aruba TACACS read-only Access]	TACACS	System-defined profile for read-only access to Aruba device
9.	☐	[Aruba TACACS root Access]	TACACS	System-defined profile for root access to Aruba device
10.	☐	[Aruba Terminate Session]	RADIUS_CoA	System-defined profile to disconnect user (Aruba)

Showing 1-10 of 36 ▶▶ Copy Export Delete

2. Click **Add** at the top-right corner.

The **Add Enforcement Profile** dialog opens.

Figure 335: *Add Enforcement Profile Dialog*

Configuration » Enforcement » Profiles » Add Enforcement Profile

Enforcement Profiles

Profile **Attributes** **Summary**

Template:

Name:

Description:

Type: RADIUS

Action: ☒ Accept ☐ Reject ☐ Drop

Device Group List:

Remove
View Details
Modify

The following table describes the default set of enforcement profiles included with W-Policy Manager:

Table 178: *Default Enforcement Profiles*

Profile	Available for the following Enforcement Types
[Aerohive - Terminate Session]	RADIUS_CoA
[AirGroup Personal Device]	RADIUS
[AirGroup Response]	RADIUS
[AirGroup Shared Device]	RADIUS
[Allow Access Profile]	RADIUS
[Allow Application Access Profile]	Application
[Aruba TACACS read-only Access]	TACACS
[Aruba TACACS root Access]	TACACS
[Aruba Terminate Session]	RADIUS_CoA
[Cisco - Bounce-Host-Port]	RADIUS_CoA
[Cisco - Disable Host-Port]	RADIUS_CoA
[Cisco - Reauthenticate-Session]	RADIUS_CoA
[Cisco - Terminate-Session]	RADIUS_CoA
[Deny Access Profile]	RADIUS
[Deny Application Access Profile]	Application
[Drop Access Profile]	RADIUS
[Handle AirGroup Time Sharing]	HTTP
[HP - Terminate Session]	RADIUS_CoA
[Juniper Terminate Session]	RADIUS_CoA
[Motorola - Terminate Session]	RADIUS_CoA
[Operator Login - Admin Users]	Application
[Operator Login - Local Users]	Application
[TACACS API Admin]	TACACS
[TACACS Deny Profile]	TACACS
[TACACS Help Desk]	TACACS

Table 178: *Default Enforcement Profiles (Continued)*

Profile	Available for the following Enforcement Types
[TACACS Network Admin]	TACACS
[TACACS Read-only Admin]	TACACS
[TACACS Receptionist]	TACACS
[TACACS Super Admin]	TACACS
[Trapeze - Terminate Session]	RADIUS_CoA
[Update Endpoint Known]	Post-Authentication

Modifying an Existing Enforcement Profile

To modify an existing enforcement profile:

1. Navigate to the **Configuration > Enforcement > Profiles** page.
2. Click the name of the profile in the **Enforcement Profile** list that you wish to modify.
The **Edit Enforcement Profile** dialog for the selected profile opens. The parameters vary according to which profile is selected.
3. Make the necessary changes in the **Profile** and **Attributes** dialogs, then click **Save**.

Agent Enforcement

To configure profile and attribute parameters for an Agent Enforcement profile:

1. Navigate to **Configuration > Enforcement > Profiles**.
The **Enforcement Profiles** page opens.
2. Click **Add**.
The **Add Enforcement Profiles > Profile** tab opens.
3. From the **Template** drop-down, select **Agent Enforcement**.
The following figure displays the **Agent Enforcement > Profile** dialog:

Figure 336: *Agent Enforcement > Profile Tab*

Configuration » Enforcement » Profiles » Add Enforcement Profile

Enforcement Profiles

Profile | Attributes | Summary

Template: Agent Enforcement

Name:

Description:

Type: Agent

Action: ☒ Accept ☐ Reject ☐ Drop

Device Group List:

Remove View Details Modify

[Add new Device Group](#)

4. Specify the **Add Agent Enforcement > Profile** parameters as described in the following table:

Table 179: *Add Agent Enforcement > Profile Parameters*

Parameter	Description
Template	Select the template from the drop-down list. In this context, select Agent Enforcement .
Name	Enter the name of the enforcement profile.
Description	Optionally, enter a description of the enforcement profile (recommended).
Type	This field is populated automatically with type Agent .
Action	By default, this field is disabled. It is enabled only when RADIUS type is selected.
Device Group List	Select a device group from the drop-down list. The list displays all configured device groups. All configured device groups are listed in the Configuration > Network > Device Groups page. After you add one or more device groups, you can select a group and take one of the following actions: • To delete the selected Device Group List entry, click Remove. • To see the device group parameters, click View Details. • To change the parameters of the selected device group, click Modify.
Add new Device Group	To add a new device group, click the Add new Device Group link. For more information, see Adding and Modifying Device Groups on page 438 .

Attributes Tab

Use the **Attributes** tab to configure the attribute name and attribute value for each attribute you add. The following figure displays the **Agent Enforcement > Attributes** tab:

Figure 337: *Agent Enforcement > Attributes Tab*

Configuration » Enforcement » Profiles » Edit Enforcement Profile - agent-enf

Enforcement Profiles - agent-enf

Summary Profile **Attributes**

Attribute Name	Attribute Value	
1. Bounce Client	= false	
2. Health Check Interval (in hours)	= 0	
3. Click to add...		

Specify the **Agent Enforcement > Attributes** parameters as described in the following table:

Table 180: *Agent Enforcement > Attributes Tab Parameters*

Attribute	Action/Description
Attribute Name	Select one of the following attribute names: • Bounce Client: To terminate the network connection, set the value to True. • Message: Enter the message that needs to be notified on the endpoint. • Enable to hide Retry button: To set to True, check the check box. • Enable to hide Logout button: To hide the Retry button in the OnGuard Agent, set the value to True. • Enable to hide Quit option: To set to True, check the check box. • Health Check Interval (in hours): Specify the health check interval value in hours for different Agent Enforcement Profiles for different users. The allowed range is of 0 to 1000 hours. NOTE: The value of the Policy result cache timeout parameter (Administration > Server Manager > Server Configuration > Cluster-Wide Parameters > General tab) must be greater than the highest value of all the Health Check Interval (in hours) field values. Note the following information when you set the Health Check Interval parameter: ■ You can set this parameter if OnGuard mode is set to Health only. ■ This parameter is valid only for wired and wireless interface types. ■ This parameter is not applicable for the OnGuard Dissolvable Agent, VPN, and other interface types. • Session Timeout (in seconds): Configure the agent session timeout interval to reevaluate the system health. OnGuard triggers auto-remediation using this value to enable or disable an AV-RTP status check on the endpoint. Agent reauthentication is based on the session timeout value. You can specify the session timeout interval from 60 to 600 seconds. Setting the lower value for the session timeout interval results in numerous authentication requests in the Access Tracker page. The default value is 0.
Attribute Value	The value set depends on the selected Attribute Name .

Summary Tab

The **Summary** tab summarizes the parameters configured in the **Profile** and **Attribute** tabs. The following figure displays the **Agent Enforcement > Summary** tab:

Figure 338: *Agent Enforcement > Summary Tab*

Enforcement Policies - Agent-enforcement

Summary	Enforcement	Rules
Enforcement:		
Name:	Agent-enforcement	
Description:		
Enforcement Type:	WEBAUTH	
Default Profile:	Agent-initial	
Rules:		
Rules Evaluation Algorithm:	First applicable	
Conditions	Actions	
1. (Tips:Posture EQUALS HEALTHY (0))	Agent-healthy	

Aruba Downloadable Role Enforcement

Use this page to configure profile and role configuration attributes for the **Aruba Downloadable Role Enforcement** profile. The **Aruba Downloadable Role Enforcement** profile contains the following tabs:

- [Profile Tab on page 351](#)

- [Role Configuration Tab on page 352](#)
- [Summary Tab on page 360](#)

Profile Tab

Use the **Profile** tab to configure the template, type of the profile, and device group list. The following figure displays the **Aruba Downloadable Role Enforcement - Profile** tab:

Figure 339: *Aruba Downloadable Role Enforcement - Profile Tab*

The screenshot shows the 'Profile' tab of the 'Aruba Downloadable Role Enforcement' configuration. It includes a 'Template' dropdown set to 'Aruba Downloadable Role Enforcement', a 'Name' field, a 'Description' field, a 'Type' dropdown set to 'RADIUS', an 'Action' section with radio buttons for 'Accept', 'Reject', and 'Drop', a 'Device Group List' section with a dropdown menu and buttons for 'Remove', 'View Details', and 'Modify', and a 'Role Configuration Mode' section with radio buttons for 'Standard' and 'Advanced'. There is also a link to 'Add new Device Group'.

The following table describes the **Aruba Downloadable Role Enforcement - Profile** parameters:

Table 181: *Aruba Downloadable Role Enforcement - Profile Tab Parameters*

Parameter	Description
Template	Select the template from the drop-down list. In this context, select Aruba Downloadable Role Enforcement.
Name	Enter the name of the profile. The name is displayed in the Name column on the Configuration > Enforcement > Profiles page.
Description	Enter a description of the profile. This description is displayed in the Description column on the Configuration > Enforcement > Profiles page.
Type	Specifies the type of authentication. In this context, RADIUS. This field is automatically populated.
Action	Click Accept , Reject , or Drop to define the action taken on the request. The default action is Accept .
Device Group List	Select a device group from the drop-down list. The list displays all configured device groups. All configured device groups are listed in the Device Groups (Configuration > Network > Device Groups) page. After adding one or more device group(s), you can select a group and perform one of the following actions: • Click Remove to delete the selected device group list entry. • Click View Details to see the device group parameters. • Click Modify to change the parameters of the selected device group.
Add new Device Group	To add a new device group, click the Add new Device Group link. For more information, see Adding and Modifying Device Groups on page 438 .

Role Configuration Tab

The fields on the **Role Configuration** tab require you to select a link to launch a new page where you set role configuration attributes. For example, adding a **Captive Portal** profile. The following figure displays the **Aruba Downloadable Role Enforcement Role Configuration** tab:

Figure 340: Aruba Downloadable Role Enforcement Role - Configuration Tab

The following table describes the **Role Configuration - Attributes** parameters:

Table 182: Role Configuration - Attributes Page Parameters

Parameters	Configuration
Captive Portal Profile	Select the captive portal profile from the drop-down list if already configured. Click Add Captive Portal Profile link to add a new captive portal profile. For more information, see Captive Portal Profile on page 353 .
Policer Profile	Select the policer profile from the drop-down list if already configured. Click Add Policer Profile link to add a new policer profile. For more information, see Policer Profile on page 354 .
QoS Profile	Select the QoS profile from the drop-down list if already configured. Click Add QoS Profile link to add a new QoS profile. For more information, see QoS Profile on page 355 .
VoIP Profile	Select the VoIP profile from the drop-down list if already configured. Click Add VoIP Profile link to add a new VoIP profile. For more information, see VoIP Profile on page 356 .
Reauthentication Interval Time (0-4096)	Enter the number of minutes between reauthentication intervals. You can select the range between 0 to 4096 minutes.
VLAN To Be Assigned (1-4904)	Enter a number between 1 and 4094 that defines when the VLAN is to be assigned.
NetService Configuration	Select the Manage NetServices link to add, edit, and delete the NetService definitions.
NetDestination Configuration	Select the Manage NetDestinations link to add, edit, and delete the NetDestinations definitions.

Table 182: Role Configuration - Attributes Page Parameters (Continued)

Parameters	Configuration
Time Range Configuration	Select the Manage Time Ranges link to add, edit, and delete time range definitions.
NAT Pool Configuration	Select the Manage NAT Pool link to add, edit and delete NAT Pool definitions.
ACL Type	Select from the following ACL types: • Ethertype • MAC • Session • Stateless
ACL Name	Click the name of the ACL type. Click Add to move the ACL Name to the ACL field. Click Move Up , Move Down , or Remove to modify the names in the ACL list.
User Role Configuration	Check the Summary tab for generated role configuration.

Captive Portal Profile

Click the **Add Captive Portal Profile** link. Enter a name of the profile and configure the required attributes. The following figure displays the **Add Captive Portal Profile** pop-up:

Figure 341: Add Captive Portal Profile Pop-up

Profile Configuration

Profile Type: Captive Portal Profile

Name:

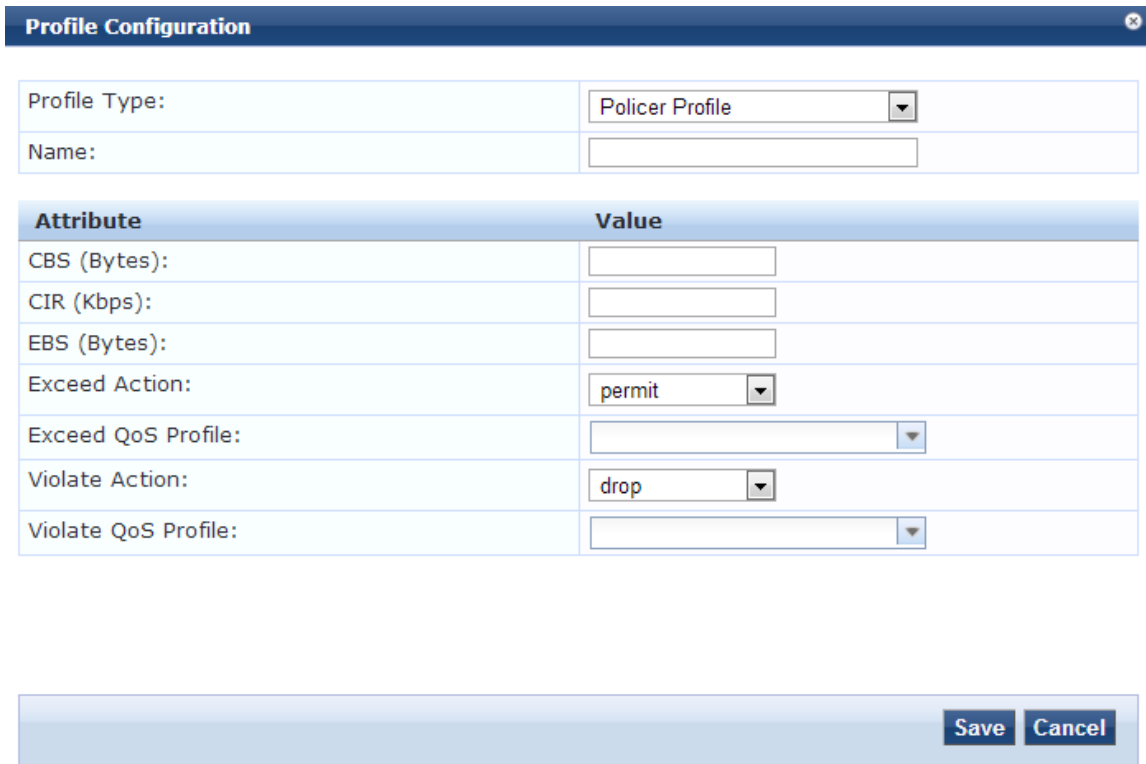
Attribute	Value
Server Group:	
Default Role:	
Default Guest Role:	
Redirect Pause (0-60 sec):	
User Login:	Yes
Guest Login:	No
Logout Popup Window:	Yes
Use HTTP for Authentication:	No
Logon Wait Minimum Delay (1-10 sec):	
Logon Wait Maximum Delay (1-10 sec):	

Save Cancel

Policer Profile

Click the **Add Policer Profile** link. Enter a name of the profile and configure the required attributes. The following figure displays the **Add Policer Profile** pop-up:

Figure 342: Add Policer Profile Pop-up



The figure shows a 'Profile Configuration' pop-up window. It contains a 'Profile Type' dropdown set to 'Policer Profile' and a 'Name' text field. Below these is a table with two columns: 'Attribute' and 'Value'. The table has seven rows for configuring CBS, CIR, EBS, Exceed Action, Exceed QoS Profile, Violate Action, and Violate QoS Profile. At the bottom are 'Save' and 'Cancel' buttons.

Attribute	Value
Profile Type:	Policer Profile
Name:	
CBS (Bytes):	
CIR (Kbps):	
EBS (Bytes):	
Exceed Action:	permit
Exceed QoS Profile:	
Violate Action:	drop
Violate QoS Profile:	

Save Cancel

QOs Profile

Click the **Add QoS Profile** link. Enter a name of the profile and configure the required attributes. The following figure displays the **Add QoS Profile** pop-up:

Figure 343: *Add QoSProfile Pop-up*

The screenshot shows a 'Profile Configuration' dialog box. It has a title bar with a close button. The main area contains a form with the following fields:

- Profile Type:** A dropdown menu with 'QoS Profile' selected.
- Name:** An empty text input field.
- Attribute Value Table:** A table with two columns: 'Attribute' and 'Value'.

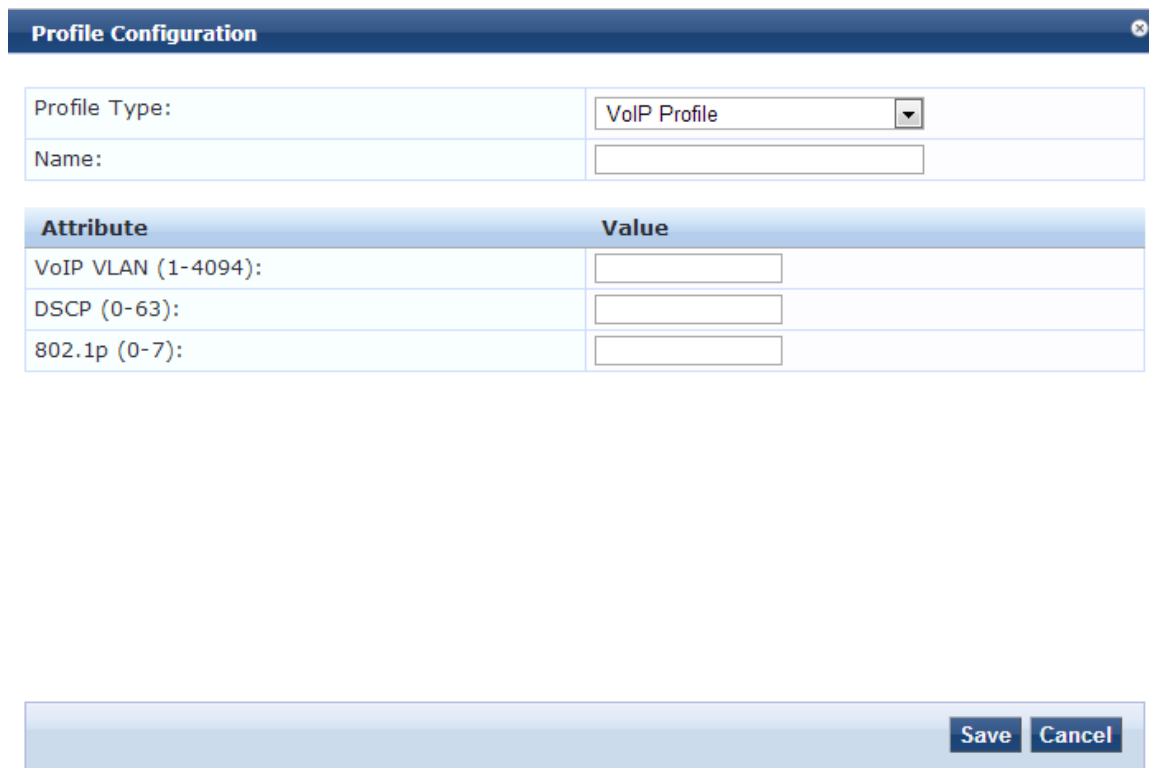
Attribute	Value
Traffic Class (0-7):	
Drop Precedence:	low v
DSCP (0-63):	
802.1p (0-7):	

At the bottom right of the dialog, there are two buttons: 'Save' and 'Cancel'.

VoIP Profile

Click the **Add VoIP Profile** link. Enter a name for the profile and configure the required attributes. The following figure displays the **Add VoIP Profile** pop-up:

Figure 344: Add VoIP Profile Pop-up



The 'Profile Configuration' window contains the following fields:

Profile Type:	VoIP Profile
Name:	

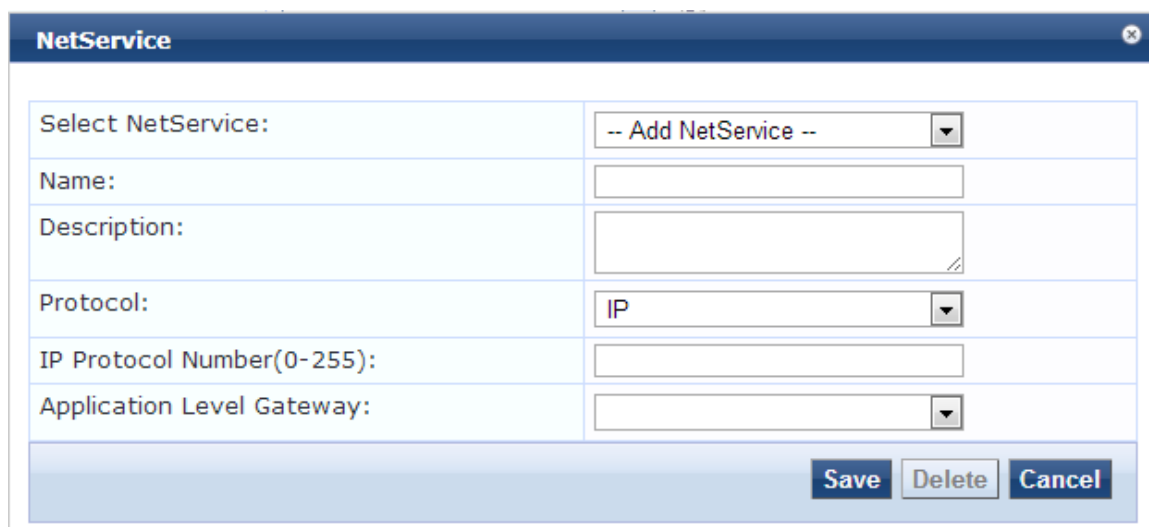
Attribute	Value
VoIP VLAN (1-4094):	
DSCP (0-63):	
802.1p (0-7):	

Buttons: Save, Cancel

NetService Configuration

Click the **Manage NetServices** link and configure the required attributes. The following figure displays the **Manage NetServices** pop-up:

Figure 345: Manage NetServices Pop-up



The 'NetService' window contains the following fields:

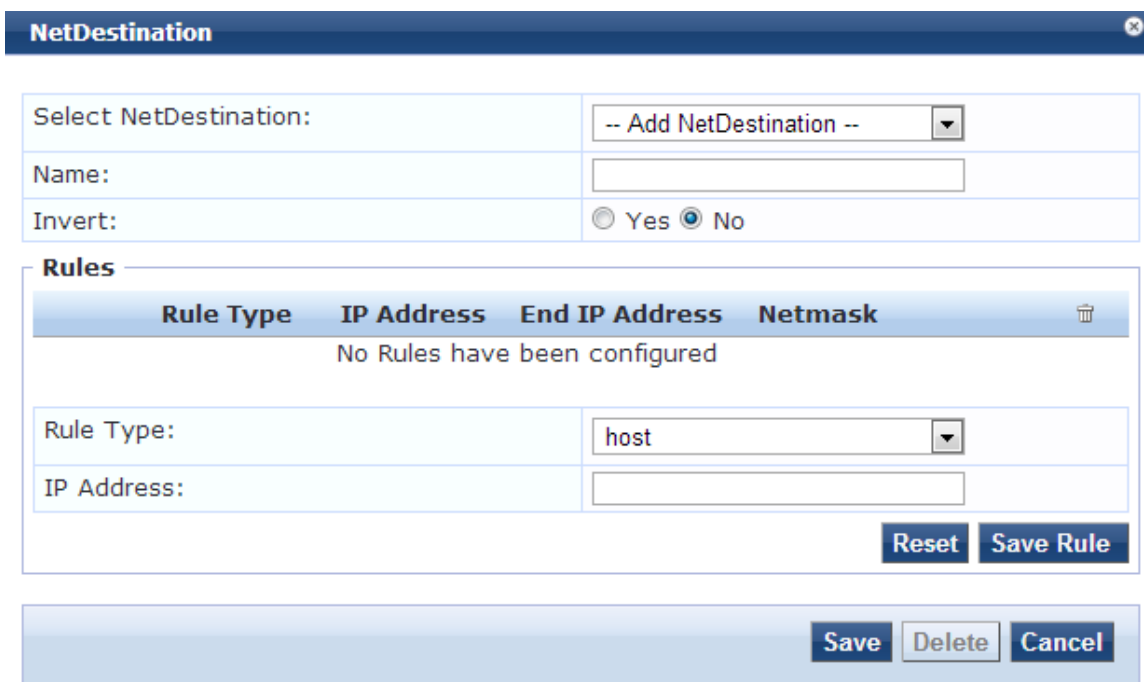
Select NetService:	-- Add NetService --
Name:	
Description:	
Protocol:	IP
IP Protocol Number(0-255):	
Application Level Gateway:	

Buttons: Save, Delete, Cancel

NetDestination Configuration

Click the **Manage NetDestinations** link and configure the required attributes. The following figure displays the **Manage NetDestinations** pop-up:

Figure 346: *Manage NetDestinations Pop-up*



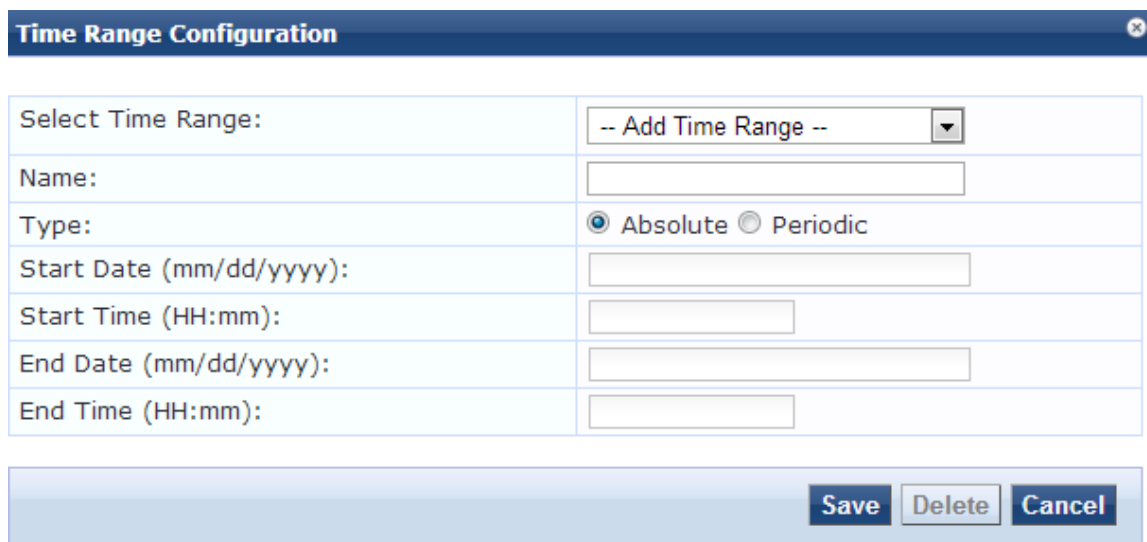
The **NetDestination** pop-up window contains the following fields and controls:

- Select NetDestination:** A dropdown menu with the option **-- Add NetDestination --**.
- Name:** A text input field.
- Invert:** Radio buttons for **Yes** and **No**, with **No** selected.
- Rules** section:
 - A table header with **Rule Type**, **IP Address**, **End IP Address**, and **Netmask**, and a trash icon.
 - A message: **No Rules have been configured**.
 - Rule Type:** A dropdown menu with the value **host**.
 - IP Address:** A text input field.
 - Reset** and **Save Rule** buttons.
- Save**, **Delete**, and **Cancel** buttons at the bottom.

Time Range Configuration

Click the **Manage Time Ranges** link and configure the required attributes. The following figure displays the **Manage Time Ranges** pop-up:

Figure 347: *Time Range Configuration Pop-up*



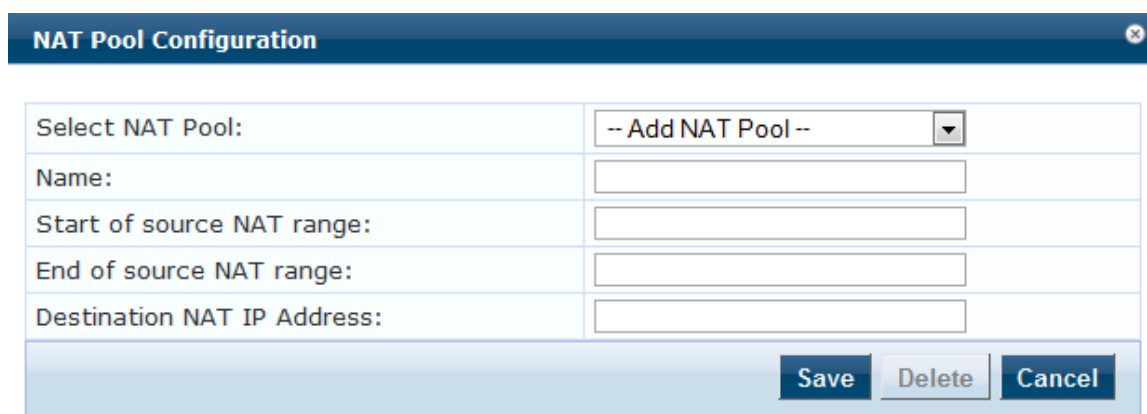
The **Time Range Configuration** pop-up window contains the following fields and controls:

- Select Time Range:** A dropdown menu with the option **-- Add Time Range --**.
- Name:** A text input field.
- Type:** Radio buttons for **Absolute** and **Periodic**, with **Absolute** selected.
- Start Date (mm/dd/yyyy):** A text input field.
- Start Time (HH:mm):** A text input field.
- End Date (mm/dd/yyyy):** A text input field.
- End Time (HH:mm):** A text input field.
- Save**, **Delete**, and **Cancel** buttons at the bottom.

NAT Pool Configuration

Use the **NAT Pool Configuration** page to configure the start and end of the source NAT range and associate them with session ACLs. The following figure displays the **NAT Pool Configuration** pop-up:

Figure 348: NAT Pool Configuration Pop-up



The NAT Pool Configuration pop-up window has a title bar "NAT Pool Configuration" with a close button. It contains a form with the following fields:

Select NAT Pool:	-- Add NAT Pool --
Name:	
Start of source NAT range:	
End of source NAT range:	
Destination NAT IP Address:	

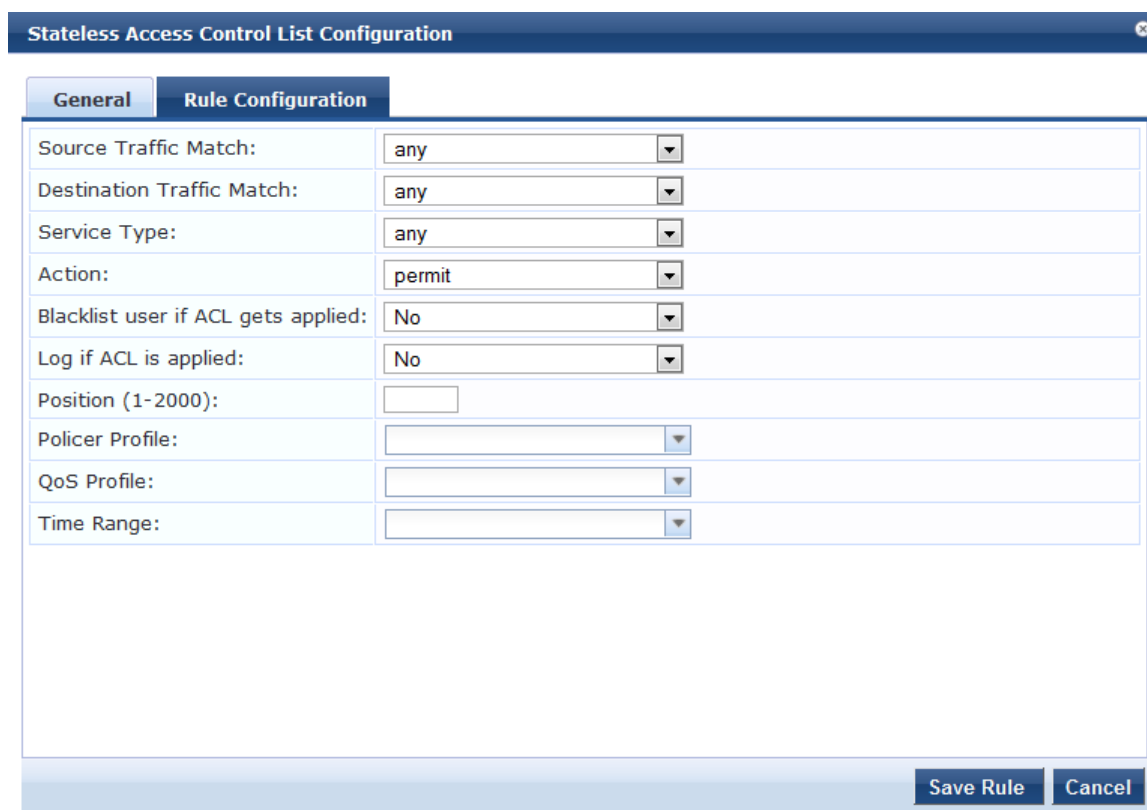
At the bottom right, there are three buttons: **Save**, **Delete**, and **Cancel**.

ACL

Click the **Add Stateless Access Control List** link. Enter a name for the Stateless ACL. Click the **Add Rule** link on the **General** tab. Enter the required attributes in the **Rule Configuration** tab and click **Save Rule** or **Cancel**.

The following figure displays the **Add Stateless Access Control List** pop-up:

Figure 349: Stateless Access Control List Configuration Pop-up



The Stateless Access Control List Configuration pop-up window has a title bar "Stateless Access Control List Configuration" with a close button. It contains two tabs: **General** and **Rule Configuration**. The **Rule Configuration** tab is active, showing the following fields:

Source Traffic Match:	any
Destination Traffic Match:	any
Service Type:	any
Action:	permit
Blacklist user if ACL gets applied:	No
Log if ACL is applied:	No
Position (1-2000):	
Policer Profile:	
QoS Profile:	
Time Range:	

At the bottom right, there are two buttons: **Save Rule** and **Cancel**.

Click the **Add Session Access Control List** link and enter the name for the Session ACL. Click the **Add Rule** link on the **General** tab. You can view different fields depends on the **Action** type you choose from the drop-

down list. For example, if you select the dual-nat action type, you can view the **Dual NAT Pool** field additionally to specify the action. Enter the required attributes in the **Rule Configuration** tab and click **Save Rule** or **Cancel**.

The following figure displays the **Session Access Control List Attributes** pop-up:

Figure 350: *Session Access Control List Attributes Pop-up*

The image shows a pop-up window titled "Session Access Control List Configuration". It has two tabs: "General" and "Rule Configuration". The "Rule Configuration" tab is active. The form contains the following fields:

Source Traffic Match:	any
Destination Traffic Match:	any
Service Type:	any
Action:	permit
Blacklist user if ACL gets applied:	No
802.1p Priority (0-7):	
Log if ACL is applied:	No
Mirror:	No
Position (1-2000):	
Queue Priority:	
Time Range:	
TOS (0-63):	

At the bottom right of the form are two buttons: "Save Rule" and "Cancel".

Click the **Add Ethernet/MAC Access Control List** link. Enter a name for the Ethernet/MAC ACL. Enter the required attributes in the **Rules** section of the page and click **Reset**, **Save Rule**. Then click **Save** or **Cancel**.

The following figure displays the **Ethernet/MAC Access Control List Attributes** pop-up:

Figure 351: Ethernet/MAC Access Control List Attributes Pop-up

Access Control List Configuration

ACL Type: Ethertype

Name:

Rules

Action	Value
No Rules have been configured	

Action: Permit

Ethertype number: Any

Reset Save Rule

Save Cancel

Summary Tab

The **Summary** tab summarizes the parameters configured in the **Profile** and **Role Configuration** tabs. The following figure displays the **Aruba Downloadable Role Enforcement - Summary** tab:

Figure 352: Aruba Downloadable Role Enforcement - Summary Tab

Enforcement Profiles

Profile **Role Configuration** **Summary**

Profile:

Template: Aruba Downloadable Role Enforcement

Name: test

Description:

Type: RADIUS

Action: Accept

Device Group List: -

Role Configuration:

Captive Portal Profile: Captive_Portal_Profile

Policer Profile: -

QoS Profile: -

VoIP Profile: -

Reauthentication Interval Time (0-4096): - minutes

VLAN To Be Assigned (1-4094): -

ACL:

User Role Configuration :

```
aaa authentication captive-portal Captive_Portal_Profile
server-group Test Group
default-role Admin
default-guest-role Guest
redirect-pause 60
user-logon
```

Aruba RADIUS Enforcement

Use this page to configure profile and attribute parameters for the **Aruba RADIUS Enforcement** profile. The the **Aruba RADIUS Enforcement** profile contains the following configuration tabs:

- [Profile Tab on page 361](#)
- [Attributes Tab on page 362](#)

- [Summary Tab on page 362](#)

Profile Tab

Use the **Profile** tab to configure the template, type of the profile, and device group list. The following figure displays the **Aruba RADIUS Enforcement - Profile** tab:

Figure 353: Aruba RADIUS Enforcement - Profile Tab

The screenshot shows the 'Enforcement Profiles' configuration page. At the top, there are three tabs: 'Profile', 'Attributes', and 'Summary'. The 'Profile' tab is selected. Below the tabs, there are several input fields: 'Template' (a dropdown menu showing 'Aruba RADIUS Enforcement'), 'Name' (a text input field), 'Description' (a text input field), 'Type' (a dropdown menu showing 'RADIUS'), 'Action' (radio buttons for 'Accept', 'Reject', and 'Drop'), and 'Device Group List' (a dropdown menu with a 'Add new Device Group' link). To the right of the 'Device Group List' dropdown, there are three buttons: 'Remove', 'View Details', and 'Modify'.

The following table describes the **Aruba RADIUS Enforcement - Profile** tab parameters:

Table 183: Aruba RADIUS Enforcement - Profile Tab Parameters

Parameter	Description
Template	Select the template from the drop-down list. In this context, select Aruba RADIUS Enforcement.
Name	Enter the name of the profile. The name is displayed in the Name column on the Configuration > Enforcement > Profiles page.
Description	Enter a description that provides additional information about the profile. This description is displayed in the Description column on the Configuration > Enforcement > Profiles page.
Type	This field is populated automatically.
Action	Click Accept , Reject , or Drop to define the action taken on the request.
Device Group List	Select a device group from the drop-down list. The list displays all configured device groups. All configured device groups are listed in the Device Groups (Configuration > Network > Device Groups) page. After adding one or more device group(s), you can select a group and take one of the following actions: • Click Remove to delete the selected Device Group List entry. • Click View Details to see the device group parameters. • Click Modify to change the parameters of the selected device group.
Add new Device Group	Click this link to add a new device group, For more information, see Adding and Modifying Device Groups on page 438 .

Attributes Tab

Use the **Attribute** tab to configure the attribute type, name, and value for the enforcement profile. The following figure displays the **Aruba RADIUS Enforcement - Attributes** tab:

Figure 354: Aruba RADIUS Enforcement - Attributes Tab

Enforcement Profiles

Profile Attributes Summary

Type	Name	Value
1. Radius:Aruba	Aruba-User-Role (1)	=
2. Click to add...		

The following table describes the **Aruba RADIUS Enforcement - Attributes** tab parameters:

Table 184: Aruba RADIUS Enforcement - Attributes Tab Parameters

Attribute	Description
Type	Select one of the following attribute types: ● Radius:Aruba ● Radius:IETF ● Radius:Cisco ● Radius:Microsoft ● Radius:Avenda For more information, see RADIUS Namespaces on page 854 .
Name	Specifies the options displayed for the Name attribute depend on the Type attribute selected.
Value	Specifies the options displayed for the Value attribute depend on the Type and Name attributes selected.

Summary Tab

The **Summary** tab summarizes the parameters configured in the **Profile** and **Attributes** tab. The following figure displays the **Aruba RADIUS Enforcement - Summary** tab:

Figure 355: Aruba RADIUS Enforcement - Summary Tab

Enforcement Profiles

Profile Attributes Summary

Profile:

Template:	Aruba RADIUS Enforcement
Name:	RADIUS Enf
Description:	System-defined profile to re-authenticate session (Aruba RADIUS Enf)
Type:	RADIUS
Action:	Accept
Device Group List:	-

Attributes:

Type	Name	Value
1. Radius:Aruba	Aruba-Admin-Role	= %Authorization:172.31.1.11:Groups

Cisco Downloadable ACL Enforcement

Use this page to configure profile and attribute parameters for the Cisco Downloadable ACL Enforcement profile. The **Cisco Downloadable ACL Enforcement** profile contains the following configuration tabs:

- [Profile Tab on page 363](#)
- [Attributes Tab on page 363](#)
- [Summary Tab on page 364](#)

Profile Tab

Use the **Profile** tab to configure the template, type of the profile, and device group list. The following figure displays the **Cisco Downloadable ACL Enforcement - Profile** tab:

Figure 356: Cisco Downloadable ACL Enforcement - Profile Tab

Enforcement Profiles

Profile	Attributes	Summary
Template:	Cisco Downloadable ACL Enforcement	
Name:		
Description:		
Type:	RADIUS	
Action:	☒ Accept ☐ Reject ☐ Drop	
Device Group List:	--Select-- Remove View Details Modify Add new Device Group	

The following table describes the **Cisco Downloadable ACL Enforcement - Profile** parameters:

Table 185: Cisco Downloadable ACL Enforcement - Profile Tab Parameters

Parameter	Description
Template	Select the template from the drop-down list. In this context, select Cisco Downloadable ACL Enforcement .
Name	Enter the name of the profile. The name is displayed in the Name column on the Configuration > Enforcement > Profiles page.
Description	Enter a description of the profile. The description is displayed in the Description column on the Configuration > Enforcement > Profiles page.
Type	The field is populated automatically.
Action	Click Accept, Reject, or Drop to define the action taken on the request.
Device Group List	Select a Device Group from the drop-down list. The list displays all configured device groups. All configured device groups are listed in the Device Groups (Configuration > Network > Device Groups) page. After adding one or more device group(s), you can select a group and take one of the following actions: - Click Remove to delete the selected device group List entry. - Click View Details to see the device group parameters. - Click Modify to change the parameters of the selected device group.
Add new Device Group	To add a new a device group, click the Add new Device Group link. For more information, see Adding and Modifying Device Groups on page 438 .

Attributes Tab

Use the **Attribute** tab to configure the attribute type, name, and value for the enforcement profile. The following figure displays the **Cisco Downloadable ACL Enforcement - Attributes** tab:

Figure 357: Cisco Downloadable ACL Enforcement - Attributes Tab

Enforcement Profiles

Profile	Attributes	Summary
Type	Name	Value
1. Radius: Cisco	Cisco-IP-Downloadable-ACL	= permit ip any any
2. Click to add...		

The following table describes the **Cisco Downloadable ACL Enforcement - Attributes** parameters:

Table 186: *Cisco Downloadable ACL Enforcement - Attributes Tab Parameters*

Parameter	Description
Type	Select one of the following attribute types: • Radius:Aruba • Radius:IETF • Radius:Cisco • Radius:Microsoft • Radius:Avenda For more information, see RADIUS Namespaces on page 854
Name	The options displayed for the Name attribute depend on the Type attribute that was selected.
Value	The options displayed for the Value attribute depend on the Type and Name attributes that were selected.

Summary Tab

The **Summary** tab summarizes the parameters configured in the **Profile** and **Attribute** tabs. The following figure displays the **Cisco Downloadable ACL Enforcement - Summary** tab:

Figure 358: *Cisco Downloadable ACL Enforcement - Summary Tab*

Enforcement Profiles

Profile	Attributes	Summary
Profile:		
Template:	Cisco Downloadable ACL Enforcement	
Name:	Cisco_Enf	
Description:		
Type:	RADIUS	
Action:	Accept	
Device Group List:	-	
Attributes:		
Type	Name	Value
1. Radius:Cisco	Cisco-IP-Downloadable-ACL	= permit ip any any

Cisco Web Authentication Enforcement

Use this page to configure profile and attribute parameters for the **Cisco Web Authentication Enforcement** profile. The **Cisco Web Authentication Enforcement** profile contains the following tabs:

- [Profile Tab on page 365](#)
- [Attributes Tab on page 365](#)
- [Summary Tab on page 366](#)

Profile Tab

Use the **Profile** tab to configure the template, type of the profile, and device group list. The following figure displays the **Cisco Web Authentication Enforcement - Profile** tab:

Figure 359: Cisco Web Authentication Enforcement - Profile Tab

Enforcement Profiles

Profile	Attributes	Summary
Template:	Cisco Web Authentication Enforcement	
Name:		
Description:		
Type:	RADIUS	
Action:	☒ Accept ☐ Reject ☐ Drop	
Device Group List:	Remove View Details Modify Add new Device Group	
	--Select--	

The following table describes the **Cisco Web Authentication Enforcement - Profile** tab parameters:

Table 187: Cisco Web Authentication Enforcement - Profile Tab Parameters

Parameter	Description
Template	Select the template from the drop-down list. In this context, select Cisco Web Authentication Enforcement.
Name	Enter the name of the profile. The name is displayed in the Name column on the Configuration > Enforcement > Profiles page.
Description	Enter a description that provides additional information about the profile. This description is displayed in the Description column on the Configuration > Enforcement > Profiles page.
Type	This field is populated automatically.
Action	Click Accept , Reject , or Drop to define the action taken on the request.
Device Group List	Select a device group from the drop-down list. The list displays all configured device groups. All configured device groups are listed in the Device Groups (Configuration > Network > Device Groups) page. After adding one or more device group(s), you can select a group and take one of the following actions: - Click Remove to delete the selected Device Group List entry. - Click View Details to see the device group parameters. - Click Modify to change the parameters of the selected device group.
Add new Device Group	Click this link to add a new device group, For more information, see Adding and Modifying Device Groups on page 438 .

Attributes Tab

Use the **Attributes** tab to configure the attribute name and attribute value. The following figure displays the **Cisco Web Authentication Enforcement - Profile** tab:

Figure 360: Cisco Web Authentication Enforcement - Attributes Tab

Enforcement Profiles

Profile	Attributes	Summary
Type	Name	Value
1. Radius: Cisco	Cisco-AVPair	= priv-lvl=15
2. Radius: Cisco	Cisco-AVPair	= proxyacl# 10=permit ip any any
3. Click to add...		

The following table describes the **Cisco Web Authentication Enforcement - Attribute** parameters:

Table 188: *Cisco Web Authentication Enforcement - Attribute Tab Parameters*

Parameter	Description
Type	Select one of the following attribute types: - Radius:Aruba - Radius:IETF - Radius:Cisco - Radius:Microsoft - Radius:Avenda For more information, see RADIUS Namespaces on page 854
Name	The options displayed for the Name attribute depend on the Type attribute that was selected.
Value	The options displayed for the Value attribute depend on the Type and Name attributes that were selected.

Summary Tab

The **Summary** tab summarizes the parameters configured in the **Profile** and **Attribute** tabs. The following figure displays the **Cisco Web Authentication Enforcement - Summary** tab:

Figure 361: *Cisco Web Authentication Enforcement - Summary Tab*

Enforcement Profiles

Profile	Attributes	Summary
Profile:		
Template:	Cisco Web Authentication Enforcement	
Name:	Cisco_WebAuth_Enf	
Description:		
Type:	RADIUS	
Action:	Accept	
Device Group List:	-	
Attributes:		
Type	Name	Value
1. Radius: Cisco	Cisco- AVPair	= priv-lvl=15
2. Radius: Cisco	Cisco- AVPair	= proxyacl# 10=permit ip any any

ClearPass Entity Update Enforcement

Use this page to configure profile and attribute parameters for the **ClearPass Entity Update Enforcement** profile. The **ClearPass Entity Update Enforcement** profile contains the following tabs:

- [Profile Tab on page 367](#)
- [Attributes Tab on page 367](#)
- [Summary Tab on page 368](#)

Profile Tab

Use the **Profile** tab to configure the template, type of the profile, and device group list. The following figure displays the **ClearPass Entity Update Enforcement - Profile** tab:

Figure 362: ClearPass Entity Update Enforcement - Profile Tab

Enforcement Profiles

Profile	Attributes	Summary
Template:	ClearPass Entity Update Enforcement	
Name:		
Description:		
Type:	Post_Authentication	
Action:	☒ Accept ☐ Reject ☐ Drop	
Device Group List:	Remove View Details Modify	

[Add new Device Group](#)

The following table describes the **ClearPass Entity Update Enforcement - Profile** tab parameters:

Table 189: ClearPass Entity Update Enforcement - Profile Tab Parameters

Parameter	Description
Template	Select the template from the drop-down list. In this context, select ClearPass Entity Update Enforcement.
Name	Enter the name of the profile. The name is displayed in the Name column on the Configuration > Enforcement > Profiles page.
Description	Enter a description that provides additional information about the profile. This description is displayed in the Description column on the Configuration > Enforcement > Profiles page.
Type	This field is populated automatically.
Action	Click Accept , Reject , or Drop to define the action taken on the request.
Device Group List	Select a device group from the drop-down list. The list displays all configured device groups. All configured device groups are listed in the Device Groups (Configuration > Network > Device Groups) page. After adding one or more device group(s), you can select a group and take one of the following actions: - Click Remove to delete the selected Device Group List entry. - Click View Details to see the device group parameters. - Click Modify to change the parameters of the selected device group.
Add new Device Group	Click this link to add a new device group, For more information, see Adding and Modifying Device Groups on page 438 .

Attributes Tab

Use the **Attribute** tab to configure the attribute type, name, and value for the enforcement profile. The following figure displays the **ClearPass Entity Update Enforcement - Attributes** tab:

Figure 363: ClearPass Entity Update Enforcement Attributes tab

Enforcement Profiles

Profile	Attributes	Summary
Type	Name	Value
1. Endpoint	Device Type	=
2. Click to add...		

The following table describes the **ClearPass Entity Update Enforcement - Attributes** tab parameters:

Table 190: *ClearPass Entity Update Enforcement - Attributes Tab Parameters*

Attribute	Description
Type	Select one of the following attribute types: - Endpoint - Expire-Time-Update - GuestUser - Status-Update
Name	The options displayed for the Name attribute depend on the Type attribute that was selected.
Value	The options displayed for the Value attribute depend on the Type and Name attributes that were selected.

Summary Tab

The **Summary** tab summarizes the parameters configured in the **Profile** and **Attributes** tab. The following figure displays the **ClearPass Entity Update Enforcement - Summary** tab:

Figure 364: *ClearPass Entity Update Enforcement - Summary Tab*

Enforcement Profiles

Profile	Attributes	Summary
Profile:		
Template:	ClearPass Entity Update Enforcement	
Name:	Ent_update_Enf	
Description:		
Type:	Post_Authentication	
Action:	Accept	
Device Group List:	-	
Attributes:		
Type	Name	Value
1. Endpoint	Enabled By	= Admin
2. Expire-Time-Update	GuestUser	= User1
3. GuestUser	Location	= Sunnyvale

CLI Based Enforcement

Use this page to configure profile and attribute parameters for the **CLI Based Enforcement** profile. The **CLI Based Enforcement** profile contains the following tabs:

- [Profile Tab on page 369](#)
- [Attributes Tab on page 369](#)
- [Summary Tab on page 370](#)

Profile Tab

Use the **Profile** tab to configure the template, type of the profile, and device group list. The following figure displays the **CLI Based Enforcement - Profile** tab:

Figure 365: CLI Based Enforcement - Profile Tab

Enforcement Profiles

Profile	Attributes	Summary
Template:	CLI Based Enforcement	
Name:		
Description:		
Type:	CLI	
Action:	☒ Accept ☐ Reject ☐ Drop	
Device Group List:	--Select-- Remove View Details Modify Add new Device Group	

The following table describes the **CLI Based Enforcement - Profile** tab parameters:

Table 191: CLI Based Enforcement - Profile Tab Parameters

Parameter	Description
Template	Select the template from the drop-down list. In this context, select CLI Based Enforcement.
Name	Enter the name of the profile. The name is displayed in the Name column on the Configuration > Enforcement > Profiles page.
Description	Enter a description that provides additional information about the profile. This description is displayed in the Description column on the Configuration > Enforcement > Profiles page.
Type	This field is populated automatically.
Action	Click Accept , Reject , or Drop to define the action taken on the request.
Device Group List	Select a device group from the drop-down list. The list displays all configured device groups. All configured device groups are listed in the Device Groups (Configuration > Network > Device Groups) page. After adding one or more device group(s), you can select a group and take one of the following actions: - Click Remove to delete the selected Device Group List entry. - Click View Details to see the device group parameters. - Click Modify to change the parameters of the selected device group.
Add new Device Group	Click this link to add a new device group, For more information, see Adding and Modifying Device Groups on page 438 .

Attributes Tab

Use the **Attribute** tab to configure the attribute type, name, and value for the enforcement profile. The following figure displays the **CLI Based Enforcement - Attributes** tab:

Figure 366: CLI Based Enforcement - Attributes Tab

Enforcement Profiles

Profile	Attributes	Summary												
<table><thead><tr><th>Attribute Name</th><th>Attribute Value</th><th></th></tr></thead><tbody><tr><td>1. Target Device</td><td>=</td><td>%(Connection:NAD-IP-Address)</td></tr><tr><td>2. Command</td><td>=</td><td>Enter Command</td></tr><tr><td>3. Click to add...</td><td></td><td></td></tr></tbody></table>			Attribute Name	Attribute Value		1. Target Device	=	%(Connection:NAD-IP-Address)	2. Command	=	Enter Command	3. Click to add...		
Attribute Name	Attribute Value													
1. Target Device	=	%(Connection:NAD-IP-Address)												
2. Command	=	Enter Command												
3. Click to add...														

The following table describes the **CLI Based Enforcement - Attributes** tab parameters:

Table 192: CLI Based Enforcement - Attributes Tab Parameters

Attribute	Parameter
Attribute Name	Select Command or Target Device.
Attribute Value	Displays the options for the Attribute Value depend on the selected Attribute Name .

Summary Tab

The **Summary** tab summarizes the parameters configured in the **Profile** and **Attributes** tab. The following figure displays the **CLI Based Enforcement - Summary** tab:

Figure 367: CLI Based Enforcement - Summary Tab

Enforcement Profiles

Profile	Attributes	Summary
Profile:		
Template:	CLI Based Enforcement	
Name:	CLI_Enf	
Description:		
Type:	CLI	
Action:	Accept	
Device Group List:	-	
Attributes:		
Attribute Name	Attribute Value	
1. Target Device	=	%{Connection:NAD-IP-Address}
2. Command	=	get

Filter ID Based Enforcement

Use this page to configure profile and attribute parameters for the Filter ID based enforcement profile. The **Filter ID Based Enforcement** profile contains the following tabs:

- [Profile Tab on page 370](#)
- [Attributes Tab on page 371](#)

Profile Tab

The following figure displays the **Filter ID Based Enforcement - Profile** tab:

Figure 368: Filter ID Based Enforcement Profile tab

Enforcement Profiles

Profile	Attributes	Summary
Profile:		
Template:	Filter ID Based Enforcement	
Name:		
Description:		
Type:	RADIUS	
Action:	☒ Accept ☐ Reject ☐ Drop	
Device Group List:	Remove View Details Modify Add new Device Group	
	--Select--	

The following table describes the **Filter ID Based Enforcement Profile** tab parameters:

Table 193: *Filter ID Based Enforcement - Profile Tab Parameters*

Parameter	Description
Template	Select the template from the drop-down list. In this context, select Filter ID Based Enforcement
Name	Enter the name of the profile. The name is displayed in the Name column on the Configuration > Enforcement > Profiles page.
Description	Enter a description of the profile. The Description is displayed in the Description column on the Configuration > Enforcement > Profiles page.
Type	RADIUS. The field is populated automatically.
Action	Enabled. Click Accept, Reject, or Drop to define the action taken on the request.
Device Group List	Select a Device Group from the drop-down list. The list displays all configured Device Groups. All configured device groups are listed in the Device Groups page: Configuration > Network > Device Groups. After you add one or more device group(s), you can select a group and take one of the following actions: - Click Remove to delete the selected Device Group List entry. - Click View Details to see the device group parameters. - Click Modify to change the parameters of the selected device group.
Add new Device Group	To add a new a device group, click the Add new Device Group link and see Adding and Modifying Device Groups on page 438 .

Attributes Tab

The following figure displays the **Filter ID Based Enforcement Profile - Attributes** tab:

Figure 369: *Filter ID Based Enforcement Profile - Attributes Tab*

Enforcement Profiles

Type	Name	Value
1. Radius:IETF	Filter-Id	= Enter Filter Name
2. Click to add...		

The following table describes the **Filter ID Based Enforcement - Attributes** tab parameters:

Table 194: *Filter ID Based Enforcement Profile - Attributes Tab Parameters*

Parameter	Description
Type	Select one of the following attribute types: ● Radius:Aruba ● Radius:IETF ● Radius:Cisco ● Radius:Microsoft ● Radius:Avenda For more information, see RADIUS Namespaces on page 854
Name	The options displayed for the Name attribute depend on the attribute that was selected.
Value	The options displayed for the Value attribute depend on the Type attribute and Name attribute that were selected.

Generic Application Enforcement

Use this page to configure profile and attribute parameters for the **Generic Application Enforcement** profile. The **Generic Application Enforcement** profile contains the following tabs:

- [Profile Tab on page 372](#)
- [Attributes Tab on page 373](#)
- [Summary Tab on page 374](#)

Profile Tab

Use the **Profile** tab to configure the template, type of the profile, and device group list. The following figure displays the **Generic Application Enforcement - Profile** tab:

Figure 370: *Generic Application Enforcement - Profile Tab*

Enforcement Profiles

Profile	Attributes	Summary
Template: Generic Application Enforcement		
Name:		
Description:		
Type: Application		
Action: ☒ Accept ☐ Reject ☐ Drop		
Device Group List:	Remove View Details Modify	Add new Device Group

The following table describes the **Generic Application Enforcement - Profile** tab parameters:

Table 195: *Generic Application Enforcement - Profile Tab Parameters*

Parameter	Description
Template	Select the template from the drop-down list. In this context, select Generic Application Enforcement.
Name	Enter the name of the profile. The name is displayed in the Name column on the Configuration > Enforcement > Profiles page.
Description	Enter a description that provides additional information about the profile. This description is displayed in the Description column on the Configuration > Enforcement > Profiles page.
Type	This field is populated automatically.
Action	Click Accept , Reject , or Drop to define the action taken on the request.
Device Group List	Select a device group from the drop-down list. The list displays all configured device groups. All configured device groups are listed in the Device Groups (Configuration > Network > Device Groups) page. After adding one or more device group(s), you can select a group and take one of the following actions: - Click Remove to delete the selected Device Group List entry. - Click View Details to see the device group parameters. - Click Modify to change the parameters of the selected device group.
Add new Device Group	Click this link to add a new device group, For more information, see Adding and Modifying Device Groups on page 438 .

Attributes Tab

Use the **Attribute** tab to configure the attribute type, name, and value for the enforcement profile. The following figure displays the **Generic Application Enforcement - Attributes** tab:

Figure 371: *Generic Application Enforcement - Attributes Tab*

Enforcement Profiles

Profile Attributes Summary

Attribute Name	Attribute Value
1. Click to add...	

The following table describes the **Generic Application Enforcement - Attributes** tab parameters:

Table 196: *Generic Application Enforcement - Attributes Tab Parameters*

Parameter	Description
Attribute Name	Select an attribute name from the drop-down list. The list has multiple names.
Attribute Value	Displays the options for the Attribute Value depend on the selected Attribute Name .

Summary Tab

The **Summary** tab summarizes the parameters configured in the **Profile** and **Attributes** tab. The following figure displays the **Generic Application Enforcement - Summary** tab:

Figure 372: *Generic Application Enforcement - Summary Tab*

Enforcement Profiles

Profile	Attributes	Summary
Profile:		
Template:	Generic Application Enforcement	
Name:	GEN APP Enf	
Description:	Generic Application Enforcement	
Type:	Application	
Action:	Accept	
Device Group List:	-	
Attributes:		
Attribute Name	Attribute Value	
1. SSO-Role	= Network Administrator	

HTTP Based Enforcement

Use this page to configure profile and attribute parameters for the HTTP based enforcement profile.

Profile Tab

The following figure displays the **HTTP Based Enforcement - Profile** tab:

Figure 373: *HTTP Based Enforcement Profile tab*

Enforcement Profiles

Profile	Attributes	Summary
Profile:		
Template:	HTTP Based Enforcement	
Name:		
Description:		
Type:	HTTP	
Action:	☒ Accept ☐ Reject ☐ Drop	
Device Group List:	--Select-- Remove View Details Modify Add new Device Group	

The following table describes the **HTTP Based Enforcement - Profile** tab parameters:

Table 197: *HTTP Based Enforcement Profile tab Parameters*

Parameter	Description
Template	Select the template from the drop-down list. In this context, select HTTP Based Enforcement.
Name	Enter the name of the profile. The name is displayed in the Name column on the Configuration > Enforcement > Profiles page.
Description	Enter a description of the profile. The description is displayed in the Description column on the Configuration > Enforcement > Profiles page.
Type	Specifies the type of authentication. In this context, HTTP. This field is populated automatically.

Table 197: HTTP Based Enforcement Profile tab Parameters (Continued)

Parameter	Description
Action	Disabled.
Device Group List	Select a Device Group from the drop-down list. The list displays all configured Device Groups. All configured device groups are listed in the Device Groups page: Configuration > Network > Device Groups . After you add one or more device group(s), you can select a group and take one of the following actions: - Click Remove to delete the selected Device Group List entry. - Click View Details to see the device group parameters. - Click Modify to change the parameters of the selected device group.
Add new Device Group	To add a new a device group, click the Add new Device Group link and see Adding and Modifying Device Groups on page 438 .

Attributes Tab

Figure 374: HTTP Based Enforcement Attributes tab

Enforcement Profiles

Profile	Attributes	Summary
Attribute Name		
Attribute Value		
1. Target Server	=	Select server
2. Action	=	Select action
3. Click to add...		

Table 198: HTTP Based Enforcement Attributes tab Parameters

Parameter	Description
Attribute Name	Select Target Server or Action.
Attribute Value	The options displayed for the Attribute Value depend on the Attribute Name that was selected.

RADIUS Based Enforcement

Use this page to configure profile and attribute parameters for the RADIUS based enforcement profiles.

Profile Tab

The following figure displays the **RADIUS Based Enforcement Profile** tab:

Figure 375: RADIUS Based Enforcement - Profile Tab

Enforcement Profiles

Profile	Attributes	Summary
Template:	RADIUS Based Enforcement	
Name:		
Description:		
Type:	RADIUS	
Action:	☒ Accept ☐ Reject ☐ Drop	
Device Group List:	Remove View Details Modify Add new Device Group	
	--Select--	

The following table describes the **RADIUS Based Enforcement Profile** tab parameters:

Table 199: *RADIUS Based Enforcement Profile Tab Parameters*

Parameter	Description
Template	Select the template from the drop-down list. In this context, select RADIUS Based Enforcement.
Name	Enter the name of the profile. The name is displayed in the Name column on the Configuration > Enforcement > Profiles page.
Description	Enter a description of the profile. The Description is displayed in the Description column on the Configuration > Enforcement > Profiles page.
Type	RADIUS. The field is populated automatically.
Action	Enabled. Click Accept, Reject or Drop to define the action taken on the request.
Device Group List	Select a Device Group from the drop-down list. The list displays all configured Device Groups. All configured device groups are listed in the Device GroupsConfiguration > Network > Device Groups page. After you add one or more device group(s), you can select a group and take one of the following actions: - Click Remove to delete the selected Device Group List entry - Click View Details to see the device group parameters - Click Modify to change the parameters of the selected device group
Add new Device Group	To add a new a device group, click the Add new Device Group link and see Adding and Modifying Device Groups on page 438 .

Attributes Tab

The following figure displays the **RADIUS Based Enforcement - Attributes** tab:

Figure 376: *RADIUS Based Enforcement Attributes Tab*

Enforcement Profiles

Profile Attributes Summary

Type	Name	Value
1. Radius:Aruba	Aruba-AP-Group (10)	=
2. Click to add...		

The following table describes the **RADIUS Based Enforcement - Attributes** tab parameters:

Table 200: *RADIUS Based Enforcement - Attributes Tab Parameters*

Parameter	Description
Type	Select one of the following attribute types: ● Radius:Aruba ● Radius:IETF ● Radius:Cisco ● Radius:Microsoft ● Radius:Avenda For more information, see RADIUS Namespaces on page 854
Name	The options displayed for the Name attribute depend on the Type attribute that was selected.
Value	The options displayed for the Value attribute depend on the Type and Name attributes that were selected.

RADIUS Change of Authorization (CoA)

Use this page to configure profile and attribute parameters for the RADIUS Change of Authorization (CoA) enforcement profile.

Profile Tab

The following figure displays the **Radius Change of Authorization (CoA) - Profile** tab:

Figure 377: *Radius Change of Authorization (CoA) Profile Tab*

Enforcement Profiles

Profile	Attributes	Summary
Template:	RADIUS Change of Authorization (CoA)	
Name:		
Description:		
Type:	RADIUS_CoA	
Action:	☒ Accept ☐ Reject ☐ Drop	
Device Group List:	--Select-- Remove View Details Modify Add new Device Group	

The following table describes the **Radius Change of Authorization (CoA) - Profile** tab parameters:

Table 201: *Radius Change of Authorization (CoA) Profile Tab Parameters*

Parameter	Description
Template	Select from: • Cisco-Disable-Host-Port • Cisco - Bounce-Host-Port • Cisco - Reauthenticate-Session • HP - Change-VLAN • HP - Generic-CoA • Aruba - Change-User-Role • IETF - Terminate-Session-IETF • Aruba - Change-VPN-User-Role • IETF- Generic-CoA-IETF
Type	Select one of the following attribute types: • Radius:Aruba • Radius:IETF • Radius:Cisco • Radius:Microsoft • Radius:Avenda For more information, see RADIUS Namespaces on page 854
Name	The options displayed for the Name Attribute depend on the RADIUS CoA Template selected and the Type Attribute that were selected.
Value	The options displayed for the Value Attribute depend on the RADIUS CoA Template selected and the Type Attribute that were selected.
Type	RADIUS_CoA. The field is populated automatically.
Action	Disabled.
Device Group List	Select a Device Group from the drop-down list. The list displays all configured Device Groups. All configured device groups are listed on the Device Groups page: Configuration > Network > Device Groups. After you add one or more device group(s), you can select a group and take one of the following actions: • Click Remove to delete the selected Device Group List entry. • Click View Details to see the device group parameters. • Click Modify to change the parameters of the selected device group.
Add new Device Group	To add a new a device group, click the Add new Device Group link and see Adding and Modifying Device Groups on page 438 .

Attributes Tab

The following figure displays the **Radius Change of Authorization (CoA) - Attributes** tab:

Figure 378: *Radius Change of Authorization (CoA) - Attributes Tab*

Enforcement Profiles

Profile Attributes Summary

Select RADIUS CoA Template: Cisco-Disable-Host-Port

Type	Name	Value
1. Radius:IETF	Calling-Station-Id	= %{Radius:IETF:Calling-Station-Id}
2. Radius:Cisco	Cisco-AVPair	= subscriber:command=disable-host-port
3. Click to add...		

The following table describes the **Radius Change of Authorization (CoA) - Attributes** tab parameters:

Table 202: *Radius Change of Authorization (CoA) Attributes Tab Parameters*

Parameter	Description
RADIUS CoA Template	Select from: • Cisco-Disable-Host-Port • Cisco - Bounce-Host-Port • Cisco - Reauthenticate-Session • HP - Change-VLAN • HP - Generic-CoA • Aruba - Change-User-Role • IETF - Terminate-Session-IETF • Aruba - Change-VPN-User-Role • IETF- Generic-CoA-IETF
Type	Select one of the following attribute types: • Radius:Aruba • Radius:IETF • Radius:Cisco • Radius:Microsoft • Radius:Avenda For more information, see RADIUS Namespaces on page 854
Name	The options displayed for the Name Attribute depend on the Template and Type Attribute that were selected.
Value	The options displayed for the Value Attribute depend on the Template, Type Attribute and Name Attribute that were selected.

Session Notification Enforcement

Use this page to configure profile and attribute parameters for **Session Notification Enforcement** profile. Notification of a change in IP address can now be sent to any external context server (such as a firewall) by configuring that server as a generic HTTP server and adding the appropriate generic HTTP context server actions. The content of the payload to be posted by W-Policy Manager to the external server is based on the REST API defined by the external server for communication.

The **Session Notification Enforcement** page contains the following tabs:

- [Profile Tab on page 380](#)
- [Attributes Tab on page 380](#)

- [Summary Tab on page 381](#)

Profile Tab

The following figure displays the **Session Notification Enforcement - Profile** tab:

Figure 379: Session Notification Enforcement - Profile Tab

Configuration » Enforcement » Profiles » Add Enforcement Profile

Enforcement Profiles

Profile	Attributes	Summary
Template:	Session Notification Enforcement	
Name:	SessionNotification	
Description:		
Type:	Post_Authentication	
Action:	☒ Accept ☐ Reject ☐ Drop	
Device Group List:		Add new Device Group Remove View Details Modify

The following table describes the **Session Notification Enforcement - Profile** tab parameters:

Table 203: Session Notification Enforcement Profile Tab Parameters

Parameter	Description
Template	Select Session Notification Enforcement .
Name	Enter the name of the profile. The name is displayed in the Name column on the Configuration > Enforcement > Profiles page.
Description	Enter a description of the profile. The Description is displayed in the Description column on the Configuration > Enforcement > Profiles page.
Type	Post_Authentication. The field is populated automatically.
Action	Disabled.
Device Group List	Select a device group from the drop-down list. The list displays all configured device groups. All configured device groups are listed in the Device Groups Configuration > Network > Device Groups page.
Add new Device Group	To add a new a device group, click the Add new Device Group link and see Adding and Modifying Device Groups on page 438 .

Attributes Tab

The following figure displays the **Session Notification Enforcement - Attributes** tab:

Figure 380: Session Notification Enforcement - Attributes Tab

Configuration » Enforcement » Profiles » Add Enforcement Profile

Enforcement Profiles

Profile

Attributes

Summary

Type	Name	Value	
1. Session-Check	Username	= admin	 
2. Session-Notify	Logout Action	=	 
3. Click to add...			

The following table describes the **Session Notification Enforcement - Attributes** tab:

Table 204: Session Notification Enforcement - Attributes Tab

Parameter	Description
Type	Select from: - Session-Check - Session-Notify Palo Alto integration is extended to Guest MAC Caching use cases. Configure the following: Session-Check::Username = %{Endpoint:Username} NOTE: Post Auth sends the Guest username instead of the MAC Address in the user id updates. For Session-Notify Type attribute, the Name can be Server Type, Server IP, Login Action, or Logout Action. The values for Server Type can be Generic HTTP, Palo Alto Networks Panorama, or Palo Alto Networks Firewall. Selecting Server IP for Name provides a choice of ipaddress/hostnames for corresponding type of server as Value. Once the server IP is selected, Login Action and Logout Action can be selected (the list of actions defined for the selected server will be shown as available choices for value). This enforcement type should be used both for Palo Alto Devices and any Generic HTTP servers. Pre-6.5 configurations containing Session Restrictions Enforcement profile for Palo Alto devices (with attribute Session-Check::IP-Address-Change-Notify) will be migrated to this new enforcement profile during an upgrade (any profiles defined with more than one Palo Alto device or combined with any other Session Restrictions attributes will not be migrated and need to re-configured).
Name	The options displayed for the Name attribute depend on the Type attribute that was selected.
Value	The options displayed for the Value attribute depend on the Type attribute and Name attribute that were selected.

Summary Tab

This tab summarizes the parameters configured in the **Summary** tab. The following figure displays the **Session Notification Enforcement - Summary** tab:

Figure 381: Session Notification Enforcement - Summary Tab

Enforcement Profiles

Profile	Attributes	Summary
Profile:		
Template:	Session Notification Enforcement	
Name:	SessionNotification	
Description:		
Type:	Post_Authentication	
Action:	Accept	
Device Group List:	-	
Attributes:		
Type	Name	Value
1. Session-Check	Username	= admin
2. Session-Notify	Logout Action	=

Session Restrictions Enforcement

W-ClearPass uses Keep-Alive messages to issue CoA (Change of Authorization) for a Session Restrictions Enforcement Profile if OnGuard Agent is disconnected (see below, [Examples of Session-Check Enforcement Profile Configurations](#)). For related information, see [OnGuard Global Agent Settings on page 654](#).

To configure Profile and Attribute parameters for a Session Restrictions Enforcement profile:

1. Navigate to **Configuration > Enforcement > Profiles**.

The **Enforcement Profiles** page opens.

2. Click **Add**.

The **Add Enforcement Profiles > Profile** tab opens.

3. From the **Template** drop-down, select **Session Restrictions Enforcement**.

The **Add Session Restrictions Enforcement > Profile** dialog opens:

Figure 382: Add Session Restrictions Enforcement > Profile Tab

Configuration » Enforcement » Profiles » Add Enforcement Profile

Enforcement Profiles

Profile Attributes Summary

Template: Session Restrictions Enforcement

Name:

Description:

Type: Post_Authentication

Action: ☒ Accept ☐ Reject ☐ Drop

Device Group List:

Remove View Details Modify

[Add new Device Group](#)

4. Specify the **Session Restrictions Enforcement > Profile** parameters as described in the following table:

Table 205: Session Restrictions Enforcement Profile Parameters

Parameter	Action/Description
Template	Select Session Restrictions Enforcement from the drop-down list.
Name	Enter the name of the enforcement profile.
Description	Optionally, enter a description of the enforcement profile (recommended).
Type	Post_Authentication. The Type field is populated automatically when you select the Session Restrictions Enforcement template.
Action	By default, this field is disabled. It is enabled only when RADIUS type is selected.
Device Group List	Select a device group from the drop-down list. The list displays all configured device groups. All configured device groups are listed in the Configuration > Network > Device Groups page. After you add one or more device groups, select a group and take one of the following actions: • To delete the selected device group list entry, click Remove. • To see the device group parameters, click View Details. • To change the parameters of the selected device group, click Modify.
Add New Device Group	To add a new a device group, click the Add New Device Group link. For more information, see Adding and Modifying Device Groups on page 438 .

Attributes Tab

The following figure displays the **Session Restrictions Enforcement > Attributes** tab:

Figure 383: *Session Restrictions Enforcement Profile > Attributes Dialog*

Configuration » Enforcement » Profiles » Add Enforcement Profile

Enforcement Profiles

Profile Attributes Summary

Type	Name	Value	
1. Post-Auth-Check	Action	= Disconnect	
2. Session-Check	Agent-Connection	= Down	
3. Click to add...			

1. Specify the **Session Restrictions Enforcement > Attributes** parameters as described in [Table 206](#):

Table 206: Session Restrictions Enforcement Attributes Parameters

Parameter	Description
Type	Select from the following attribute types: • Bandwidth-Check • Expiry-Check • Post-Auth-Check • Session-Check
Name	The options displayed for the Name attribute depend on the Type attribute that was selected. • Type: Bandwidth-Check ■ Allowed-Limit: Defines the total bandwidth limit to be allowed per user or endpoint. ■ Check-Type: Defines the period/interval for bandwidth-based checks. Applicable only with Allowed-Limit. ■ Limit-Units: Defines the metric for bandwidth-based checks (KB, MB, GB, TB). Applicable only with Allowed-Limit. ■ Start-Date: Defines the start date for bandwidth-based checks. Applicable only with Allowed-Limit. ■ Start-Time: Defines the start time for bandwidth-based checks. Applicable only with Allowed-Limit. ■ Stop-Date: Defines the stop date for bandwidth-based checks. Applicable only with Allowed-Limit. ■ Stop-Time: Defines the stop time for bandwidth-based checks. Applicable only with Allowed-Limit. For configuration examples, see the next section, Examples of Bandwidth-Check Enforcement Profile Configurations. • Type: Expiry-Check ■ Expiry-Action • Type: Post-Auth-Check ■ Action • Type: Session-Check ■ Active-Session-Count: Defines the number of active sessions to be allowed per user or endpoint. ■ Agent-Connection: Set the value to Down to have W-ClearPass check to see if the OnGuard Agent is down. ■ Allowed-Duration: Defines the total session duration to be allowed per user or endpoint. ■ Check-Type: Defines the period or interval for duration-based checks. Applicable only with Allowed-Duration. ■ Duration-Units: Defines the metric for duration-based checks. Applicable only with Allowed-Duration. ■ Start-Date: Defines the start date for duration-based checks. Applicable only with Allowed-Duration. ■ Start-Time: Defines the start time for duration-based checks. Applicable only with Allowed-Duration. ■ Stop-Date: Defines the stop date for duration-based checks. Applicable only with Allowed-Duration. ■ Stop-Time: Defines the stop time for duration-based checks. Applicable only with Allowed Duration.

Table 206: *Session Restrictions Enforcement Attributes Parameters (Continued)*

Parameter	Description
	■ Username: Defines the username for which session restrictions are enabled. Used when the client MAC address is to be defined as a username. For configuration examples, see the section below, Examples of Session-Check Enforcement Profile Configurations.
Value	The options displayed for the Value attribute depend on the Type and Name attributes that were selected.

Examples of Bandwidth-Check Enforcement Profile Configurations

The following are typical examples of **Session Restriction > Bandwidth-Check** enforcement profile configurations:

1. **Allowed-Limit:** Users/Endpoints will be disconnected after exceeding the 50 MB daily limit:
 - Bandwidth-Check > Allowed-Limit = 50
 - Bandwidth-Check > Limit-Units = MB
 - Bandwidth-Check > Check-Type = Daily
 - Post-Auth-Check > Action = Disconnect
2. **Allowed-Limit:** Users/Endpoints will be disconnected after exceeding 1 GB total bandwidth consumption. Also, users are allowed access to the network only during the defined period (between 9:00 a.m. and 6:00 p.m.).
 - Bandwidth-Check > Allowed-Limit = 1
 - Bandwidth-Check > Limit-Units = GB
 - Bandwidth-Check > Check-Type = Total
 - Bandwidth-Check > Start-Time = 09:00:00
 - Bandwidth-Check > Stop-Time = 18:00:00
 - Post-Auth-Check > Action = Disconnect

Examples of Session-Check Enforcement Profile Configurations

The following are typical examples of **Session Restriction > Session-Check** enforcement profile configurations:

1. **Active Session Count:** The Users/Endpoints active session count is set to **5**. Users/Endpoints connecting after the session count reaches **5** are disconnected:
 - Session-Check > Active-Session-Count = 5
 - Post-Auth-Check > Action = Disconnect
2. **Agent-Connection:** You can disconnect a session if OnGuard Agent is down:
 - Session-Check > Agent-Connection = Down
 - Post-Auth-Check > Action = Disconnect
3. **Session Duration:** The User/Endpoint is allowed access for 60 minutes daily. Users/Endpoints that exceed this session duration limit are disconnected:
 - Session-Check > Allowed-Duration = 60
 - Session-Check > Duration-Units = Minutes
 - Session-Check > Check-Type = Daily

- Post-Auth-Check > Action = Disconnect
4. **Session Duration:** The User/Endpoint is allowed access to the network daily for three hours in a specified time period (between 9:00 a.m. and 5:00 p.m.)
- Session-Check > Allowed-Duration = 3
 - Session-Check > Duration-Units = Hours
 - Session-Check > Check-Type = Daily
 - Session-Check > Start-Time = 09:00:00
 - Session-Check Stop-Time = 17:00:00
 - Post-Auth-Check > Action = Disconnect

SNMP Based Enforcement

Use this page to configure profile and attribute parameters for the SNMP based enforcement profile.

Profile Tab

The following figure displays the **SNMP Based Enforcement - Profile** tab:

Figure 384: *SNMP Based Enforcement - Profile Tab*

The screenshot shows the 'Profile' tab of the 'Enforcement Profiles' configuration page. The 'Template' dropdown is set to 'SNMP Based Enforcement'. The 'Name' and 'Description' fields are empty. The 'Type' is set to 'SNMP'. The 'Action' section has radio buttons for 'Accept', 'Reject', and 'Drop'. The 'Device Group List' section has a dropdown menu with '--Select--' and buttons for 'Remove', 'View Details', and 'Modify'. A link 'Add new Device Group' is also present.

The following table describes the **SNMP Based Enforcement - Profile** parameters:

Table 207: *SNMP Based Enforcement - Profile Tab Parameters*

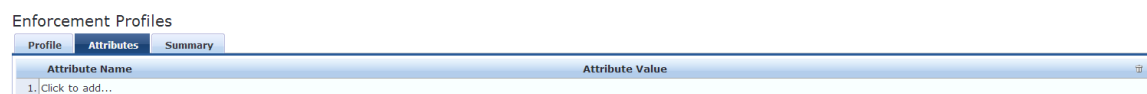
Parameter	Description
Template	Select the template from the drop-down list. In this context, select SNMP Based Enforcement.
Name	Enter the name of the profile. The name is displayed in the Name column on the Configuration > Enforcement > Profiles page.
Description	Enter a description of the profile. The Description is displayed in the Description column on the Configuration > Enforcement > Profiles page.
Type	SNMP. The field is populated automatically.

Table 207: SNMP Based Enforcement - Profile Tab Parameters (Continued)

Parameter	Description
Action	Disabled.
Device Group List	Select a Device Group from the drop-down list. The list displays all configured Device Groups. All configured device groups are listed in the Device Groups page: Configuration > Network > Device Groups. After you add one or more device group(s), you can select a group and take one of the following actions: - Click Remove to delete the selected Device Group List entry. - Click View Details to see the device group parameters. - Click Modify to change the parameters of the selected device group.
Add new Device Group	To add a new a device group, click the Add new Device Group link and see Adding and Modifying Device Groups on page 438 .

Attributes tab

The following figure displays the **SNMP Based Enforcement - Attributes** tab:

Figure 385: SNMP Based Enforcement - Attributes Tab

The following table describes the **SNMP Based Enforcement - Attributes** tab parameters:

Table 208: SNMP Based Enforcement Attributes Tab Parameters

Parameter	Description
Attribute Name	Select from: - VLAN ID - Session Timeout (in seconds) - Reset Connection (after the settings are applied)
Attribute Value	The options displayed for the Attribute value is depend on the Attribute name that was selected.

TACACS+ Based Enforcement

Use this page to configure profile, service, and attribute parameters for the TACACS+ based enforcement profile.

Profile Tab

The following figure displays the **TACACS+ Based Enforcement - Profile** tab:

Figure 386: TACACS+ Based Enforcement Profile Tab

Enforcement Profiles

Profile	Services	Summary
Template:	TACACS+ Based Enforcement	
Name:		
Description:		
Type:	TACACS	
Action:	☒ Accept ☐ Reject ☐ Drop	
Device Group List:	Remove View Details Modify	Add new Device Group
	--Select--	

The following table describes the **TACACS+ Based Enforcement Profile - Profile** tab parameters:

Table 209: TACACS+ Based Enforcement Profile Tab Parameters

Parameter	Description
Template	Select the template from the drop-down list. In this context, select TACACS+ Based Enforcement.
Name	Enter the name of the profile. The name is displayed in the Name column on the Configuration > Enforcement > Profiles page.
Description	Enter a description of the profile. The Description is displayed in the Description column on the Configuration > Enforcement > Profiles page.
Type	TACACS. The field is populated automatically.
Action	Disabled.
Device Group List	Select a Device Group from the drop-down list. The list displays all configured Device Groups. All configured device groups are listed in the Device Groups (Configuration > Network > Device Groups) page. After you add one or more device group(s), you can select a group and take one of the following actions: - Click Remove to delete the selected Device Group List entry. - Click View Details to see the device group parameters. - Click Modify to change the parameters of the selected device group.
Add new Device Group	To add a new a device group, click the Add new Device Group link and see Adding and Modifying Device Groups on page 438 .

Services Tab

The following figure displays the **TACACS+ Based Enforcement - Services** tab:

Figure 387: TACACS+ Based Enforcement Services Tab

Enforcement Profiles

Profile Services Summary

Privilege Level: 0 (Minimum)

Selected Services: Remove [Export TACACS+ Services Dictionary](#)

Custom Services: To add new TACACS+ services / attributes, upload the modified dictionary xml - [Update TACACS+ Services Dictionary](#)

Service Attributes

Type	Name	Value
1. Click to add...		

The following table describes the **TACACS+ Based Enforcement Profile - Service** tab parameters:

Table 210: TACACS+ Based Enforcement Services Tab Parameters

Parameter	Description
Privilege Level	Select a level between 0 and 15.
Selected Services	Select a service from the list and add it to the Selected Services: field. Click Remove to remove a service from the field.
Export All	Click this link to download the TACACS+ Services dictionary is downloaded to the local computer.
Custom Services	To add new TACACS+ services / attributes, upload the modified dictionary xml click Update TACACS+ Services Dictionary.
Type	Select a service attribute parameter from the list.
Name	The options displayed for the Name attribute depend on the Type attribute that was selected.
Value	The options displayed for the Value attribute depend on the Type and Name attributes that were selected.

VLAN Enforcement

Use this page to configure profile and attribute parameters for the VLAN enforcement profile.

Profile Tab

The following figure displays the **VLAN Enforcement - Profile** tab:

Figure 388: VLAN Enforcement - Profile Tab

Enforcement Profiles

Profile Attributes Summary

Template: VLAN Enforcement

Name:

Description:

Type: RADIUS

Action: ☒ Accept ☐ Reject ☐ Drop

Device Group List: Remove View Details Modify [Add new Device Group](#)

--Select--

The following table describes the **VLAN Enforcement - Profile** tab parameters:

Table 211: *VLAN Enforcement - Profile Tab Parameters*

Parameter	Description
Template	Select the template from the drop-down list. In this context, select VLAN Enforcement.
Name	Enter the name of the profile. The name is displayed in the Name column on the Configuration > Enforcement > Profiles page.
Description	Enter a description of the profile. The Description is displayed in the Description column on the Configuration > Enforcement > Profiles page.
Type	RADIUS. The field is populated automatically.
Action	Enabled. Click Accept, Reject, or Drop to define the action taken on the request.
Device Group List	Select a Device Group from the drop-down list. The list displays all configured Device Groups. All configured device groups are listed in the Device Groups page: Configuration > Network > Device Groups . After you add one or more device group(s), you can select a group and take one of the following actions: - Click Remove to delete the selected Device Group List entry. - Click View Details to see the device group parameters. - Click Modify to change the parameters of the selected device group.
Add new Device Group	To add a new a device group, click the Add new Device Group link and see Adding and Modifying Device Groups on page 438 .

Attributes Tab

The following figure displays the **VLAN Enforcement - Attributes** tab:

Figure 389: *VLAN Enforcement Attributes Tab*

Enforcement Profiles

Profile	Attributes	Summary
Type	Name	Value
1. Radius:IETF	Session-Timeout	= 10800
2. Radius:IETF	Termination-Action	= RADIUS-Request (1)
3. Radius:IETF	Tunnel-Type	= VLAN (13)
4. Radius:IETF	Tunnel-Medium-Type	= IEEE-802 (6)
5. Radius:IETF	Tunnel-Private-Group-Id	= Enter VLAN
6. Click to add...		

The following table describes the **RADIUS Based Enforcement - Attributes** tab parameters:

Table 212: *VLAN Enforcement Attributes Tab Parameters*

Parameter	Description
Type	Select one of the following attribute types: ● Radius:Aruba ● Radius:IETF ● Radius:Cisco ● Radius:Microsoft ● Radius:Avenda For more information, see RADIUS Namespaces on page 854
Name	The options displayed for the Name attribute depend on the Type attribute that was selected.
Value	The options displayed for the Value attribute depend on the Type and Name attributes that were selected.

This chapter describes the following types of simulations:

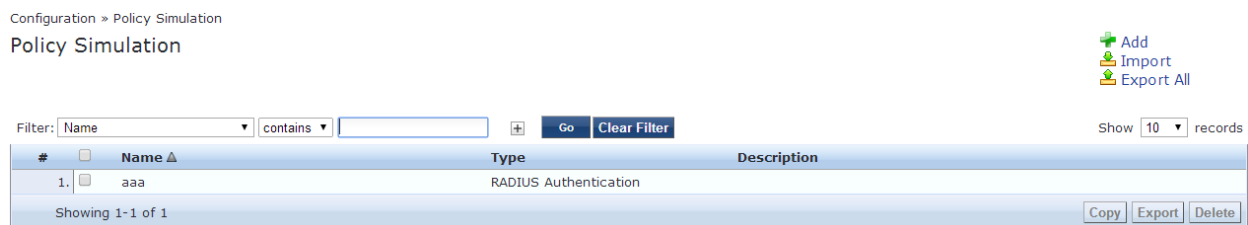
- [Active Directory Authentication Simulation](#)
- [Application Authentication Simulation](#)
- [Audit Simulation](#)
- [Chained Simulation](#)
- [Enforcement Policy Simulation](#)
- [RADIUS Authentication Simulation](#)
- [Role Mapping Simulation](#)
- [Service Categorization Simulation](#)

After creating the policies, use the **Policy Simulation** utility in the **Configuration > Policy Simulation** page to evaluate those policies before deployment.

The **Policy Simulation** utility applies a set of request parameters as input against a given policy component and displays the outcome.

The following figure displays the **Policy Simulation** page:

Figure 390: *Policy Simulation Page*



The following table describes the **Policy Simulation** page parameters:

Table 213: *Policy Simulation Configuration Parameters*

Parameter	Description
Name	Displays the name of the name of the policy simulation.
Type	Displays the type of the policy simulation.
Description	Displays additional information about the policy simulation.

Active Directory Authentication Simulation

This section provides the following information:

- [Adding an Active Directory Simulation](#)
- [Viewing the Simulation Results](#)

This simulation tests authentication against an Active Directory domain or trusted domain to verify that the W-ClearPass Policy Manager domain membership is valid.



The **Attributes** tab is not available for this simulation type.

Adding an Active Directory Simulation

To add the RADIUS authentication server for the authentication test:

1. Navigate to the **Configuration > Policy Simulation > Add** page.

The **Add Policy Simulation** dialog appears.

2. Enter the **Name** of the simulation.

3. From the **Type** drop-down list, select **Active Directory Authentication**.

The following figure displays the **Active Directory Authentication Simulation** dialog.

Figure 391: Active Directory Authentication - Simulation Tab

Configuration > Policy Simulation > Add
Policy Simulation

Simulation Results

Name:
Description:
Type:

Simulation Details

Test authentication against an Active Directory domain or trusted domain to verify that CPPM's domain membership is proper

Active Directory Domain:
Username:
Password:

The following table describes the **Active Directory Authentication - Simulation** tab parameters:

Table 214: Active Directory Authentication Simulation Tab Parameters

Parameter	Description
Active Directory Domain	Select the domain(s) to which the node is joined.
Username	Enter the username to login to the domain.
Password	Enter the password to login to the domain.

Viewing the Simulation Results

The **Results** tab for the **Active Directory Authentication** simulation displays a summary of the Authentication test and provides a status message.

The following figure displays the **Active Directory Authentication - Results** tab:

Figure 392: Active Directory Authentication Results Tab

Configuration > Policy Simulation > Add
Policy Simulation

Simulation **Results**

Summary -

Authentication	Active Directory Authentication successful

Status -

Status Message(s)	INFO - NT_STATUS_OK: Success (0x0)

Table 215: Active Directory Authentication Results Tab Parameters

Parameter	Description
Summary	Displays the results of the Active Directory Authentication simulation.
Status	Displays the status message.

Application Authentication Simulation

This simulation tests authentication requests generated from W-ClearPass Guest. The following figure displays the **Application Authentication** policy simulation settings available on the **Configuration > Policy Simulation > Add** page:

Simulation Tab

Figure 393: Application Authentication - Simulation Tab

The screenshot shows the 'Simulation' tab of the 'Application Authentication' policy configuration. It includes a 'Name' field, a 'Description' field, and a 'Type' dropdown menu set to 'Application Authentication'. Below this is a 'Simulation Details' section with a description: 'Test authentication requests generated from applications like ClearPass Guest and Workspace'. It contains three input fields: 'CPPM IP Address/FQDN' with the value '127.0.0.1', 'Username', and 'Password'.

Table 216: Application Authentication Simulation Tab Parameters

Parameter	Description
CPPM IP Address/FQDN	Enter the IP Address or FQDN of the domain(s) to which the node is joined.
Username	Enter the username.
Password	Enter the password.

Attributes Tab

Enter the attributes of the policy component to be tested. The following figure displays the **Application Authentication - Attributes** tab:

Figure 394: Application Authentication - Attributes Tab

The screenshot shows the 'Attributes' tab of the 'Application Authentication' policy configuration. It displays a table with the following data:

Type	Name	Value
1. Application	Name	= Enter App Name
2. Click to add...		

Table 217: *Application Authentication - Attributes Tab Parameters*

Attribute	Parameter
Type	Select Application or select Application:ClearPass. See Application Namespace on page 846
Name	The options displayed for the Name Attribute depend on the Type Attribute that was selected.
Value	The options displayed for the Value Attribute depend on the Type Attribute and Name Attribute that were selected.

Results tab

The Results tab of the Application Authentication simulation displays the outcome of the **Authentication Result** and the **Application Authentication Output Attributes**. The following figure displays the **Application Authentication Results** tab:

Figure 395: *Application Authentication Results Tab*

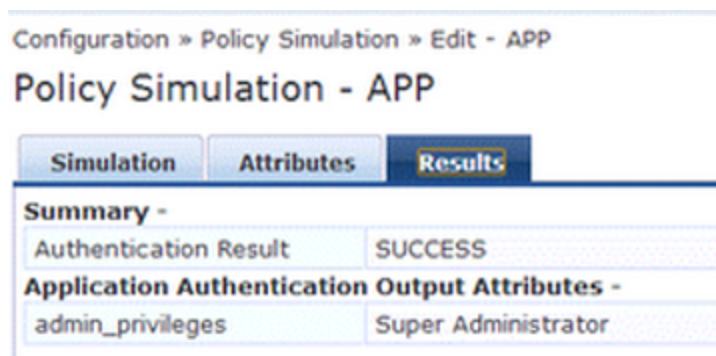


Table 218: *Application Authentication Results Tab Parameters*

Parameter	Description
Summary	Displays the results of the Active Directory Authentication simulation.
Application Authentication Output Attributes	Displays the output attributes, such as Super Administrator.

Audit Simulation

This simulation allows you to specify an audit against a Nessus Server or Nmap Server with its IP address.

The **Attributes** tab is not available for this simulation type.



Audit simulations can take more than 30 minutes. An *AuditInProgress* status message is displayed until the audit is completed.

The following figure displays the **Audit Simulation** tab:

Figure 396: *Audit Simulation - Simulation Tab*

Policy Simulation

Simulation **Results**

Name:

Description:

Type:

Simulation Details

Test Network Audit against specified Audit Server for a host machine, given its IP address

Audit Server:

Audit Host IP Address:

The following table describes the **Audit Simulation - Simulation** tab parameters:

Table 219: *Audit Simulation Tab Parameters*

Parameter	Description
Audit Server	Select [Nessus Server] or [Nmap Audit].
Audit Host IP Address	Enter the host IP address of the audit host.

Results Tab

The following figure displays the **Audit Simulation - Results** tab:

Figure 397: *Audit Simulation Results Tab*

Configuration » Policy Simulation » Edit - audit

Policy Simulation - audit

Simulation **Results**

Summary -

Audit Status	AuditInProgress
Temporary Status	TRANSITION (15)
Audit Timeout	60 seconds

Audit Output Attributes -

Avenda:Audit:Audit-Status	AUDIT_INPROGRESS

The following table describes the **Audit Simulation - Results** tab parameters:

Table 220: *Audit Results Tab Parameters*

Parameter	Description
Summary	Displays information about the Audit Status, Temporary Status, and Audit Timeout.
Audit Output Attributes	Displays the Audit-Status such as AUDIT_INPROGRESS.

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.

Simulation Tab

The following figure displays the **Chained Simulation Simulation** tab:

Figure 398: *Chained Simulation Tab*

Policy Simulation

Simulation | Attributes | Results

Name:

Description:

Type:

Simulation Details

Test end-to-end policy evaluation that includes Role-Mapping and Enforcement policies given a Service and input details

Service:

Authentication Source:

Username:

Test Date and Time:

The following table describes the **Chained Simulation - Results** tab parameters:

Table 221: *Chained Simulation Tab Parameters*

Parameters	Description
Service	Select from: • [Policy Manager Admin Network Login Service] • [AirGroup Authorization Service] • [Aruba Device Access Service] • [Guest Operator Logins] • Guest Access • Guest Access With MAC Caching
Authentication Source	Default Value = [Local User Repository] if you select: • [Policy Manager Admin Network Login Service] • [Aruba Device Access Service] Default Value = [Guest Device Repository] if you select: • [AirGroup Authorization Service] • Guest Access • Guest Access With MAC Caching Values = [Guest Device Repository] or [Local User Repository] if you select [Guest Operator Logins]
Username	Enter the username.
Test Date and Time	Click the calendar icon to select a start date and time for simulation test. For more information, see Date Namespaces on page 852

Attributes Tab

Enter the attributes of the policy component to be tested.

Figure 399: *Chained Simulation Attributes Tab*

Policy Simulation

Simulation **Attributes** Results

Type	Name	Value
1. Cisco:HIPS	CSAOperationalState	
2. Click to add...		

The following table describes the **Chained Simulation Attributes - Results** tab parameters:

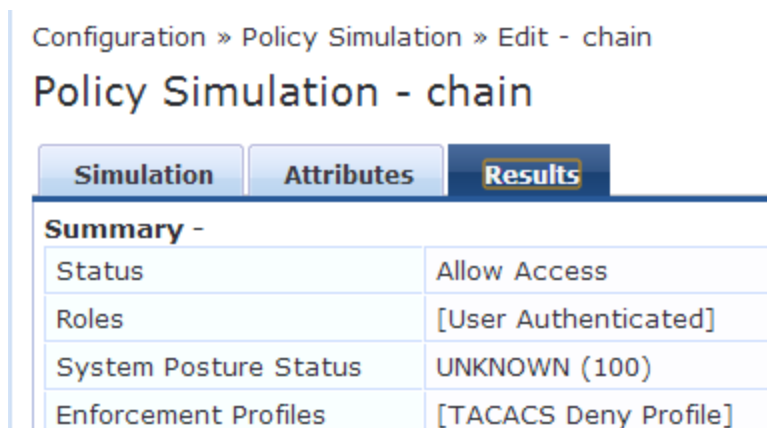
Table 222: *Chained Simulation Attributes tab Parameters*

Attribute	Parameter
Type	Select the type of attributes from the drop-down list.
Host	See Host Namespaces on page 853
Authentication	See Authentication Namespaces on page 847
Connection	See Connection Namespaces on page 851
Application	See Application Namespace on page 846
Certificate	See Certificate Namespaces on page 850
• Radius:IETF • Radius:Cisco • Radius:Microsoft • Radius:Avenda • Radius:Aruba • Trend:AV • Cisco: HIPS • Cisco:HOST • Cisco:PA • NAI:AV • Symantec:AV	See RADIUS Namespaces on page 854
Name	The options displayed for the Name attribute depend on the Type attribute that was selected.
Value	The options displayed for the Value attribute depend on the Type and Name attributes that were selected.

Results Tab

The following figure displays the **Chained Simulation - Results** tab:

Figure 400: Chained Simulation Results Tab



The screenshot shows the 'Policy Simulation - chain' interface with three tabs: 'Simulation', 'Attributes', and 'Results'. The 'Results' tab is active, displaying a 'Summary -' table with the following data:

Summary -	
Status	Allow Access
Roles	[User Authenticated]
System Posture Status	UNKNOWN (100)
Enforcement Profiles	[TACACS Deny Profile]

Table 223: Chained Simulation Results Tab Parameters

Parameter	Description
Summary	Provides the following information about the chained simulation: • Status • Roles • System Posture Status • Enforcement Profiles

Enforcement Policy Simulation

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.

Authentication Source and User Name inputs are used to derive dynamic values in the enforcement profile that are retrieved from the authorization source. These inputs are optional.

Dynamic roles are attributes that are enabled as a role retrieved from the authorization source. For an example of enabling attributes as a role, see [Generic LDAP and Active Directory on page 194](#).

Simulation Tab

The following figure displays the **Enforcement Policy Simulation** tab:

Figure 401: *Enforcement Policy Simulation Tab*

Policy Simulation

Simulation **Attributes** **Results**

Name:

Description:

Type:

Simulation Details

Test Enforcement policy rules to determine which Enforcement Profiles will be output given the input details

Service:

Enforcement Policy:

Authentication Source:

Username:

Roles:

Dynamic Roles:

System Posture Status:

Test Date and Time:

The following table describes the **Enforcement Policy Simulation** tab parameters:

Table 224: *Enforcement Policy Simulation tab Parameters*

Parameter	Description
Service	Select from: • [Policy Manager Admin Network Login Service] • [AirGroup Authorization Service] • [Aruba Device Access Service] • [Guest Operator Logins] • Guest Access • Guest Access With MAC Caching
Enforcement Policy	• Autofilled with [Admin Network Login Policy] if you select [Policy Manager Admin Network Login Service] • Autofilled with [AirGroup Enforcement Policy] if you select [AirGroup Authorization Service] • Autofilled with [Aruba Device Access Policy] if you select [Aruba Device Access Service] • Autofilled with [Guest Operator Logins] if you select [Guest Operator Logins] service • Autofilled with Copy_of_Guest Access Policy if you select Guest Access service • Autofilled with Guest Access With MAC Caching Policy if you select Guest Access With MAC Caching
Authentication Source	Value = [Local User Repository] if you select: • [Policy Manager Admin Network Login Service] • [Aruba Device Access Service] Value = [Guest Device Repository] if you select: • [AirGroup Authorization Service] • Guest Access • Guest Access With MAC Caching

Table 224: *Enforcement Policy Simulation tab Parameters (Continued)*

Parameter	Description
	Values = [Local User Repository] or [Guest Device Repository] if you select Guest Operator Logins
Username	Enter username.
Roles	Select from: • [Machine Authenticated] • [User Authenticated] • [Guest] • [TACACS Read-only Admin] • [TACACS API Admin] • [TACACS Help Desk] • [TACACS Receptionist] • [TACACS Network Admin] • [TACACS Super Admin] • [Contractor] • [Other] • [Employee] • [MAC Caching] • [Onboard Android] • [Onboard Windows] • [Onboard Mac OS X] • Onboard iOS] • [Aruba TACACS root Admin] • [Aruba TACACS read-only Admin] • [Device Registration] • [BYOD Operator] • [AirGroup V1] • [AirGroup v2]
Dynamic Roles	Add Role: Enter the name of a dynamic role in the Add Role field and click the Add Role button to populate the Dynamic Roles list. Remove role: Highlight a dynamic role and click Remove Role button.
System Posture Status	Select from: • HEALTHY (0) • CHECKUP (10) • TRANSITION (15) • QUARANTINE (20) • INFECTED (30) • UNKNOWN (100) See Posture Namespaces on page 854
Test Date and Time	Click calendar icon to select start date and time for simulation test. See Date Namespaces on page 852

Attributes tab

Enter the attributes of the policy component to be tested. The following figure displays the **Enforcement Policy - Attributes** tab:

Figure 402: *Enforcement Policy Attributes Tab*

Policy Simulation

Simulation Attributes Results

Type	Name	Value
1. Radius:Microsoft	MS-BAP-Usage	= Allowed (1)
2. Click to add...		

Table 225: *Enforcement Policy Attributes tab Parameters*

Attribute	Description
Type:	Select the type of attributes from the drop-down list.
Host	See Host Namespaces on page 853
Authentication	See Authentication Namespaces on page 847
Connection	See Connection Namespaces on page 851
Application	See Application Namespace on page 846
- Radius:IETF - Radius:Cisco - Radius:Microsoft - Radius:Avenda - Radius:Aruba	See RADIUS Namespaces on page 854
Name	The options displayed for the Name attribute depend on the Type attribute that was selected.
Value	The options displayed for the Value attribute depend on the Type and Name attributes that were selected.

Results Tab

The following figure displays the **Enforcement Policy - Results** tab:

Figure 403: *Policy Simulation Results Tab*

Configuration » Policy Simulation » Add

Policy Simulation

Simulation Attributes Results

Summary -	
Deny Access	false
Enforcement Profiles	[TACACS Deny Profile]

Table 226: *Enforcement Policy Results Tab Parameters*

Parameter	Description
Deny Access	Displays the output of the Deny Access test.
Enforcement Profile	Displays the name of the Enforcement Profile.

RADIUS Authentication Simulation

This section provides the following information:

- [Adding a RADIUS Authentication Simulation](#)
- [Setting the Attributes to Be Tested](#)
- [Viewing the Simulation Results](#)

Dictionaries in the RADIUS namespace come prepackaged with the W-ClearPass Policy Manager. The administration interface does provide a way to add dictionaries into the system (see [RADIUS Dictionary on page 637](#) for more information).

The RADIUS namespace uses the notation `RADIUS:Vendor`, where *Vendor* is the name of the company that has defined attributes in the dictionary. The same vendor can have multiple dictionaries, in which case the "Vendor" portion includes a suffix or some other unique string by the name of the device to differentiate the dictionaries.

Adding a RADIUS Authentication Simulation

To add the RADIUS authentication server for the authentication test:

1. Navigate to the **Configuration > Policy Simulation > Add** page.
The **Add Policy Simulation** dialog opens.
2. Enter the **Name** of the simulation.
3. From the **Type** drop-down list, select **RADIUS Authentication**.

[Figure 404](#) displays the **RADIUS Authentication Simulation Details** dialog, with the **Server** parameter set to **Remote**.

Figure 404: RADIUS Authentication Simulation Details Dialog

Configuration » Policy Simulation » Add

Policy Simulation

Simulation	Attributes	Results
Name:	RADIUS Authentication Simulation	
Description:		
Type:	RADIUS Authentication	
Simulation Details		
Test RADIUS authentication request processing against CPPM		
Server:	Remote	
CPPM IP Address/FQDN		
Port	admin	
Shared Secret	Shared secret between the target CPPM and this node. This node has to be added as a Network Device on the target CPPM	
NAS IP Address (optional):	IP address of the Network Device to populate the NAS-IP-Address attribute in RADIUS request. Note that his setting may have side effects such as a RADIUS CoA being fired to this Network Device 	
NAS Type:	Type of Network Device to simulate in terms of RADIUS attributes in the request Generic	
Authentication outer method:	PAP	
Authentication inner method:		
Client MAC Address (optional):	Client MAC address to be populated in the request. Note that this setting may have side effects such as the device getting blacklisted, etc. 	
Username		
Password		

- Enter the values for each of the **RADIUS Simulation** parameters as described in [Table 227](#).

Table 227: RADIUS Simulation Tab Parameters

Parameter	Action/Description
Server	1. Specify Local or Remote .
CPPM IP Address or FQDN	This field is displayed only if Remote Server is selected. 2. Enter the IP address or the fully qualified domain name (FQDN) of the remote W-ClearPass Policy Manager server.
Shared Secret	Displayed only if Remote Server is selected. 3. Enter the shared secret between the target W-ClearPass server and this node. You must add the node as a Network Device on the target W-ClearPass server. (For details, see Adding a Network Device on page 430).
NAS IP Address (optional)	4. To populate the NAS-IP-Address attribute in a RADIUS request, enter the IP address of the network device.
NAS Type	5. Select the type of network device to simulate in terms of RADIUS attributes in the request. The NAS types are: ■ Dell Wireless Controller ■ Dell Wired Switch ■ Cisco Wireless Controller ■ Generic

Table 227: RADIUS Simulation Tab Parameters (Continued)

Parameter	Action/Description
Authentication outer method	6. Specify one of the following authentication outer methods: • PAP • CHAP • MSCHAPv2 • PEAP: Authentication inner method: <i>enabled</i>. Select one of the following PEAP Authentication inner methods: ■ EAP-MSCHAPv2 ■ EAP-GTC ■ EAP-TLS • TTLS: Authentication inner method field: <i>enabled</i>. Select one of the following TTLS Authentication inner methods: ■ PAP ■ CHAP ■ MSCHAPv2 ■ EAP-MSCHAPv2 ■ EAP-GTC ■ EAP-TLS • TLS
Client MAC Address (optional)	7. Enter the client MAC address of the network device to populate the NAS-IP address attribute in the RADIUS request.
Username	8. Enter the user name.
CA Certificate (optional)	This is the optional Root CA certificate needed to verify the RADIUS server's certificate. 9. Click Browse and navigate to the optional Root CA certificate. Click Open, then click Upload.
Client Certificate PKCS12 (PFX)*	This is the client certificate that is used for TLS in PKCS12 (Public-Key Cryptography Standards). Formats: .pfx or .p12 10. Click Browse and navigate to the Client Certificate PKCS12. Click Open, then click Upload.
Passphrase for PFX file*	11. Enter the pass phrase for the selected PFX file.
* These fields are displayed only if you select TTLS or PEAP as the authentication outer method <i>and</i> you select EAP-TLS as the authentication inner method.	
	12. Click Save , or click Next to proceed to the Attributes tab.

Setting the Attributes to Be Tested



The attributes that you can set depend on the NAS **Type** selected on the **Policy Simulation** page (see [Figure 404](#)).

To set the attributes to be tested:

1. From the **Attributes** tab, click **Click to add**.
The **Add Policy Simulation Attributes** dialog opens.
2. From the **Type** drop-down, select the attribute **Type**.

Figure 405: *Specifying Policy Simulation Attributes*

Configuration » Policy Simulation » Add

Policy Simulation

Type	Name	Value
1. Radius:IETF	Acct-Authentic	= RADIUS (1)
2. Radius:IETF		
Radius:Cisco		
Radius:Hewlett-Packard-Enterprise		
Radius:Alcatel-Lucent-Enterprise		
Radius:Microsoft		
Radius:Avenda		
Radius:Aruba		

3. Select the attribute **Name**.
4. Select the attribute **Value**.
5. Repeat these steps for each additional attribute you wish to add.
6. Click **Save**, or click **Next** to proceed to the **Results** tab.

NAS Type: Aruba Wireless Controller

Figure 406: *Aruba Wireless Controller Type - Attributes*

Configuration » Policy Simulation » Add

Policy Simulation

Simulation			
Attributes			
Results			
Type	Name	Value	
1. Radius:IETF	NAS-Port-Type	= Wireless-802.11 (19)	
2. Radius:IETF	Service-Type	= Login-User (1)	
3. Radius:Aruba	Aruba-Essid-Name	= SSID	

Table 228: *Dell Wireless Controller Required - Attribute Settings*

Attribute	Parameter
Line 1: - Type = Radius:IETF - Name = NAS-Port-Type - Value = Wireless-802.11 (19)	
Line 2: - Type = Radius:IETF - Name = Service-Type - Value = Login-User (1)	
Line 3: - Type = Radius:Aruba - Name = Dell-Essid-Name - Value = SSID	

NAS Type: Aruba Wired Switch Controller

Figure 407: NAS Type: Aruba Wired Switch Controller Attributes Tab

Configuration » Policy Simulation » Add

Policy Simulation

Simulation				Attributes		Results	
Type	Name	Value					
1. Radius:IETF	NAS-Port-Type	= Ethernet (15)					
2. Radius:IETF	Service-Type	= Login-User (1)					

Table 229: NAS Type: Aruba Wired Switch Controller—Required Attribute Settings

Attribute
Line 1: - Type = Radius:IETF - Name = NAS-Port-Type - Value = Ethernet (15)
Line 2: - Type = Radius:IETF - Name = Service-Type - Value = Login-User (1)

NAS Type: Cisco Wireless Switch

Figure 408: NAS Type: Cisco Wireless Switch Attributes

Configuration » Policy Simulation » Add

Policy Simulation

Simulation				Attributes		Results	
Type	Name	Value					
1. Radius:IETF	NAS-Port-Type	= Wireless-802.11 (19)					
2. Radius:IETF	Service-Type	= Framed-User (2)					

Table 230: NAS Type: Cisco Wireless Switch Required Attribute Settings

Attribute
Line 1: - Type = Radius:IETF - Name = NAS-Port-Type - Value = 802.11(19)
Line 2: - Type = Radius:IETF - Name = Service-Type - Value = Framed-User(2)

Viewing the Simulation Results

The following figure displays the **Policy Simulation RADIUS - Results** dialog:

Figure 409: Results Tab

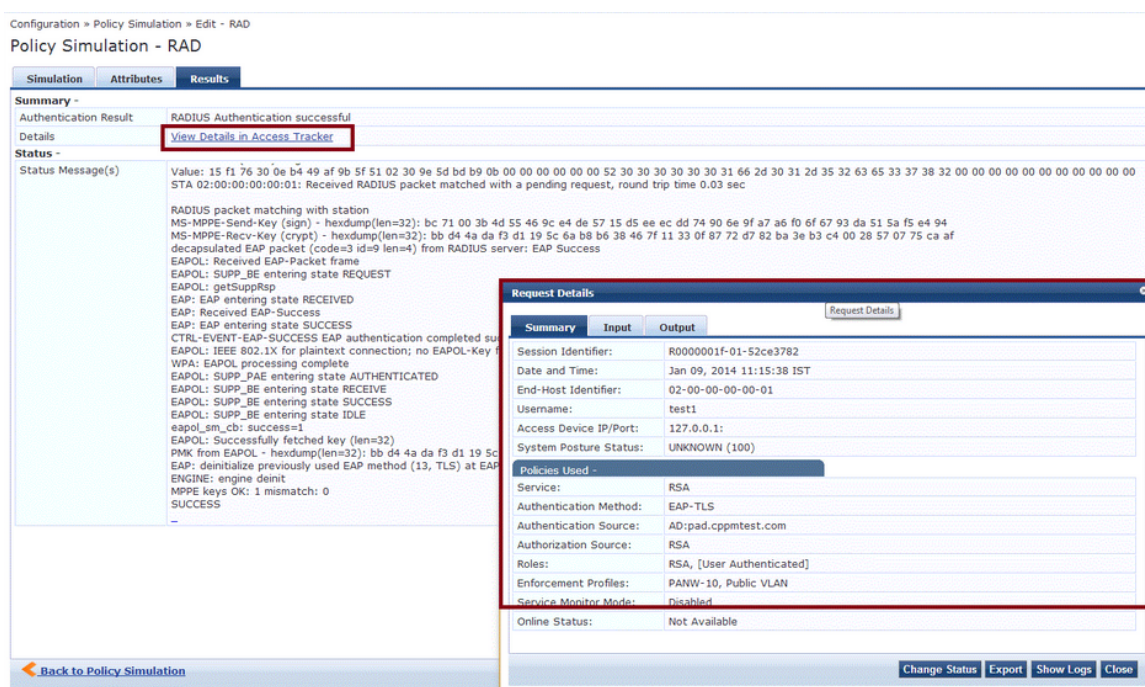


Table 231: RADIUS Authentication Results Tab Parameters

Parameter	Description
Summary	Displays a summary of the simulation.
Authentication Result	Displays the outcome of the Authentication test.
Details	Click this link to open a dialog that provides details about the Authentication test. You can take the following actions: - Click the Summary, Input, or Output tabs. - Click the Change Status, Show Logs, Export, or Close buttons.
Status Message(s)	Displays the status messages resulting from the test.

Role Mapping Simulation

The role mapping simulation tests Role-Mapping policy rules to determine which roles will be output, given the service name (and associated role mapping policy), the authentication source and the user name.

You can also use role mapping simulation to test whether the specified authentication source is reachable.

Simulation Tab

The following figure displays the **Role Mapping Simulation** tab:

Figure 410: Role Mapping Simulation Tab

Policy Simulation

Simulation **Attributes** **Results**

Name:

Description:

Type:

Simulation Details

Test Role-Mapping policy rules to determine which Roles will be output given the input details

Service:

Role Mapping Policy:

Authentication Source:

Username:

Test Date and Time: 

Table 232: Role Mapping Simulation Tab Parameters

Parameter	Description
Service	Select from: • [Policy Manager Admin Network Login Service] • [AirGroup Authorization Service] • [Aruba Device Access Service] • [Guest Operator Logins] • Guest Access • Guest Access With MAC Caching
Role Mapping Policy	Field is disabled if you select: • [Policy Manager Admin Network Login Service] • [Aruba Device Access Service] • [Guest Operator Logins] • Field is auto-filled with [AirGroup Version Match] if you select [AirGroup Authorization Service] • Field is autofilled with [Guest Roles] if you select Guest Access • Field is autofilled with Guest MAC Authentication Role Mapping if you select Guest Access With MAC Caching
Authentication Source	Value = [Local User Repository] if you select: • [Policy Manager Admin Network Login Service] • [Aruba Device Access Service] Value = [Guest Device Repository] if you select: • [AirGroup Authorization Service] • Guest Access • Guest Access With MAC Caching Values = [Guest Device Repository] or [Local User Repository] if you select [Guest Operator Logins]
Username	Enter the user name.
Test Date and Time	Click calendar icon to select start date and time for simulation test. For more information, see Date Namespaces on page 852

Attributes Tab

Enter the attributes of the policy component to be tested. The following figure displays the **Role Mapping Simulation Attributes** tab:

Figure 411: *Role Mapping Simulation Attributes Tab*

Policy Simulation

Simulation Attributes Results

Type	Name	Value
1. Radius:IETF	ARAP-Security-Data	
2. Click to add...		

The following table describes the **Role Mapping Simulation Attributes** tab parameters:

Table 233: *Role Mapping Simulation Attributes Tab Parameters*

Attribute	Parameter
Type	Select the type of attributes from the drop-down list.
Host	See Host Namespaces on page 853
Authentication	See Authentication Namespaces on page 847
Connection	See Connection Namespaces on page 851
Application	See Application Namespace on page 846
Certificate	See Certificate Namespaces on page 850
- Radius:IETF - Radius:Cisco - Radius:Microsoft - Radius:Avenda - Radius:Aruba	See RADIUS Namespaces on page 854
Name	The options displayed for the Name attribute depend on the Type attribute that was selected.
Value	The options displayed for the Value attribute depend on the Type and Name attributes that were selected.

Results Tab

The following figure displays the **Role Mapping Simulation - Results** tab:

Figure 412: *Results Tab*

Configuration » Policy Simulation » Edit - test2

Policy Simulation - test2

Simulation Attributes Results

Summary -

Roles	[User Authenticated]

The following table describes the **Role Mapping Simulation - Results** tab parameters:

Table 234: *Role Mapping Results Tab Parameters*

Parameter	Description
Summary	Displays the results of the simulation.

Service Categorization Simulation

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.

Simulation Tab

The following figure displays the **Service Categorization Simulation - Simulation** tab:

Figure 413: *Service Categorization Simulation Tab*

Policy Simulation

Simulation Attributes Results

Name:

Description:

Type:

Simulation Details

Test Service classification rules to determine which Service will match given the input details

Test Date and Time:

Table 235: *Service Categorization Simulation Tab Parameters*

Parameter Type	Namespace Details
Test Date and Time	Click calendar widget and select: - Test start date - Test start time

Attributes Tab

Enter the attributes of the policy component to be tested. The following figure displays the **Service Categorization Simulation - Attributes** tab:

Figure 414: *Service Categorization Attributes Tab*

Policy Simulation

Simulation Attributes Results

Type	Name	Value
1. Connection	Protocol	= RADIUS
2. Authentication	Posture	= Capable
3. Click to add...		

Table 236: *Service Categorization Simulation Attributes Tab Parameters*

Attribute	Parameter
Type	Select the type of attributes from the drop-down list.
Host	See Host Namespaces on page 853
Authentication	See Authentication Namespaces on page 847
Connection	See Connection Namespaces on page 851
Application	See Application Namespace on page 846
• Radius:IETF • Radius:Cisco • Radius:Microsoft • Radius:Aruba	See RADIUS Namespaces on page 854
Name	The options displayed for the Name attribute depend on the Type attribute that was selected.
Value	The options displayed for the Value attribute depend on the Type and Name attributes that were selected.

Results Tab

The following figure displays the **Service Categorization - Results** tab:

Figure 415: *Results Tab*

Policy Simulation - service_cat

Simulation		Attributes		Results	
Summary -					
Service Name					
Status -					
Status Message(s)		No service found for request parameters			

The following table describes the **Service Categorization Simulation Results** tab parameters:

Table 237: *Service Configuration Results Tab Parameters*

Parameter	Description
Summary	Gives the name of the service.

Import and Export Simulations

Navigate to **Configuration > Policy Simulation** and select the **Import** link. The following figure shows an example of the **Import from file** page.

Figure 416: *Import Simulations*

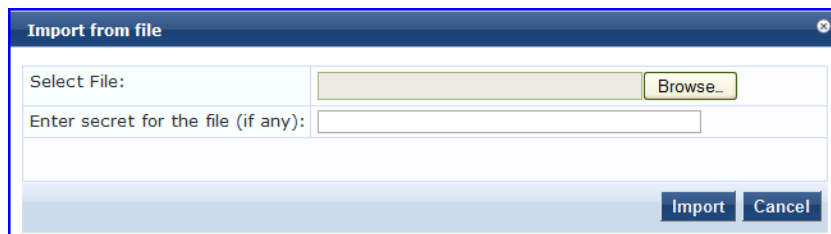


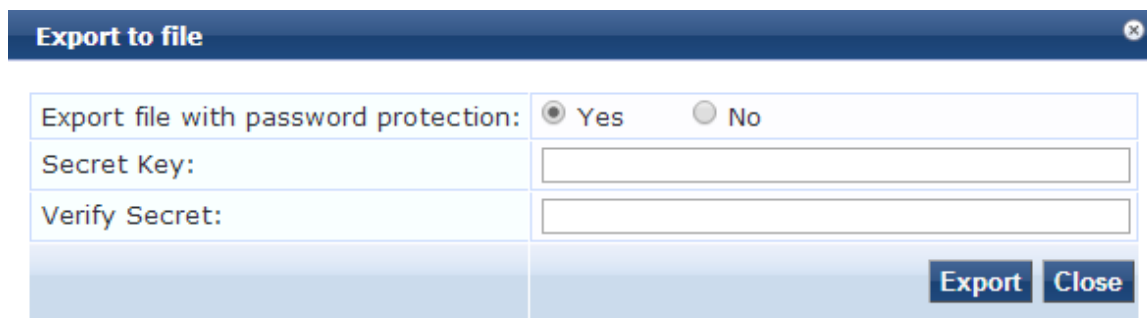
Table 238: *Import from file page Parameters*

Parameter	Description
Select file	Browse to select name of simulations to import.
Enter secret for the file (if any)	If the file was exported with a secret key for encryption, enter the same key here.

Export Simulations

Click the **Export All** link to export all simulations. The browser displays the **Save As** dialog box in which you can enter the name of the XML file to export all simulations. The following image shows an example of the **Export** page to file page.

Figure 417: *Export Simulations*



To export a specific simulation, click **Export**. In the **Save As** dialog box, enter the name of the XML file to contain the export data.

Table 239: *Export Simulations*

Parameter	Description
Export file with password protection	Select Yes to export the file with password protection.
Secret Key	Enter the secret key in this field.
Verify Secret	Enter the same secret key to confirm and complete export.

This chapter contains the following information:

- [W-ClearPass Profile Overview](#)
- [About the Device Profile](#)
- [Endpoint Information Collectors](#)

W-ClearPass Profile Overview

This section contains the following information:

- [Introduction](#)
- [Enabling Endpoint Classification](#)
- [Configuring CoA for an Endpoint-Connected Device](#)
- [How W-ClearPass Profile Classifies Endpoints](#)
- [Fingerprint Dictionaries](#)
- [Viewing Live Endpoint Information for a Specific Device](#)

Introduction

W-ClearPass Profile is a W-ClearPass Policy Manager module that automatically classifies endpoints using attributes obtained from software components called *Collectors*.

W-ClearPass Profile associates an endpoint with a specific user or location and offers an efficient and accurate way to differentiate access by endpoint type (for example, laptop or tablet).

Profiling allows you to gather device type and operating system information by inspecting packets that are sent by these devices in the network. For example, you can identify that a device is a smart device, a laptop, or a printer or IP phone.

You can use this information to implement Bring Your Own Device (BYOD) flows during enforcement, assigning the appropriate privileges and access to users based on their device type and the identity of the user.

Enabling Endpoint Classification

When you enable W-ClearPass Profile on a W-ClearPass server, you enable the server for endpoint classification. This associates each endpoint with a specific user or location and secures access for devices.

To enable W-ClearPass Profile:

1. Navigate to **Administration > Server Manager > Server Configuration**.
The Server Configuration page appears.
2. Select the W-ClearPass node in the zone that you want to designate as a Profiler.
The **System** tab for the **Server Configuration** page appears.

Figure 418: Enable Profile Option

System	Services Control	Service Parameters	System Monitoring	Network	FIPS
Hostname:		VM-204			
FQDN:					
Policy Manager Zone:		default		Manage Policy Manager Zones	
Enable Profile:		☒ Enable this server for endpoint classification			
Enable Performance Monitoring Display:		☒ Enable this server for performance monitoring display			
Insight Setting:		☐ Enable Insight			
Enable Ingress Events Processing:		☐ Enable Ingress Events processing on this server			
Span Port:		-- None --			
		IPv4	IPv6	Action	

3. If it is not already enabled, select the **Enable this server for endpoint classification** check box, then click **Save**.

Configuring CoA for an Endpoint-Connected Device

After profiling an endpoint, use the **Profiler** page to configure Change of Authorization (CoA) on the network device to which an endpoint is connected.

The **Profiler** tab is not displayed by default. To access the **Profiler** tab:

1. Navigate to **Configuration > Services**, then click **Add**.
2. Enter the name of the service.
3. From the **More Options** field on the **Service** tab, enable the **Profile Endpoints** check box .

The **Profiler** tab is added to the **Services** tabs:

Figure 419: Adding the Profiler Page

Configuration » Services » Add

Services

Service	Authentication	Roles	Enforcement	Profiler	Summary
Type:	MAC Authentication				
Name:					
Description:	MAC-based Authentication Service				
Monitor Mode:	☐ Enable to monitor network access without enforcement				
More Options:	☐ Authorization ☐ Audit End-hosts ☒ Profile Endpoints ☐ Accounting Proxy				
Service Rule					
Matches ☐ ANY or ☒ ALL of the following conditions:					
Type	Name	Operator	Value		
1. Radius:IETF	NAS-Port-Type	BELONGS_TO	Ethernet (15), Wireless-802.11 (19)		

4. Select the **Profiler** tab.
The **Profiler** page appears.

Figure 420: Profiler Page

Service Authentication Roles Enforcement **Profiler** Summary

Endpoint Classification: Select the classification(s) after which an action must be triggered -

SmartDevice
Home Audio/Video Equipment
Projectors
-- Select --

Remove

RADIUS CoA Action: [Aruba Terminate Session] View Details Modify Add new RADIUS CoA Action

Back to Services Next > Save Cancel

5. You can select a set of categories and a CoA profile to be applied when the profile matches one of the selected categories.

CoA is triggered using the selected CoA profile. You can use any option from Endpoint Classification to invoke CoA on a change of any one of the fields (category, family, and name).

Table 240 describes the **Profiler** page parameters:

Table 240: Profiler Page Parameters

Parameter	Action/Description
Endpoint Classification	1. Select one or more endpoint classification items from the drop-down list. You can select a new action, or remove a current action.
RADIUS CoA Action	2. Select the RADIUS CoA action from the drop-down list. 3. To view the Policy Manager Entity Details page with the summary of enforcement profile details, click View Details . 4. To view the Summary tab with profile details, click Modify .
Add new RADIUS CoA Action	5. To create a new RADIUS CoA action, click the Add New RADIUS CoA Action link.

6. When finished, click **Save**.

How W-ClearPass Profile Classifies Endpoints

The W-ClearPass Profile module uses a two-stage approach to classify endpoints using input attributes.

Stage 1: Deriving Device Profiles

During Stage 1, W-ClearPass Profile derives device profiles using static dictionary lookups. Based on the available attributes available, Stage 1 looks up DHCP, HTTP, ActiveSync, MAC OUI, and SNMP dictionaries and derives multiple matching profiles.

After multiple matches are returned, the priority of the source that provided the attribute is used to select the appropriate profile.

The following list shows the profile order of priority, from highest priority to lowest:

- a. OnGuard/ActiveSync plugin
- b. HTTP User-Agent
- c. SNMP

- d. DHCP
- e. MAC OUI

Stage 2: Refining Results

W-ClearPass Policy Manager includes a set of rules that evaluates a device profile. The Rules engine uses all input attributes and device profiles from Stage 1. The resulting rule evaluation may or may not result in a profile. Stage 2 refines the results of profiling.

Example

With DHCP options, Stage 1 can identify an Android device. Stage 2 uses rules to combine this with the MAC OUI to further classify an Android device as Samsung Android and HTC Android.

Fingerprint Dictionaries

W-ClearPass Policy Manager uses a set of dictionaries and rules to perform device fingerprinting.

Because these dictionaries can change frequently, W-ClearPass Policy Manager provides a way to automatically update fingerprints from a hosted portal. The device fingerprints are updated from the Dell W-ClearPass Update Portal (for more information, see [Updating Policy Manager Software on page 646](#)).

To view the contents of the fingerprints dictionary:

1. Navigate to **Administration > Dictionaries > Fingerprints**.

The **Device Fingerprints** page appears. This page lists all the device fingerprints recognized by the Profile module.

Figure 421: Device Fingerprints Page

Administration » Dictionaries » Fingerprints

Device Fingerprints

Filter: contains Show records

#	Category ▲	Family	Name
1.	Access Points	Symbol	Symbol AP
2.	Access Points	Motorola	Motorola AP
3.	Access Points	Cisco	Cisco AP
4.	Access Points	Trendnet	Trendnet AP
5.	Access Points	Enterasys	Enterasys HiPath AP
6.	Access Points	Trapeze	Trapeze AP
7.	Access Points	AeroHive	AeroHive AP
8.	Access Points	Ruckus	Ruckus Wireless
9.	Access Points	Aruba	Aruba RAP
10.	Access Points	Aruba	Aruba AP

Showing 1-10 of 319

2. To view the device fingerprint dictionary attributes, select the device fingerprint of interest.
The attributes for the selected Device Fingerprint Dictionary are displayed:

Figure 422: *Device Fingerprint Dictionary Attributes Page*

Device Fingerprint Dictionary Attributes

Category:

Access Points

Family:

Symbol

Name:

Symbol AP

#	Field	Value
1.	DHCP Option55	[1,3,6,12,15,43,66,67,128,129,130,131,132,133,134,135]
2.	DHCP Option60	[S24AP]
3.	Nmap Device Type	[[Symbol, WAP]]

Close

- To exit, click **Close**.

Viewing Live Endpoint Information for a Specific Device

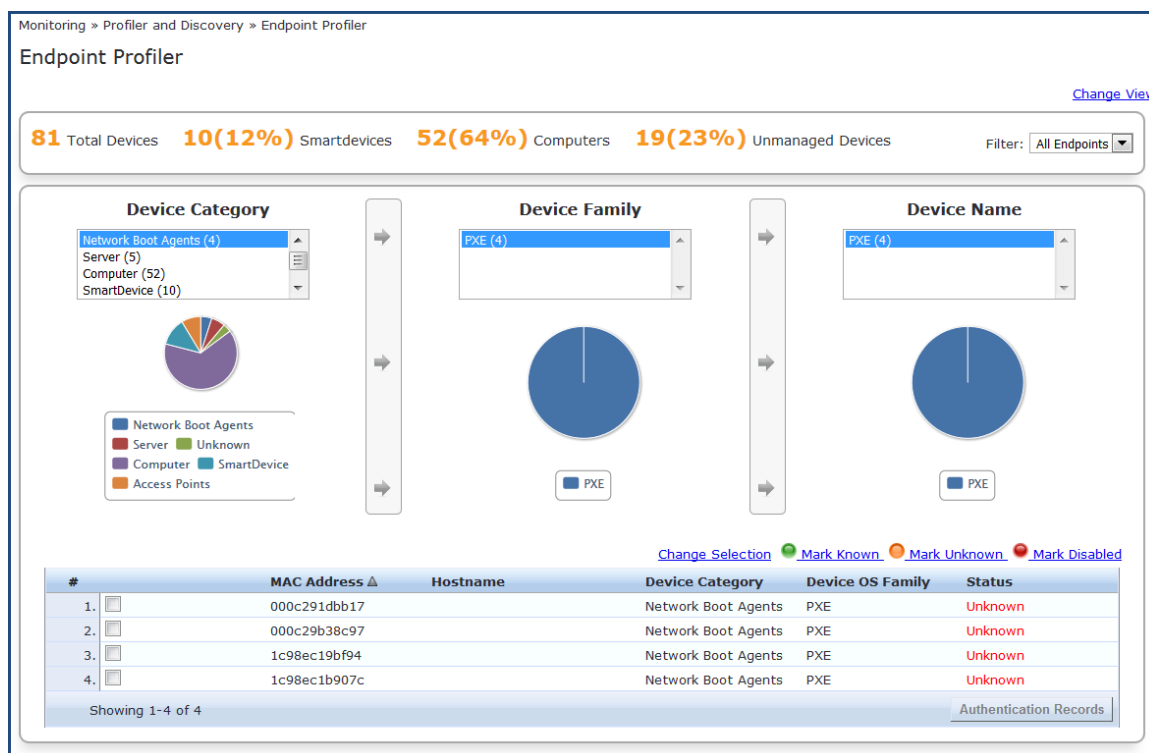
The W-ClearPass Live Monitoring feature allows you to view endpoint information in graphic format for the device category, device family, and device name items you selected. You can also examine the endpoint details and attributes about a specific device .

To access the Endpoint Profiler Live Monitoring information:

- Navigate to **Monitoring > Profile and Discovery > Endpoint Profiler**.

The Endpoint Profiler appears.

Figure 423: *Endpoint Profiler*



- To view endpoint details about a specific device, click a device in the table below the graphs.

3. To return to the **Endpoint Profiler** page, click **Cancel**.

For more information, see:

- [Profiler and Discovery: Endpoint Profiler on page 139](#)

The Cluster Status Dashboard widget shows basic distribution of device types. For more information, see:

- [Using the W-Policy Manager Dashboard on page 26](#)

About the Device Profile

A device profile is a hierarchical model consisting of three elements that are derived by the endpoint attributes—*DeviceCategory*, *DeviceFamily*, and *DeviceName*.

Table 241: *Elements of a Device Profile*

Endpoint Attributes	Description
DeviceCategory	Denotes the type of the device, for example, Computer, Smart Device, Printer, or Access Point.
DeviceFamily	Classifies devices based on the type of operating system or vendor. For example, when the category is <i>Computer</i> , W-ClearPass Policy Manager shows a device family of Windows, Linux, or Mac OS X.
DeviceName	Denotes the name of the device. Devices in a family are organized based on characteristics such as their operating system version. For example, in a DeviceFamily of <i>Windows</i> , W-ClearPass Policy Manager shows a DeviceName of <i>Windows 8.1</i> or <i>Windows Server 2012</i> .

This hierarchical model provides a structured view of all endpoints accessing the network. In addition to these, a device profile also collects and stores the following:

- IP address
- Host name
- Device vendor (via MAC OUI)
- Timestamp indicating when the device was first discovered
- Timestamp indicating when the device was last seen

Endpoint Information Collectors

Collectors are the network elements that provide data in order to profile endpoints. This section contains the following information:

- [DHCP Collector](#)
- [W-ClearPass Onboard Collector](#)
- [HTTP User-Agent Strings Collector](#)
- [MAC OUI Collector](#)
- [ActiveSync Plug-in Collector](#)
- [W-ClearPass OnGuard Agent](#)
- [SNMP Collector](#)
- [Subnet Scan Collector](#)

- [SNMP Configuration for Wired Network Profiling](#)
- [Information Regarding SSH and WMI Configuration](#)

DHCP Collector

Dynamic Host Configuration Protocol (DHCP) attributes such as **option 55** (parameter request list), **option 60** (vendor class), and the options list from the Discover and Request packets can uniquely fingerprint most devices that use the DHCP mechanism to acquire an IP address on the network.

You can configure switches and controllers to forward DHCP Discover, Request, and Inform packets to W-ClearPass. These DHCP packets are decoded by W-ClearPass Policy Manager to arrive at the appropriate device category, family, and device name. In addition to fingerprints, DHCP also provides the host name and IP address.

Sending DHCP Traffic to the W-ClearPassServer

To configure your Dell mobility controller and Cisco switch to send DHCP traffic to the W-ClearPass server, enter the following CLI commands:

```
interface <vlan_name>
ip address <ip_addr> <netmask>
ip helper-address <dhcp_server_IO>
ip helper-address <clearpass_IP> end
end
```

You can configure multiple **ip helper-address** statements to send DHCP packets to servers other than the DHCP server.

W-ClearPass Onboard Collector

W-ClearPass Onboard collects authentic device information from all devices during the onboarding process. Onboard then posts this information to W-ClearPass Profile via the Profile API.

Because the information collected is definitive, W-ClearPass Profile can directly classify these devices into their category, family, and name without having to rely on any other fingerprinting information.

HTTP User-Agent Strings Collector

In some cases, DHCP fingerprinting alone cannot fully classify a device. A common example is the Apple family of smart devices; for example, DHCP fingerprints cannot distinguish between an iPad and an iPhone.

In these scenarios, user-agent strings sent by browsers in the HTTP protocol are useful to further refine classification results.

User-agent strings are collected from the following:

- W-ClearPass Guest
- W-ClearPass Onboard
- Dell mobility controller through an IF-MAP (Interface for Metadata Access Points) interface

MAC OUI Collector

The MAC OUI (Organization Unique Identifier) is expressed in the first 24 bits of a MAC address for a network-connected device. Thus, the MAC OUI indicates the specific vendor for that device. The MAC OUI is acquired through various authentication mechanisms, such as 802.1X and MAC authentication.

The MAC OUI can be useful in some cases to more accurately classify endpoints. An example is Android™ devices where DHCP fingerprints can only classify a device as generic Android, but it cannot provide more details regarding the vendor.

Combining this information with MAC OUI, the W-ClearPass Profiler can classify a device as HTC™ Android, Samsung™ Android, or Motorola® Android, etc.

The MAC OUI is also useful to profile devices such as printers that might be configured with static IP addresses.

ActiveSync Plug-in Collector

You can install the ActiveSync plug-in on Microsoft Exchange servers.

When a device communicates with an Exchange server using the Active Sync protocol, the device provides attributes such as device-type and user-agent.

These attributes are collected by the ActiveSync plug-in and sent to the W-ClearPass Profiler. Profiler uses dictionaries to derive profiles from these attributes.

W-ClearPass OnGuard Agent

The W-ClearPass OnGuard agent performs advanced endpoint posture assessment. This agent can collect and send operating system details from endpoints during authentication.

The W-Policy Manager Profiler uses the OnGuard **os_type** attribute to derive a profile.

SNMP Collector

Endpoint information obtained by reading the Simple Network Management Protocol (SNMP) MIBs of network devices is used to discover and profile static IP devices in the network. For related information, see [SNMP Configuration for Wired Network Profiling on page 426](#).

[Table 242](#) describes the MIBs used by the SNMP Collector.

Table 242: *SNMP MIBs Used by the SNMP Collector*

MIB	Description
SysDescr	A textual description of the entity used both for profiling switches, controllers, and routers configured in W-ClearPass, and for profiling printers and other static IP devices discovered through SNMP or subnet scans (RFC1213).
cdpCacheTable	Provides the cached information obtained via receiving CDP (Cisco Discovery Protocol) messages from CDP-capable devices. Used to discover neighbor devices connected to the switch or controller configured in W-ClearPass.
IldpRemTable	This table contains one or more rows per physical network connection known to this agent read from LLDP (Link Layer Discovery Protocol)-capable devices. Used to discover and profile neighbor devices connected to the switch or controller configured in W-ClearPass.
ARPtable	Address Resolution Protocol (ARP) information read from the network devices. Used as a means to discover endpoints in the network.

Setting SNMP Community Attributes

The SNMP-based mechanism is capable of profiling devices only if they respond to SNMP, or if the device advertises its capability via LLDP (Link Layer Discovery Protocol). When performing SNMP reads for a device, W-ClearPass uses SNMP Read credentials configured in Network Devices, or defaults to using SNMPv2 with "public" community strings specified.

To specify SNMPv2 with community strings:

1. Navigate to **Configuration > Network > Devices**.
2. From the Network Devices screen, select the appropriate device for configuration.
The **Edit Device Details** dialog appears.
3. Select the **SNMP Read Settings** tab.

Figure 424: Specifying SNMP v2 with Community Strings

The screenshot shows the 'Edit Device Details' dialog with the 'SNMP Read Settings' tab selected. The dialog contains the following fields and options:

- Device** (selected tab)
- SNMP Read Settings** (selected tab)
- SNMP Write Settings** (tab)
- CLI Settings** (tab)
- Allow SNMP Read:** ☒ Enable Policy Manager to perform SNMP read operations
- SNMP Read Setting:** SNMP v2 with community strings (dropdown menu)
- Community String:** [Redacted] **Verify:** [Redacted]
- Force Read:** ☒ Always read information from this device
- Read ARP Table Info:** ☒ Read ARP table from this device
- Buttons:** Copy, Save, Cancel

- a. If not already enabled, enable the **Allow SNMP Read** check box.
 - b. From the **SNMP Read Setting** drop-down, select **SNMPv2 with community strings**.
 - c. Enter the **Community String** value.
 - d. Enable the **Force Read** check box to ensure that all W-ClearPass nodes in the cluster read SNMP information from this device regardless of trap configuration on the device.
This option is especially useful when demonstrating static IP-based device profiling because the **Force Read** option does not require any trap configuration on the network device.
 - e. Enable the **Read ARP Table Info** check box if this is a Layer-3 device, and you want to use the ARP table on this device as a way to discover endpoints in the network.
Static IP endpoints discovered this way are further probed via SNMP to profile the device.
4. Click **Save**.

Configuring the Device Info Poll Interval

Network devices configured with **SNMP Read** enabled are polled periodically for updates based on the time interval configured in the **Device Info Poll Interval** (the default is 60 minutes).

To set this poll interval, navigate to **Administration > Server Configuration > Service Parameters > W-ClearPass network services > Device Info Poll Interval**.

Figure 425: Specifying the Device Info Poll Interval

Administration » Server Manager » Server Configuration - AV-CP65-VA500-1

Server Configuration - AV-CP65-VA500-1 (10.10.10.23)

The screenshot shows the 'Service Parameters' tab for 'ClearPass network services'. The interface includes a table with columns: Parameter Name, Parameter Value, Default Value, and Allowed Values. The 'Device Info Poll Interval' is highlighted in red.

Parameter Name	Parameter Value	Default Value	Allowed Values
DhcpSnooper			
MAC to IP Request Hold time	120 seconds	120	60-300
DHCP Request Probation Time	30 seconds	30	10-60
SnmpService			
SNMP Timeout	4 seconds	4	2-30
SNMP v3 Trap			1-5
SNMP v3 Trap Authentication Key			
SNMP v3 Trap Privacy Key			
Device Info Poll Interval	60 minutes	60	10-1500

5. In the **Minutes** field, enter the **Device Info Poll Interval**, then click **Save**.

Subnet Scan Collector

A network subnet scan discovers the IP addresses of devices in the network.

The devices discovered in this way are further probed using SNMP to fingerprint and assign a profile to the device. Network subnets to be scanned are configured per W-Policy Manager Zone.

This is particularly useful in deployments that are geographically distributed. In such deployments, it is recommended that you:

1. Assign the W-ClearPass Policy Manager nodes in a cluster to multiple zones depending on the geographical area served by that node.

To set up W-Policy Manager Zones, navigate to **Administration > Server Manager > Server Configuration > Manage Policy Manager Zones**.

2. Then enable the profile for a minimum of one node per zone.

For more information, see [Manage Policy Manager Zones on page 500](#).

Configuring Subnet Scans

To configure the subnet scans:

1. Navigate to the **Configuration > Profile Settings** page.

Figure 426: Profile Settings: Subnet Scans Dialog

Configuration » Profile Settings

Profile Settings

The following additional Profile techniques may be configured

Subnet Scans

Specify the IP subnets to be scanned for discovering hosts and their capabilities - [On-Demand Subnet Scan](#)

Policy Manager Zone	IP Subnet to Scan
1. Click to add...	

SNMP Configuration

Specify SNMP configuration used for querying hosts discovered by a Subnet Scan [Add SNMP configuration](#)

IP Subnet

2. In the **Subnet Scans** section, select a W-Policy Manager Zone by clicking **Click to add**.



If W-Policy Manager Zones have not yet been set up, you can select the **default** zone, which will allow you to proceed with the configuration procedure.

After you select the Policy Manager Zone, the **IP Subnet to Scan** text field appears.

3. In the **IP Subnet to Scan** text field, enter the IP addresses for the subnets you wish to scan, then click the **Save** icon (see [Figure 427](#)).

Figure 427: Specifying the Subnets to Be Scanned

Configuration » Profile Settings

Profile Settings

Subnet Scans **SNMP Configuration** **SSH Configuration** **WMI Configuration**

Specify the IP subnets to be scanned for discovering hosts and their capabilities -

Policy Manager Zone	IP Subnet to Scan
1. default	10.15.0.0/16
2. Click to add...	

Click the icon to save

You return to the Subnet Scans dialog where the IP subnets are listed in the IP Subnet to Scan text field (see [Figure 428](#)).

Initiating an On-Demand Subnet Scan

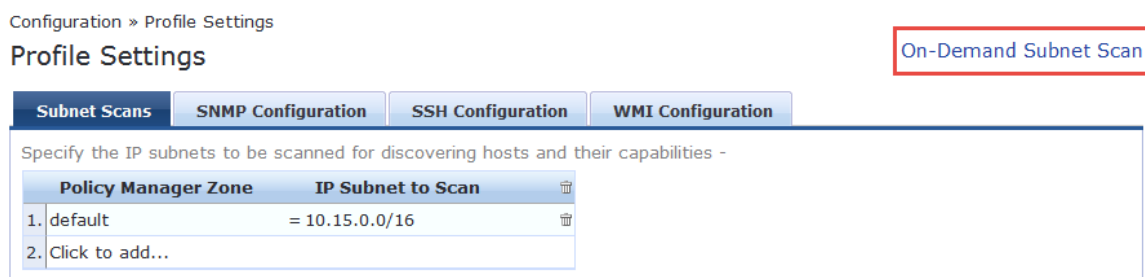
In cases in which you wish to initiate a subnet scan without saving the configuration, you can run an On-Demand Subnet Scan.

To run an On-Demand Subnet Scan:

1. Navigate to **Configuration > Profile Settings**.

The **Profile Settings** dialog appears.

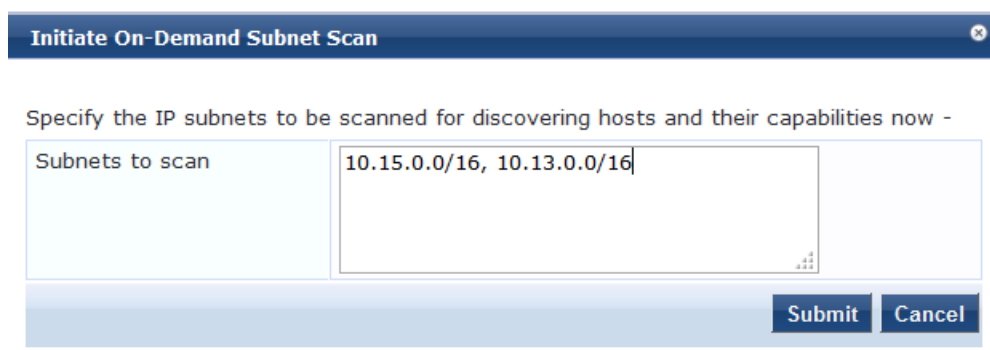
Figure 428: *Initiating an On-Demand Subnet Scan*



2. Click **On-Demand Subnet Scan**.

The **Initiate On-Demand Subnet Scan** dialog opens.

Figure 429: *Initiate On-Demand Subnet Scan Dialog*



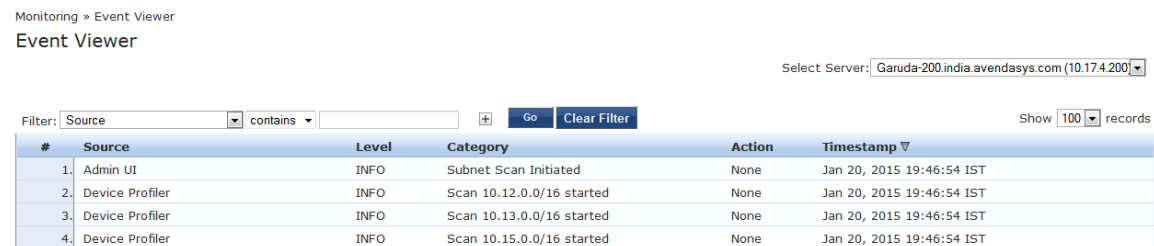
3. To discover hosts, specify the IP subnets to be scanned in the **Subnets to scan** text field. Separate multiple subnets with commas.

4. Click **Submit**.

The subnet scan progress is shown on the **Profile Settings** page. You can view the subnet scan events in the **Monitoring > Event Viewer** page.

Figure 430 displays the subnet scan logs in the **Event Viewer** page:

Figure 430: *Subnet Scan Logs*



SNMP Configuration for Wired Network Profiling

For wired network profiling, you can configure a list of multiple SNMP community strings to query static IP devices discovered by the Profiler.

If a static IP device does not respond to queries from the default public community string, the SNMP service can use the credentials from this custom list to query the device.

To configure SNMP for wired network profiling:

1. Navigate to **Configuration > Profile Settings**.

Figure 431 displays the Profile **SNMP Configuration** page:

2. Click the **SNMP Configuration** tab.

Figure 431: Profile SNMP Configuration Page

The screenshot shows the 'Profile Settings' page with the 'SNMP Configuration' tab selected. The page title is 'Configuration » Profile Settings'. In the top right corner, there is a link for 'On-Demand Subnet Scan'. Below the tabs, there is a section titled 'Specify SNMP configuration used for querying hosts discovered by a Subnet Scan'. On the right side of this section, there is a red-bordered button labeled 'Add SNMP configuration'. Below this, there is a table with the header 'IP Subnets/IP Addresses' and one entry: '1. 10.17.8.0/24'.

3. Click **Add SNMP Configuration**.
The **SNMP Configuration** dialog appears.

Figure 432: Configuring SNMP Community Strings

The screenshot shows the 'SNMP Configuration' dialog box. It has a title bar with a close button. Inside, there is a section for 'IP Subnets/IP Addresses' with a text box containing '10.15.0.0/16'. Below this is an 'Entries' section with a table header: 'Version', 'Username', and 'Description'. The table is empty, and a message 'No configuration exists' is displayed. Below the table, there are fields for 'SNMP Version:' (a dropdown menu showing 'SNMP v1 with community strings'), 'Description:' (a text box with 'SNMP configuration 1'), and 'Community String:' (a text box with masked characters). To the right of the 'Community String' field is a 'Verify:' field, also with masked characters. At the bottom right, there are buttons for 'Reset', 'Save Entry', 'Save', and 'Cancel'.

4. Enter the following information in the **SNMP Configuration** dialog:
 - a. **IP Subnets/IP Addresses:** Enter one or more IP subnet addresses and their subnet masks.
For multiple entries, separate multiple IP addresses with commas.
 - b. **SNMP Version:** From the drop-down, select the appropriate SNMP version.
 - c. **Description:** Optionally, enter a description of this SNMP configuration.
 - d. **Community String:** Enter the community string, then reenter the community string in the **Verify** field.
5. When finished, click **Save Entry**, then click **Save**.

Information Regarding SSH and WMI Configuration

For information on configuring SSH and WMI credentials:

- **SSH credentials**

For Linux server or network device discovery, specify SSH configuration credentials. For more information, see [SSH Credentials Configuration on page 142](#).

- **WMI credentials**

For Windows device discovery, specify WMI (Windows Management Instrumentation) credentials. For more information, see [WMI Credentials Configuration on page 144](#).

This chapter describes the following tasks that you can perform by using the W-Policy Manager user interface:

- [Adding and Modifying Network Devices on page 430](#)
- [Adding and Modifying Device Groups on page 438](#)
- [Adding and Modifying Proxy Targets on page 440](#)
- [Configuring the Ingress Event Sources on page 678](#)

Introduction

A W-Policy Manager device represents a Network Access Device (NAD) that sends network access requests to W-Policy Manager using the supported RADIUS, TACACS+, or SNMP protocol. You can add or modify a device or a device group from the W-Policy Manager server.

For related information, see [SNMP Private MIB, SNMP Traps, System Events, Error Codes on page 779](#).

For the W-Policy Manager server to discover and access the network devices, you must perform the following tasks:

- Configure SNMP read credentials on the network device to enable W-Policy Manager server to query against network devices or perform SNMP write operations. For details, see [SNMP Credentials Configuration on page 141](#).
- Configure SNMP trap configurations on the network device to send SNMP traps to the W-Policy Manager server. For details, see [SNMP Trap Receivers on page 533](#).
- Ensure that the same SNMP Trap credentials are configured in the **SnmpService** section under the **Administration > Server Configuration > Service Parameters** tab of the W-Policy Manager user interface.
- Configure SNMPTRAPD on the W-Policy Manager server to receive SNMP traps. For details, see [SNMP Private MIB, SNMP Traps, System Events, Error Codes on page 779](#).

For SNMP enforcement on the network device, one or more of the following traps must be configured on the device:

- Link Up trap
- Link Down trap
- MAC Notification trap

In addition, the device must also support one or more of the following SNMP MIBs:

- RFC-1213 MIB
- IF-MIB, BRIDGE-MIB
- ENTITY-MIB
- Q-BRIDGE-MIB
- CISCO-VLANMEMBERSHIP-MIB
- CISCO-STACK-MIB
- CISCO-MAC-NOTIFICATION-MIB

These traps and MIBs enable W-Policy Manager to correlate the MAC address, IP address, switch port, and switch information.

- Configure SSH CLI data on the W-Policy Manager server to allow a phantom login to network devices. For details, see [SSH Credentials Configuration on page 142](#).

- Configure DHCP Relay configuration on the network device to ensure that DHCP requests are forwarded from the clients. For more information, see [DHCP Collector on page 421](#).

Adding and Modifying Network Devices

A Network Access Device (NAD) must belong to the global list of devices in the W-Policy Manager database in order to connect to W-Policy Manager using any of the supported protocols.

The W-Policy Manager **Network Devices** page displays the device name, IP address or subnet address, and a brief description of each configured device.

To view this page, navigate to **Configuration > Network > Devices**.

The **Network Devices** page opens:

Figure 433: *Network Devices Page*

Configuration > Network > Devices

Network Devices

Device Dell Controller Building 3 added

[Add Device](#)
[Import Devices](#)
[Export Devices](#)

Filter: Name contains Show 10 records

#	☐	Name ▲	IP or Subnet Address	Description
1.	☐	Dell Controller 1	192.168.5.68	
2.	☐	Dell Controller Building 3	192.168.68.17	

Showing 1-2 of 2

This page includes the following additional tasks:

- [Adding a Network Device on page 430](#)
- [Additional Tasks on page 437](#)

Adding a Network Device

This section describes the following tabs used to configure a new network device:

- [Device Parameters](#)
- [SNMP Read Settings Parameters](#)
- [SNMP Write Settings Parameters](#)
- [CLI Parameters](#)
- [Enabling W-ClearPass OnConnect Enforcement on a Network Device](#)

To add a network device:

1. Navigate to the **Configuration > Network > Devices** page.
The **Network Devices** page opens.
2. Click the **Add** link at the top-right corner.
The **Add Device** page opens.

Device Parameters

Use the **Add Device > Device** tab to define the device name, IP address, RADIUS and TACACS+ shared secret, vendor name, and device attributes.

Figure 434: Add Device > Device Dialog

Add Device

Device | SNMP Read Settings | SNMP Write Settings | CLI Settings | OnConnect Enforcement

Name:

IP or Subnet Address: (e.g., 192.168.1.10 or 192.168.1.1/24 or 192.168.1.1-20)

Description:

RADIUS Shared Secret: Verify:

TACACS+ Shared Secret: Verify:

Vendor Name:

Enable RADIUS CoA: ☒ RADIUS CoA Port:

Attributes

Attribute	Value
1. Click to add...	

Add **Cancel**

3. Enter the **Add Device > Device** parameters as described in [Table 243](#):

Table 243: Add Device > Device Parameters

Parameter	Action/Description
Name	Enter the name of the device.
IP Address or Subnet	Specify the IP address or the subnet of the device. You can use a hyphen to indicate the range of device IP addresses following the format a.b.c.d-e . For example, 192.168.1.1-20 .
Description	Enter a description that provides additional information to identify the device.
RADIUS Shared Secret	Enter the RADIUS shared secret.
TACACS+ Shared Secret	Enter the TACACS+ shared secret.
Vendor Name	Specify the name of the vendor to load the dictionary associated with this vendor for this device. This field is optional.

Table 243: Add Device > Device Parameters (Continued)

Parameter	Action/Description
	NOTE: RADIUS:IETF, the dictionary containing the standard set of RADIUS attributes, is always loaded. When you specify a vendor here, the RADIUS dictionary associated with this vendor is automatically enabled.
Enable RADIUS CoA	To set the UDP port on the device to send CoA (Change of Authorization) actions, enable RADIUS CoA (RFC 3576/5176) for this device. RADIUS CoA Port: The default value is 3799.
Attributes	To add custom attributes for this device, click Click to add.... By default, four custom attributes appear in the Attribute drop down: Location, OS-Version, Device-Type, and Device-Vendor. You can enter any name in the Attribute field. All attributes are of string datatype. The Value field can be populated with any string. Each time you enter a new custom attribute, it's available for selection in the Attribute drop-down for all devices. NOTE: All attributes entered for a device are available in the role-mapping Rules Editor under the Device namespace.

SNMP Read Settings Parameters

Use the **SNMP Read Settings** tab to define values that allow W-ClearPass Policy Manager to read information from the device using SNMPv1, SNMPv2, or SNMPv3.



Large or geographically-spread cluster deployments typically do not require each W-ClearPass node to probe all SNMP configured devices. By default, a W-ClearPass node in a cluster only reads network device information for devices configured to send traps to that node.

1. From the **Add Device** page, select the **SNMP Read Settings** tab.

The **SNMP Read Settings** dialog opens:

Figure 435: Add Device > SNMP Read Settings Dialog

Add Device

Device | **SNMP Read Settings** | SNMP Write Settings | CLI Settings | OnConnect Enforcement

Allow SNMP Read: ☒ Enable Policy Manager to perform SNMP read operations

SNMP Read Setting: SNMP v2 with community strings

Community String: Verify:

Force Read: ☒ Always read information from this device

Read ARP Table Info: ☒ Read ARP table from this device

Add Cancel

2. Enter the **SNMP Read Settings** parameters as described in [Table 244](#):

Table 244: Add Device > SNMP Read Settings Parameters

Parameter	Action/Description
Allow SNMP Read	Toggle to enable or disable SNMP Read operations.
SNMP Read Setting	Specify the SNMP Read settings for the network device. Specify one of the following options: ■ SNMP v1 with community strings ■ SNMP v2 with community strings ■ SNMP v3 with no Authentication ■ SNMP v3 with Authentication using MD5 and no Privacy ■ SNMP v3 with Authentication using MD5 and with Privacy ■ SNMP v3 with Authentication using SHA and no Privacy ■ SNMP v3 with Authentication using SHA and with Privacy NOTE: The MD5 authentication type is not supported if you use W-ClearPass Policy Manager in FIPS mode.
Community String	Enter the community string for sending the traps. NOTE: Available in SNMP v2 only.
Verify	Reenter the community string for sending the traps.
Force Read	Enable Force Read to ensure that all W-ClearPass Policy Manager nodes in the cluster read SNMP information from this device regardless of the trap configuration on the device. This option is useful when demonstrating a static IP-based device profiling because this does not require any trap configuration on the network device. NOTE: Available in SNMP v1 and SNMP v2 only.
Read ARP Table Info	Enable this setting on a Layer 3 device if you intend to use the ARP table on this device to discover endpoints in the network. Static IP endpoints that are discovered this way are further probed using SNMP to profile the device.
Username	Specify the Admin user name to use for SNMP read operations. NOTE: Available in SNMP v3 only.

Table 244: Add Device > SNMP Read Settings Parameters (Continued)

Parameter	Action/Description
Authentication Key	Specify the SNMP v3 with authentication option (SHA or MD5). NOTE: The EAP-MD5 authentication type is not supported if you run W-ClearPass Policy Manager in FIPS mode. NOTE: Authentication Key is available in SNMP v3 only.
Privacy Key	Specify the SNMP v3 with privacy option. NOTE: Available in SNMP v3 only.
Privacy Protocol	Choose one of the available privacy protocols: ■ DES-CBC ■ AES-128 NOTE: Available in SNMP v3 with Privacy only. Privacy allows for encryption of SNMP v3 messages to ensure confidentiality of data.

SNMP Write Settings Parameters

Use the **SNMP Write Settings** tab to define values that allow W-ClearPass Policy Manager to write to (manage) the device using SNMPv1, SNMPv2, or SNMPv3.

- From the **Add Device** page, select the **SNMP Write Settings** tab.

The **SNMP Write Settings** dialog opens:

Figure 436: Add Device > SNMP Write Settings Dialog

- Enter the **SNMP Write Settings** parameters as described in [Table 245](#).

Table 245: Add Device > SNMP Write Settings Parameters

Parameter	Action/Description
Allow SNMP Write	Toggle to enable or disable SNMP write.
Default VLAN	Specify the VLAN port setting after the SNMP-enforced session expires.
SNMP Write Setting	Specify the SNMP Write setting for the device. You can set any of the following options: ■ SNMP v1 with community strings

Table 245: Add Device > SNMP Write Settings Parameters (Continued)

Parameter	Action/Description
	■ SNMP v2 with community strings ■ SNMP v3 with no Authentication ■ SNMP v3 with Authentication using MD5 and no Privacy ■ SNMP v3 with Authentication using MD5 and with Privacy ■ SNMP v3 with Authentication using SHA and no Privacy ■ SNMP v3 with Authentication using SHA and with Privacy NOTE: The MD5 authentication type is not supported if you use W-ClearPass Policy Manager in FIPS mode.
Community String	Enter the community string for sending the traps.
Verify	Reenter the community string for sending the traps.

CLI Parameters

Use the **CLI Settings** tab to enable or disable the CLI, and define user names, passwords, and port settings for accessing the CLI.

1. From the **Add Device** page, select the **CLI Settings** tab.

The **CLI Settings** dialog opens:

Figure 437: Add Device > CLI Settings Dialog

Add Device

Device | SNMP Read Settings | SNMP Write Settings | **CLI Settings** | OnConnect Enforcement

Allow CLI Access: ☒ Enable Policy Manager to perform CLI operations

Access Type: ☒ SSH ☐ Telnet

Port:

Username:

Password: Verify Password:

Username Prompt Regex:

Password Prompt Regex:

Command Prompt Regex:

Enable Prompt Regex:

Enable Password: Verify Password:

Add **Cancel**

2. Enter the **CLI Settings** parameters as described in [Table 246](#):

Table 246: Add Device > CLI Parameters

Parameter	Action/Description
Allow CLI Access	Toggle to enable or disable CLI access.
Access Type	Select SSH or Telnet . W-Policy Manager uses the selected access method to log into the device CLI.
Port	Specify the SSH or Telnet TCP port number.
Username	Enter the username to log into the CLI.
Password	Enter the password to log into the CLI.
Username Prompt Regex	Specify the regular expression for the username prompt. W-Policy Manager looks for this pattern to recognize the Telnet username prompt.
Password Prompt Regex	Specify the regular expression for the password prompt. W-Policy Manager looks for this pattern to recognize the Telnet password prompt.
Command Prompt Regex	Specify the regular expression for the command line prompt. W-Policy Manager looks for this pattern to recognize the Telnet command-line prompt.
Enable Prompt Regex	Specify the regular expression for the command line in the enable prompt. W-Policy Manager looks for this pattern to recognize the Telnet command-line prompt.
Enable Password	Enter then reenter the credentials for the Enable password in the CLI.

Enabling W-ClearPass OnConnect Enforcement on a Network Device

OnConnect Enforcement is an enforcement model that allows you to use non-802.1X methods for device scans, VLAN placement, and so on. OnConnect Enforcement allows enforcement in non-802.1X environments without the need for an agent, such as OnGuard, on the endpoint.

When this feature is enabled, W-ClearPass performs the following actions:

- Detects when a new endpoint connects to the network.
- Scans the endpoint to identify the logged-in user and other device-specific information.
- Triggers a Web-based authentication (WebAuth) for the device.
- Performs SNMP-based enforcement to change the network access profile for the device.

To enable W-ClearPass OnConnect Enforcement on a Network Device:

1. From the **Add Device** page, select the **OnConnect Enforcement** tab.
The **OnConnect Enforcement** dialog opens:

Figure 438: Add Device > OnConnect Enforcement Dialog

2. Enter the **OnConnect Enforcement** parameters as described in [Table 247](#).

Table 247: Add Device > OnConnect Enforcement Parameters

Parameter	Action/Description
Enable	Select this check box to enable W-ClearPass OnConnect on the network access device being added.
Zone	From the Zone drop-down, select the zone assigned to the network device that is being added. OnConnect Enforcement is triggered when a trap from a NAD is received by a W-ClearPass node. If the zone assigned to a W-ClearPass node is not same as the zone configured in the OnConnect Enforcement tab, then agentless enforcement is not triggered on that W-ClearPass node.
Port Names	Specify the names and descriptions of the ports (in comma-separated format) of the network device being added. Only the ports added in the Port Names field will have OnConnect Enforcement enabled. For example, if you add the port names Fa1/0/3,Fa1/0/5 , when clients connect to any of these ports on the specified network device, OnConnect Enforcement is triggered on that network device. NOTE: Use an empty string to enable OnConnect Enforcement for all ports. Ports determined to be uplink ports or trunk ports will be ignored; multiple clients behind a Hub-connected port are also ignored.

Additional Tasks

Importing a Device

To import a device:

1. Click **Import**.
2. In the **Import from File** page, browse to select a file, and then click **Import**.
3. If you entered a secret key to encrypt the exported file, enter the same secret key to import the device back.

Exporting All Devices

To export all devices from the configuration:

1. Click **Export**.
2. In the **Export to File** page, specify a file path, then click **Export**.
3. In the **Export to File** page, 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 with which you exported.

Exporting a Single Device

To export a single device from the configuration:

1. Select it (using the check box on the left).
2. click **Export**.
3. In the **Save As** dialog, specify a file path, then click **Export**.

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 belong to the device groups.

Administrators configure device groups at the global level. Device groups can contain the members of the IP address of a specified subnet, regular expression-based variation, or devices that are previously configured in the W-Policy Manager database.

W-Policy Manager lists all configured device groups in the **Device Groups** page (**Configuration > Network > Device Groups**). The following figure displays the **Network Device Groups** page:

Figure 439: Device Groups Page

Configuration > Network > Device Groups

Network Device Groups

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

Filter: Name contains [] [Go] [Clear Filter] Show 10 records

#	☐	Name ▲	Format	Description
1.	☐	Admin Switch	Subnet	Edge Switches at Admin Building 10.26.0.0/16
2.	☐	LIB Switch	Subnet	10.23.0.0/16
3.	☐	SBZ Switch	Subnet	10.22.0.0/16
4.	☐	SESS Switch	Subnet	10.25.0.0/16
5.	☐	SIS Switch	Subnet	10.21.0.0/16
6.	☐	SOA Switch	Subnet	10.21.0.0/16

Showing 1-6 of 6

[Export](#) [Delete](#)

To add a device group, click **Add** at the top-right corner of the **Network Device Groups** page. Complete the fields in the **Add New Device Group** page as described in the following figure:

Figure 440: Add New Device Group Page

The figure displays three overlapping screenshots of the 'Add New Device Group' dialog box, illustrating different configuration options for the 'Format' field.

- Top Screenshot:** The 'Format' field is set to 'Subnet'. The 'Name' field contains 'TestDevice Group' and the 'Description' field contains 'This is a test device group'. The 'Subnet' field is empty, with a hint '(e.g., 192.168.1.1/24)' below it.
- Middle Screenshot:** The 'Format' field is set to 'Regular Expression'. The 'Name' field contains 'Test Device Group 2' and the 'Description' field contains 'This is a test device group 2'. The 'Regular Expression' field contains the pattern '(e.g., ^192([0-9]*){3}\$)'.
- Bottom Screenshot:** The 'Format' field is set to 'List'. The 'Name' field contains 'Test Device Group 2' and the 'Description' field contains 'This is a test device group 2'. The 'List' field shows a list of available IP addresses: 192.168.150.204, 192.168.150.60, 192.168.150.80, 192.168.5.12, 192.168.5.208, and 192.168.5.214. There are 'Filter' buttons and '>>'/'<<' arrows for moving items between the 'Available Devices' and 'Selected Devices' lists.

At the bottom right of the dialog box, there are 'Save' and 'Cancel' buttons.

The following table describes the **Add New Device Group** page parameters:

Table 248: Add New Device Group Page

Parameter	Description
Name	Enter the name of the device group.
Description	Enter the description that provides additional information about the device group.
Format	Select the format: Subnet, Regular Expression, or List.

Table 248: Add New Device Group Page (Continued)

Parameter	Description
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.

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 be used in configuring RADIUS proxy services. Refer to [Policy Manager Service Types on page 70](#) for more information. Policy Manager lists all configured proxy servers in the **Proxy Targets** page. To view the **Proxy Targets** page, navigate to **Configuration > Network > Proxy Targets**.

The following figure displays the **Proxy Targets** page:

Figure 441: Proxy Targets Page

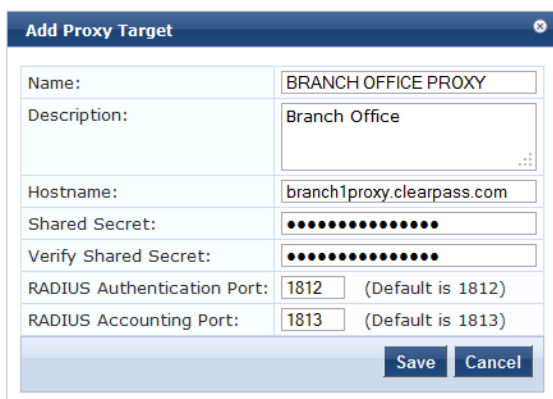


Adding a Proxy Target

To add a proxy target, click **Add** and complete the fields in the **Add Proxy Target** popup. You can also add a new proxy target from the **Services** page (**Configuration > Services**) as part of the flow of the **Add Service** wizard for a RADIUS proxy service type.

The following figure displays the **Add Proxy Target** pop-up:

Figure 442: *Add Proxy Target Pop-up*



The following table describes the **Add Proxy Target** pop-up parameters:

Table 249: *Add Proxy Target pop-up*

Parameter	Description
Name	Enter the name of the proxy target.
Description	Enter the description that provides additional information about the proxy target.
Hostname/Shared Secret	Specify the 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.

Configuring the Ingress Event Sources

The Event Source is the device that sends Syslog events to W-ClearPass. Any events sent that are not from configured event sources are ignored.

To configure the Event Source (in this example, a Juniper Networks SRX gateway):

1. Navigate to **Configuration > Network > Event Sources**.
The **Event Sources** page appears.
2. To add the Event Source for the desired vendor, click **Add**.
The **Add Events Source** dialog appears.

Figure 443: Adding an Event Source

Name:	192.0.2.100
Description:	Juniper Networks SRX device that sends events to ClearPass
IP Address:	192.0.2.100
Type:	Syslog
Vendor:	Juniper Networks
Enable:	☒

3. Populate the **Add Event Source** parameters as described in [Table 250](#).

Table 250: Configuring the Event Source Parameters

Parameter	Action/Description
Name	1. Enter the IP address of the device that will send Syslog events to W-ClearPass.
Description	Optionally, enter a description of this Event Source.
IP Address	2. Enter the IP address of the device that will send Syslog events to W-ClearPass.
Type	3. From the drop-down, select the Event Source Type .
Vendor	4. From the drop-down, select the Event Source Vendor .
Enable	5. Select this check box to enable the device as an Event Source.

6. When finished, click **Add**.

The **Event Sources** page now displays the new Event Sources (see [Figure 444](#)).

Figure 444: Event Sources Page

Configuration » Network » Event Sources

Event Sources

Event Source 192.0.2.100 added successfully

Filter: Name contains Go Clear Filter

Show 10 records

#	Name	Description	IP Address	Type	Vendor	Enabled
1.	192.0.2.100	Juniper Networks SRX device that sends events to ClearPass	192.0.2.100	Syslog	Juniper Networks	true

Showing 1-1 of 1

Export Delete

Add Import Export All

The IP address displayed in [Figure 444](#) is the IP address and host name of the Juniper SRX gateway that sends Syslog events to W-ClearPass.

All administrative activities including server configuration, log management, certificate and dictionary maintenance, portal definitions, and administrator user account maintenance are done from the following Administration menus:

- W-ClearPass Portal
 - [W-ClearPass Guest Portal on page 444](#)
- Users and privileges
 - [Managing Admin Users on page 445](#)
 - [Managing Admin Privileges on page 449](#)
- Server Manager
 - [Server Configuration on page 457](#)
 - [Log Configuration on page 523](#)
 - [Local Shared Folders on page 526](#)
 - [License Management on page 527](#)
- External Servers
 - [SNMP Trap Receivers on page 533](#)
 - [Syslog Targets on page 537](#)
 - [Syslog Export Filters on page 541](#)
 - [Messaging Setup on page 553](#)
 - [Endpoint Context Servers on page 555](#)
 - [File Backup Servers on page 619](#)
- Certificates
 - [Server Certificate on page 621](#)
 - [Certificate Trust List on page 633](#)
 - [Certificate Revocation Lists on page 635](#)
- Dictionaries
 - [RADIUS Dictionary on page 637](#)
 - [TACACS+ Services Dictionary on page 638](#)
 - [Fingerprints Dictionary on page 640](#)
 - [Dictionary Attributes on page 641](#)
 - [Applications Dictionaries on page 645](#)
 - [Configuring Endpoint Context Server Actions on page 563](#)
- Agents and Software Updates
 - [OnGuard Settings on page 651](#)
 - [Updating Policy Manager Software on page 646](#)
- Support
 - [Contact Support on page 657](#)
 - [Remote Assistance on page 658](#)
 - [Documentation on page 1](#)

W-ClearPass Guest Portal

The W-ClearPass Guest Portal lets you customize the content for your enterprise.

Navigate to the **Administration > W-ClearPass Portal** page.

The following figure displays the W-ClearPass Guest Portal page:

Figure 445: W-ClearPass Guest Portal

Administration > Agents and Software Updates > Guest Portal Global Portal Settings

Guest Portal

Name:	default	
Portal URL:	https://DELL-OEM/agent/portal/	
Select Mode:	Authenticate - no health checks (HTML form) Enter authentication details Username : Password : <input type="submit" value="Submit"/>	
Usage Terms Text:	☐ Enable to show terms and conditions of use	
Resource Files:	No resource files were uploaded. A ZIP archive containing resource files is supported Upload	
Customize Portal:	☒ Use default template ☐ Upload custom template Title Logo Image Header Footer Copyright Guest Access Portal - Dell GUEST PORTAL Guests must login with the username and password provided to access the network Note: If you can not access an enterprise resource, it may be because you are in the quarantine network. Please visit Guest Policy Example for more information © Copyright 2012 Aruba Networks. All rights reserved. Save Cancel	

The following table describes the W-ClearPass Guest Portal parameters:

Table 251: W-ClearPass Guest Portal Parameters

Parameter	Action/Description
Select Option	1. Select the page that the user first sees after logging in to W-ClearPass: ■ Default Landing Page ■ Application Login Page: ■ W-ClearPass Policy Manager ■ W-ClearPass Guest ■ W-ClearPass Insight ■ W-ClearPass Onboard ■ Guest Portal
Page Title	2. Click and enter the text to appear as the page title in the default landing page.
Logo Image	3. Click and browse to select an image for the banner in the default landing page.

Table 251: W-ClearPass Guest Portal Parameters (Continued)

Parameter	Action/Description
Top section	4. Click and enter the text to appear as the header in the default landing page.
Bottom section	5. Click and enter the text to appear as the footer in the default landing page.
Copyright	6. Click and enter the copyright text to appear in the default landing page.
	7. Click Save .



Both the HTTP and HTTPS protocols are supported for Guest Portal redirection.

Managing Admin Users

This section describes the following topics:

- [Changing the Administration Password](#)
- [Adding an Admin User](#)
- [Importing and Exporting Admin Users](#)
- [Setting Password Policy for Admin Users](#)
- [Disabling Admin User Accounts](#)

Changing the Administration Password

After activating the W-ClearPass appliance, the recommended next task is to change the administration password for the newly-activated W-ClearPass server.

To change the administration password:

1. Navigate to **Administration > Users and Privileges > Admin Users**.

The **Admin Users** page opens.

Figure 446: Admin Users Page

Administration » Users and Privileges » Admin Users				
Admin Users				
Filter: User ID contains [] Go Clear Filter				
Show 10 records				
#	User ID	Name	Privilege Level	Status
1.	admin	Super Admin	Super Administrator	Enabled
2.	apiadmin	API Admin	API Administrator	Enabled
Showing 1-2 of 2				Export Delete

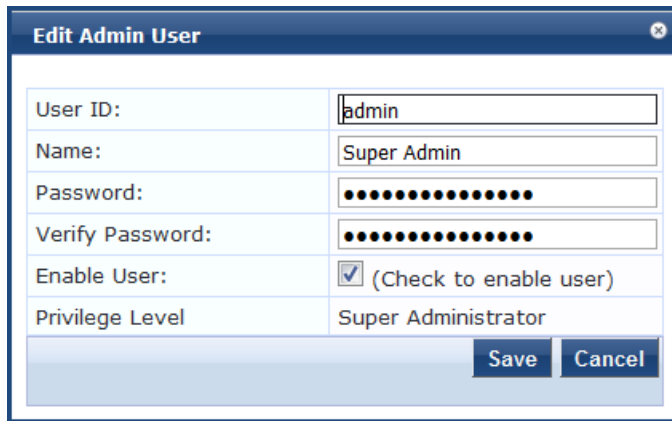
In this page, you can view the administrator details such as user ID, user name, and privilege level.

You can also change the admin password, and add, import, export, and set password policies for the admin users by using the links provided at the top-right corner of this page.

2. Select the Admin user you want to modify.

The **Edit Admin User** dialog opens.

Figure 447: *Changing the Administration Password*



3. Change the administration password, then click **Save**.

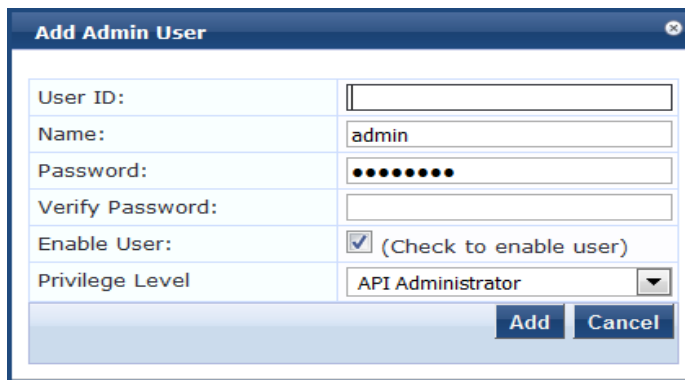
Adding an Admin User

To add a new admin user:

1. Navigate to **Administration > Users and Privileges > Admin Users**.
2. Click the **Add** link at the top-right corner the page.

The **Add Admin User** dialog opens.

Figure 448: *Adding an Admin User*



3. Specify the **Add Admin User** parameters as described in the following table, then click **Save**:

Table 252: *Adding an Admin User Parameters*

Parameter	Action/Description
User ID	1. Specify a user ID for this administrator.
Name	2. Specify the name for the admin user.
Password/ Verify Password	3. Specify a password for the local user, then verify the password.

Table 252: Adding an Admin User Parameters (Continued)

Parameter	Action/Description
Enable User	4. You must enable this check box to enable the admin user account (is is enabled by default). Otherwise, the admin user account is disabled.
Privilege Level	5. From the drop-down list, select one of the following admin user privilege levels: ■ API Administrator ■ Help Desk ■ Network Administrator ■ Read-only Administrator ■ Receptionist ■ Super Administrator

Importing and Exporting Admin Users

You can import or export the admin user accounts by using the **Import** and **Export All** links at the top-right corner of the **Admin Users** page.

You can also export specific admin user accounts by using the **Export** button that appears after selecting one or more admin user accounts from the list.

For more information, refer to [Importing and Exporting Information on page 32](#).



The passwords of the admin user accounts are not stored in clear text when exported to an XML file.

Setting Password Policy for Admin Users

To set password policies for the administrators:

1. Navigate to **Administration > Users and Privileges > Admin Users**.
2. Click the **Account Settings** link at the top-right corner of the **Admin Users** page.

The **Password Policy Settings** dialog opens.

Figure 449: Admin Users > Setting Password Policy

The image shows a screenshot of the "Account Settings" dialog box. It has two tabs: "Password Policy" (selected) and "Disable Accounts". Under "Password Policy", there are several fields: "Minimum Length" with a value of 6, "Complexity" with a dropdown menu set to "No password complexity requirement", "Disallowed Characters" with an empty text box, and "Disallowed Words (CSV)" with an empty text box. Below these are two checkboxes under "Additional checks": "May not contain User ID or its characters in reversed order" and "May not contain repeated character four or more times consecutively". The "Expiry Days" field has a value of 0. At the bottom, there is a note: "Note: Password characters validation will take effect for users created or modified after changes are saved. Other settings will be applied to all users." and two buttons: "Save" and "Cancel".

3. Specify the **Password Policy** parameters as described in [Table 253](#), then click **Save**:

Table 253: *Password Policy Parameters*

Parameter	Action/Description
Minimum Length	1. Specify the minimum length required for the password.
Complexity	2. Select the complexity setting from the Complexity drop-down list. The complexity settings can be one of the following: ■ No password complexity requirement ■ At least one uppercase and one lowercase letter ■ At least one digit ■ At lease one letter and one digit ■ At least one of each: uppercase letter, lowercase letter, digit ■ At least one symbol ■ At least one of each: uppercase letter, lowercase letter, digit, and symbol
Disallowed Characters	3. Specify the characters not to be allowed in the password.
Disallowed Words (CSV)	4. Specify the words not to be allowed in the password
Additional Checks	5. Select any additional checks, if required. The options are: ■ May not contain User ID or its characters in reversed order. ■ May not contain repeated character four or more times consecutively.
Expiry Days	6. Set the password expiry time for the local users. The allowed range is 0 to 500 days. The default value is 0 . NOTE: If the value is set to 0 , the password never expires. For any other value, local users are forced to reset the expired password when they log in. W-ClearPass alerts users five days before the password expires.



Password Policy settings are effective only for the users created or modified after the changes are saved.

Disabling Admin User Accounts

- The **Disable Account** check occurs every day at midnight.
- Other Local User configuration settings are applied to all local users.

To specify the conditions for disabling admin user accounts:

1. Navigate to **Administration > Users and Privileges > Admin Users**.
2. Click the **Account Settings** link at the top-right corner of the **Admin Users** page.
The **Account Settings** page opens.
3. Select the **Disable Accounts** tab.
The **Disable Accounts** dialog opens.

Figure 450: *Admin Users > Disable Accounts Dialog*

The screenshot shows a window titled "Account Settings" with a close button in the top right corner. It contains two tabs: "Password Policy" and "Disable Accounts". The "Disable Accounts" tab is active. Inside this tab, there is a section for "Failed attempts count" with a text input field and the text "times (1-100)". Below this is a section for "Reset failed attempts count" with the text "To reset failed attempts count and enable those users, click:" followed by a "Reset" button. At the bottom right of the dialog are "Save" and "Cancel" buttons.

4. Specify the **Disable Accounts** parameters as described in [Table 254](#), then click **Save**.

Table 254: *Admin Users > Disable Accounts Parameters*

Parameter	Action/Description
Failed attempts count	1. Specify the number of failed log-in attempts are allowed before the account is disabled. The range is from 1 to 100 attempts.
Reset failed attempts count	2. To reset the failed attempts count to zero and reenable those admin users who were disabled after exceeding the failed attempts count, click Reset .

Managing Admin Privileges

This section provides the following information:

- [Overview](#)
- [Defining Custom Admin Privileges](#)
- [Creating Custom Administrator Privileges on page 452](#)
- [Administrator Privilege XML File Structure on page 452](#)
- [Administrator Privileges and IDs on page 453](#)
- [Sample Administrator Privilege XML File on page 456](#)

Overview

W-ClearPass Policy Manager ships with the following default administrator admin privileges XML files:

- API Administrator
- Help Desk
- Network Administrator
- Read-only Administrator
- Receptionist
- Super Administrator

Each of these default admin privileges administrators, define the admin privileges for W-Policy Manager and for Insight. The default set of admin privileges cannot be modified.

You can export one or more default files and modify the file to create a customized administrator privileges file.

Customized administrator privileges are defined in an XML file with a specific format and then imported into W-ClearPass Policy Manager on the **Admin Privileges** page.

Defining Custom Admin Privileges

When a different set of admin privileges is needed (for example, if you require different admin privileges for the Report module than the admin privileges defined for the other Insight modules), you must create a new admin privileges administrator.

To define custom admin privileges for W-ClearPass and Insight:

1. Navigate to the **Administration > Users and Privileges > Admin Privileges** page.

The **Admin Privileges** page opens:

Figure 451: Admin Privileges Page

Administration » Users and Privileges » Admin Privileges

Admin Privileges

Filter: Name contains [] Go Clear Filter

Show 10 records

#	Name	Description
1.	API Administrator	An API administrator is only allowed API access to read/write all configuration elements
2.	Help Desk	A help desk person logs in to troubleshoot problems reported by end users
3.	Network Administrator	A network administrator is allowed to configure all the policies in the system
4.	Read-only Administrator	A read-only administrator is only allowed to read all configuration elements
5.	Receptionist	A receptionist is allowed access to main monitoring screens
6.	Super Administrator	A super administrator is allowed read/write access to all configuration elements

Showing 1-6 of 6

Export Delete

2. Click the **Add** link.

The **Add Admin Privileges** dialog opens.

Figure 452: Add Admin Privileges Page: Basic Information Tab

Add Admin Privileges

Basic Information Policy Manager Insight

Name: []

Description: []

Access Type: Give full access to the Admin

Allow Passwords: []

Save Cancel

3. Specify the parameters in the **Basic Information** tab as described in [Table 255](#).

Table 255: Add Admin Privileges Parameters: Basic Information Tab

Parameter	Action/Description
Name	1. Enter the name of the Admin Privileges administrator.
Description	2. Provide a description of this new admin privileges administrator.
Access Type	3. Select one of the following Access Types: ■ Give full access to the Admin ■ Give UI access to the Admin ■ Give API access to the Admin
Allow Passwords	4. Select this check box if you want to allow password access.

Configuring Policy Manager Admin Privileges

To configure the W-Policy Manager admin privileges:

1. Select the **Policy Manager** tab.

The following dialog opens:

Figure 453: Specifying Policy Manager Admin Privileges

Edit Admin Privileges			
General		Policy Manager	Insight
	Dashboard	☒ Read	☐ Read,Write ☐ Read,Write,Delete
[-]	Monitoring	☒ Read	☐ Read,Write ☐ Read,Write,Delete
[+]	Live Monitoring	☐ Read	☐ Read,Write ☐ Read,Write,Delete
[+]	Profiler and Discovery	☐ Read	☐ Read,Write ☐ Read,Write,Delete
	Audit Viewer	☐ Read	☐ Read,Write ☐ Read,Write,Delete
	Event Viewer	☐ Read	☐ Read,Write ☐ Read,Write,Delete
	Data Filters	☐ Read	☐ Read,Write ☐ Read,Write,Delete
	Blacklisted Users	☐ Read	☐ Read,Write ☐ Read,Write,Delete
[-]	Configuration	☒ Read	☐ Read,Write ☐ Read,Write,Delete
	Start Here	☐ Read	☐ Read,Write ☐ Read,Write,Delete
	Services	☐ Read	☐ Read,Write ☐ Read,Write,Delete
[+]	Authentication	☐ Read	☐ Read,Write ☐ Read,Write,Delete

Save Cancel

2. Specify the admin privileges for each of the W-ClearPass components, then click **Save**.

Configuring Insight Admin Privileges

To configure the Insight admin privileges:

1. Select the **Insight** tab.

The following dialog opens:

Figure 454: *Specifying Insight Admin Privileges*

	Read	Read, Write	Read, Write, Delete
Dashboard	☒	☐	☐
Report	☒	☐	☐
Alert	☒	☐	☐
Admin	☒	☐	☐

2. Specify the admin privileges for each of the Insight modules, then click **Save**.

Creating Custom Administrator Privileges

To create a custom admin privilege XML file, you must use a plain text or XML editor.



Do not use word processing applications such as Microsoft Word which introduce tags and corrupt the XML file.

To create a custom administrator privilege:

1. Create an XML file that defines a privilege.
2. Store the new file.
3. Navigate to **Administration > Users and Privileges > Admin Privileges**.
4. Click **Import Admin Privileges**.
5. Import the administrator privilege file you created in step 1.

After you complete steps 1 through 5, the new administrator privileges document is displayed on the **Admin Privileges** page.

Administrator Privilege XML File Structure

Admin privilege files are XML files with a specific structure. It must have a header at the beginning of the file in the following format:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
```

The root tag is `TipsContents`. It is a container for the data in the XML file which must be in the following format:

```
<TipsContents xmlns="http://www.avendasys.com/tipsapiDefs/1.0">
:
</TipsContents>
```

An optional `TipsHeader` tag can follow the `TipsContents` tag. The actual admin privileges information is defined with the `AdminPrivilege` and `AdminTask` tags. You can use one `AdminPrivilege` tag for each admin privilege you want to define. The `AdminPrivilege` tag contains the following two attributes:

- `name`
- `description`

You can have one or more `AdminTask` tags inside the `AdminPrivilege` tag. Each `AdminTask` tag defines a place within the W-ClearPass Policy Manager application that a user with that privilege can view or change. The `AdminTask` tag contains one `taskid` attribute and a single `AdminTaskAction` tag. The `AdminTaskAction` tag contains an attribute, `type` which can take a value, `RO` (read only) or `RW` (read/write).

The following sample gives the basic structure of an admin privilege file:

```
<AdminPrivileges>
  <AdminPrivilege name="" description="">
    <AdminTask taskid="">
      <AdminTaskAction type=""/>
    </AdminTask>
    <AdminTask taskid="">
      <AdminTaskAction type=""/>
    </AdminTask>
  </AdminPrivilege>
</AdminPrivileges>
```

Administrator Privileges and IDs

Every UI element in the W-ClearPass Policy Manager application has a task ID associated with it. The users have access to the elements based on the permissions set for each task or element. By default, any permission provided for a task is applicable for all its sub-tasks. For example, if you give RW permissions for the task, **Enforcements** (con.en), it is automatically applied to its sub-tasks, **Policies** (con.en.epo) and **Profiles** (con.en.epr). Hence, you need not explicitly define the same permission for those sub-tasks.

The following list provides the tasks and sub-tasks of the W-ClearPass Policy Manager application and their associated task IDs:

Table 256: *Administrator Privileges and IDs*

Area (W-ClearPass Policy Manager Menu)	Task ID
Dashboard	dnd
Monitoring	mon
• Live Monitoring	mon.li
■ Access Tracker	mon.li.ad
■ Accounting	mon.li.ac
■ Onguard Activity	mon.li.ag
■ Analysis and Trending	mon.li.sp
■ Endpoint Profiles	mon.li.ep
■ System Monitor	mon.li.sy
• Audit Viewer	mon.av
• Blacklisted Users	mon.bl
• Event Viewer	mon.ev

Table 256: Administrator Privileges and IDs (Continued)

Area (W-ClearPass Policy Manager Menu)	Task ID
• Data Filters	mon.df
Configuration	con
• Start Here (Services Wizard)	con.sh
• Services	con.se
• Service Templates	con.st
• Authentication	con.au
■ Methods	con.au.am
■ Sources	con.au.as
• Identity	con.id
■ Single Sign-On	con.id.sso
■ Local Users	con.id.lu
■ Endpoints	con.id.ep
■ Static Host Lists	con.id.sh
■ Roles	con.id.rs
■ Role Mappings	con.id.rm
• Posture	con.pv
■ Posture Policies	con.pv.in
■ Posture Servers	con.pv.ex
■ Audit Servers	con.pv.au
• Enforcements	con.en
■ Policies	con.en.epo
■ Profiles	con.en.epr
• Network	con.nw
■ Devices	con.nw.nd
■ Device Groups	con.nw.ng

Table 256: Administrator Privileges and IDs (Continued)

Area (W-ClearPass Policy Manager Menu)	Task ID
■ Proxy Targets	con.nw.pr
Policy Simulation	con.ps
Profile Settings	con.prs
Administration	adm
● User and Privileges	adm.us
■ ClearPass Portal	adm.po.cp
■ Admin Users	adm.us.au
■ Admin Privileges	adm.us.ap
● Server Manager	adm.mg
■ Server Configuration	adm.mg.sc
■ Log Configuration	adm.mg.ls
■ Local Shared Folders	adm.mg.sf
■ Licensing	adm.mg.li
● External Servers	adm.xs
■ SNMP Trap Receivers	adm.xs.st
■ Syslog Targets	adm.xs.es
■ Syslog Export Filters	adm.xs.sx
■ Messaging Setup	adm.xs.me
■ Endpoint Context Servers	adm.xs.cs
■ Context Server Actions	adm.di.csa
● Certificates	adm.cm
■ Server Certificate	adm.cm.mc
■ Trust List	adm.cm.ctl
■ Revocation List	adm.cm.crl
● Dictionaries	adm.di

Table 256: Administrator Privileges and IDs (Continued)

Area (W-ClearPass Policy Manager Menu)	Task ID
■ RADIUS	adm.di.rd
■ Posture	adm.di.pd
■ TACACS+ Services	adm.di.td
■ Fingerprints	adm.di.df
■ Attributes	adm.di.at
■ Applications	adm.di.ad
● Agents and Software Updates	adm.po
■ Onguard Settings	adm.po.aas
■ Software Updates	adm.po.es
● Support	adm.su
■ Contact Support	adm.su.cs
■ Remote Assistance	adm.su.ra
■ Documentation	adm.su.doc

If you provide permission for an area, the same permission for all sub-areas is included by default. For example, if you give RW permissions for Enforcements (con.en), you grant permissions for its sub-areas, in this case, Policies (con.en.epo) and Profiles (con.en.epr), and you do not have to explicitly define the same permission for those sub-areas.

Sample Administrator Privilege XML File

This section provides sample XML files with different admin privileges for various UI elements.

The following sample provides Read Only (R) Privilege to all the sections (dnd, con, mon, adm):

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<TipsContents xmlns="http://www.avendasys.com/tipsapiDefs/1.0">
<TipsHeader exportTime="Thu Jul 26 17:57:50 IST 2012" version="6.0"/>
<AdminPrivileges>
  <AdminPrivilege name="Read-only Administrator" description="A read-only administrator is only allowed to read all configuration elements">
    <AdminTask taskid="con"> //Refers to Configuration
      <AdminTaskAction type="R"/>
    </AdminTask>
    <AdminTask taskid="dnd"> //Refers to DashBoard
      <AdminTaskAction type="R"/>
    </AdminTask>
    <AdminTask taskid="mon"> //Refers to Monitoring
      <AdminTaskAction type="R"/>
    </AdminTask>
    <AdminTask taskid="adm"> //Refers to Administration
      <AdminTaskAction type="R"/>
    </AdminTask>
  </AdminPrivilege>
</AdminPrivileges>
```

```

    </AdminPrivilege>
  </AdminPrivileges>
</TipsContents>

```

The following sample provides Read/Write access only to Guest, Local and Endpoint Repository:

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<TipsContents xmlns="http://www.avendasys.com/tipsapiDefs/1.0">
<TipsHeader exportTime="Thu Jul 26 17:57:50 IST 2012" version="6.0"/>
  <AdminPrivileges>
    <AdminPrivilege name="Read/Write Access to Guest, Local and Endpoint Repository" description="A read-only administrator is only allowed to read all configuration elements">
      <AdminTask taskid="con.id.lu"> //Refers to Local Users Section
        <AdminTaskAction type="RW"/>
      </AdminTask>
      <AdminTask taskid="con.id.gu"> //Refers to Guest Users Section
        <AdminTaskAction type="RW"/>
      </AdminTask>
      <AdminTask taskid="con.id.ep"> //Refers to Endpoints Section
        <AdminTaskAction type="RW"/>
      </AdminTask>
    </AdminPrivilege>
  </AdminPrivileges>
</TipsContents>

```

The following sample provides Read/Write permissions to DashBoard/ Monitoring and ReadOnly permissions to Server Configuration:

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<TipsContents xmlns="http://www.avendasys.com/tipsapiDefs/1.0">
<TipsHeader exportTime="Thu Jul 26 17:57:50 IST 2012" version="6.0"/>
  <AdminPrivileges>
    <AdminPrivilege name="Limited access permission" description="A read-only administrator is only allowed to read all configuration elements">
      <AdminTask taskid="dnd"> //Refers to DashBoard
        <AdminTaskAction type="RW"/>
      </AdminTask>
      <AdminTask taskid="mon"> //Refers to Monitoring
        <AdminTaskAction type="RW"/>
      </AdminTask>
      <AdminTask taskid="adm.mg.sc"> //Refers to Server Configuration
        <AdminTaskAction type="R"/>
      </AdminTask>
    </AdminPrivilege>
  </AdminPrivileges>
</TipsContents>

```

Server Configuration

This section describes the following server configuration tasks:

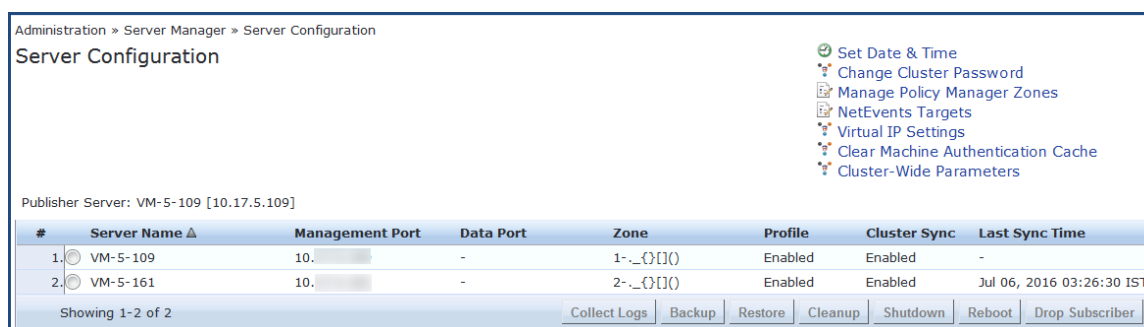
- [Edit Server Configuration Settings on page 458](#)
- [Set Date & Time on page 497](#)
- [Change Cluster Password on page 499](#)
- [Manage Policy Manager Zones on page 500](#)
- [NetEvents Targets on page 502](#)
- [Virtual IP Settings on page 504](#)
- [Clear Machine Authentication Cache on page 504](#)
- [Cluster-Wide Parameters on page 505](#)

- [Make Subscriber on page 517](#)
- [Collect Logs on page 518](#)
- [Backup on page 519](#)
- [Restore on page 520](#)
- [Shutdown/Reboot on page 523](#)
- [Drop Subscriber on page 523](#)

You can perform numerous server configuration tasks by navigating to **Administration > Server Manager > Server Configuration** page in W-ClearPass Policy Manager.

The following figure displays the **Server Configuration** page:

Figure 455: *Server Configuration Page*



Edit Server Configuration Settings

You can edit the configuration settings of a server by clicking the server name listed in the **Administration > Server Manager > Server Configuration** page.

You can perform the following additional tasks only for a disabled node:

- Setting Time Zone
- Synchronizing Cluster Password
- Promoting to Publisher
- Joining a Server Back to Cluster

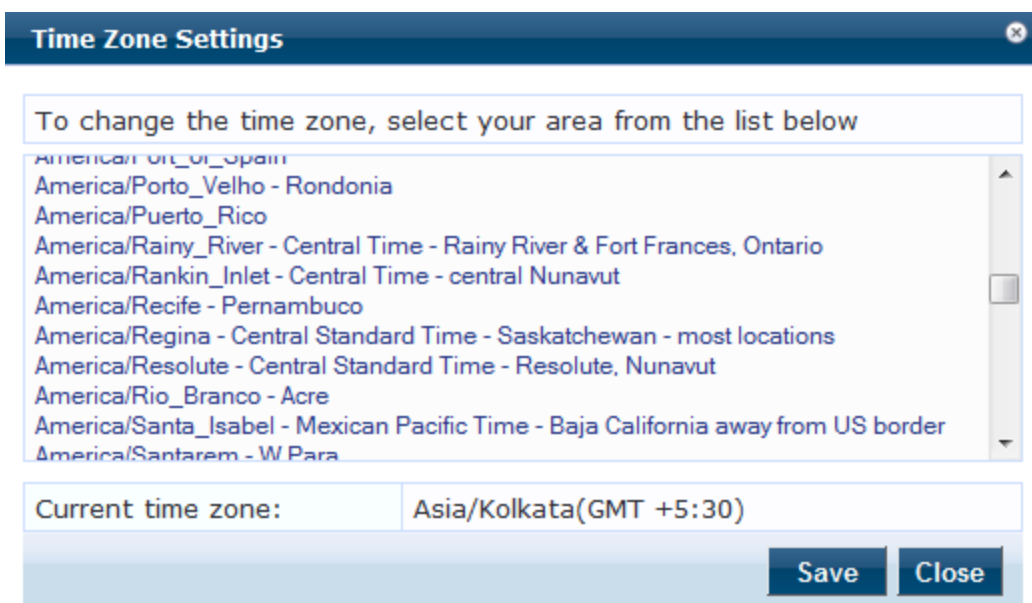
The **Server Configuration** pop-up contains the following tabs:

- [System Tab on page 462](#)
- [Services Control Tab on page 469](#)
- [Service Parameters Tab on page 470](#)
- [System Monitoring Tab on page 486](#)
- [Network Tab on page 487](#)
- [FIPS Tab on page 494](#)

Setting Date and Time

Use the **Set Time Zone** link at the top-right corner of the **Server Configuration (Administration > Server Manager > Server Configuration)** page to set the date and time specific to the selected node in a cluster. To set the date and time, select a time zone from the areas listed. The selected time zone is displayed in the **Current time zone** field. The following figure displays the **Time Zone Settings** pop-up:

Figure 456: Time Zone Settings



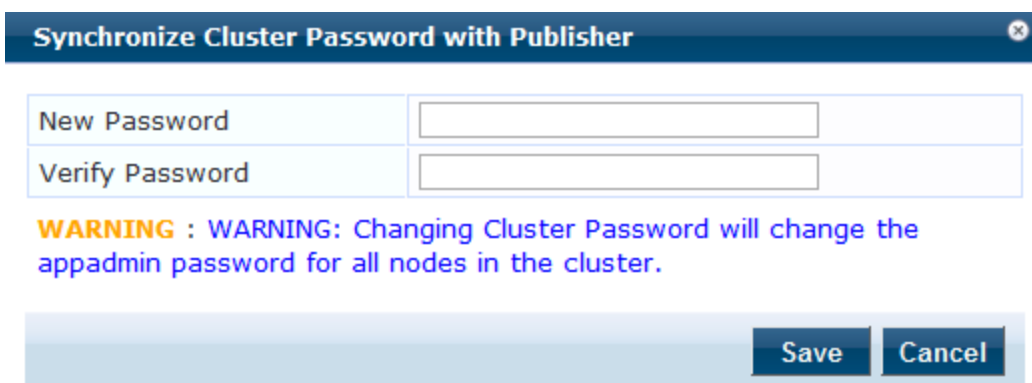
The 'Time Zone Settings' dialog box has a dark blue title bar with a close button. Below the title bar is a light blue instruction box: 'To change the time zone, select your area from the list below'. This is followed by a scrollable list of time zones, including 'America/Porto_Velho - Rondonia', 'America/Puerto_Rico', 'America/Rainy_River - Central Time - Rainy River & Fort Frances, Ontario', 'America/Rankin_Inlet - Central Time - central Nunavut', 'America/Recife - Pernambuco', 'America/Regina - Central Standard Time - Saskatchewan - most locations', 'America/Resolute - Central Standard Time - Resolute, Nunavut', 'America/Rio_Branco - Acre', 'America/Santa_Isabel - Mexican Pacific Time - Baja California away from US border', and 'America/Santarem - W Para'. Below the list is a section with 'Current time zone:' and 'Asia/Kolkata(GMT +5:30)'. At the bottom right are 'Save' and 'Close' buttons.

Synchronizing Cluster Password

Use the **Synchronize Cluster Password** link to synchronize the password of the selected node with cluster. Synchronizing the cluster password will change the appadmin password for all the nodes in the cluster.

The following figure displays the **Synchronize Cluster Password with Publisher** pop-up:

Figure 457: Synchronize Cluster Password with Publisher

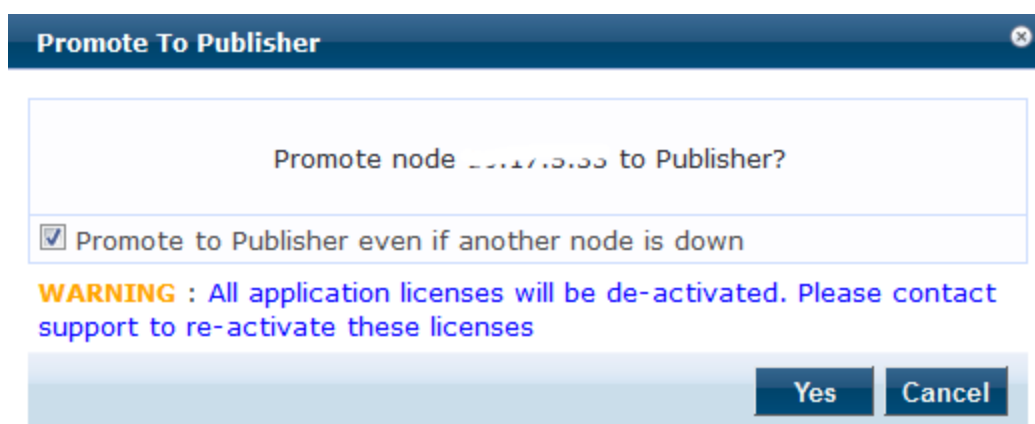


The 'Synchronize Cluster Password with Publisher' dialog box has a dark blue title bar with a close button. Below the title bar are two input fields: 'New Password' and 'Verify Password'. Below these fields is a warning message in orange and blue text: 'WARNING : WARNING: Changing Cluster Password will change the appadmin password for all nodes in the cluster.' At the bottom right are 'Save' and 'Cancel' buttons.

Promoting to Publisher

Use the **Promote To Publisher** link to promote the selected node as a publisher node. You can enable this node as a publisher node using any other active node which is part of the same cluster. All application licenses will be de-activated and you need to contact support to re-activate these licenses. The following figure displays the **Promote To Publisher** pop-up:

Figure 458: *Promote to publisher*



Joining a Server Back to Cluster

Use the **Join server back to cluster** link to join server back to cluster. You can use this option only to a server that is in the **Disabled** state in the **Server Configuration (Administration > Server Manager > Server Configuration)** page.

The following figure displays the **Server Configuration** page:

Figure 459: *Server Configuration Page with Disabled Node*

Administration > Server Manager > Server Configuration
Server Configuration

- Set Date & Time
- Change Cluster Password
- Manage Policy Manager Zones
- NetEvents Targets
- Virtual IP Settings
- Clear Machine Authentication Cache
- Cluster-Wide Parameters

Publisher Server: vm-69 [10.17.5.69]

#	Server Name ▲	Management Port	Data Port	Zone	Profile	Cluster Sync	Last Sync Time
1.	vm-65	10.17.5.55	-	default	Enabled	Disabled	Jan 16, 2015 14:08:28 IST
2.	vm-66	10.17.5.56	-	default	Enabled	Enabled	Jan 16, 2015 14:26:29 IST
3.	vm-69	10.17.5.69	-	default	Enabled	Enabled	-

Showing 1-3 of 3

Collect Logs Backup Restore Cleanup Shutdown Reboot Drop Subscriber

For more information on the **Service Configuration**, see [Server Configuration on page 457](#).



The users with Admin access only can join a server back to cluster.

To join a server back to the cluster, use the following steps:

1. Select a subscriber node which is in **Disabled** state. The **Server Configuration – System** tab opens.

Figure 460: Server configuration - Join server back to cluster

Administration » Server Manager » Server Configuration - vm-69
Server Configuration - vm-69 (10.17.5.69)

- Set Time Zone
- Synchronize Cluster Password
- Promote To Publisher
- Join server back to cluster

System	Services Control	Service Parameters	System Monitoring	Network	FIPS
Hostname: vm-69					
FQDN:					
Policy Manager Zone: default Manage Policy Manager Zones					
Enable Profile: ☒ Enable this server for endpoint classification					
Enable Performance Monitoring Display: ☐ Enable this server for performance monitoring display					
Insight Setting: ☒ Enable Insight					
Span Port: -- None --					
		IPv4	IPv6	Action	
Management Port	IP Address	10.17.5.69		Configure	
	Subnet Mask	255.255.255.0			
	Default Gateway	10.17.5.1			
Data/External Port	IP Address			Configure	
	Subnet Mask				
	Default Gateway				
	Primary	10.17.5.10			

- Click the **Join server back to cluster** link at the top-right corner. A warning message appears with a prompt to promote the node to 'Publisher'. This option can only be triggered from a node that is currently active in the cluster. The following message displays the warning message:

Figure 461: Join server back to cluster

Join server back to cluster

Join server 10.17.5.69 back to cluster?

☐ Promote to Publisher?

WARNING : All data that is not synced from the failed publisher will be lost (like new guest accounts that does not exist in current running publisher).

- Click **Yes** from the warning message pop-up. A progress indicator shows the progress with log entries.

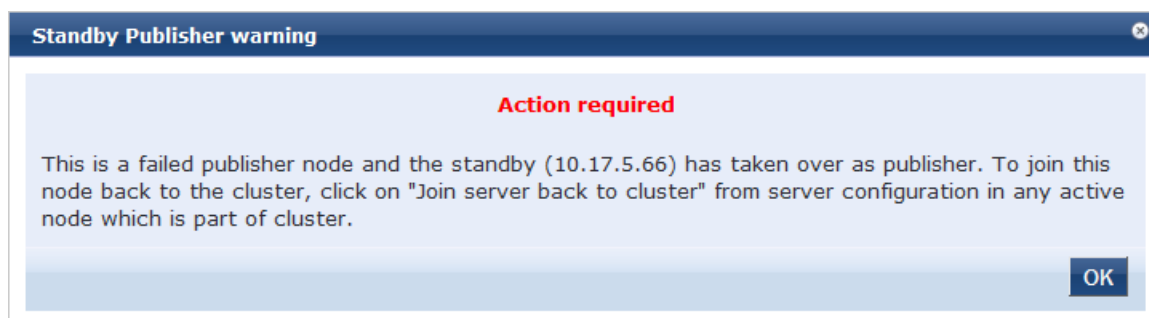
The following figure displays the Join server back to cluster progress indicator:

Figure 462: *Join server back to cluster - Progress*



4. For a failed publisher node, the following message will be displayed in the **Dashboard** page:

Figure 463: *Publisher Warning Message*



System Tab

By default, the **Server Configuration** page opens on the **System** tab.

Figure 464 displays the **Server Configuration > System** dialog:

Figure 464: *Server Configuration > System Dialog*

Administration » Server Manager » Server Configuration - NIGHTLY-CPPM-31
Server Configuration - NIGHTLY-CPPM-31 (10.2.51.18)

System | Services Control | Service Parameters | System Monitoring | Network | FIPS

Hostname: NIGHTLY-CPPM-31
 FQDN:
 Policy Manager Zone: default [Manage Policy Manager Zones](#)
 Enable Profile: ☒ Enable this server for endpoint classification
 Enable Performance Monitoring Display: ☒ Enable this server for performance monitoring display
 Insight Setting: ☒ Enable Insight ☒ Enable as Insight Master Current Master: NIGHTLY-CPPM-31(10.2.51.18)
 Enable Ingress Events Processing: ☒ Enable Ingress Events processing on this server
 Span Port: -- None --

	IPv4	IPv6	Action
Management Port	IP Address	10.2.51.31	Configure
	Subnet Mask	255.255.255.0	
	Default Gateway	10.2.51.1	
Data/External Port	IP Address	10.2.51.1	Configure
	Subnet Mask		
	Default Gateway		
DNS Settings	Primary	10.2.51.18	Configure
	Secondary		
	Tertiary		

AD Domains: [Join AD Domain](#)

Domain Controller	NetBIOS Name	Password Servers	Action
1. CPATS.AVENDASYS.COM	CPATS	-	Leave AD Domain

describes the **System** dialog parameters:

Table 257: *Server Configuration > System Dialog Parameters*

Parameter	Action/Description
Hostname	1. Specify the hostname of W-Policy Manager server. NOTE: You need not enter the fully qualified domain name in this field.
FQDN	2. Enter the Fully-Qualified Domain Name (FQDN) of the W-Policy Manager server.
Policy Manager Zone	3. To add or delete zones, select a previously configured zone from the drop-down list, then click the Policy Manager Zones link. For more information on adding or deleting zones, see Managing Policy Manager Zones .
Enable Profile	4. To enable the W-Policy Manager server to perform endpoint classifications, select the Enable Profile check box.
Enable Performance Monitoring	5. To enable the W-ClearPass Policy Manager server to perform performance monitoring, select the Enable Performance Monitoring check box.
Insight Setting	6. To enable the Insight reporting tool on this node, select the Enable Insight check box. NOTE: - When you enable this check box for Insight on a node in a cluster, the [Insight Repository] configuration is updated automatically to point to the management IP address of that server. - When this check box is enabled for other servers in the cluster, they are added as backups for the same authentication source. - The order of the primary and backup servers in the [Insight Repository] is the same order in which the user enables Insight on the server.

Table 257: *Server Configuration > System Dialog Parameters (Continued)*

Parameter	Action/Description
Enable Ingress Events Processing	7. Check this check box to enable ingress events processing on this server. For more information, see Configuring Processing for Ingress Events .
Enable as Insight Master	8. To specify the current server in a cluster as an Insight Master, select this check box. NOTE: This option is available only when Insight Setting > Enable Insight is enabled.
Span Port	9. If necessary, select a port for DHCP spanning. On selecting a port, the Enable TCP/ARP Fingerprinting check box appears. This field is optional.
Enable TCP/ARP Fingerprinting	10. To enable TCP/ARP fingerprinting, select the Enable TCP/ARP Fingerprinting check box. This feature allows the Netbridge service to capture TCP and ARP packets and post the derived inputs to the Device Profiler. NOTE: This option appears only when you specify a Span Port .
Management Port	11. To configure the Management Port parameters, click Configure . The Configure Management Port dialog opens. For details, see Management Port Configuration on page 464 .
Data/External Port	12. To configure the Data/External port, click Configure . For details, see Data/External Port Configuration on page 465 .
DNS Settings	13. To configure the DNS settings, click Configure . For details, see DNS Settings Configuration on page 465 .
AD Domains	Displays a list of the joined Active Directory domains. 14. To join an active directory domain, click Join Domain . For details on joining an AD domain, see Join AD Domain Configuration on page 466

Management Port Configuration

To configure the W-ClearPass server's Management port:

1. From the **Server Configuration** page > **System** tab > **Management Port**, click **Configure**.

The **Configure Management Port** dialog opens.

Figure 465: *Configure Management Port Dialog*

Configure Management Port

Select IP version: ☒ IPv4 ☐ IPv6

IP Address: 10.

Subnet Mask: 255.255.255.0

Default Gateway: 10. .1

WARNING: Changing IP details might cause system to lose network connectivity and require relogin. Save Server Configuration page for changes to take effect

Update Cancel

2. **Select IP Version:** Select the IP version—**IPv4** or **IPv6**.
3. **IP Address:** Specify the IP address (IPv4 or IPv6) to access the W-ClearPass Policy Manager.
4. **Subnet Mask:** Specify the management interface subnet mask for an IPv4 address.
IPv6 addresses do not require a netmask as they use Classless Inter-Domain Routing (CIDR).
5. **Default Gateway:** Specify the default gateway for the management interface.
6. Click **Update**.

Data/External Port Configuration

To configure the W-ClearPass server's Data/External port:

1. From the **Server Configuration** page > **System** tab > **Data/External Port**, click **Configure**.
The **Configure Data/External Port** dialog opens.

Figure 466: *Configure Data/External Port Dialog*

Configure Data/External Port	
Select IP version	☒ IPv4 ☐ IPv6
IP Address:	
Subnet Mask:	
Default Gateway:	
WARNING: Changing IP details might cause system to lose network connectivity and require relogin. Save Server Configuration page for changes to take effect	
Update Cancel	

2. **Select IP Version:** Select the IP version—**IPv4** or **IPv6**.
3. **IP Address:** Specify the IP address (IPv4 or IPv6) of the W-ClearPass server's data interface.
4. **Subnet Mask:** Specify the data interface subnet mask for an IPv4 address.
IPv6 addresses do not require a netmask as they use Classless Inter-Domain Routing (CIDR).
5. **Default Gateway:** Specify the default gateway for the data interface.
6. Click **Update**.

DNS Settings Configuration

To configure the W-ClearPass server's Data/External port:

1. From the **Server Configuration** page > **System** tab > **DNS Settings**, click **Configure**.
The **Configure DNS Setting** dialog opens.

Figure 467: *Configure DNS Settings Dialog*

Configure DNS Settings	
Primary:	10.1.10.10
Secondary:	10.2.51.106
Tertiary:	
Note: Save Server Configuration page for changes to take effect	
Update Cancel	

2. **Primary:** Specify the primary DNS server for name look-up.



A DNS server can be primary for one domain and secondary for another. Only one DNS server should be configured as primary for a domain, but you can have any number of secondary DNS servers.

3. **Secondary:** Specify one or more secondary DNS servers for name look-up.



The recommended practice is to configure the primary and secondary DNS servers on separate machines, on separate Internet connections, and in separate geographic locations.

4. **Tertiary:** Optionally, in the rare event of both the primary and secondary DNS servers going down, you can configure a tertiary DNS server.
5. Click **Update**.

Join AD Domain Configuration

To join the selected W-ClearPass server to an Active Directory domain:

1. Click **Join AD Domain**.

The **Join AD Domain** dialog opens.

Figure 468: *Join AD Domain Dialog*

Join AD Domain

Enter the FQDN of the controller and the short (NETBIOS) name for the domain:

Domain Controller

NetBIOS Name

In case of a controller name conflict

☒ Use specified Domain Controller

☐ Use Domain Controller returned by DNS query

☐ Fail on conflict

☒ Use default domain admin user [Administrator]

Username

Password

Save Cancel

2. **Domain Controller:** Enter the Fully Qualified Domain Name (FQDN) of the domain controller, then press **Tab**.

The following message is displayed: *Trying to determine the NetBIOS name...*

W-ClearPass searches for the NetBIOS name for the domain.



NetBIOS is another term for the short domain name, or the NT4 domain name, also known as the pre-Windows 2000 domain name.

If W-ClearPass determines the NetBIOS name, the **NetBIOS Name** field is automatically populated.

3. **In case of a controller name conflict:**
- Use specified Domain Controller:** Accept the default setting.
 - Use default domain admin user [Administrator]:** Accept the default setting.



In a production environment, it is likely that an Administrative username that has permissions to join machines to the domain would be used for the default domain admin user. In that case, 1) disable (uncheck) the **Use default domain**

admin user [Administrator] check box and 2) enter the Administrative username and password in the fields provided.

- c. **Password:** Enter the password for the user account that will join W-ClearPass with the domain, then click **Save**.

The **Join AD Domain** status screen opens. The screen displays the message *"Adding host to AD domain,"* and the screen displays status during the joining process.

When the joining process completes successfully, you see the message *"Added host to the domain."*

4. Click **Close**.

You return to the **Server Configuration** page, and it now shows that the W-ClearPass server is joined to the domain.

Now that the W-ClearPass Policy Manager server has joined the domain, the server can authenticate users with Active Directory.

After an Active Directory Domain is added, the domain controller can be setup as a password server. For more information on adding a password server, see [Add Password Server on page 469](#).

Join AD Domain

You can join W-ClearPass Policy Manager to an Active Directory (AD) domain to authenticate users and computers that are members of an Active Directory domain. If you join W-ClearPass to an Active Directory domain, it creates a computer account for the W-ClearPass node in the Active Directory database.

Users can then authenticate into the network using 802.1X and EAP methods, such as PEAP-MSCHAPv2, with their own their own AD credentials.

If you need to authenticate users belonging to multiple Active Directory forests or domains in your network, and there is no trust relationship between these entities, then you must join W-ClearPass to each of these untrusted forests or domains.



W-ClearPass does not require to join multiple domains belonging to the same Active Directory forest because a one-way trust relationship exists between those domains. In this case, W-ClearPass can join the root domain.

W-ClearPass can join or leave an Active Directory domain by using the following two buttons in the **System** tab of the **Server Configuration** page:

- **Join Domain**—Click **Join Domain** to join this W-ClearPass appliance to an Active Directory domain. Password servers can be configured after W-Policy Manager is successfully joined. For more information on adding a password server, see [Add Password Server on page 469](#).
- **Leave Domain**— If the server is already part of multiple Active Directory domains, click **Leave Domain** to disassociate this W-ClearPass appliance from an Active Directory domain.



For most use cases, if you have multiple nodes in the cluster, you must join each node to the same Active Directory domain.

The following figure displays the **Join AD Domain** window:

Figure 469: *Join AD Domain*

The following table describes the **Join AD Domain** parameters:

Table 258: *Join AD Domain Parameters*

Parameter	Action/Description
Domain Controller	Enter the fully qualified name of the Active Directory domain controller.
NETBIOS name (optional)	Enter the 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 Active Directory administrator about the NetBIOS name. NOTE: If you enter an incorrect value for the NetBIOS name, you see a warning message in the user interface. 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 correct NetBIOS name.
Domain Controller name conflict	Specify the action to take in the event of a domain controller name conflict. 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 can: • Use specified Domain Controller: Continue to use the domain controller name that you entered. • Use Domain Controller returned by DNS query: Use the domain controller name returned by the DNS query. • Fail on conflict: Abort the Join Domain operation.
Use default domain admin user	Check this box to use the Administrator user name to join the domain
Username	Enter the user ID of the domain administrator account. This field is disabled if the Use default domain admin user checkbox is selected.
Password	Enter the password of the domain administrator account.

Add Password Server

After W-ClearPass successfully joins an Active Directory domain, you can configure a restricted list of domain controllers to be used for MSCHAP authentication. If this is not configured, then all available domain controllers obtained from DNS will be included.

To add a password server:

1. In the **AD Domains** section of the **System** tab, click the Add Password Server icon . This icon appears only after W-ClearPass joins at least one Active Directory domain (see [Figure 470](#)).

Figure 470: Add Password Server icon

AD Domains:				Join AD Domain
Domain Controller	NetBIOS Name	Password Servers	Action	
1 AMG-AD.LOCALDOMAIN.COM	AMG-AD	-		Leave AD Domain

The **Configure AD Password Servers** page opens.

2. Specify the domain name, NetBIOS Name, and the password servers.

The password servers can be a hostname or an IP address. Use a new line for each entry.

3. Click **Save** to complete adding the password servers.

The following figure displays the **Configure AD Password Servers** dialog with the password servers added to the configuration:

Figure 471: AD Password Serves Added

Configure AD Password Servers

Configure a restricted list of domain controllers to be used for MSCHAP authentication if desired. All available domain controllers would be included otherwise

Domain Controller:	AMG-AD.LOCADOMAIN.COM
NetBIOS Name:	AMG-AD
Password Servers:	10.2.100.120 1.1.1.1

Note: Enter Hostname or IP Address in the Password Servers textbox, one entry per line

Reset Save Cancel

Services Control Tab

From the **Services Control** tab, you can view a service status and control (stop or start) various Policy Manager services, including any AD Domains that the server joins.

The following figure displays the Services Control tab:

Figure 472: Services Control Tab

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

[Back to Server Configuration](#)
Save Cancel

Service Parameters Tab

Navigate to the **Administration > Server Manager > Server Configuration > Service Parameters** page to change system parameters of the services listed below.

This section describes the following topics:

- [Async Network Services Options on page 471](#)
- [W-ClearPass IPsec Service on page 472](#)
- [W-ClearPass Network Services Options on page 472](#)
- [W-ClearPass System Services Options on page 475](#)
- [Ingress Logger Service on page 478](#)
- [Policy Server Options on page 479](#)
- [RADIUS Server Options on page 480](#)
- [Stats Collection Service Options on page 484](#)
- [System Monitor Service Options on page 484](#)
- [TACACS Server Options on page 485](#)

The following figure displays the **Service Parameters** page:

Figure 473: Service Parameters Page

System	Services Control	Service Parameters	System Monitoring	Network	FIPS
Select Service: Policy server					
Parameter Name		Parameter Value		Default Value	Allowed Values
Machine Authentication Cache Timeout		24	hours	24	0-1000
LDAP Primary Retry Interval		600	seconds	600	0-864000
External Posture Server Thread Pool Size		5	threads	5	5-40
External Posture Server Primary Retry Interval		600	seconds	600	0-864000
Audit SPT Default Timeout		600	seconds	600	1-86400
Additional time before session deletion from multi-master cache		0	seconds	0	0-864000
Number of request processing threads		16	threads	16	1-200
HTTP Thread Pool Size		32	threads	32	1-200
Authentication Thread Pool Size		32	threads	32	1-200

[Back to Server Configuration](#)
Save Cancel

Async Network Services Options

Configure the **Ingress Event**, **Command Control**, and **Post-Auth** parameters for the Async network service.

The following figure displays the **Service Parameters > Async network services** parameters:

Figure 474: Async Network Services

System	Services Control	Service Parameters	System Monitoring	Network	FIPS
Select Service: Async network services					
Parameter Name		Parameter Value	Default Value	Allowed Values	
Ingress Event					
Batch Processing Interval		30 seconds	30	10-300	
Command Control					
CoA Delay		2 seconds	2	0-15	
Enable SNMP Bounce Action		FALSE	FALSE		
Post Auth					
Number of request processing threads		20 threads	20	20-100	
Lazy handler polling frequency		5 minutes	5	3-10	
Eager handler polling frequency		30 seconds	30	3-300	
Send Posture Data		FALSE	FALSE		
Connection Timeout		10 seconds	10	10-300	

Enter the **Service Parameters > Async Network Services** parameters as described in [Table 259](#)

Table 259: Service Parameters > Async Network Services

Parameter	Action/Description
Ingress Event	
Batch Processing Interval	Specify the batch processing interval for ingress event processing. The default interval is 30 seconds. The range of values is 10 to 300 seconds. NOTE: For changes to the Batch Processing Interval to take effect, you must restart the Async Network service.
Post Auth	
Number of request processing threads	Set the number of request processing threads. The default value is 20 threads, and the range of values is between 20 and 100 .
Lazy handler polling frequency	Set the Lazy handler polling frequency (in minutes). The default value is 5 minutes, and the allowed values are from 3 to 10 minutes. Lazy handler polling is employed when an attribute may not require to be updated unless it explicitly asks for it. When it is required, even if there is no available fresh value, it can be fetched by initiating a separate request.
Eager handler polling frequency	Set the Eager handler polling frequency (in seconds). The default value is 30 seconds, and the allowed values are from 10 to 300 seconds. Eager handler polling is employed when an attribute requires the freshest possible value.
Send Posture Data	To send posture data to the Palo Alto Firewall server, set this to TRUE .

Table 259: *Service Parameters > Async Network Services (Continued)*

Parameter	Action/Description
Command Control	
CoA Delay	Set the CoA Delay value (in seconds). The default value is 2 , and the allowed values are from 0 to 15 seconds.
Enable SNMP Bounce Action	Set the Enable SNMP Bounce Action value. The default value is FALSE .

W-ClearPass IPsec Service

When a network device requests an IPsec connection between the device and a W-ClearPass server, W-ClearPass uses the Online Certificate Status Protocol (OCSP) URI specified in [Figure 475](#) to contact a third-party server that checks to see if the certificate sent by the requesting device is valid.

If the certificate is confirmed as valid, an IPsec connection between the W-ClearPass server and the requesting network device is established.

To configure the W-ClearPass IPsec service:

1. Navigate to **Administration > Server Manager > Server Configuration**, then select the W-ClearPass server.
2. Select the **Service Parameters** tab.
3. From the **Select Service** drop-down, select **W-ClearPass IPsec service**.

The following dialog opens:

Figure 475: *W-ClearPass IPsec Service Dialog*

Parameter Name	Parameter Value	Default Value	Allowed Values
OCSP URI			

4. Specify the **Service Parameters > W-ClearPassIPsec Service** parameter as described in [Table 260](#), then click **Save**.

Table 260: *Service Parameters > W-ClearPass IPsec Service*

Parameter	Action/Description
OCSP URI	In the Parameter Value field, specify the HTTP or HTTPS URL for the Online Certificate Status Protocol (OCSP) URI. OCSP enables the W-ClearPass server to determine the revocation state of a certificate presented by a peer—for example a network device requesting an IPsec connection to the W-ClearPass server.

W-ClearPass Network Services Options

The **W-ClearPass Network Services** parameters aggregate service parameters from the following services:

- SNMP Service
- Certificate Authentication Service
- Web Authentication Service

- Posture Service
- DHCP Snooper Service

The following figure displays the **Service Parameters** tab > **W-ClearPass Network Services** parameters (partial view):

Figure 476: *Service Parameters > W-ClearPass Network Services*

Parameter Name	Parameter Value	Default Value	Allowed Values
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 MAC Threshold	5	5	0-20
SNMP v2c Trap Community		public	
SNMP v3 Trap Username	shaaes128	aruba	
SNMP v3 Trap Authentication Protocol	SHA		
SNMP v3 Trap Privacy Protocol	AES_128		
SNMP v3 Trap Authentication Key			
SNMP v3 Trap Privacy Key			
Device Info Poll Interval	60 minutes	60	10-1500
Certificate Auth			
OCSP Check	None	None	
WebAuthService			
Max time to determine network device where client is connected	0 seconds	0	0-100
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

The following figure displays the **Service Parameters** tab > **W-ClearPass Network Services** parameters in FIPS mode:

Figure 477: *Service Parameters > W-ClearPass Network Services in FIPS Mode*

Parameter Name	Parameter Value	Default Value	Allowed Values
DhcpSnooper			
MAC to IP Request Hold time	120 seconds	120	60-300
DHCP Request Probation Time	30 seconds	30	10-60
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	aruba	aruba	
SNMP v3 Trap Authentication Protocol	SHA		
SNMP v3 Trap Privacy Protocol			
SNMP v3 Trap Authentication Key			
SNMP v3 Trap Privacy Key			
Device Info Poll Interval	60 minutes	60	10-1500

Specify the **W-ClearPass Network Services** parameters as described in the following table:

Table 261: *Service Parameters > W-ClearPass Network Services*

Service Parameters	Action/Description
SnmpService	
SNMP Timeout	Specify the seconds to wait for an SNMP response from the network device.
SNMP Retries	Specify the number of retries for SNMP requests.
LinkUp Timeout	Specify the seconds to wait before processing link-up traps. If a MAC notification trap arrives in this time, the SNMP service does not try to poll the switch for MAC addresses behind a port for link-up processing.
IP Address Cache Timeout	Specify the duration in seconds for which MAC-to-IP lookup response is cached.
Uplink Port Detection Threshold	Specify the 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. The default value is 5 , with a range from 0 to 20 .
SNMP v2c Trap Community	Specify the community string that must be checked in all incoming SNMP v2 traps.
SNMP v3 Trap Username	Specify the SNMP v3 Username to be used for all incoming traps.
SNMP v3 Trap Authentication Protocol	Specify the SNMP v3 Authentication protocol for traps. The options are: MD5 , SHA , or empty (to disable authentication). NOTE: The EAP-MD5 authentication type is not supported if you use W-ClearPass Policy Manager in FIPS mode.
SNMP v3 Trap Privacy Protocol	Specify the SNMP v3 Privacy protocol for traps. The options are: DES_CBC , AES_128 , or empty (to disable privacy). NOTE: The DES_CBC privacy protocol is not supported if you use W-ClearPass Policy Manager in FIPS mode.
SNMP v3 Trap Authentication Key	Specify the SNMP v3 authentication key and privacy key for incoming traps.
SNMP v3 Trap Privacy Key	
Device Info Poll Interval	Specify the time (in minutes) between polling for device information.
Certificate Auth	

Table 261: *Service Parameters > W-ClearPass Network Services (Continued)*

Service Parameters	Action/Description
OCSP Check	Specify one of the following options for initiating an Online Certificate Status Protocol (OCSP) check: • None (the default setting) • Optional • Required
WebAuthService	
Max time to determine network device where client is connected	Specifies the maximum time to wait for W-Policy Manager to determine the network device to which the 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 connected through an out-of-band SNMP mechanism. The network device deduction process can take some time.
PostureService	
Audit Thread Pool Size	Specify the number of threads to use for connections to audit servers.
Audit Result Cache Timeout	Specify the time (in seconds) for which audit result entries are cached by W-Policy Manager.
Audit Host Ping Timeout	Specify the number of seconds for which W-Policy Manager pings an end-host before giving up and deeming the host to be unreachable.
DhcpSnooper	
MAC to IP Request Hold time	Specify the number of seconds to wait before responding to a query to get an IP address corresponding to a MAC address. Any DHCP message received in this time period refreshes the MAC address-to-IP address binding. Typically, an audit service requests a MAC-to-IP mapping as soon the RADIUS request is received, but the client may take some more time to receive the IP address through DHCP. This wait period takes into account the latest DHCP IP address that the client received.
DHCP Request Probation Time	Specify the number of seconds to wait before considering the MAC-to-IP binding received in a DHCPREQUEST message as final. This wait handles cases where a client receives a DHCPNAK for a DHCPREQUEST and receives a new IP address after going through the DHCPDISCOVER process again.

W-ClearPass System Services Options

You can use the W-ClearPass system service parameters for PHP configuration and for HTTP traffic flowing through a proxy server.

W-ClearPass Policy Manager relies on an HTTP connection for the W-ClearPass Update Portal to download the latest information for system services.

The following figure displays the **Service Parameters > W-ClearPass System Services** parameters (partial view):

Figure 478: *W-ClearPass System Services Parameters*

Parameter Name	Parameter Value	Default Value	Allowed Values
PHP System Configuration			
Memory Limit	256 Megabytes	256	256-1024
Form POST Size	15 Megabytes	15	1-256
File Upload Size	15 Megabytes	15	1-256
Input Time	60 seconds	60	0-600
Socket Timeout	60 seconds	60	5-600
Enable zlib output compression	FALSE	FALSE	
Include PHP header in web server response	TRUE	TRUE	
TCP Keep Alive Configuration			
Keep Alive Time	7200 seconds	7200	10-86400
Keep Alive Interval	75 seconds	75	1-3600
Keep Alive Probes	9	9	1-100
Database Configurations			
Maximum Connections	700	700	300-2000
HTTP Proxy			
Proxy Server			
Port	3128	3128	1-65535
Username			
Password			
Web Server Configuration			
Timeout	20 seconds	20	1-60

Specify the **Service Parameters > W-ClearPass System Services** parameters as described in the following table.

Table 262: *Service Parameters > W-ClearPass System Services*

Service Parameter	Action/Description
PHP System Configuration	
Memory Limit	Specify the maximum memory that can be used by the PHP applications.
Form POST Size	Specify the maximum HTTP POST content size that can be sent to the PHP application.
File Upload Size	Specify the maximum file size that can be uploaded into the PHP application.
Input Time	Specify the time limit after which the server will detect no activity from the user and will take some action.
Socket Timeout	Specify the maximum time for any socket connections.
Enable zlib output compression	Specify the setting to compress the output files.
Include PHP header in web server response	Specify the setting to include PHP header in the HTTP responses.

Table 262: *Service Parameters > W-ClearPass System Services (Continued)*

Service Parameter	Action/Description
HTTP Proxy	
Proxy Server	Specify the hostname or IP address of the proxy server.
Port	Specify the port at which the proxy server listens for HTTP traffic.
Username	Specify the user name to authenticate with the proxy server.
Password	Specify the password to authenticate with the proxy server.
Database Configuration	
Maximum connections	Specify a number between 300 and 2000 for a maximum number of allowed connections.
TCP Keepalive Configurations	
Keep Alive Time	Specify a value in seconds from 10 to 86400.
Keep Alive Interval	Specify a value in seconds from 1 to 3600.
Keep Alive Probes	Specify a value from 1 to 100 for the number of probes.
Web Server Configuration	
Maximum Clients	Specify a value from 10 to 20000 for the maximum number of clients allowed.
Timeout	Specify a server timeout value in seconds from 1 to 60.
Keep Alive	To enable or disable keep-alive for the web server, select TRUE or FALSE .
Request Wait	Specify the request wait time in seconds from 1 to 60. The default value is 4 seconds.

Table 262: Service Parameters > W-ClearPass System Services (Continued)

Service Parameter	Action/Description
Maximum Requests	Specify a number between 0 and 3000 for the maximum number of requests allowed. The default value is 500 .
Enable Host Header check	Specify whether to enable the host header check. The default value is TRUE . - When you set this value to TRUE, the Host Header Restriction check is enabled and only the allowed or whitelisted host headers are allowed. - When you set this value to FALSE, irrespective of Host Headers in the http packet, W-ClearPass Policy Manager redirects to <a href="https://<W-ClearPass-server>/tips">https://<W-ClearPass-server>/tips.
WhiteList Host Names	When the Enable Host Header check value is set to TRUE , the web access is allowed for Whitelist Host Names, hostnames, IP addresses, and VIP addresses in W-ClearPass Policy Manager. The comma separated whitelist host names are allowed to support multiple hostnames. When the Enable Host Header check value is set to TRUE and the WhiteList Host Names field is blank, the web access is allowed only for hostnames, IP addresses, and VIP addresses in W-ClearPass Policy Manager.

Ingress Logger Service

When Ingress Event Processing is enabled and configured on W-ClearPass (see [Configuring Processing for Ingress Events on page 677](#)), logging of ingress events occurs automatically.

By default, the W-ClearPass server listens for Ingress Events on **TCP port 514** and **UDP port 514**.

If necessary, you can change these Syslog Ingress Logger ports. To do so:

1. Navigate to **Administration > Server Manager > Server Configuration**, then select the W-ClearPass server.
2. Select the **Service Parameters** tab.
3. From the **Select Service** drop-down, select **Ingress Logger Service**.

The following dialog opens:

Figure 479: Ingress Logger Service Dialog

Parameter Name	Parameter Value	Default Value	Allowed Values
Syslog Configuration			
TCP Port	514	514	1-65535
UDP Port	514	514	1-65535

4. To change the Ingress Logger **TCP Port**, enter the new port number in the **Parameter Value** field.
5. To change the Ingress Logger **UDP Port**, enter the new port number.
6. Click **Save**.

Policy Server Options

The following figure displays the **Service Parameters > Policy Server** dialog:

Figure 480: Policy Server Service Parameters

Parameter Name	Parameter Value	Default Value	Allowed Values
Machine Authentication Cache Timeout	24 hours	24	0-1000
LDAP Primary Retry Interval	600 seconds	600	0-864000
External Posture Server Thread Pool Size	5 threads	5	5-40
External Posture Server Primary Retry Interval	600 seconds	600	0-864000
Audit SPT Default Timeout	600 seconds	600	1-86400
Additional time before session deletion from multi-master cache	0 seconds	0	0-864000
Number of request processing threads	16 threads	16	1-200
HTTP Thread Pool Size	32 threads	32	1-200
Authentication Thread Pool Size	32 threads	32	1-200

Specify the **Service Parameters > Policy Server** parameters.

Table 263: Service Parameters > Policy Server Service

Service Parameter	Action/Description
Machine Authentication Cache Timeout	1. Specify the time (in hours) for which machine authentication entries are cached by W-ClearPass Policy Manager. The default is 24 hours .
LDAP Primary Retry Interval	After a primary LDAP server is down, the W-ClearPass server connects to one of the backup servers. 2. Specify how long the W-ClearPass server waits (in seconds) before it tries to connect to the primary server again.
Audit SPT Default Timeout	3. Specify the time (in seconds) for which an Audit success or error response is cached in the Policy server.
Additional time before session deletion from multi-master cache	4. Specify the number of seconds the Policy server will wait before deleting the multi-master entry. The default value is 0 . This parameter handles roaming scenarios where an Accounting-Start occurs without an authentication request. If the value for this parameter is 0 , the Policy server deletes the multi-master entry when an Accounting-Stop is received. The RADIUS server updates the multi-master entry with attribute values from the accounting request. These can be used in the Change of Authorization (CoA). In a roaming scenario, this NAS information update from the accounting request helps W-ClearPass send the CoA to the correct NAS.
Number of request processing threads	5. Specify the maximum number of threads used to process requests.

Table 263: Service Parameters > Policy Server Service (Continued)

Service Parameter	Action/Description
HTTP Thread Pool Size	6. Specify the number of threads allotted for the HTTP thread pool.
Authentication Thread Pool Size	7. Specify the number of threads to use for LDAP/AD and SQL connections.
	8. Click Save .

RADIUS Server Options

The following figure displays the **Service Parameters** tab > **RADIUS Server** parameters (partial list):

Figure 481: RADIUS Server Parameters Dialog

Administration » Server Manager » Server Configuration - NIGHTLY-CPPM-31

Server Configuration - NIGHTLY-CPPM-31 (10. .)

Parameter Name	Parameter Value	Default Value	Allowed Value
EAP-FAST			
Master Key Expire Time	1 weeks	1 weeks	
Master Key Grace Time	3 weeks	3 weeks	
PACs are valid across cluster	TRUE	TRUE	
Proxy			
Maximum Response Delay	5 seconds	5	1-5
Maximum Reactivation Time	120 seconds	120	60-3600
Maximum Retry Counts	5 retries	5	2-10
Accounting			
Log Accounting Interim-Update Packets	FALSE	FALSE	
Thread Pool			
Maximum Number of Threads	80 threads	80	10-300
Number of Initial Threads	40 threads	40	5-300

Specify the **Service Parameters** > **RADIUS server** parameters as described in the following table:

Table 264: Service Parameters > RADIUS Server Service

Service Parameter	Action/Description
EAP-FAST	
Master Key Expire Time	Specify the lifetime of a generated EAP-FAST master key.
Master Key Grace Time	Specify the grace period for an EAP-FAST master key after its lifetime expires. The default is 3 weeks . If a client presents a PAC (Protected Access Credential) that is encrypted using the master key in this period after its TTL (Time-to-Live), it is accepted and a new PAC encrypted with the latest master key is provisioned on the client.
PACs are valid across cluster	If PACs (Protected Access Credentials) generated by this server are valid across the cluster, set to TRUE (the default setting).

Table 264: *Service Parameters > RADIUS Server Service (Continued)*

Service Parameter	Action/Description
	If not, select FALSE .
Proxy	
Maximum Response Delay	If the target server has not responded, specify the time delay before retrying a proxy request. The default is 5 seconds.
Maximum Reactivation Time	Specify the time to elapse before retrying a dead proxy server.
Maximum Retry Counts	If the target server doesn't respond, specify the maximum number of times to retry a proxy request.
Accounting	
Log Accounting Interim-Update Packets	To store the Interim-Update packets in session logs, select TRUE . FALSE is the default setting.
Thread Pool	
Maximum Number of Threads	Specify the maximum number of threads in the RADIUS server thread pool to process requests.
Number of Initial Threads	Specify the initial number of threads in the RADIUS server thread pool to process requests.
Active Directory Errors	
Window Size	Enter a duration during which Active Directory errors are accumulated for possible action. The default is 5 minutes .
Number of Errors	Enter a number to specify the number of Active Directory errors that can occur within the defined Window Size and have the self-healing Recovery Action taken. The default is 150 .
Recovery Action	Select one of the following recovery actions from the drop-down list: • None: To initiate no self-recovery action. This is the default. • Exit: To restart the RADIUS server. (The monitoring daemon will restart it.) • Restart Domain Service: To restart the Domain service.
Security	
Reject Packet Delay	Specify the delay time before sending an actual RADIUS Access-Reject message after the server decides to reject the request.
Maximum Attributes	Specify the maximum number of RADIUS attributes allowed in a request. The

Table 264: *Service Parameters > RADIUS Server Service (Continued)*

Service Parameter	Action/Description
	default is 200 .
Process Server-Status Request	• TRUE: Send replies to Status-Server RADIUS packets. • FALSE: Do not send replies to Status-Server RADIUS packets. This is the default setting.
Main	
Authentication Port	Specify the ports on which the RADIUS server listens for authentication requests. Default values are ports 1645 and 1812 . NOTE: You can configure the Authentication Port to different values if desired.
Accounting Port	Specify the ports on which the RADIUS server listens for accounting requests. The default values are 1646 and 1813 . NOTE: You can configure the Accounting Port to different values if desired.
Maximum Request Time	Specify the maximum time (in seconds) allowed for processing a request after which it is considered timed out. The default is 30 seconds .
Cleanup Time	Specify the time to cache the response sent to a RADIUS request after sending it. The range is from 2 to 10 seconds. The default is 5 seconds. If the RADIUS server gets a duplicate request for which the response is already sent, and the duplicate request arrives within this time period, the cached response is resent.
Local DB Authentication Source Connection Count	Specify the maximum number of Local DB connections opened.
AD/LDAP Authentication Source Connection Count	Specify the maximum number of Active Directory and LDAP (Lightweight Directory Access Protocol) connections opened. The range is from 5 to 300 . The default is 64 .
SQL DB Authentication Source Connection Count	Specify the maximum number of SQL DB.
Kerberos Authentication Source Connection Count	Specify the maximum number of Kerberos connections opened.
EAP-TLS Fragment Size	Specify the maximum allowed size (in bytes) for the EAP-TLS fragment.
Use Inner Identity in Access-Accept Reply	To use the inner identity in the Access-Accept replies, select TRUE . FALSE is the default setting.
Reject if OSCP response does not have Nonce	To reject an OSCP response without a nonce, select TRUE . Else, select FALSE .

Table 264: *Service Parameters > RADIUS Server Service (Continued)*

Service Parameter	Action/Description
Include Nonce in OCSF request	Specify one of the following: • TRUE: Select if the OCSF (Online Certificate Status Protocol) request should include the nonce. This is the default value. • FALSE: To avoid the EAP-TLS authentication failure, select if the OCSF server does not support the nonce.
Enable signing for OCSF Request	To enable signing for OCSF request, select TRUE . This determines whether W-ClearPass should sign an OCSF request with a RADIUS server certificate. The default value is FALSE .
Check the validity of all certificates in the chain against CRLs	To check the validity of all certificates in the chain against Certificate Revocation Lists (CRLs), select TRUE . Else, select FALSE .
ECDH Curve	Select one of the following ECDH curve (Elliptic Curve Diffie-Helman) options from the drop-down list: • X9.62/SECG curve over a 256-bit prime field • NIST/SECG curve over a 384-bit prime field
Disable TLS 1.2	To disable Transport Layer Security 1.2 (TLS 1.2), select TRUE . FALSE is the default setting—TLS 1.2 is enabled by default.
Check the validity of intermediary certificates in the chain using OCSF	To check the validity of intermediary certificates in the chain using OCSF, select TRUE . The default Online Certificate Status Protocol is FALSE .
Maximum Number of AD Authentication Processes	To specify the maximum number of Active Directory authentication processes, enter a number between 1 and 5 . The default is 1 .
Verify OCSF Signing Purpose	Specify one of the following: • TRUE: EAP-TLS authentication will fail unless the OCSF signing certificate also has the OCSF signing purpose set. • FALSE: The OCSF signing certificate does not need to have the OCSF signing purpose set. This is default setting.
TLS Session Cache Limit	Specify the number of TLS sessions to cache before purging the cache (used in TLS based 802.1X EAP Methods). The range is from 1,000 to 100,000 . The default is 10,000 .

Stats Collection Service Options

The following figure displays the **Service Parameters** tab > **Stats Collection Service** parameters:

Figure 482: Stats Collection Service Parameters

The screenshot shows a configuration window with tabs: System, Services Control, Service Parameters (selected), System Monitoring, Network, and FIPS. Under 'Select Service:', 'Stats collection service' is selected. A table lists parameters for 'Stats Collection':

Parameter Name	Parameter Value
Enable Stats Collection	TRUE

At the bottom, there is a 'Back to Server Configuration' link and 'Save' and 'Cancel' buttons.

The following table describes the **Service Parameters** tab > **Stats Collection Service** parameter:

Table 265: Service Parameters > Stats Collection Service

Service Parameter	Action/Description
Enable Stats Collection	Enable or disable statistics collection and aggregation. The Statistics Collection Service is enabled by default (TRUE). If this is not enabled, statistics collection and aggregation services will not run on the node. In addition, if statistics collection and aggregation is not enabled, the following error message is displayed if the admin attempts to start these services: Failed to start Stats collection service - Ignoring service start request as Stats Collection option is disabled on the node NOTE: Enabling or disabling this parameter requires a restart of the cpass-statsd-server and cpass-carbon-server.

System Monitor Service Options

The following figure displays the **Service Parameters** tab > **System Monitor Service** parameters:

Figure 483: System Monitor Service Parameters

The screenshot shows a configuration window with tabs: System, Services Control, Service Parameters (selected), System Monitoring, and Network Interfaces. Under 'Select Service:', 'System monitor service' is selected. A table lists parameters for 'System Monitor Service':

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

The following table describes the **Service Parameters** tab > **System Monitor Service** parameters:

Table 266: *Services Parameters > System Monitor Service*

Service Parameter	Action/Description
Free Disk Space Threshold	This parameter monitors the available disk space on the current W-ClearPass server node. Specify the Free Disk Space Threshold (the default is 30%). If the available disk free space falls below the specified threshold, the W-ClearPass server sends SNMP traps to the configured trap servers.
1 Min CPU load average Threshold	These parameters monitor the CPU load average of the system, specifying thresholds for 1-minute, 5-minute, and 15-minute averages, respectively. If any of these loads exceed the associated maximum value, the W-ClearPass server sends traps to the configured trap servers.
5 Min CPU load average Threshold	
15 Min CPU load average Threshold	

TACACS Server Options

The **Service Parameters > TACACS Server** dialog provides two parameters:

- TACACS+ Profiles Cache Timeout
- TACACS+ HTTP Thread Pool Size

Figure 484: *Service Parameters > TACACS+ Server Dialog*

Parameter Name	Parameter Value	Default Value
TACACS+ Profiles Cache Timeout	86400 seconds	86400
TACACS+ HTTP Thread Pool Size	100	100

Specify the **Service Parameters > TACACS server** parameters as described in the following table:

Table 267: *Service Parameters > TACACS Server*

Service Parameter	Action/Description
TACACS+ Profiles Cache Timeout	Specify the time (in seconds) for which TACACS+ profile result entries are cached by W-ClearPass Policy Manager.
TACACS+ HTTP Thread Pool Size	Specify the maximum number of simultaneous requests the server can handle. The default value is 100 . The range is from 5 to 200 . When the server has reached the limit or request threads, it defers processing new requests until the number of active requests drops below the specified amount. Increasing this value reduces HTTP response latency times.

System Monitoring Tab

You can configure the SNMP parameters in the **System Monitoring** tab under the **Administration > Server Manager > Server Configuration** page. You can edit the system configuration of a server manager by clicking a table entry. By configuring this tab, you can ensure that external Management Information Base (MIB) browsers can browse the system level MIB objects exposed by the W-ClearPass Policy Manager appliance. The options in this page vary based on the SNMP version that you select.

The following figure displays the **System Monitoring** tab:

Figure 485: System Monitoring Tab

The screenshot shows the 'System Monitoring' tab in the configuration interface. It features a tabbed menu at the top with 'System Monitoring' selected. The main area contains two identical configuration forms. The top form is for SNMP V3 configuration, showing fields for System Location, System Contact, Version (V3), User Name, Security Level (NOAUTH_NOPRIV), Authentication Protocol (MD5), Authentication key, Privacy Protocol (DES), and Privacy Key. The bottom form is for SNMP V2C configuration, showing fields for System Location, System Contact, Version (V2C), and Community String. Both forms have a 'Verify' field next to the key/string fields.

The following table describes the **System Monitoring** tab parameters:

Table 268: System Monitoring tab Parameters

Parameter	Description
System Location	Specify the location of the W-ClearPass Policy Manager appliance.
System Contact	Specify the contact information of the W-ClearPass Policy Manager appliance.
SNMP Configuration	
Version	Specify the SNMP version from the options V1, V2C, or V3. The GUI options on this page vary based on the SNMP version selected.
Community String	Enter and re-enter the community string for sending traps. This is applicable only for SNMP V1 and V2C versions
Username	Specify the user name to use for SNMP v3 communication. This field is available only if you selected the V3 as the SNMP version in the Version field.

Table 268: *System Monitoring tab Parameters (Continued)*

Parameter	Description
Security Level	Select any of the following options: • NOAUTH_NOPRIV (no authentication or privacy) - If you select this security level, only the SHA authentication protocol is available. • AUTH_NOPRIV (authenticate, but no privacy) - If you select this security level, the MD5 and SHA authentication protocols are available. • AUTH_PRIV (authenticate and keep the communication private) - If you select this security level, the MD5 and SHA authentication protocols are available. This field is available only if you selected V3 as the SNMP version in the Version field.
Authentication Protocol	Select the authentication protocol from MD5 or SHA . These protocols vary depends on the security level that you selected in the Security Level field. This field is available only if you selected V3 as the SNMP version in the Version field. NOTE: The MD5 authentication protocol is not supported in the FIPS mode.
Authentication key	Enter and re-enter the authentication key. This field is available only if you selected V3 as the SNMP version in the Version field.
Privacy Protocol	Select the privacy protocol from DES or AES . This field is available only if you selected V3 as the SNMP version in the Version field.
Privacy Key	Enter the privacy key. This field is available only if you selected V3 as the SNMP version in the Version field.

Network Tab

You can navigate to the **Network** page to perform the following tasks:

- [Adding an SSH Public Key on page 488](#)
- [Creating GRE Tunnels on page 489](#)
- [Creating IPsec Tunnels on page 490](#)
- [Creating VLANs on page 492](#)
- [Defining Application Access Restrictions on page 493](#)

The following figure displays the **Network** page:

Figure 486: *Network Interfaces Page*

Administration » Server Manager » Server Configuration - NIGHTLY-CPPM-31

Server Configuration - NIGHTLY-CPPM-31 (10.)

System	Services Control	Service Parameters	System Monitoring	Network	FIPS
Application Access Control:		No Access Restrictions added to this node			Restrict Access
SSH Public Keys:		No SSH Public Keys added for this node			Add Public Key
GRE Tunnels:		No GRE Tunnel created on this node			Create Tunnel
IPsec Tunnels:		No IPsec Tunnel configured on this node			Create IPsec Tunnel
VLANs:		No VLANs present			Create VLAN

Adding an SSH Public Key

W-ClearPass supports public key-based SSH logins. This includes public key management and the ability to enable public key authentication in W-ClearPass on a node-by-node basis.

When you add the SSH public key to the clients, W-ClearPass allows passwordless SSH public key-based authentication to the appadmin W-ClearPass console.



SSH public key-based authentication will continue to work even when the cluster password or the appadmin password have been changed.

To add an SSH public key:

1. Navigate to **Administration > Server Manager > Server Configuration**.

The **Server Configuration** page opens.

2. Select the W-ClearPass server for which passwordless SSH is needed.

The **Server Configuration** dialog for the selected server opens.

3. Select the **Network** tab.

The **Server Configuration Network** page opens.

4. From the **SSH Public Keys** option, click **Add Public Key**.

The **Add Public Key** configuration page opens.

Figure 487: *Adding a Public Key*

Add Public Key

SSH Public Key:

Example:
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQCTtHVCYsR8nzBIk2n0xz5KkuF8TsZALgyePdvZ7+B66IgCXds19afgTSRAiHFbBhXZdiM

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

5. In the **SSH Public Key** window, copy and paste the SSH public key of the client, then click **Save**.



If the SSH public key is regenerated on the client, passwordless public key-based SSH authentication will cease to work. The existing entry for that client must be deleted. Then copy and paste the new SSH public key.

6. From the **Server Configuration** page, click **Save**.

The SSH operation to the W-ClearPass server using a public key is now active, and you can perform passwordless SSH to the W-ClearPass server appadmin console.

Creating GRE Tunnels

You can navigate to the **Network** tab and click **Create Tunnel**. This protocol can be used to create a virtual point-to-point link over standard IP network or the internet.

To create a GRE tunnel:

1. From the **Server Configuration > Network Interfaces** page, select the **Network** tab.
2. From the **GRE Tunnels** option, click **Create Tunnel**.

The following figure displays the **Create Tunnel** dialog:

Figure 488: *Creating a GRE Tunnel*

A screenshot of the "Create Tunnel" dialog box. It has a title bar with "Create Tunnel" and a close button. The dialog contains five input fields: "Display Name", "Local Inner IP", "Remote Outer IP", "Remote Inner IP", and "Local Outer IP (optional)". At the bottom right, there are two buttons: "Create" and "Cancel".

The following table describes the **Create Tunnel** parameters:

Table 269: *Create Tunnel Parameters*

Parameter	Action/Description
Display Name	1. Specify the name for the tunnel interface. This name is used to identify the tunnel in the list of network interfaces.
Local Inner IP	2. Enter the local IP address of the tunnel network interface.
Remote Outer IP	3. Enter the IP address of the remote tunnel endpoint.

Table 269: *Create Tunnel Parameters (Continued)*

Parameter	Action/Description
Remote Inner IP	4. Enter the remote IP address of the tunnel network interface. Enter a value to automatically create a route to this address through the tunnel.
Local Outer IP (Optional)	5. Optionally, enter the local IP address of the tunnel endpoint.
Create/Cancel	6. Commit or dismiss your changes.

Creating IPsec Tunnels

To create VLAN interfaces, navigate to the **Network** page and click **Create IPsec Tunnel**.

The **Create IPsec Tunnel** dialog opens.

Figure 489: *Creating an IPsec Tunnel*

Create IPsec Tunnel ✕

Local Interface	10.175.61MGMT1 ▾
Remote IP Address	
IPsec Mode	Tunnel ▾
IKE Version	1 ▾
IKE Phase1 Mode	Main ▾
PRF	PRF-HMAC-MD5 ▾
Encryption Algorithm	3DES ▾
Hash Algorithm	HMAC SHA ▾
Diffie Hellman Group	Group 2 ▾
Authentication Type	Pre-Shared Key ▾
IKE Shared Secret	
Verify IKE Shared Secret	
Enabled	☒

Create **Cancel**

The following table describes the **Create IPsec Tunnel** parameters:

Table 270: *Create IPsec Tunnel Parameters*

Parameter	Action/Description
Local Interface	1. Specify the local (management) port.
Remote IP Address	2. Specify the IP address of the remote host.
IPsec Mode	3. Select the IPsec mode from the options: ■ Tunnel ■ Transport
IKE Version	4. Specify the version of the Internet Key Exchange (IKE) protocol from the options: 1 or 2 .
IKE Phase 1 Mode	5. Specify the mode of the IKE phase from the options: ■ Main ■ Aggressive
PRF	6. Specify the pseudorandom function (PRF) from the following options: ■ PRF-HMAC-MD5 ■ PRF-HMAC-SHA1 ■ PRF-HMAC-SHA256 ■ PRF-HMAC-SHA384
Encryption Algorithm	7. Select encryption algorithm to use from the following: ■ 3DES ■ AES128 ■ AES192 ■ AES256
Hash Algorithm	8. Select hash algorithm to use from the following: ■ HMAC SHA ■ HMAC-SHA256 ■ HMAC-SHA384 ■ HMAC-MD5
Diffie Hellman Group	9. Select the Diffie Hellman group from the following: ■ Group 1 ■ Group 2 ■ Group 5 ■ Group 14 ■ Group 19 ■ Group 20
Authentication Type	10. Select the authentication type from the options ■ Pre-Shared Key ■ Certificate

Table 270: *Create IPsec Tunnel Parameters (Continued)*

Parameter	Action/Description
IKE Shared Secret	11. Enter the secret key.
Verify IKE Shared Secret	12. Verify the secret key.
Enabled	13. Specify whether the IPsec tunnel is enabled or not.
	14. Click Create .

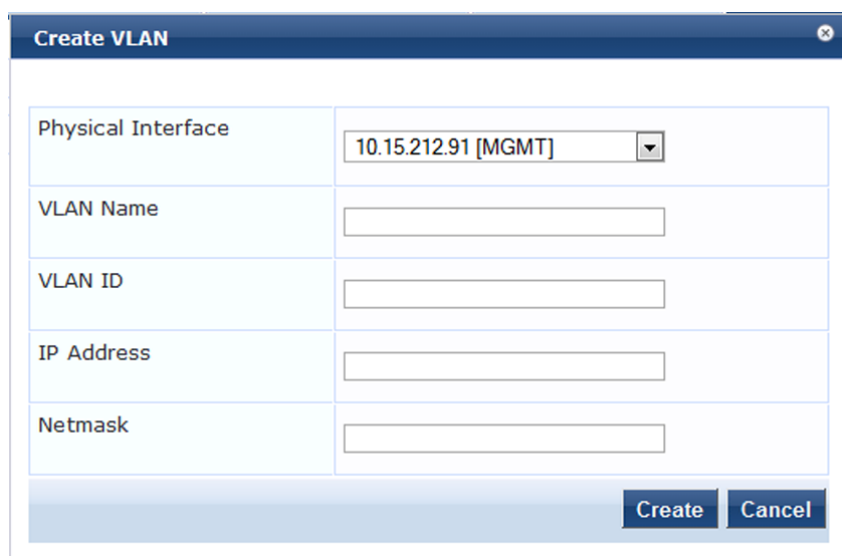
Creating VLANs

To create VLAN interfaces:

1. From the **Server Configuration > Network Interfaces** page, select the **Network** tab.
2. From the **VLANS** option, click **Create VLAN**.

The following figure displays the **Create VLAN** dialog:

Figure 490: *Creating a VLAN*



The screenshot shows a 'Create VLAN' dialog box. It has a title bar with the text 'Create VLAN' and a close button. The dialog contains five input fields arranged in a table-like structure. The first field is 'Physical Interface' with a dropdown menu showing '10.15.212.91 [MGMT]'. The other four fields are 'VLAN Name', 'VLAN ID', 'IP Address', and 'Netmask', each with a text input box. At the bottom right of the dialog are two buttons: 'Create' and 'Cancel'.

The following table describes the **Create VLAN** parameters:

Table 271: *Server Configuration > Create VLAN Parameters*

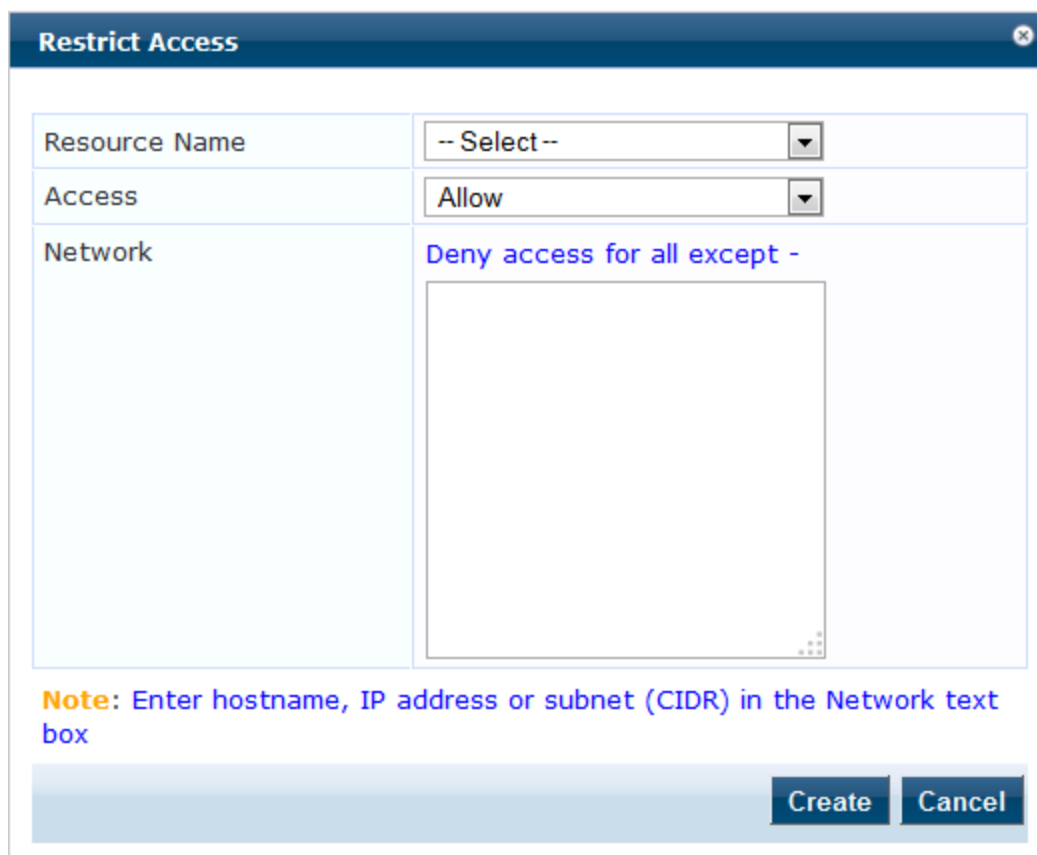
Parameter	Action/Description
Physical Interface	1. Enter the physical port on which to create the VLAN interface. This is the interface through which the VLAN traffic will be routed. NOTE: Your network infrastructure must support tagged 802.1Q packets on the physical interface selected.
VLAN Name	2. Enter the name for the VLAN interface. This name is used to identify the VLAN in the list of network interfaces.
VLAN ID	3. Specify the 802.1Q VLAN identifier. Enter a value between 1 and 4094. The VLAN ID cannot be changed after the VLAN interface has been created. NOTE: VLAN ID 1 is often reserved for use by certain network management components. Avoid using this ID unless you know it will not conflict with a VLAN already defined in your network.
IP Address	4. Enter the IP address of the VLAN.
Netmask	5. Enter the netmask for the VLAN.
Create/Cancel	6. Commit or dismiss your changes.

Defining Application Access Restrictions

Use this function to define specific network resources and allow or deny them access to specific applications. You can create multiple definitions.

1. From the **Server Configuration > Network** page, select the **Application Access Control**.
The **Restrict Access** dialog opens.

Figure 491: *Restrict Access Configuration Dialog*



The image shows a 'Restrict Access' dialog box. It has a title bar with a close button. Inside, there are three main sections: 'Resource Name' with a dropdown menu showing '-- Select --'; 'Access' with a dropdown menu showing 'Allow'; and 'Network' with a large text area. The text area contains the text 'Deny access for all except -' in blue. Below the text area is a note: 'Note: Enter hostname, IP address or subnet (CIDR) in the Network text box'. At the bottom right are 'Create' and 'Cancel' buttons.

The following table describes the **Restrict Access** parameters:

Table 272: *Restrict Access Parameters*

Parameter	Action/Description
Resource Name	1. Select the application to which you want to allow or deny access.
Access	2. Select one of the access control options: ■ Allow: Allows access to the selected application. ■ Deny: Denies access to the selected application.
Network	3. Enter one or more hostnames, IP addresses, or IP subnets per line. The devices defined by what you enter here will be either specifically allowed or specifically denied access to the application you select.
	4. Click Create .

FIPS Tab

This section provides information on using W-ClearPass Policy Manager in Federal Information Processing Standards (FIPS) 140-2 approved mode.

The U. S. Government developed FIPS 140-2 to define procedures, architectures, cryptographic algorithms, and other security techniques for use in government applications and networks that use cryptography.

When running in FIPS Approved mode, W-ClearPass Policy Manager utilizes a FIPS 140-2 validated cryptographic module. Support is not available for non-approved authentication methods such as EAP-MD5 and MD5 digest algorithms.

For details on the Validated FIPS 140-1 and FIPS 140-2 Cryptographic Modules, see:

<http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm#2577>

Enabling FIPS Mode Using CLI

You can enable FIPS mode in W-ClearPass during installation using the CLI or post-installation using the Web UI.

The following figure displays the prompt to enable FIPS mode using the CLI:

Figure 492: *Enabling FIPS Mode*

```
10) Cyprus                27) Lebanon              44) Tajikistan
11) East Timor            28) Macau                45) Thailand
12) Georgia              29) Malaysia            46) Turkmenistan
13) Hong Kong            30) Mongolia            47) United Arab Emirates
14) India                 31) Myanmar (Burma)     48) Uzbekistan
15) Indonesia            32) Nepal               49) Vietnam
16) Iran                 33) Oman                50) Yemen
17) Iraq
#? 14

The following information has been given:

      India

Therefore TimeZone='Asia/Kolkata' will be used.
Local time is now:      Wed May 14 19:33:41 IST 2014.
Universal Time is now: Wed May 14 14:03:41 UTC 2014.

Is the above information OK?
1) Yes
2) No
#? 1

Do you want to enable FIPS Mode? [y|n]: _
```

After enabling FIPS mode using the CLI commands, you can verify whether FIPS mode is enabled or not in the **Configuration Summary** page.

Figure 493: *FIPS Mode > Configuration Summary*

```

=====
                        Configuration Summary
=====
Hostname                :   UM-582
Management Port IP Address : 10.17.5.82
Management Port Subnet Mask : 255.255.255.0
Management Port Gateway   : 10.17.5.254
Data Port IP Address       : <not configured>
Data Port Subnet Mask      : <not configured>
Data Port Gateway         : <not configured>
Primary DNS               : 10.17.4.10
Secondary DNS              : <not configured>
Primary NTP Server        : pool.ntp.org
Secondary NTP Server      : <not configured>
Timezone                  : 'Asia/Kolkata'
FIPS Mode                 :   True
=====

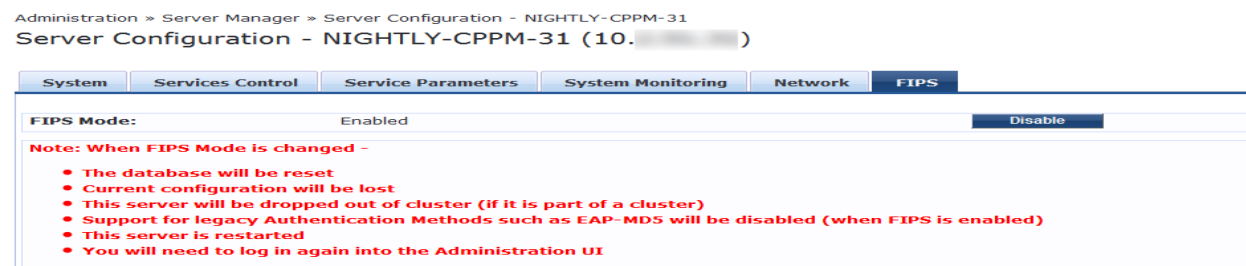
```

Enabling FIPS Mode in the W-ClearPass User Interface

Alternatively, you can enable or disable the FIPS mode in the W-ClearPass user interface:

1. Navigate to **Administration > Server Manager > Server Configuration**.
2. From the **Server Configuration** page, select the server of interest.
The **Server Configuration** dialog for the selected server opens.
3. Select the **FIPS** tab.

Figure 494: *Server Configuration > FIPS Tab*



Important Points to Remember

Note the following important points, when you enable FIPS mode in the W-ClearPass Policy Manager user interface:

- The database is reset when you enable the FIPS mode in W-ClearPass Policy Manager.



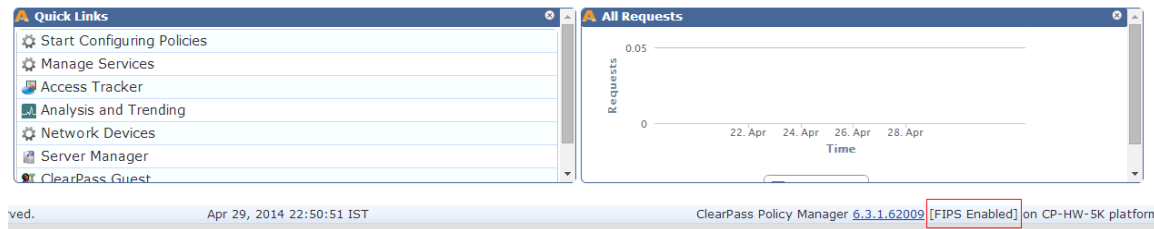
Ensure that you backed up your database before enabling FIPS mode.

- Configuration backup file from the W-ClearPass Policy Manager in non-FIPS mode cannot be restored on W-ClearPass Policy Manager in FIPS mode. However, configuration backup file from the W-ClearPass Policy Manager in FIPS mode can be restored on the W-ClearPass Policy Manager in non-FIPS mode.

- The server will be removed from the cluster if FIPS mode is enabled.
- All nodes in a cluster must be either in FIPS or non-FIPS mode. The W-ClearPass Policy Manager nodes in FIPS mode cannot be connected to the cluster whose nodes are in the non-FIPS mode.
- The legacy authentication method such as EAP-MD5 and MD5 digest algorithm are not supported in FIPS mode. You cannot import the certificates that are created with the MD5 authentication type to the **Certificates Trust List (Administration > Certificates > Certificate Trust List)** page.
- The server reboots when you enable FIPS mode. You need to log in again to the Administration interface.

You can view the status of FIPS mode in the status bar. The following figure displays the **Status** bar with the status of FIPS mode:

Figure 495: *FIPS Status*



You can also view the status of the FIPS mode using the CLI commands. For more information, see [Show Commands on page 760](#).

Set Date & Time

Click the **Set Date and Time** link under the **Administration > Server Manager > Server Configuration** page to access the **Change Date and Time** pop-up where can set the date and time for the server.

The **Change Date and Time** pop-up has the following two tabs:

- [Date & Time Tab on page 498](#)
- [Time Zone on Publisher Tab on page 498](#)

Date & Time Tab

You can set the date and time for the server using this tab. The following figure displays the **Date & Time** tab of the **Change Date and Time** pop-up:

Figure 496: *Change Date and Time - Date & Time tab*

The screenshot shows the 'Change Date and Time' dialog box with the 'Date & Time' tab selected. It includes a checkbox for 'Synchronize time with NTP server'. Below this, there are fields for 'Date' (formatted as yyyy-mm-dd, showing 2012-09-28) and 'Time' (with spinners for Hour, Minute, and Second, showing 14:50:16). A 'WARNING' message is displayed at the bottom, stating that Policy Manager services need to be restarted after execution. 'Save' and 'Cancel' buttons are at the bottom right.

The following table describes the **Date and Time** tab parameters:

Table 273: *Change Date and Time - Date & Time tab Parameters*

Parameter	Description
Date in yyyy-mm-dd format	To specify date and time, 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	To synchronize with a Network Time Protocol Server, enable this check box and specify the NTP servers. You can specify one primary and one secondary server.
NTP Server (primary)	Specify the primary NTP server.
NTP Server (secondary)	Specify the secondary NTP server.

Time Zone on Publisher Tab

After configuring the date and time, select the time zone on the **Time zone on publisher** tab. This displays a time zone list in alphabetical order. Select a time zone and click **Save**.



This option is available only on the publisher. To set time zone on the subscriber, select the specific server and set time zone from the server-specific page.

The following figure displays the **Time zone on publisher** tab of the **Change Date and Time** pop-up:

Figure 497: Time zone on publisher tab

Change Date and Time

This will change Date & Time for all nodes in the cluster

Date & Time **Time zone on publisher**

To change the time zone, select your area from the list below

- Africa/Abidjan
- Africa/Accra
- Africa/Addis_Ababa
- Africa/Algiers
- Africa/Asmara
- Africa/Bamako
- Africa/Bangui
- Africa/Banjul
- Africa/Bissau
- Africa/Blantyre

Current time zone: Etc/UTC(GMT 0:00)

WARNING: After command execution Policy Manager services need to be restarted. This may take a while.

Save **Cancel**

Change Cluster Password

To change the cluster-wide password, follow the procedure below:

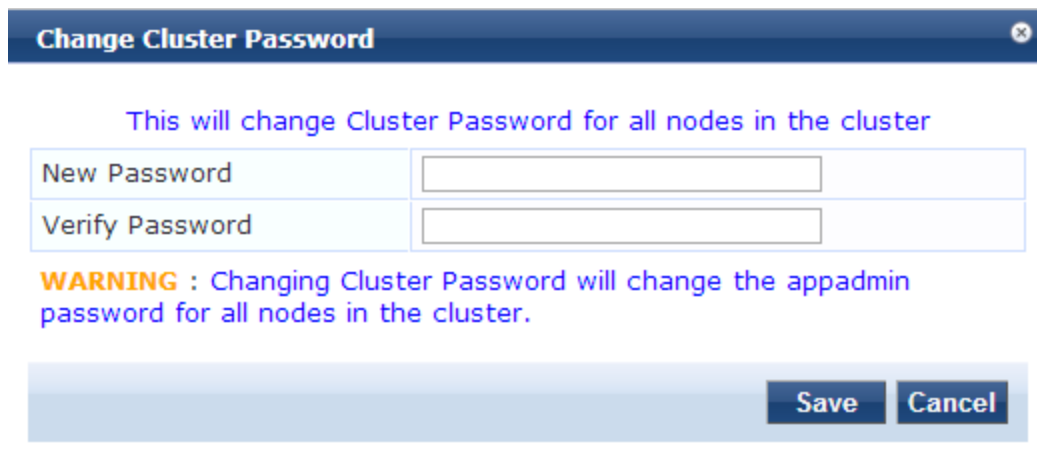
1. Navigate to the **Administration > Server Manager > Server Configuration** page and click the **Change Cluster Password** link. The **Change Cluster password** pop-up appears.
2. Enter the new password, then verify the password.
3. Click **Save**.



Changing this password changes the password for the CLI user *appadmin* as well.

The following figure displays the **Change Cluster Password** pop-up:

Figure 498: *Change Cluster Password Dialog*

The image shows a 'Change Cluster Password' dialog box. At the top, a blue header bar contains the title 'Change Cluster Password' and a close button. Below the header, a message in purple text states: 'This will change Cluster Password for all nodes in the cluster'. There are two input fields: 'New Password' and 'Verify Password', each with a corresponding text box. Below these fields, a warning message in orange and purple text reads: 'WARNING : Changing Cluster Password will change the appadmin password for all nodes in the cluster.' At the bottom right, there are two buttons: 'Save' and 'Cancel'.

Manage Policy Manager Zones

This section provides the following information:

- [About Policy Manager Zones](#)
- [Managing Policy Manager Zones](#)
- [Mapping Policy Manager Zones](#)

About Policy Manager Zones

W-ClearPass Policy Manager shares a distributed cache of runtime states across all nodes in a cluster. These runtime states include:

- Roles and postures of connected entities
- Connection status of all endpoints running OnGuard
- Endpoint details gathered by OnGuard Agent

W-ClearPass Policy Manager uses this runtime state information to make policy decisions across multiple transactions.

In a deployment where a cluster spans WAN boundaries and multiple geographic zones, it is not necessary to share all of this runtime state across all nodes in the cluster.

For example, when endpoints present in one geographical area are not likely to authenticate or be present in another area, it is more efficient from a network bandwidth usage and processing perspective to restrict the sharing of such runtime state to a given geographical area.

You can configure zones in W-ClearPass Policy Manager to match with the geographical areas in your deployment. There can be multiple zones per cluster, and each zone has a number of Dell Networking W-ClearPass Policy Manager nodes that share their runtime state.

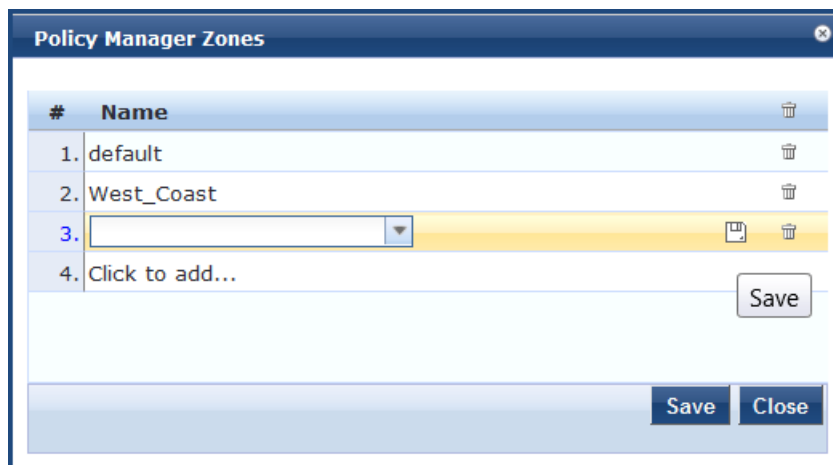
Managing Policy Manager Zones

To add or delete a W-Policy Manager Zone:

1. Navigate to the **Administration > Server Manager > Server Configuration** page.
2. Click the **Manage Policy Manager Zones** link.

Figure 499 displays the **Policy manager Zones** dialog:

Figure 499: *Policy Manager Zones Dialog*



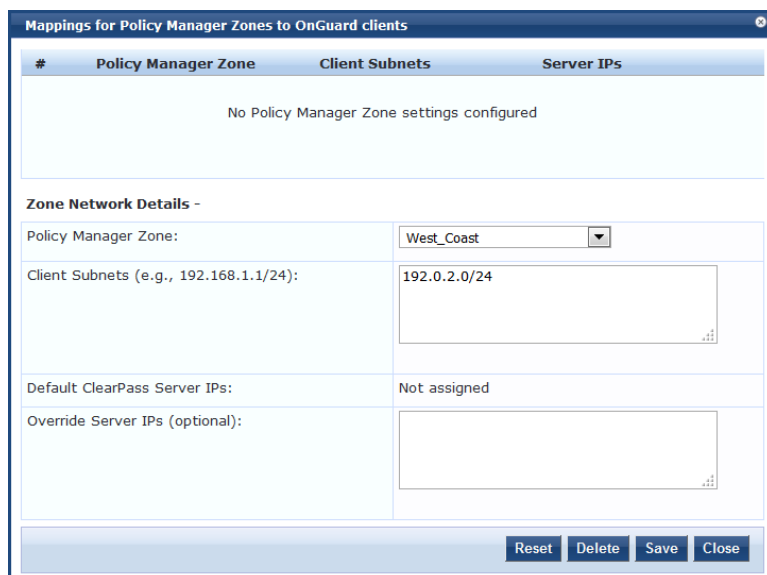
3. To add a new W-Policy Manager Zone, click **Click to add...** and enter the name of the W-Policy Manager Zone to be added, click the **Save** icon, then click **Save**.
4. To delete a zone, click the trash can icon—.

Mapping Policy Manager Zones

To configure the W-Policy Manager Zone you created:

1. Navigate to **Administration > Agents and Software Updates > OnGuard Settings**.
The **OnGuard Settings** page opens.
2. Click **Policy Manager Zones**.
The **Mappings for Policy Manager Zones to OnGuard Clients** page opens.

Figure 500: *Mappings for W-Policy Manager Zones to OnGuard Clients Page*



3. Specify the **Mappings for W-Policy Manager Zones to OnGuard Clients** parameters:

Table 274: *OnGuard Settings > W-Policy Manager Zones Parameters*

Parameter	Action/Description
W-Policy Manager Zone	Lists the W-Policy Manager zones with radial buttons for selection.
Client Subnets	Displays the client subnet addresses specific to the W-Policy Manager zone.
Server IPs	Displays the server IP addresses specific to the W-Policy Manager zone.
Zone Network Details	
W-Policy Manager Zone	1. Select the W-Policy Manager zone from the drop-down list that are created from the Administration > Server Manager > Server Configuration > Manage Policy Manager Zones page. If no W-Policy Manager zone is configured, the default W-Policy Manager zone is displayed in this field.
Client Subnets	2. Specify the client subnets that are configured for the selected W-Policy Manager zone.
Default W-ClearPass Server IPs	3. Specify the IP address of the default W-ClearPass server.
Override Server IPs	4. Optionally, specify the IP addresses or the Fully Qualified Domain Name (FQDN) to which you want the OnGuard agent to send request in the sequence. You can specify the data port or load balancer IP address in this field. The IP addresses configured here will override the IP address configured in the Default ClearPass Server IPs field. For example, if you have configured the IP addresses 10.17.XXX.1, 10.17.XXX.2, and 10.17.XXX.3, OnGuard agent will send the request in the same sequence.

NetEvents Targets

NetEvents are a collection of information regarding various W-ClearPass Policy Manager users, endpoints, guests, authentications, accounting details, and so on. This information is periodically posted to a server that is configured as the NetEvents target.

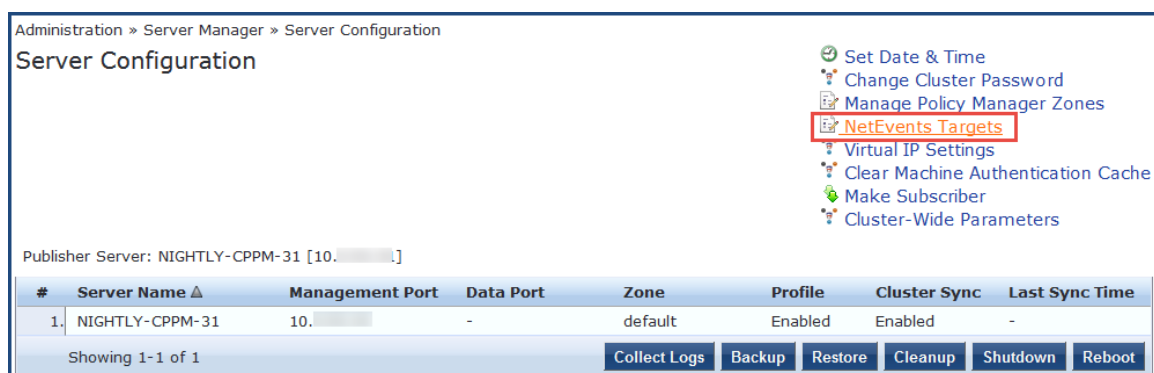
If W-ClearPass Insight is enabled on a W-ClearPass Policy Manager server (see [Enabling Insight and Specifying a Master Insight Node on page 686](#)), it will receive net events from all other server nodes within the same W-ClearPass cluster.

If you want to post these details to an external server that can aggregate these events or to an external dedicated W-ClearPass Insight server for multiple W-ClearPass clusters, you have to configure an external NetEvents Target.

To configure an external NetEvents Target:

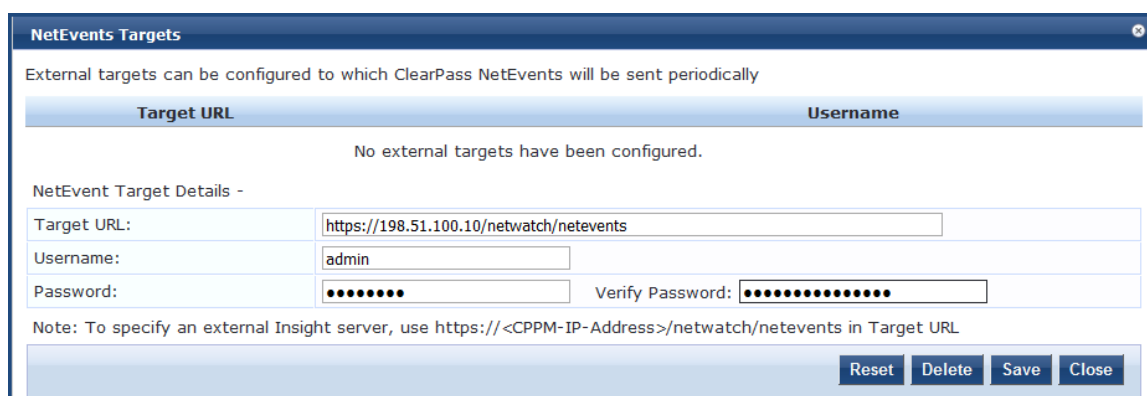
1. Navigate to the **Administration > Server Manager > Server Configuration** page.

Figure 501: *NetEvents Target Link on Server Configuration Page*



- Click the **NetEvents Targets** link.
The **NetEvents Targets** configuration dialog opens.

Figure 502: *NetEvents Targets Configuration Dialog*



- Specify the **NetEvents Targets** parameters as described in the following table:

Table 275: *NetEvents Targets Parameters*

Parameter	Action/Description
Target URL	- Enter the HTTP URL for the service that supports posting to the NetEvents target and requires authentication using username and password. - To specify an external Insight server, use the following Target URL: https://<W-ClearPass-IP-address>netwatch/netevents.
Username/Password	Enter the W-ClearPass admin credentials configured for authentication for the HTTP service that is provided in the Target URL.
Reset button	Resets the values entered in this configuration dialog.
Delete button	Deletes the specified Target URL.
	Click Save.

Virtual IP Settings

You can configure two nodes in a cluster to share a virtual IP address. The virtual IP address is bound to the primary node by default. The secondary node takes over when the primary node is unavailable.



In a virtual machine deployment of W-ClearPass Policy Manager, you must enable forged transmits on the VMWare distributed virtual switch for the Virtual IP feature to be effective.

To configure a virtual IP address:

1. Navigate to the **Administration > Server Manager > Server Configuration** page.
2. Click the **Virtual IP Settings** link.

The **Virtual IP Settings** dialog opens:

Figure 503: *Virtual IP Settings*

Virtual IP	Primary Node	Secondary Node	Status
1. 10.	VM-240 [MGMT] ●	VM-207 [MGMT]	Enabled

● Indicates current node serving Virtual IP

Virtual IP Details -

Virtual IP:

Node: Interface: Subnet:

Primary Node:

Secondary Node:

Enabled: ☒

Reset Delete Save Close

3. Specify the **Virtual IP Settings** parameters as described in the following table:

Table 276: *Virtual IP Settings Parameters*

Parameter	Action/Description
Virtual IP	Enter the IP address you want to define as the virtual IP address.
Primary Node	Select the servers to use as the primary node.
Secondary Node	Select the servers to use as the secondary node.
Interface	Select an interface on each server to which the virtual IP address is bound.
Subnet	The Subnet value is automatically filled when you select the interface.
Enabled	Select the check box to enable the virtual IP address.

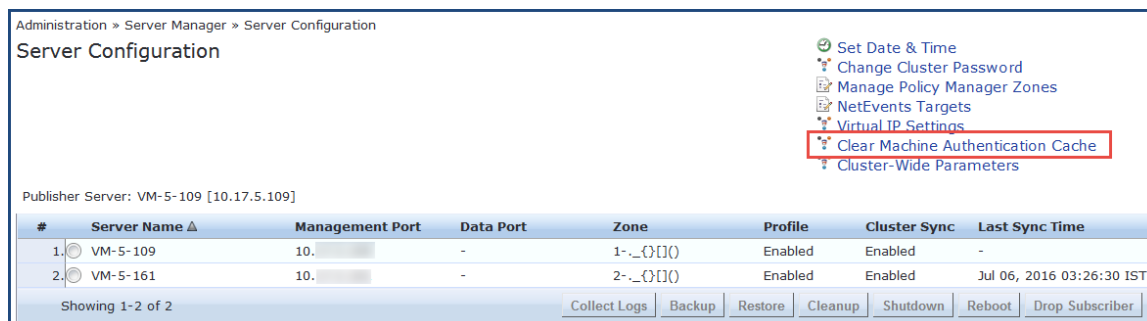
Clear Machine Authentication Cache

To clear machine authentication cache on all the nodes in a cluster:

1. Navigate to the **Administration > Server Manager > Server Configuration** page.

The **Server Configuration** page opens:

Figure 504: Server Configuration Page > Clear Machine Authentication Cache



2. Click the **Clear Machine Authentication Cache** link.

The following prompt is displayed:

Are you sure you want to clear machine authentication cache?

3. To proceed with the operation, click **Yes**.

The following message appears:

Machine authentication cache cleared from all nodes

Cluster-Wide Parameters

This section provides the following information:

- [General on page 505](#)
- [Cleanup Intervals on page 509](#)
- [Notifications on page 510](#)
- [Standby Publisher on page 511](#)
- [Virtual IP Configuration on page 512](#)
- [Mode on page 512](#)
- [Database on page 516](#)

General

You can configure the parameters that apply to all the nodes in a cluster by configuring the **Cluster-Wide Parameters**.

To configure Cluster-Wide Parameters:

1. Navigate to the **Administration > Server Manager > Server Configuration** page.

The **General** tab of the **Cluster-Wide Parameters** page opens:

Figure 505: *Cluster-Wide Parameters > General Tab*

Parameter Name	Parameter Value	Default Value
Policy result cache timeout	5 minutes	5
Free disk space threshold value	30 %	30
Free memory threshold value	20 %	20
Profile subnet scan interval	24 hours	24
Endpoint Context Servers polling interval	60 minutes	60
Automatically check for available Software Updates	TRUE	TRUE
Login Banner Text		
Admin Session Idle Timeout	30 minutes	30
Performance Monitor Rendering Port	80	80
Multi Master Cache Durability	OFF	OFF
CLI Session Idle Timeout	360 minutes	360
Disable TLSv1.0 support	None	None
Profiler Scan Ports	135,3389 TCP ports	135,3389
Process wired device information from IF-MAP interface	FALSE	FALSE
Disable Change Password for TACACS	FALSE	FALSE

Restore Defaults Save Cancel

2. Configure the **Cluster-Wide Parameters > General** parameters as described in the following table.

Table 277: Cluster-Wide Parameters > General Tab Parameters

Parameter	Action/Description
Policy result cache timeout	1. Specify the duration allowed in minutes to store the role mapping and posture results derived by the policy engine during a policy evaluation. A value of 0 disables caching. This result can then be used in subsequent evaluation of policies associated with a service, if the Use cached Roles and Posture attributes from previous sessions option is turned on for the service. NOTE: The value of the Policy result cache timeout field must be greater than the highest value set in the Health Check Interval (in hours) fields. For example, if you have created the profiles Student-Enforcement-Profile and Staff-Enforcement-Profile with health check interval configured, then the value of the Policy result cache timeout field must be greater than the highest value of the Health Check Quiet Period (in hours) value configured among the following profiles: • Global Agent Settings • Student-Enforcement-Profile • Staff-Enforcement-Profile
Free disk space threshold value	2. Specify the percentage below which disk usage warnings are issued in the Monitoring > Event Viewer page. For example, a value of 30% indicates that a warning is issued only when the available disk space is 30% or lower. An error message similar to the following may appear in the System Event Details dialog: <i>System is running with low disk space. Aggressive cleanup will be initiated when the available disk space falls below 80%. Current available disk space = 75%</i>
Free memory threshold value	3. Specify the percentage below which RAM usage warnings are issued in the W-ClearPass Event Viewer. For example, a value of 30 indicates that a warning is issued only when the available RAM is 30% or lower.
Profile subnet scan interval	4. Specify the profile subnet scan interval in hours. The default value is 24 hours.
Endpoint Context Servers polling interval	5. Enter the interval in minutes between polling of endpoint context servers. The default interval is 60 minutes.
Automatically check for available Software Updates	6. Specify whether to enable automatic checking for available software updates. The default is TRUE.
Login Banner Text	7. Customize the banner text that appears on the W-ClearPass login screen and CLI access window.
Admin Session Idle Timeout	8. Specify the maximum idle time permitted for admin users, beyond which the session times out. The default value is 30 minutes. The allowed range is 5 to 1440 minutes.

Table 277: *Cluster-Wide Parameters > General Tab Parameters (Continued)*

Parameter	Action/Description
Multi Master Cache Durability	9. For the Multi Master Cache to survive most abrupt shutdowns, set this to Normal or Full. The default value is OFF. NOTE: Enabling this feature may result in some performance degradation.
CLI Session Idle Timeout	10. Specify the maximum idle time permitted for CLI users, beyond which the session times out. The default value is 30 minutes. The allowed range is 5 to 1440 minutes. If this parameter is changed, the changes will take effect when the client opens a new CLI session. Any active CLI sessions will continue to use the old timeout, or they have to be disconnected and reconnected for the new changes to take effect.
Disable TLSv1.0 support	11. To disable Transport Layer Security (TLS) v1.0 support, select one of the following options: ■ None ■ Admin ■ Network ■ All
Profiler Scan Ports	12. To change the list of ports to scan and add custom fingerprints to classify based on them, enter the new TCP port numbers. The W-Policy Manager TCP ports scanner checks to see if the specified Profiler Scan Ports are open. The default TCP ports are 135 and 3389.
Process wired device information from IF-MAP interface	13. Choose whether to process wired device information from the IF-MAP interface. The default is FALSE.
Disable Change Password for TACACS	14. When logging in for TACACS user authentication: ■ If set to FALSE (the default setting), after entering a blank password, you are presented with an option to change the TACACS user password. ■ If set to TRUE, the option to enter the TACACS user password is displayed. The option to change the TACACS password is not displayed.

Cleanup Intervals

The following figure displays the **Cluster-Wide Parameters > Cleanup Interval** dialog:

Figure 506: Cluster-Wide Parameters > Cleanup Interval Tab

Parameter Name	Parameter Value	Default Value
Maximum inactive time for an endpoint	0 days	0
Cleanup interval for Session log details in the database	7 days	7
Cleanup interval for information stored on the disk	7 days	7
Known endpoints cleanup interval	0 days	0
Unknown endpoints cleanup interval	0 days	0
Expired guest accounts cleanup interval	365 days	365
Profiled Unknown endpoints cleanup interval	0 days	0
Static IP endpoints cleanup option	FALSE	FALSE
Old Audit Records cleanup interval	7 days	7
Profiled Known endpoints cleanup option	FALSE	FALSE

Restore Defaults Save Cancel

Specify the **Cluster-Wide Parameters > Cleanup Interval** parameters as described in the following table:

Table 278: Cluster-Wide Parameters > Cleanup Interval Tab Parameters

Parameter	Action/Description
Maximum inactive time for an endpoint	Specify the duration in number of days to which an endpoint is retained in the endpoints table since its last authentication. A value of 0 specifies that no time limit is configured. If the endpoint is not authenticated for this period, the entry is removed from the endpoint table.
Cleanup interval for Session log details in the database	- Specify the duration in number of days to keep the following data in the W-Policy Manager database: - Session logs (found on the Access Tracker page) - Event logs (found on the Event Viewer page) - Machine authentication cache The default value is 7 days.
Cleanup interval for information stored on the disk	Specify the duration in number of days to keep log files that are written to the disk. The default value is 7 days.
Known endpoints cleanup interval	Specify the duration in number of days that W-ClearPass uses to determine when to start deleting known or disabled entries from the Endpoint repository. Known entries are deleted based on the last Added At value for each Endpoint. For example, if this value is 7, then known Endpoints that do not have the Added At value within the last 7 days are deleted. The default value is 0 days. This indicates that no cleanup interval is specified.
Unknown endpoints cleanup interval	Specify the duration in number of days that W-ClearPass uses to determine when to start deleting unknown entries from the Endpoint repository.

Table 278: *Cluster-Wide Parameters > Cleanup Interval Tab Parameters (Continued)*

Parameter	Action/Description
	Unknown entries are deleted based on the last Updated At value for each Endpoint. For example, if this value is 7, then unknown Endpoints that do not have the Updated At value within the last 7 days (stale endpoints) are deleted. The default value is 0 days . This indicates that no cleanup interval is specified.
Expired guest accounts cleanup interval	6. Specify the cleanup interval for expired guest accounts. This indicates the number of days after expiry that the cleanup occurs. A value of 0 specifies no expired guest accounts cleanup interval. The default value is 365 days .
Profiled Unknown endpoints cleanup interval	7. Specify the cleanup interval in number of days that W-ClearPass uses to determine when to start deleting profiled unknown entries from the Endpoint repository. Profiled unknown entries are deleted based on their last Updated At value for each Endpoint. For example, if this value is 7, then the Profiled Unknown Endpoints that do not have an Updated At value within the last 7 days are deleted. The default value is 0 .
Static IP endpoints cleanup option	8. Specify whether to enable the option to cleanup static IP endpoints. The default option is FALSE .
Old Audit Records cleanup interval	9. Specify the cleanup interval in number of days that W-ClearPass uses to determine when to start deleting old audit records from the Audit Viewer page. The default value is 7 days.
Profiled Known endpoints cleanup option	10. Specify the cleanup interval in number of days that W-ClearPass uses to determine when to start deleting profiled known entries from the Endpoint repository. The default value is FALSE .

Notifications

The following figure displays the **Cluster-Wide Parameters > Notifications** tab:

Figure 507: *Cluster-Wide Parameters > Notifications Tab*

Cluster-Wide Parameters

General Cleanup Intervals **Notifications** Standby Publisher Virtual IP Configuration Mode Database

Parameter Name	Parameter Value	Default Value
System Alert Level	WARN	WARN
Alert Notification Timeout	Disabled hours	2
Alert Notification - eMail Address		
Alert Notification - SMS Address		

Restore Defaults Save Cancel

The following table describes the **Cluster-Wide Parameters > Notifications** tab parameters:

Table 279: *Cluster-Wide Parameters > Notifications Parameters*

Parameter	Description
System Alert Level	- Specify the alert notifications that are generated for system events logged at this level or higher. INFO: Alerts for INFO, WARN, and ERROR messages are generated. WARN: Alerts for WARN and ERROR messages are generated. ERROR: Alerts for ERROR messages only are generated. The default value is WARN.
Alert Notification Timeout	Specify the timeout in hours that determines how often alert messages are generated and distributed. If you select Disabled, alert generation is disabled. The default value is 2 hours.
Alert Notification - eMail Address	Enter a comma-separated list of email addresses to which alert messages are sent.
Alert Notification - SMS Address	Enter a comma-separated list of phone numbers to which alert messages are sent.

Standby Publisher

The Standby Publisher is the Publisher node in the cluster that is configured to come up in the event that the Publisher node goes down.

The following figure displays the **Cluster-Wide Parameters > Standby Publisher** tab:

Figure 508: *Cluster-Wide Parameters > Standby Publisher Tab*

The screenshot shows a window titled "Cluster-Wide Parameters" with several tabs: General, Cleanup Intervals, Notifications, Standby Publisher (selected), Virtual IP Configuration, Mode, and Database. The Standby Publisher tab contains a table with the following data:

Parameter Name	Parameter Value	Default Value
Enable Publisher Failover	FALSE	FALSE
Designated Standby Publisher	0	0
Failover Wait Time	10 minutes	10

At the bottom of the window are three buttons: "Restore Defaults", "Save", and "Cancel".

The following table describes the **Standby Publisher** tab parameters of **Cluster-Wide Parameters**:

Table 280: *Cluster-Wide Parameters > Standby Publisher Tab Parameters*

Parameter	Description
Enable Publisher Failover	1. To authorize a node in a cluster on the system to act as a publisher if the primary publisher fails, select TRUE . The default value is FALSE .
Designated Standby Publisher	2. Select the server in the cluster to act as the standby publisher. The default value is 0 . NOTE: If the Standby Publisher is on a different subnet from the Publisher, then ensure that a reliable connection between the two subnets is available to avoid unwanted network segmentation and potential data loss from a false failover.
Failover Wait Time	3. The time (in minutes) for which the secondary node waits before it acquires a virtual IP address after the primary node fails. The default failover wait time is 10 minutes . This prevents the secondary node from taking over when the primary node is temporarily unavailable during a restart.

Virtual IP Configuration

The following figure displays the **Cluster-Wide Parameters > Virtual IP Configuration** tab:

Figure 509: *Cluster-Wide Parameters > Virtual IP Configuration Tab*

The screenshot shows a web-based configuration window titled "Cluster-Wide Parameters". It has several tabs: General, Cleanup Intervals, Notifications, Standby Publisher, Virtual IP Configuration (which is selected), Mode, and Database. Below the tabs is a table with three columns: Parameter Name, Parameter Value, and Default Value. The table contains one entry: "Failover Wait Time" with a value of "10" and a unit of "seconds", and a default value of "10". At the bottom right of the window are three buttons: "Restore Defaults", "Save", and "Cancel".

The following table describes the **Cluster-Wide Parameters > Virtual IP Configuration** tab parameters:

Table 281: *Cluster-Wide Parameters > Virtual IP Configuration Parameters*

Parameter	Action/Description
Failover Wait Time	1. Enter the number of seconds for the secondary node to wait after primary node failure before it acquires the virtual IP address. The default failover wait time is 10 seconds so the secondary node takes over and responds quickly to authentication access and requests.



You can define a virtual IP address only with a primary server without a secondary server, if required. This can be used to add an additional IP address to the W-ClearPass Policy Manager server without any redundancy.

Mode

The **Mode** dialog in the **Cluster-Wide Parameters** page allows you to enable or disable High Capacity Guest mode. High Capacity Guest mode addresses the high-volume licensing requirements in the Public Facing

Enterprises (PFE) environment, where a large volume of unique endpoints need wireless access.

The licensing scheme in High Capacity Guest mode supports a high volume of user traffic in the following PFEs where the number of endpoints changes every day:

- Transportation: Airports and rail stations
- Hospitality: Hotels, casinos, and resorts
- Healthcare: Hospitals, clinics, and health centers
- Retail: Shopping malls
- Large public venues: Stadiums, convention centers, and theaters
- Restaurants and coffee shops: Quick-serve restaurants

In enterprise deployments, W-ClearPass Policy Manager licensing accumulates the unique endpoint count for seven days, which can cause the number of licenses to exceed their limit.

To address this license limit in the PFE environment, you can enable High Capacity Guest mode on a cluster. In High Capacity Guest mode, the count of unique endpoints is reset every day, instead of accumulating the count for seven days. In High Capacity Guest mode, only you can view the supported guest authentication methods supported in the **Authentication Methods** page.

When **High Capacity Guest** mode is enabled, you cannot enable the RADIUS services with the following authentication methods:

- EAP-FAST
- EAP-GTC
- EAP-MSCHAPv2
- EAP-PEAP
- EAP-TLS
- EAP-TTLS

Licensing Restrictions

You can add only guest licenses to High Capacity Guest mode. This mode is intended to handle only a high volume of guest users in PFE environments. After enabling High Capacity Guest mode, you cannot add enterprise licenses.

If the number of licenses used exceeds the number of licenses purchased, a warning message appears four months after the number is exceeded. The number of licenses used is based on the daily moving average.

In High Capacity Guest mode, a maximum of 2x licenses are allowed. For example, if you use the CP-HW-5K platform (which supports 5,000 licenses), a maximum of 10,000 licenses are allowed.

Cluster Restrictions

When High Capacity Guest mode is enabled in a cluster, the following restrictions apply:

- Configuration settings cannot be moved from one cluster to another cluster that operates in High Capacity Guest mode.
- Restoring configuration is allowed only with the backup files from servers that have High Capacity Guest mode enabled.
- High Capacity Guest mode is intended only for high volumes of guest access.
- Use-case related settings other than those for High Capacity Guest mode are restricted.
- OnGuard and OnBoard access is restricted.
- Default cleanup interval values are reset.
- Only guest application licenses are supported.

The following figure displays the **Cluster-Wide Parameters > Mode** dialog:

Figure 510: *Cluster-Wide Parameters > Mode Tab*

Cluster-Wide Parameters

General Cleanup Intervals Notifications Standby Publisher Virtual IP Configuration **Mode** Database

Parameter Name	Parameter Value	Default Value
High Capacity Guest Mode	FALSE	FALSE

The High Capacity Guest (HCG) Mode is intended for deployments with high volumes of guest access.

Enabling HCG Mode will restrict the following -

- ClearPass Onboard and OnGuard applications will be disabled
- Only Guest application licenses can be added
- Posture checks and Host Audit checks are not allowed
- RADIUS-based authentication methods that are disabled - EAP-FAST, EAP-GTC, EAP-MSCHAPv2, EAP-PEAP, EAP-TLS, EAP-TTLS
- Service Templates to configure 802.1X for wired / wireless or perform Posture checks are not allowed

HCG Mode requires ClearPass Insight to be enabled on at least one node in the cluster

Restore Defaults Save Cancel

The following table describes the **Cluster-Wide Parameters > Mode** parameter:

Table 282: *Cluster-Wide Parameters > Mode Parameter*

Parameter	Action/Description
High Capacity Guest Mode	To enable or disable High Capacity Guest mode, select TRUE or FALSE . The default is FALSE .

The following table describes the default cleanup interval values when High Capacity Guest mode is enabled:

Table 283: *Cleanup Interval Values in High Capacity Guest Mode*

Parameter	Description
Cleanup interval for Session log details in the database	The default value is 3 days .
Known endpoints cleanup interval	The default value of the known endpoints cleanup interval is 3 days .
Unknown endpoints cleanup interval	The default value of the unknown endpoints cleanup interval is 3 days .
Expired guest accounts cleanup interval	The default value of the Expired guest accounts cleanup interval is 10 days .

Table 283: Cleanup Interval Values in High Capacity Guest Mode (Continued)

Parameter	Description
Profiled endpoints cleanup interval	The default value of the Profiled endpoints cleanup interval is 3 days .
Old Audit Records cleanup interval	The default value of the Old Audit Records cleanup interval is 10 days .
Profiled Known endpoints cleanup option	Specify the cleanup interval in number of days that W-ClearPass uses to determine when to start deleting profiled known entries from the Endpoint repository. The default value is TRUE .

Service Templates Supported in High Capacity Guest Mode

The following service templates are supported when High Capacity Guest mode is enabled:

- W-ClearPass Admin Access (Active Directory)
- W-ClearPass Admin SSO Login (SAML SP Service)
- W-ClearPass Identity Provider (SAML IdP Service)
- Encrypted Wireless Access via 802.1X Public PEAP method
- Guest Access
- Guest Access - Web Login
- Guest MAC Authentication
- OAuth2 API User Access

Service Types Supported in High Capacity Guest Mode

The following service types are supported when High Capacity Guest mode is enabled:

- MAC Authentication
- RADIUS Authorization
- RADIUS Enforcement
- RADIUS Proxy
- Dell Application Authentication
- Dell Application Authorization
- TACACS+ Enforcement
- Web-based Authentication
- Web-based Open Network Access

Authentication Methods Supported in High Capacity Guest Mode

The following authentication methods are used in service templates in High Capacity Guest mode:

- PAP
- CHAP
- MSCHAP
- EAP_MD5
- MAC_AUTH
- AUTHORIZE

- EAP_PEAP_PUBLIC

Database

The following figure displays the **Cluster-Wide Parameters > Database** tab:

Figure 511: *Cluster-Wide Parameters > Database Tab*

Parameter Name	Parameter Value	Default Value
Auto backup configuration options	Config	Config
Database user "appexternal" password		
Replication Batch Interval	5 seconds	5
Store Password Hash for MSCHAP authentication	TRUE	TRUE
Store Local User passwords using reversible encryption	TRUE	TRUE

The following table describes the **Cluster-Wide Parameters > Database** parameters:

Table 284: *Cluster-Wide Parameters > Database Parameters*

Parameter	Action/Description
Auto backup configuration options	- Select any of the following auto-backup configuration options: Off: Select this to not to perform periodic backups. - Select Off before upgrading W-ClearPass Policy Manager to avoid the interference between Auto backup and migration process. Config: Perform a periodic backup of the configuration database only. This is the default auto backup configuration option. Config SessionInfo: Perform a backup of the configuration database and the session log database. NOTE: It is recommended that you set this option to Off or Config before starting an upgrade. This ensures the Auto Backup process does not interfere with migration post upgrade. If required, you can change this setting back to Config SessionInfo 24 hours after upgrade completion.
Database user "appexternal" password	Enter the password for the appexternal username for this connection to the database.
Replication Batch Interval	Configure the time interval (in seconds) at which the subscribers synchronize with the Publisher. The default value is 5 seconds. The allowed range is 1 to 60 seconds.

Table 284: Cluster-Wide Parameters > Database Parameters (Continued)

Parameter	Action/Description
Store Password Hash for MSCHAP authentication	4. To store passwords for admin and local users to Hash and NTLM hash formats (which enables RADIUS MSCHAP authentications against admin or local repositories), set this to TRUE . If you set this to FALSE , RADIUS MSCHAP authentications are not possible because the NTLM hash passwords are removed for all the users. NOTE: When you set this value to TRUE , you must reset all the passwords to reenale RADIUS MSCHAP authentication against the user repositories.
Store Local User Passwords using reversible encryption	5. To enable cleartext password comparison against local users, set this to TRUE . If you set this to FALSE , cleartext password comparison against local users is not possible because the reversible passwords for local users are removed. NOTE: After setting this value to TRUE , you must reset all the local user passwords to reenale cleartext password comparison against local users.

Make Subscriber

In the W-Policy Manager cluster environment, the publisher node acts as master. A W-Policy Manager cluster can contain only one publisher node. Administration, configuration, and database write operations may occur only on this master node.

The W-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. When it is a subscriber, you will not see this link.

To add a subscriber, navigate to the **Administration > Server Manager > Server Configuration** page, and click the **Make Subscriber** link. The following figure displays the **Add Subscriber Node** pop-up:

Figure 512: Add Subscriber Node

Add Subscriber Node

Publisher IP: 10.4.33.168

Publisher Password:

☒ Restore the local log database after this operation

☐ Do not backup the existing databases before this operation

WARNING : All application licenses on this server will be removed. Please contact support to add and activate these licenses.

Save Cancel

The following table describes the **Add Subscriber Node** parameters:

Table 285: *Add Subscriber Node*

Parameter	Description
Publisher IP	Specify publisher address and password. NOTE: The password specified here is the password for the CLI user <i>appadmin</i>
Publisher Password	
Restore the local log database after this operation	Select the check box to restore the log database following addition of a subscriber node.
Do not backup the existing databases before this operation	Select the check box only if you do not require a backup to the existing database.

Collect Logs

When you need to review performance or troubleshoot issues in detail, Policy Manager can compile and save transactional and diagnostic data into several log files. These files are saved in Local Shared Folders and can be downloaded to your computer.

To collect logs:

1. Navigate to **Administration > Server Manager > Server Configuration**,
2. Click **Collect Logs**. The **Collect Logs** pop-up appears.
3. Enter an output filename and add the .tar.gz extension to the filename.
4. Select the types of logging information you want to collect. The types of logging are:
 - System Logs
 - Logs from all Policy Manager services
 - Capture network packets Duration of dump



Use this option only when you want to debug a problem. System performance can be severely impacted.

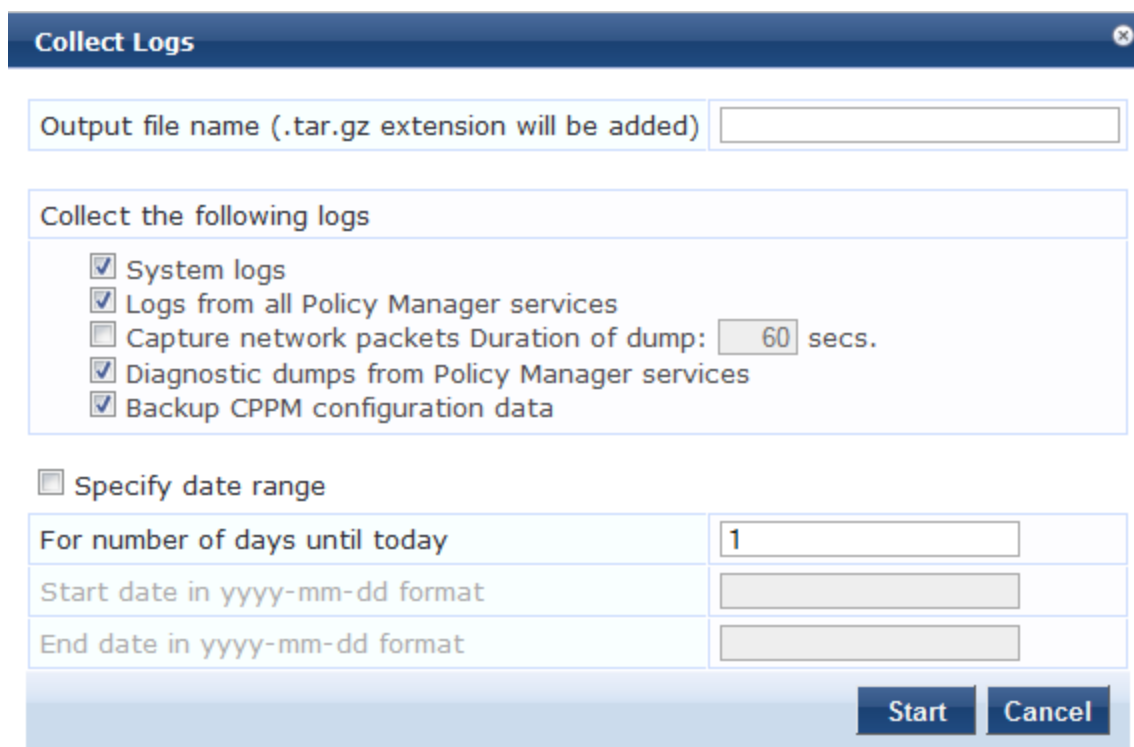
- Diagnostic dumps from Policy Manager services
 - Backup CPPM Configuration data
5. Enter the time period for which you want to collect the information.
 - Specify a number to collect logs for the number of days until the current day.
 - Select the **Specify date range** check box and enter a start date and end date in yyyy.mm.dd format in the respective fields to collect logs for the specified time period.
 6. Click **Start**. You'll see the progress of the information collection.
 7. Click **Close** to finish or click **Download File** to save the log file to your computer.



If you are attempting to open a capture file (.cap or .pcap) using WireShark, untar or unzip the file (based on the file extension). When the entire file is extracted, navigate to the PacketCapture folder. In this folder, you will find a file with a .cap extension. WireShark can be used to open this file and study the network traffic.

The following figure displays the **Collect Logs** pop-up:

Figure 513: *Collect Logs*



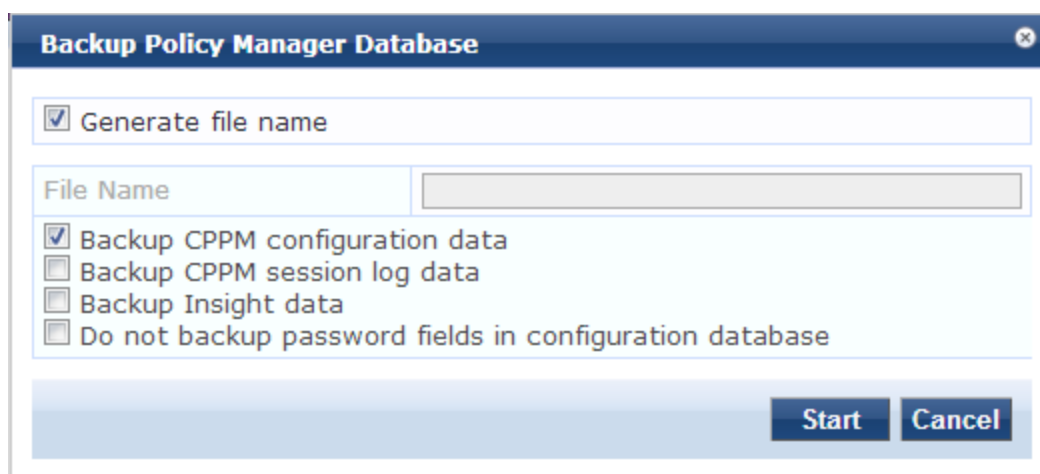
The **Collect Logs** dialog box features a title bar with a close button. Below the title bar is a text input field for the "Output file name (.tar.gz extension will be added)". The main section, titled "Collect the following logs", contains a list of checkboxes: "System logs" (checked), "Logs from all Policy Manager services" (checked), "Capture network packets Duration of dump: 60 secs." (unchecked), "Diagnostic dumps from Policy Manager services" (checked), and "Backup CPPM configuration data" (checked). Below this list is an unchecked checkbox for "Specify date range". If selected, it would reveal three input fields: "For number of days until today" (with a value of 1), "Start date in yyyy-mm-dd format", and "End date in yyyy-mm-dd format". At the bottom right are "Start" and "Cancel" buttons.

Backup

Navigate to the **Administration > Server Manager > Server Configuration** page and click the **Back Up** button.

The following figure displays the **Backup Policy Manager Database** pop-up:

Figure 514: *Backup Popup*



The **Backup Policy Manager Database** dialog box has a title bar with a close button. It contains a checked checkbox for "Generate file name", which is followed by a "File Name" input field. Below this are four checkboxes: "Backup CPPM configuration data" (checked), "Backup CPPM session log data" (unchecked), "Backup Insight data" (unchecked), and "Do not backup password fields in configuration database" (unchecked). "Start" and "Cancel" buttons are located at the bottom right.

The following table describes the **Backup Policy Manager Database** parameters:

Table 286: *Backup Policy Manager Database*

Parameter	Description
Generate filename	Select the check box to enable W-Policy Manager to generate a filename; otherwise, specify a filename. Backup files are in the gzipped tar format (tar.gz extension). The backup file is automatically placed in the <i>Shared Local Folder</i> under folder type <i>Backup Files</i> (See Local Shared Folders).
Filename	
Do not backup log database	Select the check box if you do not want to backup the log database.
Do not backup password fields in configuration database	Select the check box if you do not want to backup password fields in configuration database.
Backup databases for installed applications	Select the check box if you want the backup to include databases for installed applications.

Restore

Navigate to the **Administration > Server Manager > Server Configuration** page and click the **Restore** button to restore W-ClearPass Policy Manager configuration data.

The following figure displays the **Restore Policy Manager Database** pop-up:

Figure 515: *Restore Policy Manager Database*

Restore Policy Manager Database

Restore file location ☒ Upload file to server ☐ File is on server

Upload file:

No file selected.

☒ Restore CPPM configuration data (if it exists in the backup)
☐ Restore CPPM session log data (if it exists in the backup)
☐ Restore Insight data (if it exists in the backup)
☐ Ignore version mismatch and attempt data migration
☐ Restore cluster server/node entries from backup
☐ Do not backup the existing databases before this operation

The following table describes the **Restore Policy Manager Database** parameters:

Table 287: *Restore Policy Manager Database*

Parameter	Description
Restore file location	Select either Upload file to server or File is on server .
Upload file path	Browse to select name of backup file. NOTE: This option is available only when the Upload file to server option is selected.
Shared backup files present on the server	If the files is on a server, select a file from the files in the local shared folders. (See Local Shared Folders .) NOTE: This is displayed only when the File on server option is selected.
Restore CPPM configuration data (if it exists in the backup)	Select the check box to include an existing configuration data in the restore.
Restore CPPM session log data (if it exists in the backup).	Select the check box to include the log data in the restore.
Restore Insight data (if it exists in the backup)	Select the check box to include Insight reporting data in the restore.
Ignore version mismatch and attempt data migration	Select the check box if 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.	Select the check box to include the cluster server/node entries in the restore.
Do not backup the existing databases before this operation.	Select the check box if you do not want to backup the existing databases before performing a restore.

Cleanup

You can perform a system cleanup operation to purge the following records:

- System and application log files
- Past authentication records
- Audit records
- Expired guest accounts
- Past auto and manual backups
- Stored reports

To perform a system cleanup:

1. Navigate to the **Administration > Server Manager > Server Configuration** page and click the **Cleanup** button. The **Force Cleanup Files** pop-up is displayed.
2. Enter a number to cleanup files that are older than the specified number of days. The allowed range is 0-15.
3. Click **Start** to initiate the cleanup process.

The following figure displays the **Cleanup** option in the **Server Configuration** page:

Figure 516: *Server Configuration - Cleanup*

Administration » Server Manager » Server Configuration
Server Configuration

Publisher Server: Garuda-197 [10.17.4.197]

#	Server Name ▲	Management Port	Data Port	Zone	Profile	Cluster Sync	Last Sync Time
1.	Garuda-197	10.17.4.197	-	198-zone	Enabled	Enabled	-
2.	Garuda-198	10.17.4.198	-	198-zone	Enabled	Enabled	Dec 21, 2014 12:23:31 IST
3.	Garuda-199	10.17.4.199	-	197-zone	Enabled	Enabled	Dec 21, 2014 12:23:31 IST

Showing 1-3 of 3

[Collect Logs](#)
[Backup](#)
[Restore](#)
[Cleanup](#)
[Shutdown](#)
[Reboot](#)
[Drop Subscriber](#)

[Set Date & Time](#)
[Change Cluster Password](#)
[Manage Policy Manager Zones](#)
[NetEvents Targets](#)
[Virtual IP Settings](#)
[Clear Machine Authentication Cache](#)
[Cluster-Wide Parameters](#)

The following figure displays the **Force Cleanup Files** pop-up:

Figure 517: *Force Cleanup Files*

Force Cleanup Files

Cleanup files older than

5

days

Note:

This action will perform system cleanup operation that will result in purging of:

- System and application log files
- Past authentication records
- Audit records
- Expired guest accounts
- Past auto and manual backups
- Stored reports

Start

Cancel

The following figure displays the cleanup progress:

Figure 518: *Cleanup Progress Screen*



Shutdown/Reboot

Navigate to the **Administration > Server Manager > Server Configuration** page and click the **Shutdown** or **Reboot** buttons to shutdown or reboot the node.

Drop Subscriber

Navigate to the **Administration > Server Manager > Server Configuration** page and click the **Drop Subscriber** button to drop a subscriber from the cluster.



This option is not available in a single node deployment.

Log Configuration

To configure logs for services and system level, navigate to the **Administration > Server Manager > Log Configuration** page.

This section provides the following information:

- [Service Log Configuration](#)
- [System Level Configuration](#)

Service Log Configuration

The following figure displays the **Service Log Configuration** dialog:

Figure 519: *Log Configuration > Service Log Configuration Tab*

Administration » Server Manager » Log Configuration

Log Configuration

Select Server: 10.2.50.178

Service Log Configuration System Level

Select Service: Policy server

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	INFO
6. Common Framework	INFO
7. External Posture Validation	INFO
8. Internal Posture Validation	INFO
9. Audit Server support	INFO
10. SOAP API	INFO

The following table describes the **Service Log Configuration** parameters:

Table 288: *Log Configuration > Service Log Configuration Parameters*

Parameter	Action/Description
Select Server	1. From the Select Server drop-down, specify the server for which you want to configure logs. All nodes in the cluster appear in the drop-down list.
Select Service	2. Specify the service for which you want to configure logs.
Module Log Level Settings	3. Select the Module Log Level Settings check box to set the log level for each module individually (listed in decreasing level of verbosity). For optimal performance you must run W-Policy Manager with the log level set to ERROR or FATAL : ■ DEBUG ■ INFO ■ WARN ■ ERROR ■ FATAL If this option is disabled, then all module level logs are set to the default log level.
Default Log Level	4. Specify the default logging level for all modules. The Default Log Level drop-down list is available if the Module Log Level Settings option is disabled. Available options include the following: ■ DEBUG ■ INFO

Table 288: *Log Configuration > Service Log Configuration Parameters (Continued)*

Parameter	Action/Description
	■ WARN ■ ERROR ■ FATAL NOTE: Set this option first, and then override any specific modules as necessary.
Restore Defaults/Save	5. Click Save to save changes. ■ To restore the default settings, click Restore Defaults.

System Level Configuration

The following figure displays the **System Level** dialog:

Figure 520: *Log Configuration - System Level tab*

Administration » Server Manager » Log Configuration

Log Configuration

Select Server: 10.2.50.178

Service Log Configuration **System Level**

Number of log files: 6 (default is 6 files)

Limit each log file size to: 10 MB (default is 10 MB)

Syslog Settings:

Syslog Server:

Syslog Server Port: 514 (default is 514)

Service Name	Enable Syslog	Syslog Filter Level
1. Policy server	☐	WARN
2. Radius server	☐	WARN
3. Tacacs server	☐	WARN
4. Admin server	☐	WARN
5. Syslog client service	☐	WARN
6. ClearPass network services	☐	WARN

The following table describes the **System Level** tab parameters:

Table 289: *Log Configuration > System Level Parameters*

Parameter	Action/Description
Select Server	1. Specify the server for which you want to configure logs.
Number of log files	2. Specify the number of log files of a specific module to keep at any given time. When a log file reaches the specified size (see Limit each log file size to), W-Policy Manager rolls the log over to another file until the specified number of log files is reached. Once the number of log files exceeds the specified value, W-Policy Manager overwrites the oldest file.
Limit each log file size to	3. Specify the size of each log file before the log rolls over to the next file. The default value is 50 MB.

Table 289: Log Configuration > System Level Parameters (Continued)

Parameter	Action/Description
Syslog Settings	
Syslog Server	4. Specify the name of the syslog server. W-Policy Manager sends the configured module logs to this syslog server.
Syslog Server Port	5. Specify the syslog server port number. The default is 514 .
Enable Syslog	6. To override the Syslog Filter Level for a service, select the Enable Syslog check box.
Syslog Filter Level	7. If desired, change the Syslog Filter Level. The current Syslog Filter level is based on the default log level specified on the Service Log Configuration tab.
Restore Defaults/Save	8. Click Save to save your changes. ■ To restore the default settings, click Restore Defaults .

Local Shared Folders

The supported W-ClearPass folder types are:

- **Backup files:** Database backup files that are backed up manually.
- **Log files:** Log files backed up via the method described in [Collect Logs on page 518](#).
- **Automated Backup files:** Database backup files that are backed up automatically on a daily basis.

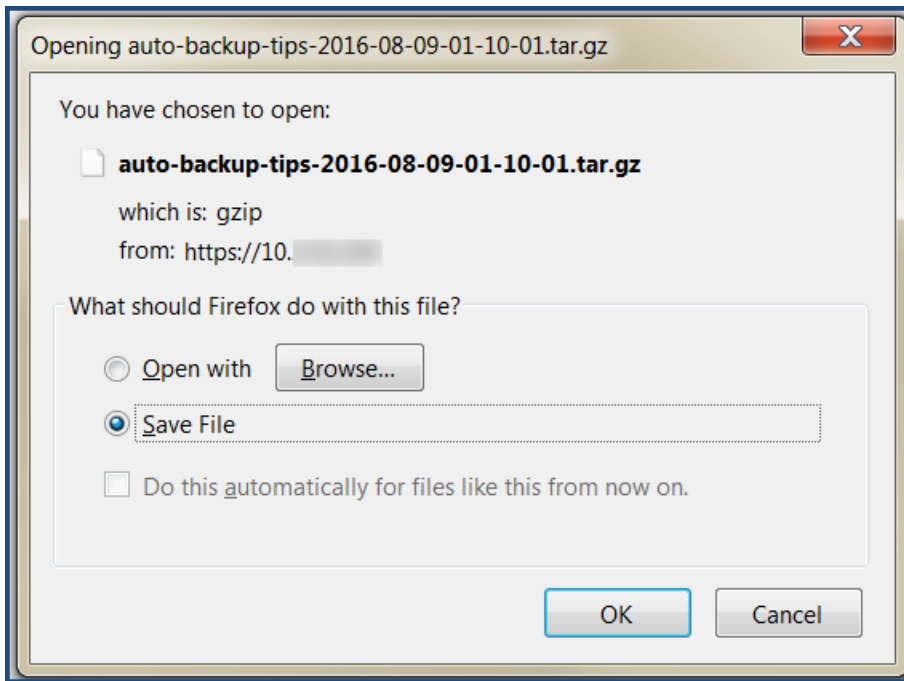
To download a local shared folder:

1. Navigate to **Administration > Server Manager > Local Shared Folders**.
The **Local Shared Folders** page opens.
2. Choose a folder type from the **Select folder** drop-down list.
The folders in the selected shared folder are displayed.

Figure 521: Local Shared Folders Page

Administration » Server Manager » Local Shared Folders			
Local Shared Folders			
Select folder: Automated Backup files			
#	File Name	File Size	Last Modified Time
1.	auto-backup-tips-2016-08-09-01-10-01.tar.gz	4.12 MB	Aug 09, 2016 01:10:05 PDT
2.	auto-backup-tips-2016-08-08-01-10-01.tar.gz	4.12 MB	Aug 08, 2016 01:10:06 PDT
3.	auto-backup-tips-2016-08-07-01-10-01.tar.gz	4.12 MB	Aug 07, 2016 01:10:06 PDT
4.	auto-backup-tips-2016-08-06-01-10-01.tar.gz	4.12 MB	Aug 06, 2016 01:10:06 PDT
5.	auto-backup-tips-2016-08-05-01-10-01.tar.gz	4.12 MB	Aug 05, 2016 01:10:07 PDT
6.	auto-backup-tips-2016-08-04-01-10-01.tar.gz	4.12 MB	Aug 04, 2016 01:10:07 PDT
7.	auto-backup-tips-2016-08-03-01-10-01.tar.gz	4.13 MB	Aug 03, 2016 01:10:06 PDT
8.	auto-backup-tips-2016-08-02-01-10-01.tar.gz	4.13 MB	Aug 02, 2016 01:10:06 PDT

3. Select the folder you want to download.
The following dialog opens:



4. You can either browse to an application to open the selected folder or save the tar.gz file to your hard disk:
 - a. To open the folder, click **Browse**, select the application to open the tar.gz file, then click **OK**.
 - b. To save the file, select **Save File**, then click **OK**.

The file is downloaded to your system.

License Management

This section describes the following topics:

- [Licensing Page on page 527](#)
- [Adding an Application License on page 528](#)
- [Activating a Server License on page 529](#)
- [Activating an Application License on page 530](#)
- [Updating a Server License on page 531](#)
- [Updating an Application License on page 532](#)

The **Licensing** page shows all the licenses that are activated for the entire W-ClearPass Policy Manager cluster. You must have a W-ClearPass Policy Manager base license for every instance of the product.



If the number of licenses used exceeds the number of licenses purchased, you will see a warning four months after the number is exceeded. The number of used licenses is based on the daily average.



On a virtual machine instance of W-ClearPass, the permanent license must be entered.

Licensing Page

To manage licenses, navigate to **Administration > Server Manager > Licensing**.

The **Licensing** page opens to the **License Summary** tab:



The **Applications** tab gets activated on adding an application license such as OnGuard, Guest, or Onboard.

License Summary Tab

You can add and activate OnGuard, Guest, Onboard, and Enterprise licenses.

The **License Summary** tab displays the number of purchased licenses for W-Policy Manager, OnGuard, Guest, Onboard, and W-ClearPass Enterprise.

The following figure displays the **Licensing > License Summary** tab:

Figure 522: *Licensing > License Summary Tab*

Administration > Server Manager > Licensing				Add License
Licensing				
License Summary Servers				
Cluster License Summary				
	License Type	Total Count	Used Count	Updated At
1	Policy Manager	5000	0	2016/08/09 03:07:01
2	ClearPass Enterprise	25	0	2016/08/09 03:07:02

Note: The license count for ClearPass Enterprise is inclusive of 25 endpoints, for every CPPM node.

Licensing > Servers Tab

The **Licensing > Servers** tab displays the W-Policy Manager server IP address, the product type, license type, license activation status, and many more parameters.

The following figure displays the **Licensing > Servers** tab:

Figure 523: *Licensing > Servers Tab*

Administration > Server Manager > Licensing									Add License
Licensing									
License Summary Servers									
#	Server IP Address	Product	License Type	Native	Number of Endpoints	Duration	Activation Status	License Added On	
1	10.10.10.10	Policy Manager	Permanent	No	5000	-	Activated	Jul 18, 2016 19:06:36 PDT	

Licensing > Applications Tab

The **Licensing > Applications** tab displays the W-ClearPass Policy Manager application license details such as product type, license type, number of endpoints, and license activation status.

The following figure displays the **Licensing > Applications** tab:

Figure 524: *Licensing > Applications Tab*

Administration > Server Manager > Licensing							Add License
Licensing							
License Summary Servers Applications							
#	Product	License Type	Number of Endpoints	Duration	Activation Status	License Added On	
1	OnGuard	Permanent	100	-	Activate	Aug 09, 2016 14:28:43 PDT	
2	Guest	Permanent	100	-	Activate	Aug 09, 2016 14:14:58 PDT	

Adding an Application License

To add an application license:

1. Navigate to **Administration > Server Manager > Licensing**.
2. Click the **Add License** link at the top-right section of the page.

The **Add License** page opens.

Figure 525: Add License Page

Add License

Product: OnGuard

License Key

Terms and Conditions

Aruba Networks, Inc. End-User Software License Agreement ("Agreement")

IMPORTANT

YOU SHOULD CAREFULLY READ THE FOLLOWING TERMS BEFORE INSTALLATION OR USE OF ANY SOFTWARE PROGRAMS FROM ARUBA NETWORKS, INC. AND ITS AFFILIATES OR AIRWAVE WIRELESS (COLLECTIVELY, "ARUBA"). INSTALLATION OR USE OF SUCH SOFTWARE PROGRAMS

☒ I agree to the above terms and conditions.

Add Cancel

3. **Product:** Choose a product from the **Product** drop-down list:
 - OnGuard
 - Guest
 - Onboard
 - W-ClearPass Enterprise
4. **License Key:** Enter the license key.
5. Click the **I agree to the above terms and conditions** check box.
The **Add** button is now enabled.
6. Click **Add**.
You return to the **Licensing > License Summary** page, where the new application license is now listed.
When you add an application license, the **Applications** tab is enabled to allow you to activate a new application license.

Activating a Server License

You activate a server license only once, when you first install W-ClearPass W-Policy Manager on a server.

To activate a W-ClearPass W-Policy Manager server license:

1. Navigate to **Administration > Server Manager > Licensing**.
2. Click the **Servers** tab.
A W-ClearPass server that is not activated has the keyword **Activate** next to the red circle in the **Activation Status** column.
3. Click **Activate**.
The **Activate License** page opens.

Figure 526: *Activate License Page*

4. In the **Online Activation** section, click **Activate Now**.

The W-ClearPass W-Policy Manager server license is now activated. The **Applications** tab > **Activation Status** column shows a green circle next to the keyword **Activated**.

If You Are Not Connected to the Internet

If you are not connected to the Internet:

1. In the **Offline Activation** section, click **Download** to download an activation request token from the W-Policy Manager server.
2. Email the activation request token file to the Dell Support Center (<https://download.dell-pcw.com>).
You will receive an activation key.
3. Click **Browse** to locate the activation key file on your system, then click **Upload**.

Activating an Application License

After you add or update an application license, it must be activated. Adding or updating an application license enables the **Applications** tab on the Licensing page.

1. Navigate to **Administration > Server Manager > Licensing**.

The **Licensing** page opens to the **License Summary** page.

2. Select the **Applications** tab.

The new application licenses are listed. The **Activation Status** column shows a red circle next to the keyword **Activate**.

Figure 527: *Application Licenses Ready to Be Activated*

Administration » Server Manager » Licensing						
Licensing + Add License						
License Summary Servers Applications						
#	Product	License Type	Number of Endpoints	Duration	Activation Status	License Added On
1	OnGuard	Permanent	100	-	Activate	Aug 09, 2016 14:28:43 PDT
2	Guest	Permanent	100	-	Activate	Aug 09, 2016 14:14:58 PDT

3. Click **Activate**.

The **Activate License** page opens.

Figure 528: *Activate License Page*

Activate License

Online Activation

Activate Now

Offline Activation

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

Step 1. Download an Activation Request Token **Download**

Step 2. Email the Activation Request Token to Aruba Networks Support (support@arubanetworks.com)

Step 3. **Browse...** No file selected. **Upload**

Upload the Activation Key received from Aruba Networks Support

4. In the **Online Activation** section, click **Activate Now**.

The selected application license is now activated. The **Applications** tab > **Activation Status** column shows a green circle next to the keyword **Activated**.

If You Are Not Connected to the Internet

If you are not connected to the Internet:

1. In the **Offline Activation** section, click **Download** to download an activation request token from the W-Policy Manager server.
2. Email the activation request token file to the Dell (<https://download.dell-pcw.com>) Support Center.
You will receive an activation key.
3. Click **Browse** to locate the activation key file on your system, then click **Upload**.

Updating a Server License

Licenses typically require updating after they expire, for example, after the evaluation license expires, or when capacity exceeds its licensed amount.

To update a W-ClearPass W-Policy Manager server license:

1. Navigate to **Administration > Server Manager > Licensing**.
The **Licensing** page opens.
2. Select the **Servers** tab.
3. Click the W-ClearPass server entry.
The **Update License** dialog opens.

Figure 529: *Update License Dialog*

Update License

Old License Key

[XXXXXXXXXXXX-XXXXXXXXXXXX-XXXXXXXXXXXX-XXXXXXXXXXXX]

New License Key

Terms and Conditions

Aruba Networks, Inc. End-User Software License Agreement ("Agreement")

IMPORTANT

YOU SHOULD CAREFULLY READ THE FOLLOWING TERMS BEFORE INSTALLATION OR USE OF ANY SOFTWARE PROGRAMS FROM ARUBA NETWORKS, INC. AND ITS AFFILIATES OR AIRWAVE

☒ I agree to the above terms and conditions.

Update

Cancel

4. Enter the new license key.
5. Click the **I agree to the above terms and conditions** check box.
The **Update** button is now activated.
6. Click **Update**.

Updating an Application License

Application licenses typically require updating after they expire, for example, after the evaluation license expires, or when capacity exceeds its licensed amount.

To update an application license:

1. Navigate to **Administration > Server Manager > Licensing**.
The **Licensing** page opens.
2. Select the **Applications** tab.
3. Select the application license you need to update.
The **Update License** dialog opens.

Figure 530: *Update License Dialog*

Update License

Old License Key

XXXXXXXXXX-XXXXXX-XXXXXX-XXXXXX-XXXXXX

New License Key

Terms and Conditions

Aruba Networks, Inc. End-User Software License Agreement ("Agreement")

IMPORTANT

YOU SHOULD CAREFULLY READ THE FOLLOWING TERMS BEFORE INSTALLATION OR USE OF ANY SOFTWARE PROGRAMS FROM ARUBA NETWORKS, INC. AND ITS AFFILIATES OR AIRWAVE

☒ I agree to the above terms and conditions.

Update

Cancel

4. Enter the new license key.
5. Click the **I agree to the above terms and conditions** check box.
The **Update** button is now activated.
6. Click **Update**.

SNMP Trap Receivers

This section provides the following information:

- [SNMP Trap Receivers Main Page on page 533](#)
- [Adding an SNMP Trap Server on page 533](#)
- [Importing an SNMP Trap Server on page 534](#)
- [Exporting All SNMP Trap Servers on page 535](#)
- [Exporting an SNMP Trap Server on page 536](#)
- [Deleting an SNMP Trap Server on page 537](#)

W-ClearPass W-Policy Manager sends SNMP traps that expose the following server information:

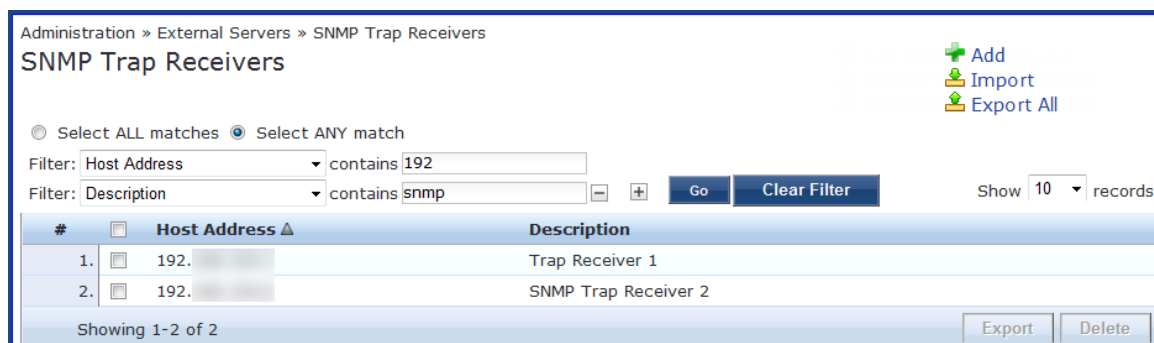
- **System up-time:** Provides information about how long the W-ClearPass server has been running.
- **Network interface statistics [up/down]:** Provides information about whether the network interface is up or down.
- **Process monitoring information:** Checks for the processes that should be running, including maximum and minimum number of allowed instances. Sends traps if there is a change in value of the maximum and minimum numbers.
- **Disk usage:** Checks for disk space usage of a partition. The agent can check the amount of available disk space and make sure it's above the set limit. The value can be in percentage as well. Sends traps if there is a change in the value.
- **CPU load information:** Checks for unreasonable load average values. For example, if CPU load average for one minute exceeds the configured value (in percentage), the W-ClearPass server sends a trap to the configured destination.
- **Memory usage:** Reports the W-ClearPass server's memory usage.

SNMP Trap Receivers Main Page

To view a list of SNMP trap receivers configured on the W-ClearPass Policy Manager server, navigate to **Administration > External Servers > SNMP Trap Receivers**.

The following figure displays the **SNMP Trap Receivers** page:

Figure 531: *SNMP Trap Receivers Page*



About the W-ClearPass SNMP Private MIB

For information about the W-ClearPass SNMP Private MIB, see [W-ClearPass SNMP Private MIB on page 779](#).

Adding an SNMP Trap Server

To add an SNMP trap server:

1. Navigate to **Administration > External Servers > SNMP Trap Receivers**.

2. Click the **Add** link on the top right section of the page. Enter the details based on [Table 290](#).
3. Click **Save**.

The following figure displays the **Add SNMP Trap Server** pop-up:

Figure 532: Add SNMP Trap Server Pop-up

The following table describes the **Add SNMP Trap Server** parameters:

Table 290: Add SNMP Trap Server Parameters

Parameter	Description
Host Address	Enter the trap destination hostname or IP address. NOTE: This server must have an SNMP trap receiver or trap viewer installed.
Description	Enter a short description of the SNMP trap server.
SNMP Version	Select the SNMP version.
Community String / Verify	Enter and re-enter the community string for sending the traps.
Server Port	Port number for sending the traps. By default, the port number is 162. NOTE: Configure the trap server firewall for traffic on this port.

Importing an SNMP Trap Server

To import an SNMP trap server:

1. Navigate to **Administration > External Servers > SNMP Trap Receivers**.
2. Click the **Import** link on the top right section of the page. Enter the details based on [Table 291](#).
3. Click **Import**.

The following figure displays the **Import from file** pop-up:

Figure 533: *Import from file Pop-up*

The screenshot shows a window titled "Import from file". Inside, there's a "Select File:" label next to a button labeled "Choose File" and a text area showing "No file chosen". Below that is a label "Enter secret for the file (if any):" followed by an empty text input field. At the bottom right of the window are two buttons: "Import" and "Cancel".

The following table describes the **Import from file** parameters:

Table 291: *Import from file Parameters*

Parameter	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 secret key here.

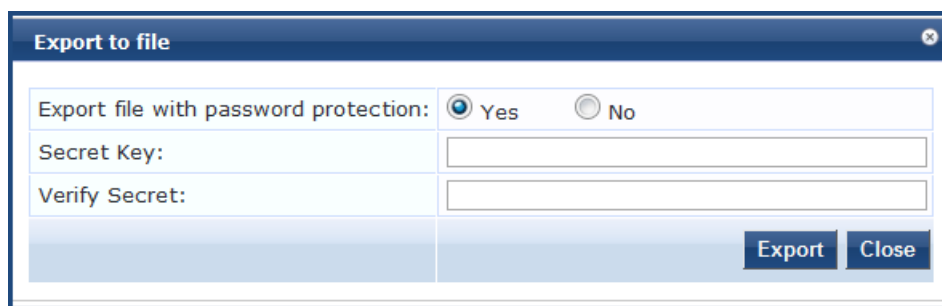
Exporting All SNMP Trap Servers

This link exports all configured SNMP Trap Receivers. To export all SNMP trap servers:

1. Navigate to **Administration > External Servers > SNMP Trap Receivers**.
2. Click the **Export All** link on the top right section of the page. Enter the details based on [Table 292](#).
3. Click **Export**.
4. Enter the XML file name in the **Save As** dialog box.
5. Click **Save**.

The following figure displays the **Export to file** pop-up:

Figure 534: *Export to file Pop-up*



The screenshot shows a dialog box titled "Export to file". It has a close button in the top right corner. The main content area has a label "Export file with password protection:" followed by two radio buttons: "Yes" (which is selected) and "No". Below this are two text input fields: "Secret Key:" and "Verify Secret:". At the bottom right of the dialog are two buttons: "Export" and "Close".

The following table describes the **Export to file** parameters:

Table 292: *Export to file Parameters*

Parameter	Description
Export file with password protection	Choose Yes to export the file with password protection.
Secret Key	Enter the secret key.
Verify Secret	Re-enter the secret key.

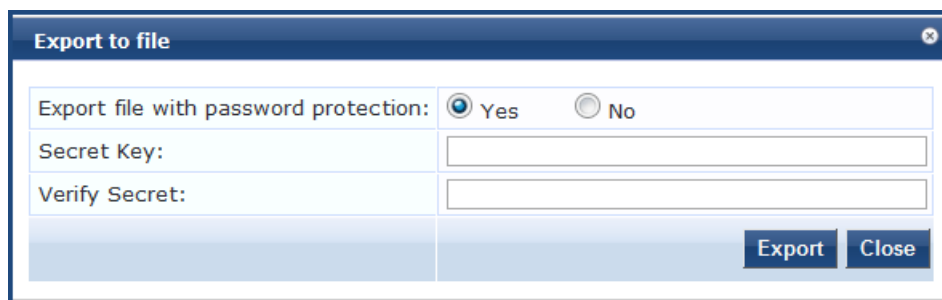
Exporting an SNMP Trap Server

To export a single SNMP trap server:

1. Navigate to **Administration > External Servers > SNMP Trap Receivers**.
2. Select the **Host Address** from the list of check boxes and click **Export**. Enter the details based on [Table 293](#).
3. Enter the name of the XML file in the **Save As** dialog.
4. Click **Save**.

The following figure displays the **Export to file** pop-up:

Figure 535: *Export to file Pop-up*



This is an identical screenshot to Figure 534, showing the "Export to file" dialog box. The "Yes" radio button is selected for "Export file with password protection". The "Secret Key" and "Verify Secret" fields are empty. The "Export" and "Close" buttons are visible at the bottom right.

The following table describes the **Export to file** parameters:

Table 293: *Export to file Parameters*

Parameter	Description
Export file with password protection	Choose Yes to export the file with password protection.
Secret Key	Enter the secret key.
Verify Secret	Re-enter the secret key.

Deleting an SNMP Trap Server

To delete a single SNMP trap server:

1. Navigate to **Administration > External Servers > SNMP Trap Receivers**.
2. Click the check box next to the **Host Address** entry and click **Delete**.
3. Click **Yes**.

Syslog Targets

W-ClearPass Policy Manager can export session data (see [Live Monitoring: Access Tracker on page 107](#)), audit records (see [Audit Viewer on page 152](#)) and event records (see [Event Viewer on page 155](#)). This information can be sent to one or more syslog targets (servers). You configure syslog targets from this page. To configure syslog target, navigate to **Administration > External Servers > Syslog Targets**.

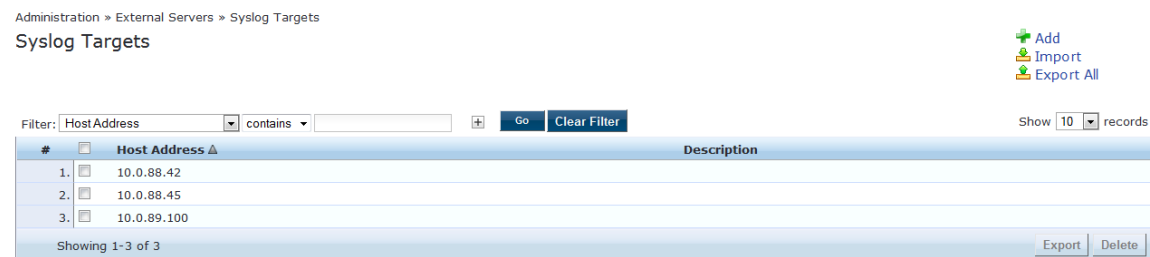
This section describes the following topics:

- [Syslog Targets Main Page on page 537](#)
- [Adding a Syslog Target on page 538](#)
- [Importing a Syslog Target on page 539](#)
- [Exporting All Syslog Target on page 540](#)
- [Exporting a Syslog Target on page 540](#)
- [Exporting a Syslog Target on page 540](#)

Syslog Targets Main Page

The following figure displays the **Syslog Targets** page:

Figure 536: *Syslog Targets Page*



The following table describes the **Syslog Targets** parameters:

Table 294: *Syslog Targets Parameters*

Parameter	Description
Add	Opens the Add Syslog Target pop-up.
Import	Opens the Import from file pop-up. You can import the syslog target from a file.
Export All	Opens the Export to file pop-up. You can export all the syslog target entries to a file.
Export	Opens the Export to file pop-up. With this option, you can export individual syslog targets.
Delete	Deletes a syslog target server.

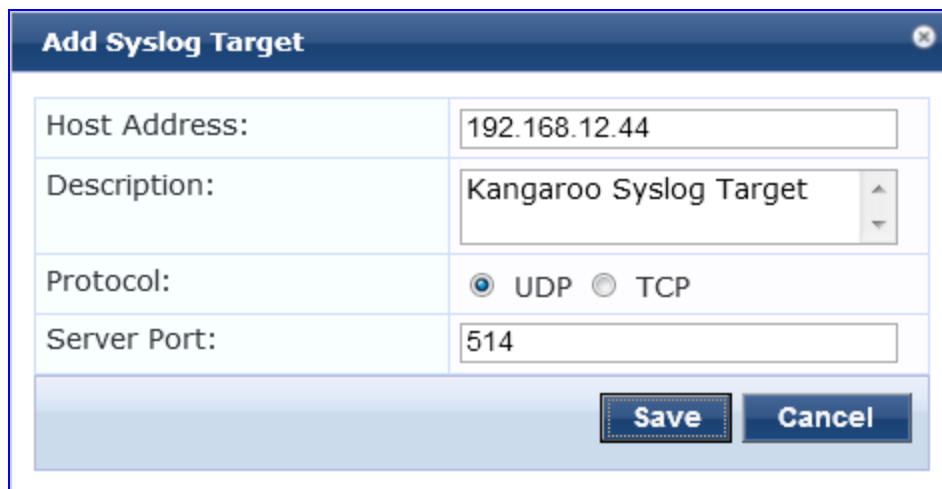
Adding a Syslog Target

To add a syslog target:

1. Navigate to **Administration > External Servers > Syslog Targets**.
2. Click the **Add** link on the top right section of the page. Enter the details based on [Table 295](#).
3. Click **Save**.

The following figure displays the **Add Syslog Target** pop-up:

Figure 537: *Add Syslog Target Pop-up*



The screenshot shows a modal window titled "Add Syslog Target". It contains the following fields and controls:

- Host Address:** A text input field containing "192.168.12.44".
- Description:** A text input field containing "Kangaroo Syslog Target".
- Protocol:** Two radio buttons, "UDP" (which is selected) and "TCP".
- Server Port:** A text input field containing "514".
- Buttons:** "Save" and "Cancel" buttons located at the bottom right of the form area.

The following table describes the **Add Syslog Target** parameters:

Table 295: Add Syslog Target Parameters

Parameter	Description
Host Address	Syslog server hostname or IP address.
Description	Enter a short description of the syslog server.
Protocol	Select one of the following options: • UDP: This option reduces overhead and latency. • TCP: this option provides error checking and packet delivery validation.
Server Port	Port number for sending the syslog messages. Default port number is 514.

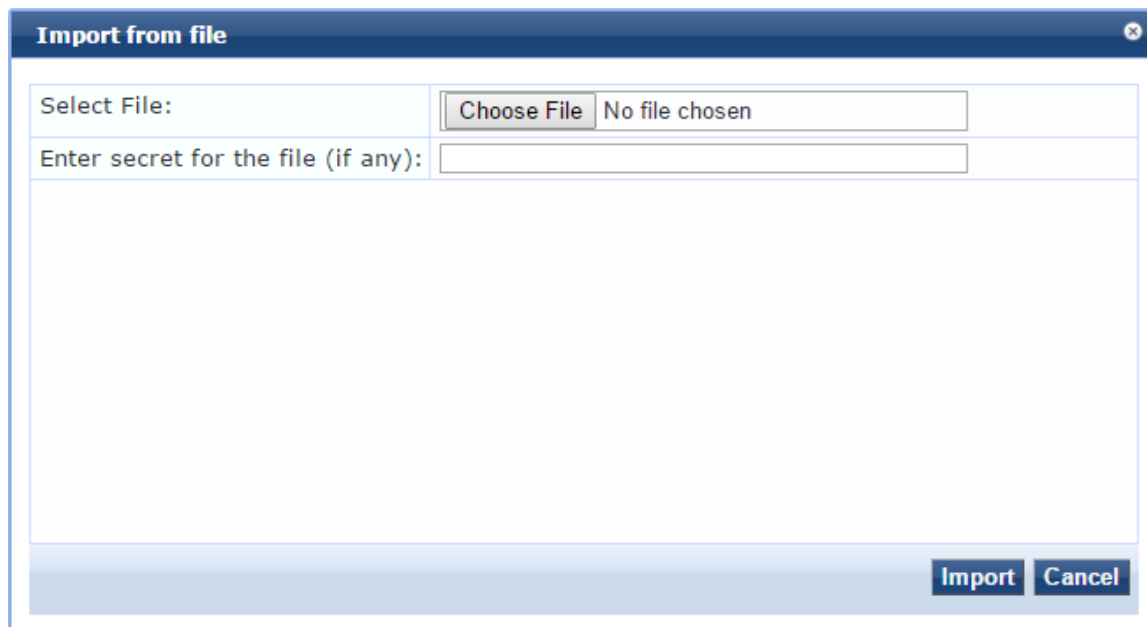
Importing a Syslog Target

To import a syslog target:

1. Navigate to **Administration > External Servers > Syslog Targets**.
2. Click the **Import** link on the top right section of the page. Enter the details based on [Table 296](#).
3. Click **Import**.

The following figure displays the **Import from file** pop-up:

Figure 538: Import from file Pop-up

The image shows a web-based dialog box titled "Import from file" with a close button (X) in the top right corner. The dialog contains a "Select File:" label followed by a "Choose File" button and a text field displaying "No file chosen". Below this is a label "Enter secret for the file (if any):" followed by an empty text input field. The bottom of the dialog features a large empty rectangular area and two buttons, "Import" and "Cancel", in the bottom right corner.

The following table describes the **Import from file** parameters:

Table 296: *Import from file Parameters*

Parameter	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.

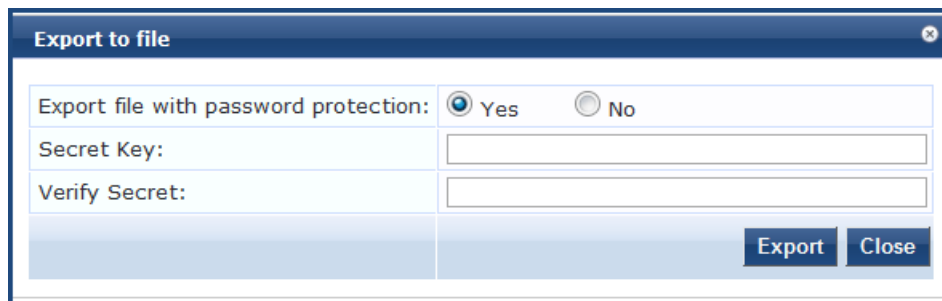
Exporting All Syslog Target

To export all syslog targets:

1. Navigate to **Administration > External Servers > Syslog Targets**.
2. Click the **Export All** link on the top right section of the page. Enter the details based on [Table 297](#).
3. Click **Export**.
4. Enter the XML file name in the **Save As** dialog box.
5. Click **Save**.

The following figure displays the **Export to file** pop-up:

Figure 539: *Export to file Pop-up*



The following table describes the **Export to file** parameters:

Table 297: *Export to file Parameters*

Parameter	Description
Export file with password protection	Choose Yes to export the file with password protection.
Secret Key	Enter the secret key.
Verify Secret	Re-enter the secret key.

Exporting a Syslog Target

To export a syslog target:

1. Navigate to **Administration > External Servers > Syslog Targets**.
2. Select the **Host Address** from the list of check boxes and click **Export**. Enter the details based on [Table 297](#).

3. Enter the name of the XML file in the **Save As** dialog.
4. Click **Save**.

The following figure displays the **Export to file** pop-up:

Figure 540: *Export to file Pop-up*

The following table describes the **Export to file** parameters:

Table 298: *Export to file Parameters*

Parameter	Description
Export file with password protection	Choose Yes to export the file with password protection.
Secret Key	Enter the secret key.
Verify Secret	Re-enter the secret key.

Deleting a Syslog Target

To delete a syslog target:

1. Navigate to **Administration > External Servers > Syslog Targets**.
2. Click the check box next to the **Host Address** entry and click **Delete**.
3. Click **Yes**.

Syslog Export Filters

This section describes the following topics:

- [About Syslog Export Filters](#)
- [Syslog Export Filters Page on page 542](#)
- [Adding a Syslog Export Filter on page 542](#)
- [Importing a Syslog Filter on page 550](#)
- [Exporting All Syslog Filter on page 551](#)
- [Exporting a Syslog Filter on page 552](#)
- [Deleting a Syslog Filter on page 553](#)

About Syslog Export Filters

W-Policy Manager can export session data (see [Live Monitoring: Access Tracker on page 107](#)), audit records (see [Audit Viewer on page 152](#)), and event records (see [Event Viewer on page 155](#)).

You configure syslog export filters to instruct W-Policy Manager where to send this information, and what kind of information should be sent through data filters.

Syslog Export Filters Page

To configure syslog export filters:

1. Navigate to **Administration > External Servers > Syslog Export Filters**.

The **Syslog Export Filters** page opens.

Figure 541: *Syslog Export Filters Page*

Administration » External Servers » Syslog Export Filters

Syslog Export Filters

Syslog filter "System Events Syslog Export Filter" has been updated

Filter: Name contains [] Go Clear Filter Show 10 records

#	Name	Description	Export Template	Export Event Format	Status
1.	System Events Syslog Export Filter	Syslog export filter to stream system events to the syslog targets	System Events	Standard	Disable

Showing 1-1 of 1

Export Delete

The following table describes the **Syslog Export Filters** parameters:

Table 299: *Syslog Export Filters Page Parameters*

Parameter	Action/Description
Name	Displays the name of the syslog export filter.
Description	Displays the description of the syslog export filter.
Export Template	Displays the name of the Export Template selected in the Add Syslog Export Filter dialog (see Adding a Syslog Export Filter on page 542).
Export Event Format	Displays the Export Event Format Type selected in the Add Syslog Export Filter dialog.
Enable/Disable	Enable or disable the syslog export filter.
Export	Opens the Export to file dialog. With this option, you can export individual syslog export filters.
Delete	Deletes a syslog export filter.

Adding a Syslog Export Filter

To add a syslog export filter:

1. From the **Syslog Export Filters** page, click **Add**.

The **Add Syslog Filters** page opens to the **General** tab.

Figure 542: Add Syslog Export Filters Page > 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 filter.

Export Template: Session Logs

Export Event Format Type: Standard

Syslog Servers:

- Standard
- LEEF
- CEF
- Select to Add--

Buttons: Remove, View Details, Modify

ClearPass Servers: If specified, syslog messages will only be sent from the selected ClearPass servers. Otherwise, it will be sent from all ClearPass servers in the cluster.

Buttons: Remove

--Select to Add--

[Add new Syslog](#)



The **Filter and Columns** tab shown in the figure above is only visible if you select **Insight Logs** or **Session Logs** as the export template. For more information, see [Filter and Columns Tab on page 547](#).

The following table describes the **Add Syslog Export Filters > General** tab parameters:

Table 300: Add Syslog Export Filters > General Tab Parameters

Parameter	Action/Description
Name	Enter the name of the syslog export filter.
Description	Enter the description that provides additional information about the syslog export filter (recommended).
Export Template	Select any one of the templates from the following options: ● Audit Records ● Insight Logs ● Session Logs ● System Events NOTE: If you select Insight Logs or Session Logs, the Filter and Columns tab is enabled. For more information, see Filter and Columns Tab on page 547.

Table 300: Add Syslog Export Filters > General Tab Parameters (Continued)

Parameter	Action/Description
Export Event Format Type	Select any one of the export event formats from the following options: ● Standard: Select this event format type to send the event types in raw syslog format. This is the default event format type. ● LEEF: Select this event format type to send the event types in Log Enhanced Event Format (LEEF). ● CEF: Select this event format type to send the event types in Common Event Format (CEF). For sample event format types, see Export Event Format Types—Examples on page 544.
Syslog Servers	Syslog servers define the receivers of syslog messages sent by servers in the W-ClearPass cluster. ● To add a W-ClearPass syslog server, select it from the Select to Add drop-down list. ● To add a new W-ClearPass syslog server, click the Add New Syslog Target link (for more information, see Adding a Syslog Target on page 538). ● To view details about a syslog server, select the syslog server, then click View Details. ● To change details about a syslog server, select the syslog server, then click Modify. For more information, see Adding a Syslog Target on page 538. ● To remove a syslog server (from receiving syslog messages), select the syslog server, then click Remove.
W-ClearPass Servers	You can designate syslog messages to be sent from exactly one server in the W-ClearPass cluster or from all of them. ● To add a W-ClearPass server, select it from the Select to Add drop-down list. ● To remove the W-ClearPass server, select the W-ClearPass server, then click Remove. NOTE: When no servers are listed, syslog messages are sent from all servers in the cluster.

Export Event Format Types—Examples

This section provides several examples of Standard, LEEF, and CEF event format types for the syslog export filter templates.

Standard Event Format Type > Audit Events

The following example describes the Standard event format type for the **Audit Events** syslog export filter template:

```
Mar 20 21:18:56 10.17.5.228 2015-01-19 21:19:50,118 10.17.5.228 Audit Logs 96 1 0
TimestampFormat=yyyy-MM-dd
HH:mm:ss,S,User=clusteradmin,Category=Endpoint,Action=ADD,EntityName=34a39527afc0,src=10.17.5.228,Timestamp=Jan 19, 2015 21:18:54 IST
Mar 20 21:20:56 10.17.5.228 2015-01-19 21:21:50,111 10.17.5.228 Audit Logs 97 1 0
TimestampFormat=yyyy-MM-dd HH:mm:ss,S,User=admin,Category=Cluster-wide
Parameter,Action=MODIFY,EntityName=Endpoint Context Servers polling
interval,src=10.17.5.228,Timestamp=Jan 19, 2015 21:20:22 IST
Mar 21 09:28:59 10.17.5.228 2015-01-20 09:29:54,3 10.17.5.228 Audit Logs 99 1 0
TimestampFormat=yyyy-MM-dd HH:mm:ss,S,User=admin,Category=Network
Device,Action=REMOVE,EntityName=1.1.1.1,src=10.17.5.228,Timestamp=Jan 20, 2015 09:29:13 IST
```

Standard Event Format Type > System Events

The following example describes the Standard event format type for the **System Events** syslog export filter template:

```
Mar 21 16:46:29 10.17.5.228 2015-01-20 16:47:23,880 10.17.5.228 System Events 0 1 0
TimestampFormat=yyyy-MM-dd HH:mm:ss,S,Description=User: arubasupport\nClient IP Address:
```

```

10.20.23.178,Category=Logged in,Action=None,Level=INFO,src=10.17.5.228,Component=Support
Shell,Timestamp=Jan 20, 2015 16:45:59 IST
Mar 21 16:49:10 10.17.5.228 2015-01-20 16:50:05,210 10.17.5.228 System Events 1 1 0
TimestampFormat=yyyy-MM-dd HH:mm:ss,S,Description='Failed to start ClearPass Virtual IP
service',Category=start,Action=Failed,Level=WARN,src=10.17.5.228,Component=ClearPass Virtual
IP service,Timestamp=Jan 20, 2015 16:48:53 IST
2015-01-20 16:50:05,210 [pool-6-thread-1] [R:] DEBUG com.avenda.tips.syslog.Syslogger - 2015-
01-20 16:50:05,210 10.17.5.228 System Events 2 1 0 TimestampFormat=yyyy-MM-dd
HH:mm:ss,S,Description=Performed action stop on cpass-domain-server_
CPATS,Category=stop,Action=Success,Level=INFO,src=10.17.5.228,Component=cpass-domain-server_
CPATS,Timestamp=Jan 20, 2015 16:48:57 IST
2015-01-20 16:50:05,211 [pool-6-thread-1] [R:] DEBUG com.avenda.tips.syslog.Syslogger - 2015-
01-20 16:50:05,211 10.17.5.228 System Events 3 1 0 TimestampFormat=yyyy-MM-dd
HH:mm:ss,S,Description=Performed action start on cpass-domain-server_
CPATS,Category=start,Action=Success,Level=INFO,src=10.17.5.228,Component=cpass-domain-server_
CPATS,Timestamp=Jan 20, 2015 16:49:00 IST

```

Standard Event Format Type > Session Events

The following example describes the Standard event format type for the **Session Events** syslog export filter template:

```

Mar 21 16:31:49 10.17.5.211 2015-01-20 16:32:41,552 10.17.5.211 Radius Session Logs 4 1 0
Common.NAS-IP-Address=10.17.4.7,RADIUS.Acct-Delay-Time=null,RADIUS.Acct-Framed-IP-
Address=null,RADIUS.Auth-Source=AD:win2008R2-64bit.bangalore.avendasys.com,RADIUS.Acct-
Timestamp=null,RADIUS.Acct-Authentic=null,RADIUS.Auth-Method=EAP-PEAP,EAP-
MSCHAPv2,Common.Host-MAC-Address=58a2b5d05ac9,RADIUS.Acct-Termination-Cause=null,RADIUS.Acct-
Service-Name=null,RADIUS.Acct-Session-Time=null,TimestampFormat=yyyy-MM-dd
HH:mm:ss,S,RADIUS.Acct-NAS-Port=null,Common.Username=test1,RADIUS.Acct-Session-
Id=null,RADIUS.Acct-Called-Station-Id=null,RADIUS.Acct-NAS-Port-
Type=null,src=10.17.5.211,RADIUS.Acct-NAS-IP-Address=null,Common.Service=Test Post
Authentication Rules,RADIUS.Acct-Input-Pkts=null,RADIUS.Acct-Status-Type=null,RADIUS.Acct-
Calling-Station-Id=null,Common.Request-Timestamp=2015-01-20 16:31:46+05:30,RADIUS.Acct-Output-
Pkts=null,RADIUS.Acct-Output-Octets=null,RADIUS.Acct-Username=null,RADIUS.Acct-Input-
Octets=null
Mar 21 16:31:49 10.17.5.211 2015-01-20 16:32:41,550 10.17.5.211 Radius Session Logs 3 2 0
Common.NAS-IP-Address=10.17.4.7,RADIUS.Acct-Delay-Time=0,RADIUS.Acct-Framed-IP-
Address=10.17.4.148,RADIUS.Auth-Source=AD:win2008R2-64bit.bangalore.avendasys.com,RADIUS.Acct-
Timestamp=2015-01-20 16:31:50+05:30,RADIUS.Acct-Authentic=RADIUS,RADIUS.Auth-Method=EAP-
PEAP,EAP-MSCHAPv2,Common.Host-MAC-Address=e0f8471a5450,RADIUS.Acct-Termination-
Cause=null,RADIUS.Acct-Service-Name=null,RADIUS.Acct-Session-Time=null,TimestampFormat=yyyy-
MM-dd HH:mm:ss,S,RADIUS.Acct-NAS-Port=0,Common.Username=test1,RADIUS.Acct-Session-
Id=test1E0F8471A5450-54BE336C,RADIUS.Acct-Called-Station-Id=000B8661CD70,RADIUS.Acct-NAS-Port-
Type=Wireless-802.11,src=10.17.5.211,RADIUS.Acct-NAS-IP-Address=10.17.4.7,Common.Service=Test
Post Authentication Rules,RADIUS.Acct-Input-Pkts=null,RADIUS.Acct-Status-
Type=Start,RADIUS.Acct-Calling-Station-Id=E0F8471A5450,Common.Request-Timestamp=2015-01-20
16:31:45+05:30,RADIUS.Acct-Output-Pkts=null
Mar 21 16:35:58 10.17.5.228 2015-01-20 16:36:52,346 10.17.5.228 Tacacs authentnications 2 1 0
TACACS.Request-Type=TACACS_AUTHORIZATION,TACACS.Enforcement-Profiles=[TACACS Super
Admin],TACACS.Acct-Flags=null,TACACS.Authen-Service=AUTHEN_SVC_NONE,TACACS.Acct-Session-
Id=null,TACACS.Remote-Address=10.20.23.178,Common.Request-Timestamp=2015-01-20
16:34:54.647+05:30,TimestampFormat=yyyy-MM-dd HH:mm:ss,S,TACACS.Authen-Action=,TACACS.Authen-
Method=AUTHEN_METH_TACACSPLUS,Common.Username=a,TACACS.Authen-Type=AUTHEN_TYPE_
PAP,TACACS.Auth-Source=[Local User Repository],src=10.17.5.228,TACACS.Privilege-
Level=1,Common.Service=[Policy Manager Admin Network Login Service]
Mar 21 16:35:58 10.17.5.228 2015-01-20 16:36:52,346 10.17.5.228 Tacacs authentnications 3 1 0
TACACS.Request-Type=TACACS_AUTHENTICATION,TACACS.Enforcement-Profiles=[TACACS Super
Admin],TACACS.Acct-Flags=null,TACACS.Authen-Service=AUTHEN_SVC_NONE,TACACS.Acct-Session-
Id=null,TACACS.Remote-Address=10.20.23.178,Common.Request-Timestamp=2015-01-20
16:34:54.647+05:30,TimestampFormat=yyyy-MM-dd HH:mm:ss,S,TACACS.Authen-Action=AUTHEN_ACTION_
LOGIN,TACACS.Authen-Method=AUTHEN_METH_TACACSPLUS,Common.Username=a,TACACS.Authen-Type=AUTHEN_
TYPE_PAP,TACACS.Auth-Source=[Local User Repository],src=10.17.5.228,TACACS.Privilege-
Level=1,Common.Service=[Policy Manager Admin Network Login Service]

```

LEEF Event Format Type > Insight Logs

The following example describes the LEEF event format type for the **Insight Logs** syslog export filter template:

```
Dec 03 2014 16:50:44.085 IST 10.17.4.208 LEEF:1.0|Dell|ClearPass|6.5.0.69058|0-1-0|Auth.Username=host/Asif-Test-PC2 Auth.Authorization-Sources=null Auth.Login-Status=216 Auth.Request-Timestamp=2014-12-03 16:48:41+05:30 Auth.Protocol=RADIUS Auth.Source=null Auth.Enforcement-Profiles=[Allow Access Profile] Auth.NAS-Port=null Auth.SSID=cppm-dot1x-test TimestampFormat=MMM dd yyyy HH:mm:ss.SSS z Auth.NAS-Port-Type=19 Auth.Error-Code=216 Auth.Roles=null Auth.Service=Test Wireless Auth.Host-MAC-Address=6817294b0636 Auth.Unhealthy=null Auth.NAS-IP-Address=10.17.4.7 src=10.17.4.208 Auth.CalledStationId=000B8661CD70 Auth.NAS-Identifier=ClearPassLab3600
```

CEF Event Format Type > Insight Logs

The following example describes the CEF event format type for the **Insight Logs** syslog export filter template:

```
Dec 03 2014 16:31:28.861 IST 10.17.4.208 CEF:0|Dell|ClearPass|6.5.0.69058|0-1-0|Insight Logs|0|Auth.Username=host/Asif-Test-PC2 Auth.Authorization-Sources=null Auth.Login-Status=216 Auth.Request-Timestamp=2014-12-03 16:28:20+05:30 Auth.Protocol=RADIUS Auth.Source=null Auth.Enforcement-Profiles=[Allow Access Profile] Auth.NAS-Port=null Auth.SSID=cppm-dot1x-test TimestampFormat=MMM dd yyyy HH:mm:ss.SSS zzz Auth.NAS-Port-Type=19 Auth.Error-Code=216 Auth.Roles=null Auth.Service=Test Wireless Auth.Host-MAC-Address=6817294b0636 Auth.Unhealthy=null Auth.NAS-IP-Address=10.17.4.7 src=10.17.4.208 Auth.CalledStationId=000B8661CD70 Auth.NAS-Identifier=ClearPassLab3600
```

CEF Event Format Type > Audit Logs

The following example describes the CEF event format type for the **Audit Logs** syslog export filter template:

```
Nov 19 2014 18:22:40.700 IST 10.17.4.221 CEF:0|Dell|ClearPass|6.5.0.68754|13-1-0|Audit Records|5|cat=Role timeFormat=MMM dd yyyy HH:mm:ss.SSS zzz rt=Nov 19, 2014 18:21:13 IST src=Test Role 10 act=ADD usrName=admin
```

LEEF Event Format Type > Audit Logs

The following example describes the LEEF event format type for the **Audit Logs** syslog export filter template:

```
Nov 19 2014 14:31:10.422 IST 10.17.4.221 LEEF:1.0|Dell|ClearPass|6.5.0.68754|0-1-0|cat=Syslog Export Data devTime=Nov 19, 2014 14:30:35 IST action=ADD src=Audit Events - LEEF usrName=admin devTimeFormat=MMM dd yyyy HH:mm:ss.SSS z
```

CEF Event Format Type > System Events

The following example describes the CEF event format type for the **System Events** syslog export filter template:

```
Nov 19 2014 17:15:52.348 IST 10.17.4.221 CEF:0|Dell|ClearPass|6.5.0.68754|0-1-0|System Events|10|cat=WebService Error level=ERROR description=No valid subscription ID\nCheck Subscription ID, Network Connectivity, http_proxy credentials.\nClick on 'Check Status Now' after correcting the configuration. timeFormat=MMM dd yyyy HH:mm:ss.SSS zzz rt=Nov 19, 2014 17:15:12 IST src=ClearPass Firmware Update Checker act=None
```

LEEF Event Format Type > System Events

The following example describes the LEEF event format type for the **System Events** syslog export filter template:

```
Dec 02 2014 20:38:40.901 IST 10.17.4.206 LEEF:1.0|Dell|ClearPass|6.5.0.68878|295-1-0|cat=start devTime=Dec 02, 2014 20:38:12 IST level=WARN description='Failed to start ClearPass Virtual IP service' action=Failed src=ClearPass Virtual IP service devTimeFormat=MMM dd yyyy HH:mm:ss.SSS z
```

CEF Event Format Type > Session Logs

The following example describes the CEF event format type for the **Session Logs** syslog export filter template:

```
Dec 01 2014 15:28:40.540 IST 10.17.4.206 CEF:0Dell|ClearPass|6.5.0.68878|1604-1-0|Session
Logs|0|RADIUS.Acct-Calling-Station-Id=00:32:b6:2c:28:95 RADIUS.Acct-Framed-IP-
Address=192.167.230.129 RADIUS.Auth-Source=AD:10.17.4.130 RADIUS.Acct-Timestamp=2014-12-01
15:26:43+05:30 RADIUS.Auth-Method=PAP RADIUS.Acct-Service-Name=Authenticate-Only RADIUS.Acct-
Session-Time=3155 TimestampFormat=MMM dd yyyy HH:mm:ss.SSS zzz RADIUS.Acct-NAS-Port=0
RADIUS.Acct-Session-Id=R00001316-01-547c3b5a RADIUS.Acct-NAS-Port-Type=Wireless-802.11
RADIUS.Acct-Output-Octets=578470212 RADIUS.Acct-Username=A_user2 RADIUS.Acct-NAS-IP-
Address=10.17.6.124 RADIUS.Acct-Input-Octets=786315664
```

LEEF Event Format Type > Session Logs

The following example describes the LEEF event format type for the **Session Logs** syslog export filter template:

```
Dec 02 2014 15:35:14.944 IST 10.17.4.206 LEEF:1.0Dell|ClearPass|6.5.0.68878|1309854-1-
0|RADIUS.Acct-Calling-Station-Id=00:88:57:2d:12:a4 RADIUS.Acct-Framed-IP-
Address=192.167.203.170 RADIUS.Auth-Source=AD:10.17.4.130 RADIUS.Acct-Timestamp=2014-12-02
15:32:47+05:30 RADIUS.Auth-Method=PAP RADIUS.Acct-Service-Name=Authenticate-Only RADIUS.Acct-
Session-Time=565 TimestampFormat=MMM dd yyyy HH:mm:ss.SSS z RADIUS.Acct-NAS-Port=0
RADIUS.Acct-Session-Id=R000a5038-01-547d8e47 RADIUS.Acct-NAS-Port-Type=Wireless-802.11
RADIUS.Acct-Output-Octets=412895267 RADIUS.Acct-Username=A_user706 RADIUS.Acct-NAS-IP-
Address=10.17.6.124 RADIUS.Acct-Input-Octets=665942581
```

Filter and Columns Tab

This section describes the parameters in the **Filter and Columns** tab of the **Administration > External Servers > Syslog Export Filters > Add** page. This tab provides two methods for configuring data filters and is only visible if you select **Insight Logs** or **Session Logs** as the export template in the **General** tab.

Insight Logs

This section describes the options if you select **Insight Logs** as the export template in the **General** tab.



The **Insight Logs** option is enabled only if the **Enable Insight** check box is selected from the **Administration > Server Manager > Server Configuration > System** tab.

The following figure displays the **Syslog Export Filters - Filter and Columns (Insight Logs)** tab.

Figure 543: Syslog Export Filters - Filter and Columns (Insight Logs) Tab

Administration » External Servers » Syslog Export Filters » Add

Syslog Export Filters

Syslog filter has not been saved

General	Filter and Columns	Summary
Columns Selection: Predefined Field Groups - - RADIUS Authentications - RADIUS Failed Authentications RADIUS Accounting - TACACS Authentication - TACACS Failed Authentication - WEBAUTH - WEBAUTH Failed Authentications Available Columns - Type: RADIUS - RADIUS.AccessPoint - RADIUS.Acct-Timestamp - RADIUS.AcctId - RADIUS.Called-Station-Id - RADIUS.End-Time - RADIUS.Framed-IP-Address - RADIUS.NAS-Identifier Selected Columns - - Radius.Username - Radius.Calling-Station-Id - Radius.NAS-IP-Address - Radius.Start-Time - Radius.Duration - Radius.Input-bytes - Radius.Output-bytes		



The data collection interval for Insight logs is -4 to -2 minutes from the current time.

The following table describes the **Syslog Export Filters - Filter and Columns (Insight Logs)** tab parameters:

Table 301: *Syslog Export Filters - Filter and Columns (Insight Logs) Tab Parameters*

Parameter	Description
Columns Selection	Determine the group of reports that you want to include in the syslog filters. The column selection limits the type of records sent to the syslog filters. NOTE: You can add only the Insight reports that are already created in Insight. You cannot create a new data filter for Insight logs.
Predefined Field Groups	Select the predefined Insight reports that are grouped for a quick addition.
Available Columns	Displays the reports specific to the group selected in the Columns Selection field.
Type	Select the type of records from the drop-down list to filter the records. This provides additional filtering option based on the type of records.
Selected Columns	After you select an entry from the Available Columns list, click >> to add the selected entry to the Selected Columns list. Click << to remove an entry from the Selected Columns list.

Session Logs

This section describes the options if you select **Session Logs** as the export template in the **General** tab. On selecting **Session Logs**, the following options are available:

- **Option 1** allows you to choose from pre-defined field groups and to select columns based on the Type.
- **Option 2** allows you to create a custom SQL query. You can view a sample template for the custom SQL by clicking the link below the text entry field.



It is recommended to contact support if you choose the option 2. Support can assist you with entering the correct information in this template.

The following figure displays the **Syslog Export Filters - Filter and Columns (Session Logs)** tab.

Figure 544: Syslog Export Filters - Filter and Columns (Session Logs) Tab

Administration » External Servers » Syslog Export Filters » Add

Syslog Export Filters

General **Filter and Columns** Summary

Option 1: For common use-cases, select Data Filter and Columns for export:

Data Filter: [All Requests] [Add new Data filter](#) [Modify](#)

Columns Selection:

Predefined Field Groups -

- Logged in users
- Failed Authentications
- RADIUS Accounting
- TACACS+ Administration

Available Columns -

Type: Common

Common.Alerts

Common.Alerts-Present

Common.Audit-Posture-Token

Common.Auth-Type

Common.Connection-Status

Common.Enforcement-Profiles

Common.Error-Code

Option 2: For advanced use-cases, specify custom SQL query for export :

Custom SQL:

```
SELECT "Common.Username", "Common.Service", "Common.Roles", "Common.Host-MAC-Address", "RADIUS.Acct-Framed-IP-Address", "Common.NAS-IP-Address", "Common.Request-Timestamp", "Common.Alerts" FROM dblink ( --DB-CONNECTION-STRING--, 'SELECT T1.user_name as "Common.Username", T1.service_name as "Common.Service", T3.roles as "Common.Roles", T1.host_mac as "Common.Host-MAC-Address", T8.framed_ip_address as "RADIUS.Acct-Framed-IP-Address"'. As an example, click here to copy a sample SQL
```

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

The following table describes the **Syslog Export Filters - Filter and Columns (Session Logs)** tab parameters:

Table 302: Syslog Export Filters - Filter and Columns (Insight Logs) Tab Parameters

Parameter	Description
Data Filter	Specify the data filter. The data filter limits the type of records sent to the syslog target.
Modify/ Add new Data filter	Modify the selected data filter, or add a new one. 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. For more information on adding a data filter, see Adding a Data Filter on page 159 .
Columns Selection	The column selection limits the type of columns sent to the syslog target. There are predefined field groups, which are column names grouped together for quick addition to the report. For example, <i>Logged in users</i> field group has seven predefined columns. When you click <i>Logged in users</i> the seven columns automatically appear in the Selected Columns list. 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. W-Policy Manager populates these column names by extracting the column names from existing sessions in the session database. After you select an entry from the Available Columns list, click >> to add the selected entry to the Selected Columns list. Click << to remove an entry from the Selected Columns list.
Custom SQL	Specify custom SQL query for export. This option is for advanced use cases. NOTE: It is recommended to contact support if you choose this option. Support can assist you with entering the correct information in this template.

Summary Tab

This section describes the parameters in the **Summary** tab of the **Administration > External Servers > Syslog Export Filters > Add** page. The following figure displays the **Syslog Export Filters - Summary** tab.

Figure 545: Syslog Export Filters - Summary Tab

General | **Filter and Columns** | **Summary**

General:

Name:

Description:

Export Template:

Syslog Servers:

ClearPass Servers:

Filter and Columns:

Option 1: For common use-cases, select Data Filter and Columns for export:

Data Filter:

Columns Selection:

Option 2: For advanced use-cases, specify custom SQL query for export :

Custom SQL:

[Back to Syslog Filters](#)

The following table describes the **Syslog Export Filters - Summary** tab parameters:

Table 303: Syslog Export Filters - Summary Tab Parameters

Parameter	Description
General	
Name	Displays the name of the syslog export filter.
Description	Displays the description that provides additional information about the syslog export filter.
Export Template	Displays the template selected as the export template.
Syslog Servers	Displays the IP address of the syslog server selected during configuration.
W-ClearPass Servers	Displays the IP address of the W-ClearPass servers selected during configuration.
Filter and Columns	
Data Filter	Displays the data filter selected when configuring option 1 in the Filter and Columns tab.
Columns Selection	Displays the predefined field groups and available columns type selected when configuring option 1 in the Filter and Columns tab.
Custom SQL	Displays the SQL query selected when configuring option 2 in the Filter and Columns tab.

Importing a Syslog Filter

To import a syslog target:

1. Navigate to **Administration > External Servers > Syslog Export Filters**.
2. Click the **Import** link on the top right section of the page. Enter the details based on [Table 304](#).
3. Click **Import**.

The following figure displays the **Import from file** pop-up:

Figure 546: *Import from file Pop-up*

The screenshot shows a web-based dialog box titled "Import from file". It has a dark blue header bar with a close button (X) on the right. The main area is white and contains two input sections. The first section is labeled "Select File:" and includes a "Choose File" button and the text "No file chosen". The second section is labeled "Enter secret for the file (if any):" and has a large, empty text input area. At the bottom right of the dialog, there are two buttons: "Import" and "Cancel".

The following table describes the **Import from file** parameters:

Table 304: *Import from file Parameters*

Parameter	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.

Exporting All Syslog Filter

To export all syslog filters:

1. Navigate to **Administration > External Servers > Syslog Export Filters**.
2. Click the **Export All** link on the top right section of the page. Enter the details based on [Table 305](#).
3. Click **Export**.
4. Enter the XML file name in the **Save As** dialog box.
5. Click **Save**.

The following figure displays the **Export to file** pop-up:

Figure 547: *Export to file Pop-up*



The following table describes the **Export to file** parameters:

Table 305: *Export to file Parameters*

Parameter	Description
Export file with password protection	Choose Yes to export the file with password protection.
Secret Key	Enter the secret key.
Verify Secret	Re-enter the secret key.

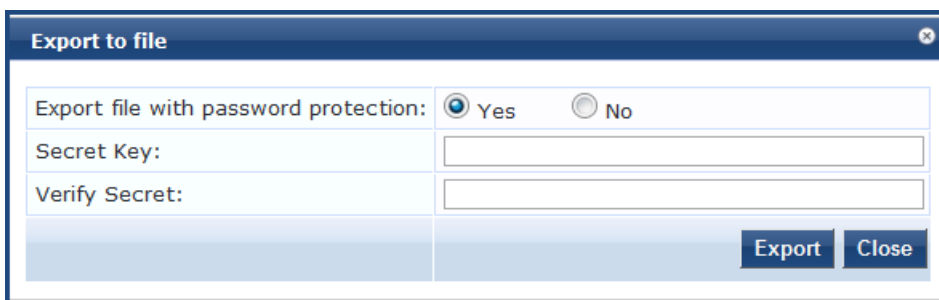
Exporting a Syslog Filter

To export a syslog filter:

1. Navigate to **Administration > External Servers > Syslog Export Filters**.
2. Select the **Host Address** from the list of check boxes and click **Export**. Enter the details based on [Table 306](#).
3. Enter the name of the XML file in the **Save As** dialog.
4. Click **Save**.

The following figure displays the **Export to file** pop-up:

Figure 548: *Export to file Pop-up*



The following table describes the **Export to file** parameters:

Table 306: *Export to file Parameters*

Parameter	Description
Export file with password protection	Choose Yes to export the file with password protection.
Secret Key	Enter the secret key.
Verify Secret	Re-enter the secret key.

Deleting a Syslog Filter

To delete a syslog filter:

1. Navigate to **Administration > External Servers > Syslog Export Filters**.
2. Click the check box next to the syslog filter entry and click **Delete**.
3. Click **Yes**.

Messaging Setup

This section provides the following information:

- [Configuring Messaging](#)
- [Sending a Test Email Message](#)
- [Sending a Test SMS Message](#)

W-ClearPass messaging setup provides an interface to configure the Simple Mail Transfer Protocol (SMTP) server for email and SMS notifications.

Configuring Messaging

To configure messaging:

1. Navigate to **Administration > External Servers > Messaging Setup**.

The **Messaging > SMTP Server** page opens.

Figure 549: *Messaging > SMTP Server Page*

Administration » External Servers » Messaging Setup

Messaging + Configure SMS Gateway

Configure SMTP mail server for email notifications :

SMTP Server

SMTP setting

Server name:		Connection Security:	None
User Name:		Port:	25
Password:		Connection timeout:	30 seconds
Verify Password:			
Default From address:			

Send Test Email

Send Test SMS

Save

2. To configure a new SMS gateway using the W-ClearPass Guest portal, click the **Configure SMS Gateway** link at the top right section of the page.

The following table describes the **Messaging > SMTP Server** page parameters:

Table 307: *Messaging > SMTP Server Page Parameters*

Parameter	Action/Description
Server name	1. Enter the Fully Qualified Domain Name (FQDN) or the IP address of the SMTP server.
User Name	2. Enter the username if your email server requires authentication for sending email messages.
Password	3. Enter the password for the specified username, then verify the password.
Default From address	4. Enter the email address that must to be displayed as the sender's address in the message.
Connection Security	5. To establish the communication with the SMTP server, select from one of the following options: ■ None: Select this option to disable secure communication with the server. ■ SSL: Select this option to have a Secured Socket Layer communication with the server. ■ Start TLS: Select this option to have a Transport Layer Security communication with the server.
Port	6. Enter the TCP port number that the SMTP server listens on. The default value of the port is 25 .
Connection timeout	7. Enter the timeout value for connection to the SMTP server (in seconds). The default value is 30 seconds.

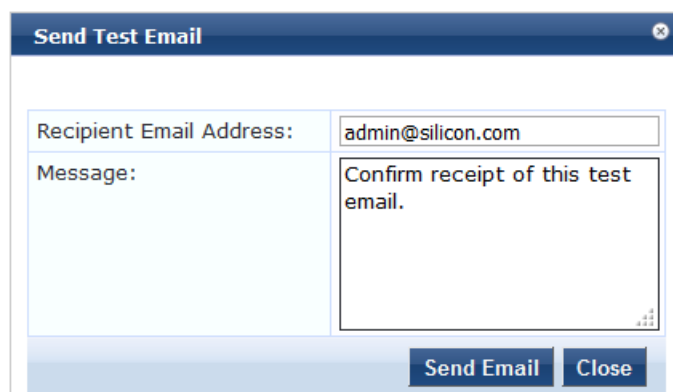
Sending a Test Email Message

To send a test mail message to the preferred email address:

1. Click **Send Test Email**.

The **Send Test Email** dialog opens.

Figure 550: *Send Test Email Dialog*



Send Test Email

Recipient Email Address: admin@silicon.com

Message: Confirm receipt of this test email.

Send Email Close

2. **Recipient Email Address:** Enter the email address of the recipient.
3. **Message:** Enter the test message.

4. Click **Send Email**.

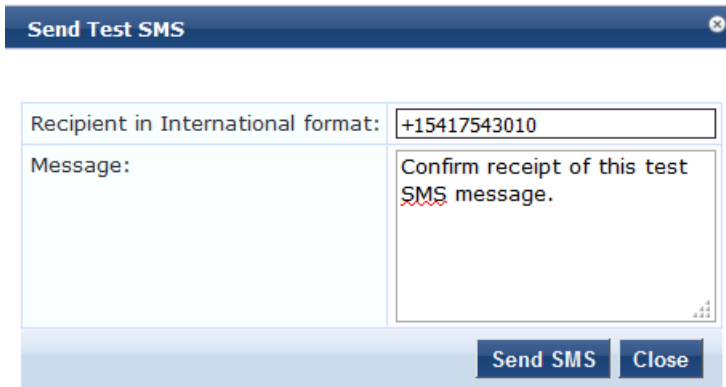
Sending a Test SMS Message

To send a test SMS message to the preferred email address:

1. Click **Send Test SMS**.

The **Send Test SMS** dialog opens.

Figure 551: *Send Test SMS Dialog*



The screenshot shows a dialog box titled "Send Test SMS". It has a light blue header bar with the title and a close button. The main area is divided into two sections. The top section is labeled "Recipient in International format:" and contains a text input field with the value "+15417543010". The bottom section is labeled "Message:" and contains a text area with the text "Confirm receipt of this test SMS message." Below the text area, there are two buttons: "Send SMS" and "Close".

2. **Recipient in International format:** Enter the mobile phone number of the recipient in international format.
The recipient's mobile number must be entered in the international format consisting of a + sign, followed by the country code and the mobile phone number (without the first '0' of the number).
3. **Message:** Enter the test message.
4. Click **Send SMS**.

Endpoint Context Servers

This section describes the following topics:

- [Introduction](#)
- [Endpoint Context Servers Page](#)
- [Adding an Endpoint Context Server](#)
- [Importing an Endpoint Context Server](#)
- [Exporting All Endpoint Context Servers](#)
- [Modifying an Endpoint Context Server](#)
- [Polling an Endpoint Context Server](#)
- [Deleting an Endpoint Context Server](#)

For related information, see:

- [Configuring Endpoint Context Server Actions on page 563](#)
- [Adding Vendor-Specific Endpoint Context Servers on page 568](#)

Introduction

The mobile device management (MDM) platforms run on MDM servers. These servers provision mobile devices to configure connectivity settings, enforce security policies, restore lost data, and other administrative services.

Information gathered from mobile devices can include policy breaches, data consumption, and existing configuration settings.

Endpoint Context Servers Page

1. To access the Endpoint Context Servers page, navigate to **Administration > External Servers > Endpoint Context Servers**.

The **Endpoint Context Servers** page appears:

Figure 552: *Endpoint Context Servers Page*

Administration » External Servers » Endpoint Context Servers

Endpoint Context Servers

 Add
 Import
 Export All

Filter: Show records

#	☐ Server Name ▲	Server Type	Status
1.	☐ localhost	Generic HTTP	Enabled

Showing 1-1 of 1

The following table describes the **Endpoint Context Servers** categories:

Table 308: *Endpoint Context Server Categories*

Parameter	Description
Server Name	Displays the name of the endpoint context server.
Server Type	Displays the type of the endpoint context server.
Status	Displays the status of the endpoint context server: Enabled or Disabled . For non-MDM servers, the status is always displayed as Disabled .

Adding an Endpoint Context Server

To add an endpoint context server:

1. Navigate to **Administration > External Servers > Endpoint Context Servers**.
2. Click the **Add** link at the top right section of the page.

The **Add Endpoint Context Server** dialog opens.

The fields and parameters that are displayed in the **Add Endpoint Context Server** dialog vary depending on which **Server Type** you select (see **Select Server Type** in [Table 309](#)).

Figure 553: Adding an Endpoint Context Server

3. In the **Add Endpoint Context Server** dialog, specify the parameters as described in [Table 309](#).
4. Click **Save**.

[Table 309](#) describes the **Add Endpoint Context Servers** parameters:

Table 309: Add Endpoint Context Server Parameters

Parameter	Description
Select Server Type	1. Choose one of the Server Types (endpoint context server vendors) from the following options. The Server Type you select determines the configuration parameters. ■ AirWatch ■ Aruba Activate ■ AirWave ■ Google Admin Console ■ Generic HTTP ■ JAMF ■ Juniper SRX ■ MaaS360 ■ MobileIron ■ Palo Alto Networks Firewall ■ Palo Alto Networks Panorama ■ SAP Afaria ■ SOTI ■ XenMobile NOTE: You can add more than one endpoint context server of the same type.
Server Name	2. Enter the name of the server or host.
Server Base URL	3. Enter the full URL for the server. The default is the name you entered above with "https://" prepended. You can append a custom port, such as for an MDM server: https://yourserver.yourcompany.com:customerportnumber.

Table 309: Add Endpoint Context Server Parameters (Continued)

Parameter	Description
Username	4. Enter the username.
Password	5. Enter the password of the server or host, then verify the password.
API Key	6. Enter the API key that was provided by the vendor, then verify the API key. This field is not displayed for all endpoint context servers.
Validate Server	7. Select the Enable to validate the server certificate check box to validate. By default, this field is disabled. NOTE: Checking this option enables the Certificate tab.
Enable Server	8. Select the Enable to fetch endpoints from the server check box to enable the endpoint context server. By default, this field is disabled. NOTE: The Bypass Proxy field is enabled only if you enable this field. Checking this option enables the Poll Status tab.
Bypass Proxy	9. Select the Enable to bypass proxy server check box to bypass the proxy server. By default, this field is disabled. You must enable the Enable Server parameter to enable this field. You can select this option to specify that the endpoint context server should not use the configured proxy settings (if a proxy is used). W-ClearPass then bypasses the proxy server for functions such MDM API, Endpoint Context Server Actions, and Generic HTTP outbound enforcement. NOTE: When this field is enabled, the proxy servers configured in the Administration > Server Manager > Server Configuration > Service Parameters tab > W-ClearPass System Services service page will be bypassed. The server discovery occurs without any issues even when the proxy servers are bypassed.

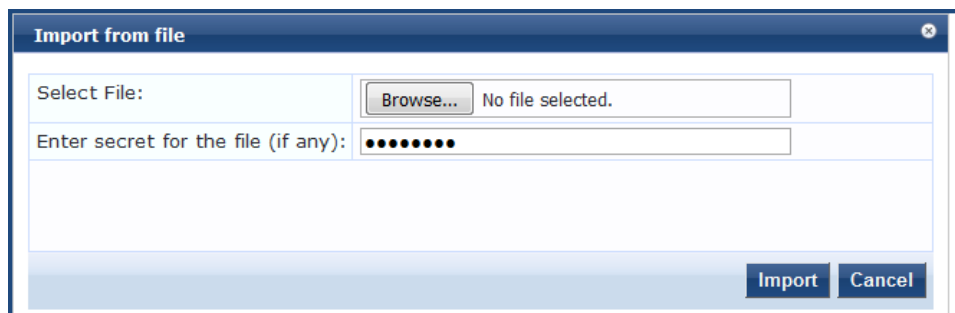
Importing an Endpoint Context Server

To import an endpoint context server:

1. Navigate to **Administration > External Servers > Endpoint Context Servers**.
2. Click the **Import** link on the top right section of the page.
3. Enter the parameters based on [Table 310](#).
4. Click **Import**.

[Figure 554](#) displays the **Import from File** dialog:

Figure 554: *Import from File Dialog*

The dialog box is titled "Import from file" and has a close button in the top right corner. It contains two main input sections. The first section is labeled "Select File:" and includes a "Browse..." button and a text field that currently displays "No file selected.". The second section is labeled "Enter secret for the file (if any):" and features a password field with ten dots for input. At the bottom right of the dialog, there are two buttons: "Import" and "Cancel".

The following table describes the **Import from file** parameters:

Table 310: *Import from File Dialog Parameters*

Parameter	Description
Select File	Browse to the Endpoint Context 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.

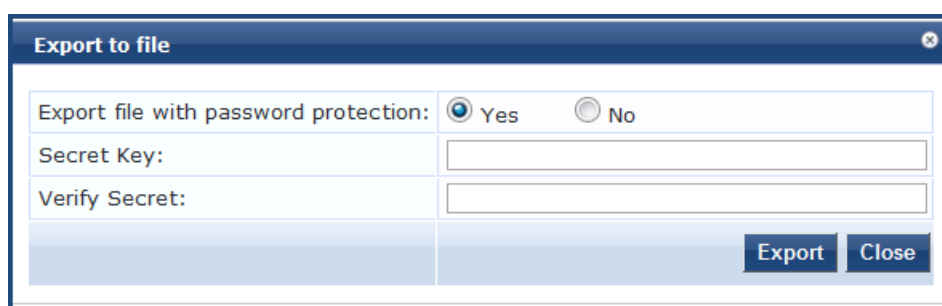
Exporting All Endpoint Context Servers

To export all endpoint context servers:

1. Navigate to **Administration > External Servers > Endpoint Context Servers**.
2. Click the **Export All** link on the top right section of the page.

The **Export to File** dialog opens.

Figure 555: *Export to File Dialog*

The dialog box is titled "Export to file" and has a close button in the top right corner. It contains three input sections. The first section is labeled "Export file with password protection:" and has two radio buttons, "Yes" (which is selected) and "No". The second section is labeled "Secret Key:" and has a text input field. The third section is labeled "Verify Secret:" and has a text input field. At the bottom right of the dialog, there are two buttons: "Export" and "Close".

3. Enter the parameters as described in [Table 311](#).
4. Click **Export**.
5. Enter the XML file name in the **Save As** dialog box.
6. Click **Save**.

Table 311 describes the **Export to file** parameters:

Table 311: *Export to File Dialog Parameters*

Parameter	Action/Description
Export file with password protection	1. To export the file with password protection, choose Yes .
Secret Key	2. Enter the secret key.
Verify Secret	3. Re-enter the secret key.

Modifying an Endpoint Context Server

To modify an endpoint context server:

1. Navigate to **Administration > External Servers > Endpoint Context Servers**.
2. In the **Endpoint Context Servers** main page, click the desired server name entry.
3. In the **Modify Endpoint Context Server** dialog, enter the details based on specific **Server Type** (vendor link) listed in Table 309, "Add Endpoint Context Server Parameters."
4. Click **Update**.



The tabs that appear when you add or modify an endpoint context server vary depending on the type (vendor) of endpoint context server selected.

Server Tab

Use the **Server** tab to modify the server name, server base URL, and API key.

You can also use this dialog to validate the server certificate and to bypass proxy servers. The following figure displays the **Modify Endpoint Context Server > Server** dialog:

Figure 556: *Modify Endpoint Context Server > Server Dialog*

The screenshot shows a dialog box titled "Modify Endpoint Context Server" with a close button in the top right corner. Inside the dialog, there are two tabs: "Server" (selected) and "Actions". The "Server" tab contains the following fields and options:

- Server Type:** A dropdown menu showing "Generic HTTP".
- Server Name:** A text input field containing "localhost".
- Server Base URL:** A text input field containing "https://localhost".
- Username:** A text input field.
- Password:** A text input field, followed by a "Verify:" label and another text input field.
- Validate Server:** A checkbox labeled "Enable to validate the server certificate", which is currently unchecked.
- Bypass Proxy:** A checkbox labeled "Enable to bypass proxy server", which is currently checked.

At the bottom right of the dialog, there are two buttons: "Update" and "Cancel".

The following table describes the **Modify Endpoint Context Server > Server** parameters:

Table 312: *Modify Endpoint Context Server > Server Parameters*

Parameter	Action Description
Server Type	The Server Type cannot be modified.
Server Name	1. Enter the name of the server or host.
Server Base URL	2. Enter the full URL for the server. The default is the name you entered above with "https://" prepended. You can append a custom port, such as for an MDM server: https://yourserver.yourcompany.com:customerportnumber
Username	3. Enter the username of the server or host.
Password	4. Enter the password of the server or host, then verify the password.
Validate Server	5. Enable this check box to validate the server certificate. By default, this field is disabled. NOTE: Checking this option enables the Certificate tab.
Bypass Proxy	6. Select the Enable to bypass proxy server check box to bypass the proxy server. By default, this field is disabled. You must enable the Enable Server parameter to enable this field. You can select this option to specify that the endpoint context server should not use the configured proxy settings (if a proxy is used). W-ClearPass then bypasses the proxy server for functions such MDM API, Endpoint Context Server Actions, and Generic HTTP outbound enforcement. NOTE: When this field is enabled, the proxy servers configured in the Administration > Server Manager > Server Configuration > Service Parameters tab > W-ClearPass System Services service page will be bypassed. The server discovery occurs without any issues even when the proxy servers are bypassed.

Actions Tab

Use the **Actions** tab to view the server action that is performed on endpoints and their description. The fields and parameters that are displayed in the **Actions** dialog vary depending on which **Server Type** you select (see the **Select Server Type** vendor links listed in [Table 309](#), "Add Endpoint Context Server Parameters").

For more information about endpoint context server actions configuration, see [Configuring Endpoint Context Server Actions on page 563](#).

The following figure displays an example of the **Modify Endpoint Context Server > Actions** tab:

Figure 557: *Modify Endpoint Context Server > Actions Tab*

Modify Endpoint Context Server	
Server	Actions
Name	Description
Check Point Login - AD User	Inform Check Point that user logged in.
Check Point Login - Guest User	Inform Check Point that user logged in.
Check Point Logout	Inform Check Point that user logged out.
Fortinet Login	Inform Fortinet that user logged in.
Fortinet Logout	Inform Fortinet that user logged out.
Handle AirGroup Time Sharing	Sends time-based sharing policy to the AirGroup notification service
Infoblox Login	This is the Endpoint Context Server Action to send user or device context to Infoblox server
Nmap Scan	Perform Nmap Scan for selected endpoint
Nmap Scan Device Profiler	Nmap Scan Device Profiler
SNMP Scan	Perform SNMP Scan for selected endpoint
Update Cancel	

Polling an Endpoint Context Server

To poll an endpoint context server:



You can poll only one server at a time. You cannot poll multiple server entries. Also, you can only poll MDM-type servers.

1. Navigate to **Administration > External Servers > Endpoint Context Servers**.
2. In the **Endpoint Context Servers** main page, click the check box next to the server name entry.

Figure 558: *Selecting the Trigger Poll Option*

Administration > External Servers > Endpoint Context Servers

Endpoint Context Servers

Filter: Server Name contains		Go	Clear Filter	Show 10 records
#	Server Name	Server Type	Status	
1.	☒ localhost	Generic HTTP	Enabled	Trigger Poll Export Delete
Showing 1-1 of 1				

3. Click **Trigger Poll**.

Deleting an Endpoint Context Server

Deleting an endpoint context server removes the configuration information from the W-Policy Manager server.

To save the endpoint context server configuration prior to deleting the server:

1. Before you delete the endpoint context server, export the server.
2. Save the configuration so that you can import it in future if necessary.

To delete an endpoint context server:

1. Navigate to **Administration > External Servers > Endpoint Context Servers**.
2. Select the check box next to the server name entry, then click **Delete**.
3. To confirm the delete operation, click **Yes**.

Configuring Endpoint Context Server Actions

This section contains the following information:

- [Filtering an Endpoint Context Server Action Report](#)
- [Configuring Endpoint Context Server Actions](#)
- [Adding machine-os and host-type Endpoint Attributes](#)

Filtering an Endpoint Context Server Action Report

Use the **Filter** controls to configure a search for a subset of Endpoint Context Server Action items.

To filter an endpoint context server action report:

1. Navigate to **Administration > Dictionaries > Context Server Actions**.
The Endpoint Context Server Actions page appears (see [Figure 559](#)).
2. From the Filter drop-down, select a filter: **ServerType**, **Action Name**, or **HTTP method**.
3. To add up to four new search fields, click the **Plus** icon.
4. Select a search argument.
The search arguments are limited to **contains** or **equals**.
5. Click **Go**.

Configuring Endpoint Context Server Actions

Use the **Endpoint Context Server Actions** page to configure actions that are performed on endpoints, such as locking a device, triggering a remote, or enterprise wipe, and so on.

The **Context Server Actions** page displays the report that shows information about all configured Endpoint Context Server Actions.

To configure endpoint context server actions:

1. Navigate to **Administration > Dictionaries > Context Server Actions > Endpoint Context Server Actions** page.

[Figure 559](#) displays an example of the **Endpoint Context Server Actions** page:

Figure 559: *Endpoint Context Server Actions Page*

Administration » Dictionaries » Context Server Actions

Endpoint Context Server Actions

 Add
 Import
 Export All

Filter: Server Type contains 

Show 10 records

#	☐ Server Type ▲	Action Name	HTTP Method	Description
1.	☐ airwatch	Clear Passcode	POST	Reset Passcode on the device
2.	☐ airwatch	Send Message	POST	Send message to the device
3.	☐ airwatch	Get Apps	GET	Get apps information for the device
4.	☐ airwatch	Remote Wipe	POST	Delete all information stored
5.	☐ airwatch	Lock Device	POST	Locks the device
6.	☐ airwatch	Send Message (Parameterized)	POST	Send message with parameters to the device
7.	☐ airwatch	Copy-Get Apps	GET	Get apps information for the device
8.	☐ airwatch	Copy_of_Send Message (Parameterized)	POST	Send message with parameters to the device
9.	☐ airwatch	Enterprise Wipe	POST	Delete only corporate information stored
10.	☐ Generic HTTP	Fortinet Logout	POST	Inform Fortinet that user logged out.

Showing 1-10 of 40  

[Table 313](#) describes the **Endpoint Context Server Actions** settings:

Table 313: *Endpoint Context Server Actions Page Settings*

Settings	Description
Server Type	Indicates the server type configured when the server action was configured.
Action Name	Indicates the name of the context server action. The available server actions vary depending on what Server Type is specified.
HTTP Method	Specifies the HTTP method selected when the server action was configured.
Description	Provides the description of the server action.

- From the **Endpoint Context Server Actions** page, click a row in the report.
The **Endpoint Content Server Details** dialog appears.

Figure 560: *Endpoint Context Server Details Dialog*

The screenshot shows the 'Endpoint Context Server Details' dialog box. It has a title bar with a close button. Below the title bar are four tabs: 'Action', 'Header', 'Content', and 'Attributes'. The 'Action' tab is currently selected. The 'Action' tab contains the following fields:

- Server Type:** A dropdown menu with 'Generic HTTP' selected.
- Server Name:** A dropdown menu with 'localhost' selected.
- Action Name:** A text input field containing 'Check Point Login'.
- Description:** A text area containing 'Inform Check Point that user logged in.'.
- HTTP Method:** A dropdown menu with 'POST' selected.
- Skip HTTP Auth:** A checkbox labeled 'Enable to skip HTTP Basic Authentication'.
- URL:** A text input field containing '/idasdk'.

At the bottom right of the dialog are two buttons: 'Save' and 'Cancel'.

- Click a tab to view details about the selected Endpoint Context Server action.
- Make any changes required, then click **Save**.

Action Tab Parameters

Use the **Action** tab to specify the server type, action name, HTTP method, and URL for the specified HTTP method.

Table 314 describes the the **Action** tab parameters.

Table 314: Action Parameters—Endpoint Context Server Details

Parameter	Description
Server Type	Specifies the server type configured when the server action was configured. You can select the server type from the drop-down list.
Server Name	Lists the context servers specific to the server type selected in the Server Type field. This field is visible only if you selected the service type Generic HTTP .
Action Name	Specifies the name of the action configured.
Description	Provides additional information about the action specified.
HTTP Method	Specifies the HTTP method selected when the server action was configured.
Skip HTTP Auth	Select this check box to disable the HTTP basic authentication for endpoint context server actions. This exposes the context server attributes to be used in context server actions.
URL	Indicates the URL for the selected HTTP method.

Header Tab Parameters

Use the **Header** tab to specify the key-value pairs to be included in the HTTP header.

Figure 561: Header Tab—Endpoint Context Server Details

Endpoint Context Server Details

Action Header Content Attributes

Specify the key-value pairs to be included in the HTTP Header -

#	Header Name	Header Value
1.	Content-Type	= application/json
2.	Click to add...	

Save Cancel

Table 315 describes the **Endpoint Context Server Details—Header** parameters:

Table 315: Header Parameters—Endpoint Context Server Details

Parameter	Description
Header Name	Specify the name of the header to be included in the HTTP header.
Header Value	Specify the value of the header specific to the name to be included in the HTTP header.

Content Tab

Use the **Content** tab to specify a content type and add non-default context server attributes (see [Figure 562](#)).

The information in the Content window is the template of what will be posted to the server. The fields preceded by the % sign are replaced with their corresponding values.

Figure 562: *Content Tab—Endpoint Context Server Details*

The screenshot shows a dialog box titled "Endpoint Context Server Details" with a close button in the top right corner. It has four tabs: "Action", "Header", "Content" (which is selected), and "Attributes". In the "Content" tab, there is a "Content-Type:" label followed by a dropdown menu showing "JSON". Below this is a "Content:" label followed by a large text area containing a JSON template:

```
{ "shared_secret": "%{shared_secret}", "request": [{"command": "add_user", "username": "%{name}", "ip": "%{ip}", "machine_name": "%{machine}", "domain": "%{domain}", "identity_source": "Aruba ClearPass Policy Manager", "timeout": "%{timeout}", "fetch_roles": 1, "fetch_groups": 1}] }
```

 At the bottom right of the dialog are "Save" and "Cancel" buttons.

[Table 316](#) describes the **Endpoint Context Server Details—Content** parameters:

Table 316: *Content Parameters—Endpoint Context Server Details*

Parameter	Description
Content-Type	Specify the type of the content. Select from the following options: • CUSTOM • HTML • JSON • PLAIN • XML
Content	Specify the content. For example, { "mac": "%{Connection:Client-Mac-Address-NoDelim}", "nmap": { "device": "%{DEVICECATEGORY}" } }.

For related information, see [Adding machine-os and host-type Endpoint Attributes on page 567](#)).

Attributes Tab Parameters

Use the **Attributes** tab to specify the mapping for attributes used in the content to parameterized values from the request.

Figure 563: *Attributes Tab—Endpoint Context Server Details*

#	Attribute Name	Attribute Value
1.	%{shared_secret}	=
2.	%{timeout}	= 28800
3.	Click to add...	

Table 317 describes the **Endpoint Context Server Details—Attributes** parameters:

Table 317: *Attributes Parameters—Endpoint Context Server Details*

Parameter	Description
Attribute Name	Enter attribute names and assign values to those names. These name/value pairs are included in context server actions.
Attribute Value	Enter the value for the selected name in the Attribute Name field.

Adding machine-os and host-type Endpoint Attributes

To be able to indicate the entire OS family (Android, Windows, Linux, etc.) and the type of device (iPad, iPhone, etc.), you can add the **machine-os** Device Family attribute and the **host-type** Device Type attribute to the default set of endpoint context attributes provided in the Content window:

To add the **machine-os** and **host-type** endpoint context attributes:

1. Navigate to **Administration > Dictionaries > Context Server Actions**.
The **Endpoint Context Server Actions** page appears.
2. Scroll to and select the **Generic HTTP/Check Point Login** server action.

Figure 564: Selecting the Check Point Login Server Action

Administration » Dictionaries » Context Server Actions

Endpoint Context Server Actions

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

Filter: contains Show records

#	Server Type	Action Name	HTTP Method	Description
11.	Generic HTTP	Nmap Scan	POST	Perform Nmap Scan for selected endpoint
12.	Generic HTTP	Nmap Scan Device Profiler	POST	Nmap Scan Device Profiler
13.	Generic HTTP	Check Point Login	POST	Inform Check Point that user logged in.
14.	Generic HTTP	Check Point Logout	POST	Inform Check Point that user logged out.
15.	Generic HTTP	Fortinet Login	POST	Inform Fortinet that user logged in.
16.	Generic HTTP	Fortinet Logout	POST	Inform Fortinet that user logged out.
17.	Generic HTTP	SNMP Scan	GET	Perform SNMP Scan for selected endpoint
18.	MaaS360	Block Device in Messaging System	POST	Block the device in Messaging System
19.	MaaS360	Check Action Status	GET	Check the status of a prior executed action
20.	MaaS360	Search Action History	GET	Search action history by Device ID.

Showing 11-20 of 40

The **Endpoint Context Server Details** dialog appears.

- Select the **Content** tab (see Figure 565).
- In the **Content** field, add the following attributes (see Figure 565):
 - "machine-os": "%{device_family}"
 - "host-type": "%{device_type}"

Figure 565: Adding Endpoint Context Server Attributes

Endpoint Context Server Details

Action

Header

Content

Attributes

Content-Type:

Content:

```
{
  "shared_secret": "%{shared_secret}",
  "request": [
    {
      "command": "add_user",
      "username": "%{name}",
      "ip": "%{ip}",
      "machine_name": "%{machine}",
      "machine-os": "%{device_family}",
      "host-type": "%{device_type}",
      "domain": "%{domain}",
      "identity_source": "Aruba ClearPass Policy Manager",
      "timeout": "%{timeout}",
      "fetch_roles": 1,
      "fetch_groups": 1
    }
  ]
}
```

- Click **Save**.

You receive the following message:

Context Server Action "Check Point Login (Generic HTTP)" updated successfully

Adding Vendor-Specific Endpoint Context Servers

This section provides information on the following topics:

- [Adding an AirWatch Endpoint Context Server](#)
- [Adding an AirWave Endpoint Context Server](#)

- [Adding an Aruba Activate Endpoint Context Server](#)
- [Adding a ClearPass Cloud Proxy Endpoint Context Server](#)
- [Adding a Generic HTTP Endpoint Context Server](#)
- [Adding a Google Admin Console Endpoint Context Server](#)
- [Integrating W-ClearPass with Infoblox](#)
- [Adding a JAMF Endpoint Context Server](#)
- [Integrating ClearPass with Juniper Networks SRX](#)
- [Adding a MaaS360 Endpoint Context Server](#)
- [Adding a MobileIron Endpoint Context Server](#)
- [Adding a Palo Alto Networks Firewall Endpoint Context Server](#)
- [Adding a Palo Alto Networks Panorama Endpoint Context Server](#)
- [Adding an SAP Afaria Endpoint Context Server](#)
- [Adding a SOTI Endpoint Context Server](#)
- [Adding a XenMobile Endpoint Context Server](#)

Adding an AirWatch Endpoint Context Server

Consult Airwatch's documentation for information about the parameters that you must enter to configure this endpoint.

To add an Airwatch Endpoint Context Server:

1. Navigate to **Administration > External Servers > Endpoint Context Servers**.

The **Endpoint Context Servers** page appears.

2. Click **Add**.

The **Add Endpoint Context Server** dialog appears. This dialog opens in the **Server** tab.

3. From the **Select Server Type** drop-down, select **airwatch**.

Server Tab

The following figure displays the **Airwatch Add Endpoint Context Server - Server** dialog:

Figure 566: Adding an Airwatch Endpoint Context Server - Server Dialog

Add Endpoint Context Server

Server **Actions**

Select Server Type: airwatch

Server Name:

Server Base URL:

Username:

Password: Verify Password:

API Key:

Validate Server: ☐ Enable to validate the server certificate

Enable Server: ☐ Enable to fetch endpoints from the server

Bypass Proxy: ☐ Enable to bypass proxy server

Save Cancel



You can add more than one endpoint context server of the same type.

The following table displays the **Add Endpoint Context Server - Server** (AirWatch) tab parameters:

Table 318: Adding an Airwatch Endpoint Context Server - Server Tab Parameters

Parameter	Description
Select Server Type	Choose AirWatch from the drop-down list.
Server Name	Enter a valid server name. You can enter an IP address or a hostname.
Server Base URL	Enter the full URL for the server. You can append a custom port, such as for an MDM server: <code>https://yourserver.yourcompany.com:customerportnumber</code>
Username	Enter the user name.
Password	Enter and verify the password.
Verify Password	
API Key	Enter the API key that is provided by the vendor.

Table 318: Adding an Airwatch Endpoint Context Server - Server Tab Parameters (Continued)

Parameter	Description
Validate Server	Enable to validate the server certificate. Checking this option activates the Certificate tab.
Enable Server	Select the Enable to fetch endpoints from the server check box to enable the endpoint context server. By default, this field is disabled. The Bypass Proxy field will be enabled only if you enable this field.
Bypass Proxy	Select the Enable to bypass proxy server check box to bypass the proxy server. When this field is enabled, the proxy servers configured in the Administration > Server Manager > Server Configuration > Service Parameters tab > ClearPass system services service page will be bypassed. The server discovery occurs without any issues even when the proxy servers are bypassed. By default, this field is disabled. You must enable the Enable Server field to enable this field.

Actions Tab

The following table displays the **Airwatch Add Endpoint Context Server - Server** dialog parameters:

Figure 567: Adding an Airwatch Endpoint Context Server - Actions Dialog

Add Endpoint Context Server	
Server Actions	
Name	Description
Clear Passcode	Reset Passcode on the device
Enterprise Wipe	Delete only corporate information stored
Get Apps	Get apps information for the device
Lock Device	Locks the device
Remote Wipe	Delete all information stored
Send Message	Send message to the device
Send Message (Parameterized)	Send message with parameters to the device

Save Cancel

The following table describes the **Airwatch Add Endpoint Context Server - Actions** dialog parameters:

Table 319: Adding an Airwatch Endpoint Context Server - Actions Tab Parameters

Parameter	Description
Clear Passcode	Reset passcode on the device.
Enterprise Wipe	Delete only stored corporate information.
Get Apps	Get application information for the device.
Lock Device	Lock the associated device.
Remote Wipe	Delete all stored information.
Send Message	Send message to the device.
Send Message (Parameterized)	Send message with parameters to the device.

Adding an AirWave Endpoint Context Server

For more information about AirWave, refer to Dell AirWave documentation.

To add an AirWave Endpoint Context Server:

1. Navigate to **Administration > External Servers > Endpoint Context Servers**.

The **Endpoint Context Servers** page opens.

2. Click **Add**.

The **Add Endpoint Context Server** dialog opens.

3. From the **Select Server Type** drop-down, select **AirWave**.

The following dialog is displayed:

Figure 568: Add an AirWave Endpoint Context Server > Server Dialog

Add Endpoint Context Server

Server

Select Server Type: AirWave

Server Name:

Server Base URL:

Username: admin

Password: Verify:

Validate Server: ☐ Enable to validate the server certificate

Bypass Proxy: ☐ Enable to bypass proxy server

Save Cancel



You can add multiple endpoint context servers of the same type.

4. Enter the appropriate values for each of the AirWave Add Endpoint Context Server parameters described in [Table 320](#).
5. When satisfied with the settings, click **Save**.

Table 320: *Adding an AirWave Endpoint Context Server > Server Parameters*

Parameter	Action/Description
Select Server Type	1. Choose AirWave from the Select Server Type drop-down list.
Server Name	2. Enter a valid server name. You can enter an IP address or hostname.
Server Base URL	3. Enter the full URL for the AirWave server. You can append a custom port, such as for an MDM server: <i>https://yourserver.yourcompany.com:customerportnumber</i>
Username	4. Enter the username for the AirWave server.
Password	5. Enter the password for the server, then verify the password.
Verify Password	
Validate Server	6. Enable Validate Server to validate the server certificate. Checking this option enables the Certificate tab.
Bypass Proxy	7. Enable Bypass Proxy to bypass the proxy server.

Adding an Aruba Activate Endpoint Context Server

For more information about Activate, refer to Aruba Activate documentation.

Server Tab

The following figure displays the **Aruba Activate Add Endpoint Context Server > Server** tab:

Figure 569: Adding an Aruba Activate Endpoint Context Server

The screenshot shows the 'Add Endpoint Context Server' configuration window with the 'Server' tab selected. The 'Certificates' tab is also visible. The configuration fields are as follows:

Field	Value
Select Server Type:	Aruba Activate
Server Name:	activate.arubanetworks.com
Server Base URL:	https://activate.arubanetworks.com
Username:	admin
Password:	••••••••
Verify:	
Device Filter:	RAP*, IAP*
Folder Filter:	*
Disable Stale Endpoints:	☐ Disable stale endpoints in the Endpoint DB
Validate Server:	☒ Enable to validate the server certificate
Enable Server:	☐ Enable to fetch endpoints from the server
Bypass Proxy:	☐ Enable to bypass proxy server

At the bottom right, there are 'Save' and 'Cancel' buttons.

The following table describes the **Aruba Activate Add Endpoint Context Server > Server** parameters:

Table 321: Adding an Aruba Activate Endpoint Context Server > Server Parameters

Parameter	Action/Description
Select Server Type	1. Choose Aruba Activate from the Select Server Type drop-down list.
Server Name	2. Enter a valid server name. You can enter an IP address or a hostname.
Server Base URL	3. Enter the complete URL for the Aruba Activate server. You can append a custom port, such as for an MDM server: https://yourserver.yourcompany.com:customerportnumber
Username	4. Enter the username for the Aruba Activate server.
Password	5. Enter the password, then verify the password.
Verify Password	
Device Filter	The Device Filter field is populated with a default regular expression to retrieve only the Remote AP (RAP) and Instant AP (IAP) information.
Folder Filter	The Folder Filter field is set to "*" by default.

Table 321: Adding an Aruba Activate Endpoint Context Server > Server Parameters (Continued)

Parameter	Action/Description
Disable Stale Endpoints	6. To disable stale endpoints in the Endpoint database, enable this option.
Validate Server	7. Enable Validate Server to validate the server certificate. Checking this option enables the Certificate tab. For information on certificate configuration, see Certificates Tab on page 575 .
Enable Server	8. Enable Enable Server to fetch endpoints from the server.
Bypass Proxy	9. Enable Bypass Proxy to bypass the proxy server.
	10. To save your configuration changes, click Save .

Certificates Tab

The following figure displays the **Aruba Activate Add Endpoint Context Server > Certificates** tab:

Figure 570: Adding an Aruba Activate Endpoint Context Server > Certificates

Add Endpoint Context Server

Server **Certificates**

The following Issuer/Root CA for the server certificates will be added to the Certificate Trust List -

Subject DN
CN=GeoTrust SSL CA - G2,O=GeoTrust Inc.,C=US

The following Issuer/Root CA for the server certificates will be enabled in the Certificate Trust List -

Subject DN
CN=GeoTrust Global CA,O=GeoTrust Inc.,C=US

Save **Cancel**

Adding a ClearPass Cloud Proxy Endpoint Context Server

The Cloud Proxy is a virtual instance configured in the cloud. This multi-tenant and single instance serves multiple customers having many CPPM nodes. Once configured, the CPPM server establishes a Cloud Tunnel to the Cloud Proxy instance given the credentials and Domain. The Domain is required as an identifier to indicate which Cloud Tunnel is applicable for which customer. Individual CPPM nodes in the cluster can be selected to establish the Cloud Tunnel, rather than all nodes in the CPPM cluster.

Figure 571: Add ClearPass Cloud Proxy Endpoint Context Server tab

Add Endpoint Context Server

Server

Select Server Type: ClearPass Cloud Proxy

Server Name: proxy.arubamdm.com

Server Base URL: wss://proxy.arubamdm.com/proxy

Username:

Password: Verify Password:

Domain:

Validate Server: ☐ Enable to validate the server certificate

Save Cancel

Table 322: Add ClearPass Cloud Proxy Endpoint Context Server Parameters

Parameter	Description
Select Server Type	ClearPass Cloud Proxy
Server Name	The hostname of the cloud instance that will proxy all requests directed to the CPPM server in the enterprise.
Server Base URL	Enter the full URL for the server. The default is the name you entered above with "https://" prepended. You can append a custom port, such as for an MDM server: https://yourserver.yourcompany.com:customerportnumber.
Username	Username/Password based authentication is used when you setup a cloud tunnel from CPPM to the Cloud Proxy instance. Enter the username.
Password	Enter the password.
Verify Password	Verify the password.
Domain	An identifier used to determine the specific Cloud Tunnel to which the request must be sent by the Cloud Proxy.
Validate Server	Click to enable validation of the server certificate.

Adding a Google Admin Console Endpoint Context Server

Consult Google Developer documentation for information about the parameters that you must enter to configure this endpoint.

Server Tab

The following figure displays the **Add Endpoint Context Server - Server** (Google Admin Console) tab:

Figure 572: Add Endpoint Context Server - Server (Google Admin Console) Tab

The screenshot shows a dialog box titled "Add Endpoint Context Server" with a close button in the top right corner. It has two tabs: "Server" (selected) and "Certificates". The "Server" tab contains the following fields and options:

- Select Server Type:** A dropdown menu with "Google Admin Console" selected. Below it, a note states: "Adding the Google Admin Console as an Endpoint Context Server requires a Project to be created in the Google Developer Console".
- Client Id:** A text input field.
- Client Secret:** A text input field.
- Google API Access:** A button labeled "Authorize ClearPass". Below it, a note states: "You will be redirected to Google to authenticate & authorize ClearPass for access to Google Admin APIs for your domain".
- Validate Server:** A checkbox labeled "Enable to validate the server certificate", which is checked.
- Enable Server:** A checkbox labeled "Enable to fetch endpoints from the server", which is unchecked.
- Bypass Proxy:** A checkbox labeled "Enable to bypass proxy server", which is unchecked.

At the bottom right of the dialog box are "Save" and "Cancel" buttons.



You can add more than one endpoint context server of the same type. For example, you can add more than one AirWatch endpoint context server.

The following table describes the **Add Endpoint Context Server - Server** (Google Admin Console) tab parameters:

Table 323: Add Endpoint Context Server - Server (Google Admin Console) Tab Parameters

Parameter	Description
Select Server Type	Choose Google Admin Console from the drop-down list.
Client Id	Enter the client ID. For example, 9169879216kpl50kxuaq6q6qqwe0i.apps.googleusercontent.com .
Client Secret	Enter the client secret. For example, gMcfg342ePaKgX1ZIXK .
Google API Access	Authenticate and authorize W-ClearPass for access to Google Admin APIs for your domain.

Table 323: Add Endpoint Context Server - Server (Google Admin Console) Tab Parameters (Continued)

Parameter	Description
Validate Server	Enable to validate the server certificate. Checking this option enables the Certificate tab. For more information on certificate, see Certificates Tab on page 578 .
Enable Server	Enable this field to fetch endpoints from the server.
Bypass Proxy	Select the Enable to bypass proxy server check box to bypass the proxy server. When this field is enabled, the proxy servers configured in the Administration > Server Manager > Server Configuration > Service Parameters tab > ClearPass system services service page will be bypassed. The server discovery occurs without any issues even when the proxy servers are bypassed. By default, this field is disabled.

Certificates Tab

The following figure displays the **Add Endpoint Context Server - Certificates** (Google Admin Console) tab:

Figure 573: Add Endpoint Context Server - Certificates (Google Admin Console) Tab

Add Endpoint Context Server

Server **Certificates**

The following Issuer/Root CA for the server certificates will be added to the Certificate Trust List -

Subject DN
CN=Google Internet Authority G2, O=Google Inc, C=US
CN=GeoTrust Global CA, O=GeoTrust Inc., C=US

The following Issuer/Root CA for the server certificates will be enabled in the Certificate Trust List -

Subject DN
C=US, O=Equifax, OU=Equifax Secure Certificate Authority

Save **Cancel**

Adding a Generic HTTP Endpoint Context Server

The following figure displays the **Generic HTTP Add Endpoint Context Server > Server** tab:

Figure 574: Adding a Generic HTTP Endpoint Context Server

The screenshot shows a window titled "Add Endpoint Context Server" with a "Server" tab selected. The form contains the following fields and options:

- Select Server Type:** A dropdown menu with "Generic HTTP" selected.
- Server Name:** A text input field.
- Server Base URL:** A text input field.
- Username:** A text input field.
- Password:** A text input field.
- Verify Password:** A text input field.
- Validate Server:** A checkbox with the label "Enable to validate the server certificate".
- Bypass Proxy:** A checkbox with the label "Enable to bypass proxy server".

At the bottom right of the dialog are "Save" and "Cancel" buttons.



You can add more than one endpoint context server of the same type. For example, you can add more than one AirWatch endpoint context server.

The following table describes the **Generic HTTP Add Endpoint Context Server > Server** parameters:

Table 324: Add Endpoint Context Server - Server (Generic HTTP) Tab Parameters

Parameter	Action/Description
Select Server Type	1. Choose Generic HTTP from the Select Server Type drop-down list.
Server Name	2. Enter a valid server name. You can enter an IP address or a hostname.
Server Base URL	3. Enter the complete URL for the server. You can append a custom port, such as for an MDM server: <i>https://yourserver.yourcompany.com:customerportnumber</i>
Username	4. Enter the username for the server.
Password	5. Enter the password, then verify the password.
Verify Password	

Table 324: Add Endpoint Context Server - Server (Generic HTTP) Tab Parameters (Continued)

Parameter	Action/Description
Validate Server	6. Enable Validate Server to validate the server certificate. Checking this option enables the Certificate tab.
Bypass Proxy	7. Enable Bypass Proxy to bypass the proxy server.
	8. Click Save to save your changes.

Integrating W-ClearPass with Infoblox

This section provides the following information:

- [Adding an Infoblox Endpoint Context Server](#)
- [Adding a Context Server Action to the Infoblox Server](#)
- [Creating an Infoblox Enforcement Profile](#)
- [Configuring an Infoblox RADIUS Enforcement Profile](#)
- [Creating an Infoblox Enforcement Policy](#)
- [Defining an Infoblox Service](#)
- [Authenticating External Devices Against the Infoblox Service](#)
- [Creating a Filter to Accept Information from the W-ClearPass Server](#)

Infoblox is a server that provides a host of services, such as DNS, DHCP, and IPAM (IP address management). Infoblox provides a DHCP management system that issues IP addresses to externally authenticated devices and also maintains a MAC address context associated with the newly allocated IP address.

Integrating W-ClearPass with Infoblox typically tags the username context, as well as the external device being authenticated, along with its respective MAC address, which further simplifies IP address management on the Infoblox side.

This section describes the configurations that you must make on the W-ClearPass server in order for the W-ClearPass server to send data to an Infoblox server.

Adding an Infoblox Endpoint Context Server

To add an Infoblox endpoint context server:

1. Navigate to **Administration > External Servers > Endpoint Context Servers**.

The **Endpoint Context Servers** page opens.

Figure 575: Endpoint Context Servers Page

Administration » External Servers » Endpoint Context Servers

Endpoint Context Servers

 Add
 Import
 Export All

Filter:	Server Name	contains		+	Go	Clear Filter	Show	10	records
#	Server Name	Server Type	Status						
1.	localhost	Generic HTTP	Enabled						
Showing 1-1 of 1				Trigger Poll Export Delete					

2. Click **Add**.

The **Add Endpoint Context Server** dialog opens. This dialog opens in the **Server** page.

Figure 576: Adding an Infoblox Endpoint Context Server

3. Enter the following information:
 - a. **Select Server Type:** From the drop-down list, select **Generic HTTP**.
 - b. **Server Name:** Enter the IP address of the Infoblox server.
 - c. **Server Base URL:** As you enter the IP address in the **Server Name** field, the **Server Base URL** is populated automatically with the same IP address.
 - d. **Password:** Enter the password for this server, then verify the password.
4. When finished defining the parameters in the **Server** page, click **Save**.
You return to the **Endpoint Context Servers** page, where the endpoint context server you added is now listed.

Adding a Context Server Action to the Infoblox Server

This section describes how to define an Infoblox Login action and specify the URL to post content from the W-ClearPass Policy Manager server to the Infoblox server.

To add a context server action to the Infoblox server:

1. Navigate to **Administration > Dictionaries > Context Server Actions**.

The **Endpoint Context Server Actions** page appears.

Administration » Dictionaries » Context Server Actions

Endpoint Context Server Actions

Filter: Server Type contains [] Go Clear Filter Show 100 records

#	Server Type	Action Name	HTTP Method	Description
1.	airwatch	Enterprise Wipe	POST	Delete only corporate information stored
2.	airwatch	Remote Wipe	POST	Delete all information stored
14.	Generic HTTP	nmap Scan	POST	Inform
15.	Generic HTTP	Check Point Login - Guest User	POST	Inform Check Point that user logged in.
16.	Generic HTTP	Infoblox Login	POST	This is the Endpoint Context Server Action to send user or device context to Infoblox server
17.	Generic HTTP	Check Point Logout	POST	Inform Check Point that user logged out.
18.	Juniper Networks SRX	Juniper Networks SRX Logout	POST	This is the Endpoint Context Server Action to send user or device logout context to Juniper SRX server

2. Select the **Infoblox Login** endpoint context server action.

The **Endpoint Context Server Details** dialog for the selected action is displayed.

For descriptions of the parameters in the **Endpoint Context Servers Details** tabs, refer to [Configuring Endpoint Context Server Actions on page 563](#).

Figure 577: *Selecting the Infoblox Server for the Endpoint Context Server Action*

Endpoint Context Server Details

Action	Header	Content	Attributes
Server Type:	Generic HTTP		
Server Name:	10.2.51.4		
Action Name:	Infoblox Login		
Description:	This is the Endpoint Context Server Action to send user or device context to Infoblox server		
HTTP Method:	POST		
Skip HTTP Auth:	☐ Enable to skip HTTP Basic Authentication		
URL:	/wapi/v2.0/macfilteraddress?		

Save Cancel

3. **Server Name:** Select the IP address of the Infoblox server.
4. **URL:** Note the URL for posting content from the W-ClearPass server to the Infoblox server:
/wapi/v2.0/macfilteraddress?
5. Click **Save**.

Attributes Sent to the Infoblox Server

6. To view the attributes that will be sent to the Infoblox server, click the **Content** tab.
As shown in [Figure 578](#), the following attributes are sent in JSON format to the Infoblox server:
 - Filter name **"ClearPass"**
 - Username and MAC addresses of the authenticated devices

Figure 578: *Attributes Sent to Infoblox Server*

Endpoint Context Server Details

Action	Header	Content	Attributes
Content-Type:	JSON		
Content:	{"filter":"ClearPass", "mac":"%{Connection:Client-Mac-Address-Colon}", "username":"%{Authentication:Full-Username}", "expiration_time":"21600"}		

Save Cancel

7. Click **Cancel**.

Creating an Infoblox Enforcement Profile

This section describes how to create a simple HTTP-based enforcement profile named "*Infoblox Notify*" that acts against the Infoblox Login action.

For details on configuring enforcement profiles, see [Configuring Enforcement Profiles on page 345](#).

To create an Infoblox enforcement profile:

1. Navigate to **Configuration > Enforcement > Profiles**.

The **Enforcement Profiles** page opens.

Figure 579: Enforcement Profiles Page

Configuration > Enforcement > Profiles

Enforcement Profiles

 Add
 Import
 Export All

Filter: contains Show records

#	☐	Name ▲	Type	Description
1.	☐	[Aerohive - Terminate Session]	RADIUS_CoA	System-defined profile to disconnect user (Aerohive)
2.	☐	[AirGroup Personal Device]	RADIUS	System-defined profile for an AirGroup personal device request
3.	☐	[AirGroup Response]	RADIUS	System-defined profile for any AirGroup request
4.	☐	[AirGroup Shared Device]	RADIUS	System-defined profile for an AirGroup shared device request
5.	☐	[Allow Access Profile]	RADIUS	System-defined profile to allow network access
6.	☐	[Allow Application Access Profile]	Application	System-defined profile to allow access to application
7.	☐	[Aruba Bounce Host-Port]	RADIUS_CoA	System-defined profile to bounce host-port (Aruba)
8.	☐	[Aruba TACACS read-only Access]	TACACS	System-defined profile for read-only access to Aruba device
9.	☐	[Aruba TACACS root Access]	TACACS	System-defined profile for root access to Aruba device
10.	☐	[Aruba Terminate Session]	RADIUS_CoA	System-defined profile to disconnect user (Aruba)

Showing 1-10 of 36 

2. Click **Add**.

The **Add Enforcement Profiles** dialog appears.

Figure 580: Adding the Infoblox Enforcement Profile

Configuration > Enforcement > Profiles > Add Enforcement Profile

Enforcement Profiles

Profile	Attributes	Summary
Template:	HTTP Based Enforcement	
Name:	Infoblox Notify	
Description:	This is an enforcement profile against the Infoblox Login action.	
Type:	HTTP	
Action:	☒ Accept ☐ Reject ☐ Drop	
Device Group List:	--Select-- Remove View Details Modify	

3. Configure the **Add Enforcement Profile** page as follows:

- a. **Template:** Select **HTTP Based Enforcement**.

For details on configuring HTTP-based enforcement profiles, see [HTTP Based Enforcement on page 374](#).

- b. **Name:** Enter **Infoblox Notify**.
- c. **Description:** Optionally, enter a description of this enforcement profile.
- d. Click **Next**.

The **Enforcement Profiles Attributes** page appears.

Figure 581: *Specifying the Target Server and Enforcement Action*

Configuration » Enforcement » Profiles » Add Enforcement Profile

Enforcement Profiles

Profile		Attributes		Summary	
Attribute Name				Attribute Value	
1.	Target Server	=		10.2.51.4	
2.	Action	=		Infoblox Login	
3.	Click to add...				

4. Configure the **Enforcement Profile Attributes** page as follows:

- a. **Target Server:** Select the IP address of the Infoblox server.
- b. **Action:** Select **Infoblox Login**.
- c. Click **Save**.

You return to the **Enforcement Profiles** page, where the Infoblox Notify enforcement profile is now listed.

Configuring an Infoblox RADIUS Enforcement Profile

This section describes how to define a RADIUS Enforcement type profile for Infoblox. This profile configures parameters to define tunnel parameters, VLAN ID, and the termination action.



This configuration is specific to the lab environments in which this feature has been tested. The RADIUS: IETF attributes can take any values, depending on the lab environment.

For details on configuring a RADIUS-based enforcement policy, see [RADIUS Based Enforcement on page 375](#).

To define a RADIUS Enforcement profile:

1. Navigate to **Configuration > Enforcement > Profiles**.

The **Enforcement Profiles** page appears.

2. Click **Add**.

The **Add Enforcement Profiles** dialog appears.

Figure 582: Adding a RADIUS-Based Enforcement Profile

Configuration » Enforcement » Profiles » Add Enforcement Profile

Enforcement Profiles

Profile	Attributes	Summary
Template:	RADIUS Based Enforcement	
Name:	Infoblox RADIUS Enforcement	
Description:	RADIUS-based enforcement that defines tunnel parameters, <u>VLAN ID</u> , and termination action.	
Type:	RADIUS	
Action:	☒ Accept ☐ Reject ☐ Drop	
Device Group List:	--Select-- Remove View Details Modify	

3. Enter the following information:
 - a. **Template:** Select **RADIUS Based Enforcement**.
 - b. **Name:** Enter **Infoblox RADIUS Enforcement**.
 - c. **Description:** Optionally, enter a description of this profile.
 - d. Click **Next**.

The Enforcement Profiles **Attributes** page opens. In the following steps, you will add the four RADIUS Enforcement attributes illustrated in [Figure 583](#).

Figure 583: Adding Attributes to the RADIUS Enforcement Profile

Configuration » Enforcement » Profiles » Add Enforcement Profile

Enforcement Profiles

Profile	Attributes	Summary
Type	Name	Value
1. Radius:IETF	Tunnel-Private-Group-Id	= data
2. Radius:IETF	Session-Timeout	= 21600
3. Radius:IETF	Tunnel-Type	= VLAN (13)
4. Radius:IETF	Termination-Action	= RADIUS-Request (1)
5. Click to add...		

Tunnel-Private_Group-Id

4. Click **Click to add...**
 - a. **Type:** Select **Radius:IETF**.
 - b. **Name:** Select **Tunnel-Private_Group-Id**.
 - c. **Value:** Enter the value configured for the **Tunnel-Private_Group-Id** attribute on the controller.

Session-Timeout

5. Click **Click to add...**
 - a. **Type:** Select **Radius:IETF**.
 - b. **Name:** Select **Session-Timeout**.

- c. **Value:** Enter **21600** (which equals six hours in seconds).

Tunnel-Type

- 6. Click **Click to add...**
 - a. **Type:** Select **Radius:IETF**.
 - b. **Name:** Select **Tunnel-Type**.
 - c. **Value:** Select **VLAN**.

Termination-Action

- 7. Click **Click to add...**
 - a. **Type:** Select **Radius:IETF**.
 - b. **Name:** Select **Termination-Action**.
 - c. **Value:** Select **RADIUS-Request**.

- 8. Click **Save**.

You return to the Enforcement Profiles page. The following message is displayed:

Enforcement profile "Infoblox RADIUS Enforcement" added

Creating an Infoblox Enforcement Policy

This section describes how to create an enforcement policy to act against the "Infoblox Notify" and "Infoblox RADIUS Enforcement" profiles so that external devices can authenticate against this policy.

For details on configuring enforcement policies, see [Configuring Enforcement Policies on page 343](#).

To create an Infoblox Enforcement Policy:

- 1. Navigate to **Configuration > Enforcement > Policies**.
The **Enforcement Policies** page opens.
- 2. Click **Add**.
The Add Enforcement Policies page appears.

Figure 584: Adding the Infoblox Enforcement Policy

Configuration » Enforcement » Policies » Add

Enforcement Policies

Enforcement	Rules	Summary
Name:	Infoblox Policy	
Description:	Enforcement policy to act against the 'Infoblox Notify' and 'Infoblox RADIUS Enforcement' profiles	
Enforcement Type:	☒ RADIUS ☐ TACACS+ ☐ WEBAUTH (SNMP/Agent/CLI/CoA) ☐ Application ☐ Event	
Default Profile:	[Allow Access Profile] View Details Modify	

- 3. Enter the following information:
 - a. **Name:** Enter **Infoblox Policy**.
 - b. **Description:** Optionally, enter a description of this profile.
 - c. **Enforcement Type:** Set by default to **RADIUS**.
 - d. Default Profile: Select **Allow Access Profile**.
 - e. Click **Next**.

The **Rules** page appears.

4. Click **Add Rule**.

The Rules Editor dialog appears.

Figure 585: Configuring Infoblox Enforcement Policy Rules

Type	Name	Operator	Value
1. Tips	Role	EQUALS	[User Authenticated]
2. Click to add...			

Profile Names:
[RADIUS] Infoblox RADIUS Enforcement
[HTTP] Infoblox Notify
--Select to Add--

Buttons: Move Up, Move Down, Remove, Save, Cancel

5. In the **Conditions** panel, click **Click to add**, then enter the following information:

- Type:** Select **Tips**.
- Name:** Select **Role**.
- Operator:** Select **EQUALS**.
- Value:** Select **User Authenticated**.

6. In the **Enforcement Profiles** panel:

- Click **Select to Add**.



You must add the enforcement profiles in the order specified here.

- Select **[RADIUS] Infoblox RADIUS Enforcement**.
- Click **Select to Add**.
- Select **[HTTP] Infoblox Notify**.

7. Click **Save**.

8. To view the Infoblox enforcement policy summary, click the **Summary** tab.

Figure 586: Summary of the Infoblox Enforcement Policy

Enforcement Policies

Enforcement	Rules	Summary
Enforcement:		
Name:	Infoblox Policy	
Description:	Enforcement policy to act against the "Infoblox Notify" and "Infoblox RADIUS Enforcement" profiles	
Enforcement Type:	RADIUS	
Default Profile:	[Allow Access Profile]	
Rules:		
Rules Evaluation Algorithm:	First applicable	
Conditions	Actions	
1. (Tips:Role EQUALS [User Authenticated])	[RADIUS] Infoblox RADIUS Enforcement, [HTTP] Infoblox Notify	

9. Check the summary information to make sure the policy is correct, make any changes if necessary, then click **Save**.

You return to the Enforcement Policies page where the new **Infoblox Policy** is now listed.

Defining an Infoblox Service

This section describes how to create a Generic RADIUS Enforcement wireless service named "Infoblox Service" for the policy "Infoblox Policy."

To create the wireless service:

1. Navigate to **Configuration > Services**.

The **Services** page opens.

2. Click **Add**.

The **Add Services** page opens.

Figure 587: Adding an Infoblox Wireless Service

Configuration » Services » Add

Services

Service	Authentication	Roles	Enforcement	Summary
Type:	802.1X Wireless			
Name:	Infoblox Wireless Service			
Description:	Infoblox Wireless Access Service			
Monitor Mode:	☐ Enable to monitor network access without enforcement			
More Options:	☐ Authorization ☐ Posture Compliance ☐ Audit End-hosts ☐ Profile Endpoints ☐ Accounting Proxy			
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...				

3. Enter the following information:

- a. **Type:** Select **802.1X Wireless**.
- b. **Name:** Enter **Infoblox Wireless Service**.
- c. **Description:** Optionally, enter a description of this service.
- d. In the **Service Rule** panel, set **Matches** to **ANY**, then click **Next**.

The **Authentication** page appears.

Figure 588: Specifying Wireless Service Authentication Settings

Configuration » Services » Add

Services

Service	Authentication	Roles	Enforcement	Summary
Authentication Methods:				
[EAP MSCHAPV2] [EAP PEAP] [EAP FAST] [EAP TLS] [EAP TTLS] --Select to Add-- Move Up Move Down Remove View Details Modify				
Authentication Sources:				
[Insight Repository] [Local SQL DB] --Select to Add-- Move Up Move Down Remove View Details Modify				
Strip Username Rules: ☐ Enable to specify a comma-separated list of rules to strip username prefixes or suffixes				

4. Enter the following information:
 - a. **Authentication Methods:** Select the authentication method.
This example uses **EAP MSCHAPv2**.
 - b. **Authentication Sources:** Select the authentication source(s).
This example uses **Local SQL DB**.
5. Select the **Enforcement** tab.

Figure 589: *Specifying the Enforcement Policy for the Service*

Configuration » Services » Add Services

Service	Authentication	Roles	Enforcement	Summary
Use Cached Results: ☐ Use cached Roles and Posture attributes from previous sessions				
Enforcement Policy:		Infoblox Policy	Modify	Add new Enforcement Policy
Enforcement Policy Details				
Description:				
Default Profile: [Allow Access Profile]				
Rules Evaluation Algorithm: first-applicable				
Conditions		Enforcement Profiles		
1. (Tips:Role EQUALS [User Authenticated])		Infoblox RADIUS Enforcement, Infoblox Notify		

6. From the **Enforcement Policy** drop down, select **Infoblox Policy**, then click **Next**.
The **Infoblox Wireless Service Summary** page is displayed.
7. Check the summary information to make sure the service is correct, make any changes if necessary, then click **Save**.
You return to the **Services** page where the new **Infoblox Wireless Service** is now listed.

Authenticating External Devices Against the Infoblox Service

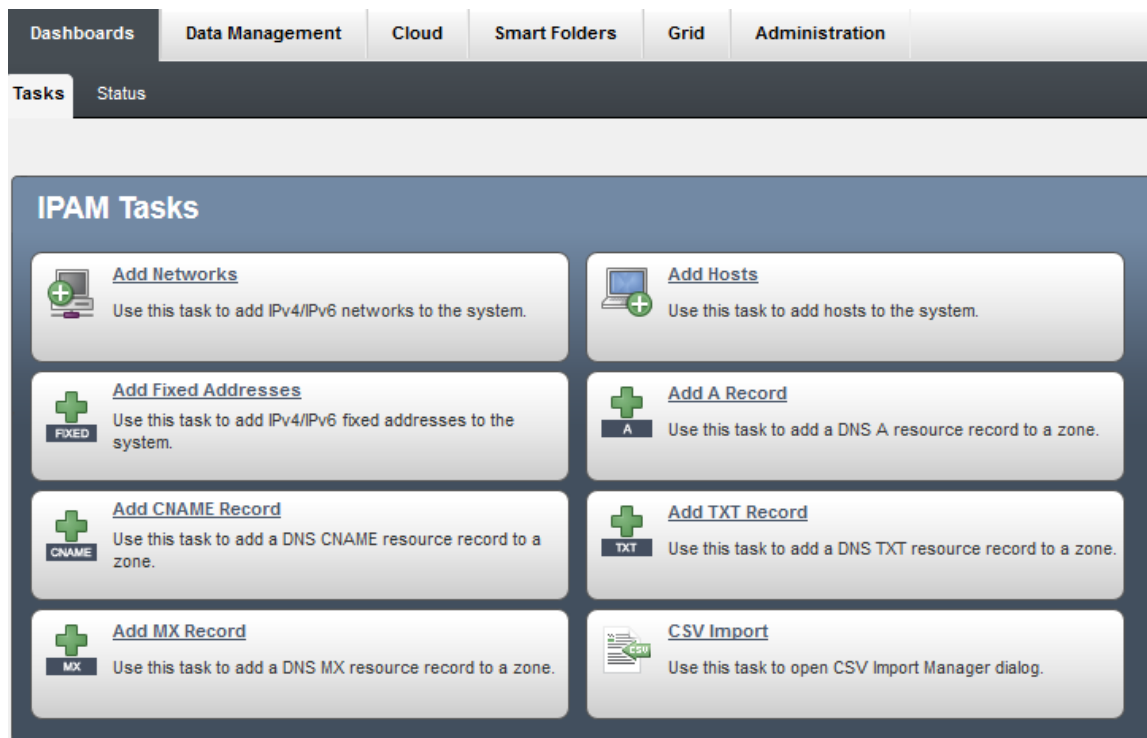
This section defines the configuration on the Infoblox server to receive the MAC address and username context from W-ClearPass.

The following procedure adds an IPv4 network that is used as a DHCP pool to assign IP addresses to the external devices that must be authenticated.

To configure an Infoblox server to authenticate external devices:

1. Log into the Infoblox server.
The **Infoblox IPAM Tasks** page opens.

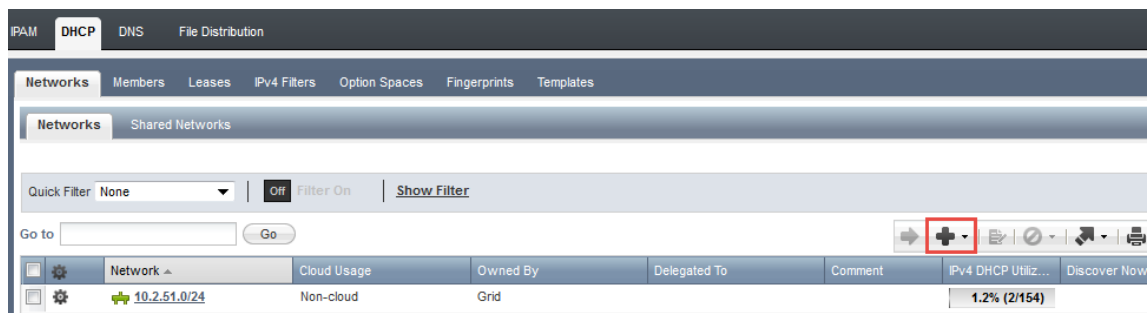
Figure 590: Infoblox Server Initial Page



2. Select the **Data Management** tab, then select the **DHCP** tab.

The **DHCP Networks** page appears.

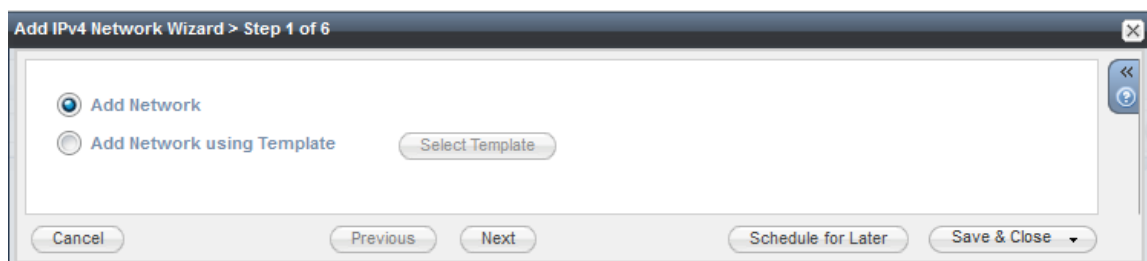
Figure 591: Adding an IPv4 Network



3. To add a new network, click the **Plus** icon.

The **Add IPv4 Network Wizard** begins.

Figure 592: Adding an IPv4 Network



4. With **Add Network** selected by default, click **Next**.

The following screen appears.

Figure 593: *Specifying the Netmask*

Add IPv4 Network Wizard > Step 2 of 6

Netmask* / 24 255.255.255.0

Networks *

Network
☒ 10.2.53.0

Comment

☐ Automatically Create Reverse-Mapping Zone

☐ Disable for DHCP

Cloud

Cancel Previous Next Schedule for Later Save & Close

5. In the **Netmask** field, specify the netmask for the new network.
The netmask is set by default to **/24** (that is, a Class C IP address), but you can set the netmask to any appropriate netmask value for your network.
6. To add an IPv4 network, in the **Networks** panel, click the **Plus** sign (see [Figure 593](#)).
7. In the **Networks** field, enter the IP address of the network, then click **Next**.
The **Members** screen appears.

Figure 594: *Adding Members*

Add IPv4 Network Wizard > Step 3 of 6

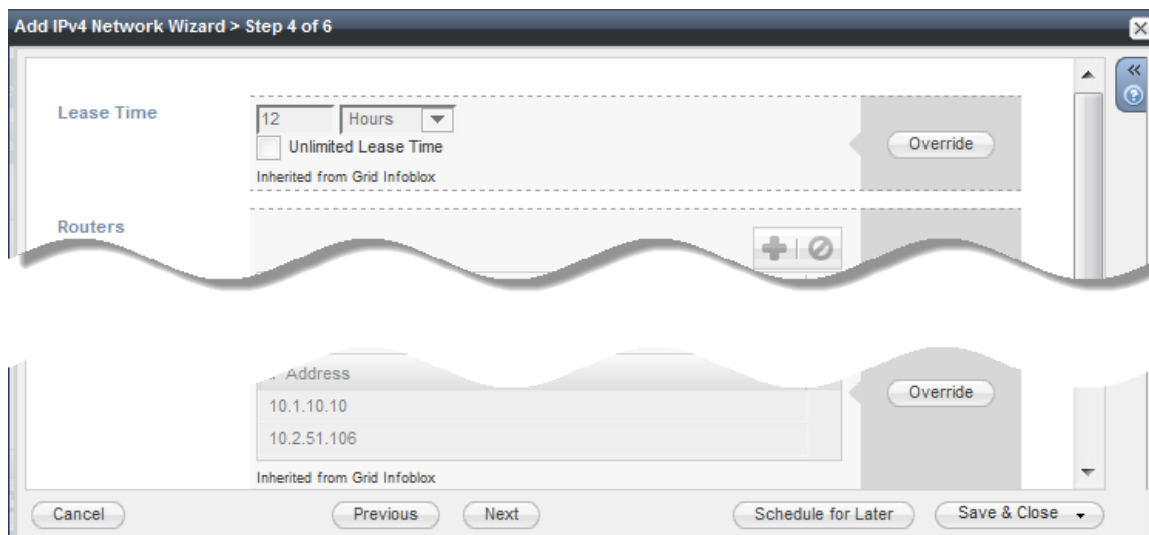
Members

Name	IPv4 Address	IPv6 Address	Comment
☒ infoblox.localdo...	10.2.51.4	2001:1868:a004...	

Cancel Previous Next Schedule for Later Save & Close

8. Click the **Plus** sign.
While adding members for the DHCP pool, the members group from **Data Management > DHCP > Members** is populated automatically.
9. Click **Next**.
The following screen appears.

Figure 595: *Specifying the Lease Time (Session-Timeout Value)*



10. In the **Lease Time Override** panel, click **Override**.

11. In the **Lease Time** field, enter **21600**; from the drop-down, select **Seconds**. Then click **Next**.



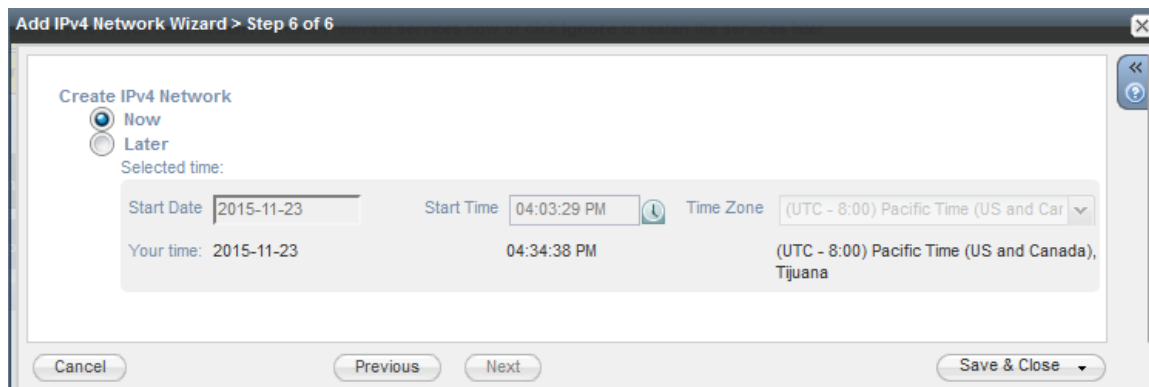
The Lease Time value you enter here must correspond to the **Session-Timeout** value defined under Infoblox RADIUS Enforcement (see [Figure 583](#)).

The **Extension Attributes** screen opens. No changes are required here.

12. Click **Next**.

The **Create IPv4 Network** screen opens. You can choose to create the network now or schedule it for a later day and time.

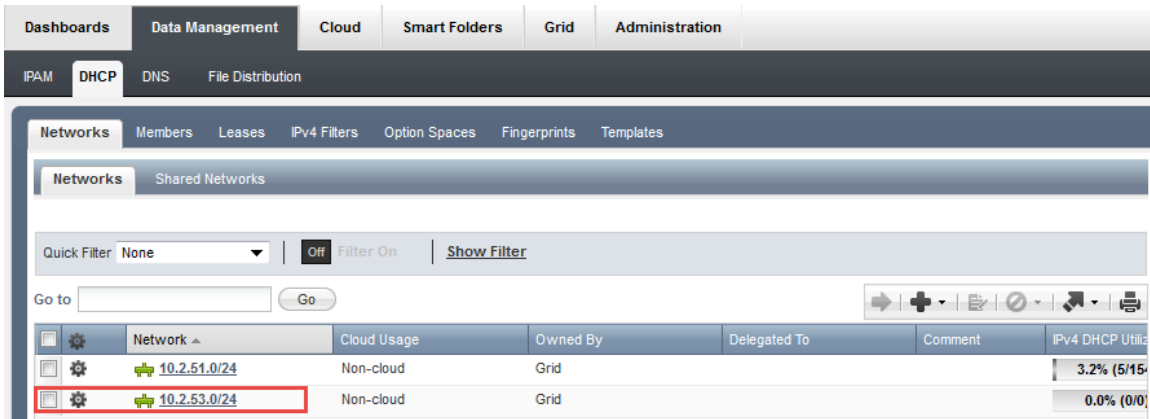
Figure 596: *Scheduling Date and Time for Creating the IPv4 Network*



13. Specify when you choose to create the IPv4 network, then click **Save & Close**.

The new network is created.

Figure 597: *New IPv4 Network Created*



Creating a Filter to Accept Information from the W-ClearPass Server

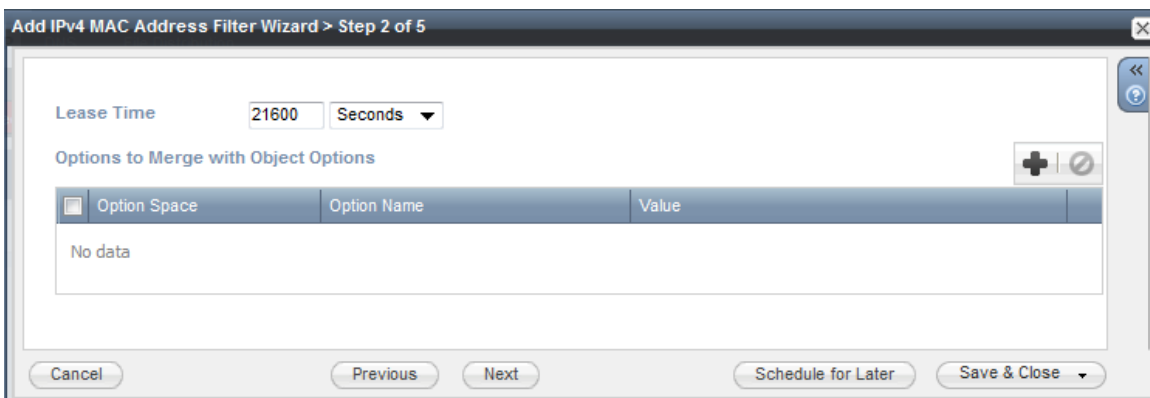
To create a filter to accept information from the W-ClearPass server:

1. From the **Data Management > DHCP** tab, select the newly created network.
The **Networks** page opens.
2. Select the **IPv4 Filters** tab.
3. To add a filter, click the **Plus** sign.
The **Add IPv4 MAC Address Filter** dialog opens.
4. In the **Name** field, enter **W-ClearPass**.

Note. the name of the filter must correspond to the filter value in the Endpoint Context Server Content page (see [Attributes Sent to the Infoblox Server on page 582](#)).

5. Optionally, enter a comment to describe this filter, then click **Next**.
Step 2 of the **Add IPv4 MAC Address Filter** wizard appears.
6. In the **Lease Time** fields, enter **21600 Seconds**, then click **Next**.

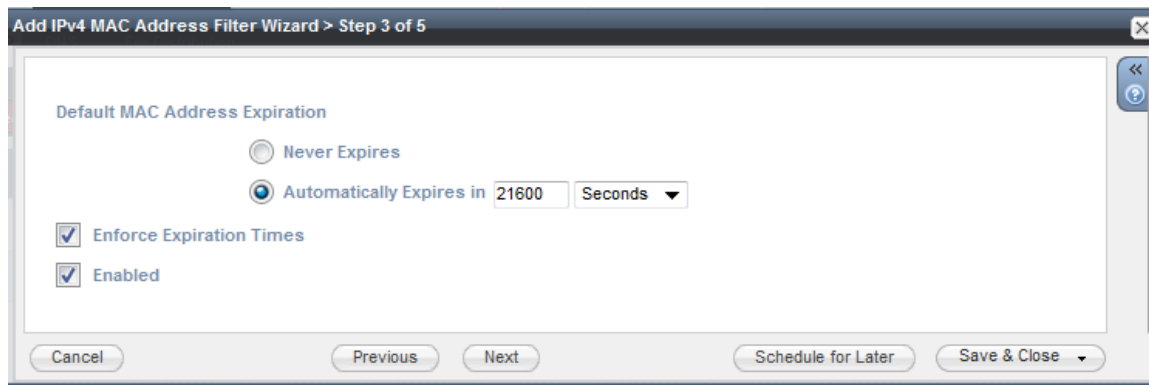
Figure 598: *Specifying Lease Time in the IPv4 MAC Address Filter*



The **Lease Time** value entered here must correspond to the **Session-Timeout** value defined under Infoblox RADIUS Enforcement Profile (see [Session-Timeout on page 585](#)).

Step 3 of the IPv4 MAC Address Filter wizard appears.

Figure 599: Specifying the MAC Address Expiration in the IPv4 MAC Address Filter



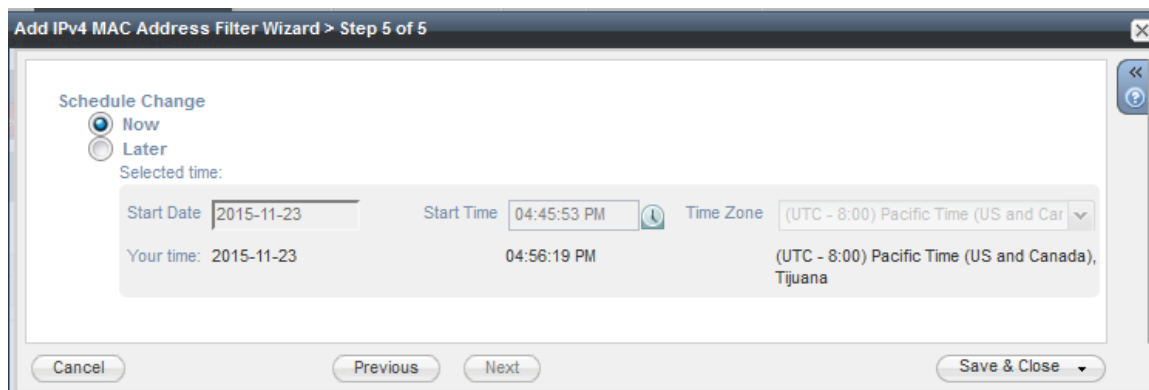
7. For the **Default MAC Address Expiration** setting:
 - a. Select the **Automatically Expires in** button.
 - b. Specify **21600 Seconds**.
 - c. Then click **Next**.

The Extensible attributes screen appears.

- 8 No changes are required for this step, so click **Next**.

In Step 5, the **Schedule Change** dialog appears.

Figure 600:



8. Specify the Schedule Change settings:
 - a. If you wish to run the MAC address filter now, select **Now**.
 - b. If you wish to schedule the MAC address filter for later, select **Later** and specify the **Start Date** and **Start Time**.
 - c. When finished with the **Schedule Change** settings, click **Save & Close**.

Integrating ClearPass with Juniper Networks SRX

This section provides the following information:

- [Adding a Juniper Networks SRX Endpoint Context Server](#)
- [Adding a Context Server Action to the Juniper SRX Server](#)
- [Viewing or Modifying Juniper Networks SRX Endpoint Context Server Actions](#)
- [Creating a Juniper SRX Enforcement Profile](#)
- [Creating a Juniper SRX Enforcement Policy](#)

- [Defining a Juniper SRX Wireless Service](#)

For more information about the parameters that you must enter to configure this endpoint context server, consult Juniper Network's documentation.

Integrating W-ClearPass with Juniper Networks SRX typically tags the username context, as well as the external devices being authenticated, along with its respective MAC address, which further simplifies IP address management on the Juniper SRX server side.

This section describes the configurations that you must make on the W-ClearPass server in order for the W-ClearPass server to send data to a Juniper Networks SRX server.

Adding a Juniper Networks SRX Endpoint Context Server

To add a Juniper Networks SRX Endpoint Context Server:

1. Navigate to **Administration > External Servers > Endpoint Context Servers**.
The **Endpoint Context Servers** page appears.
2. Click **Add**.
The **Add Endpoint Context Server** dialog appears. This dialog opens in the **Server** page.
3. From the **Select Server Type** drop-down, select **Juniper Networks SRX**.

Server Page

The following dialog is displayed (see [Figure 601](#)).

Figure 601: Adding a Juniper Networks SRX Endpoint Context Server - Server Page



You can add multiple endpoint context servers of the same type.

4. Enter the appropriate values for each of the Juniper Networks SRX Add Endpoint Context Server parameters described in [Table 325](#).
5. When satisfied with the settings, click **Save**.

Table 325: *Specifying Juniper Networks SRX Endpoint Context Server - Server Page Parameters*

Parameter	Description
Select Server Type	Choose Juniper Networks SRX from the drop-down list.
Server Name	Enter a valid server name. You can enter an IP address or a host name.
Server Base URL	Enter the full URL for the server. You can append a custom port, such as for an MDM server: <i>https://yourserver.yourcompany.com:customerportnumber</i>
Username	Enter the username.
Password	Enter and verify the password.
Verify Password	
Validate Server	Enable to validate the server certificate. Enabling this option activates the Certificate tab.
Enable Server	Enable this option to fetch endpoints from the server. Enabling this option activates the Poll Status tab.
Bypass Proxy	Enable this option to bypass the proxy server.

Adding a Context Server Action to the Juniper SRX Server

Figure 602 displays the **Juniper Network SRX Add Endpoint Context Server - Actions** page:

Figure 602: Adding a Juniper Networks SRX Endpoint Context Server - Actions Page

Administration » External Servers » Endpoint Context Servers

Endpoint Context Servers + Add
Import

Add Endpoint Context Server

Server

Actions

Name	Description
Juniper Networks SRX Login	This is the Endpoint Context Server Action to send user or device login context to Juniper SRX server
Juniper Networks SRX Logout	This is the Endpoint Context Server Action to send user or device logout context to Juniper SRX server

Save Cancel

Table 326 describes the Endpoint Context Server Actions that are available:

Table 326: Juniper Networks SRX Endpoint Context Server Actions

Action	Description
Juniper Networks SRX Login	Endpoint Context Server action to send a user or device login context to a Juniper SRX server.
Juniper Networks SRX Logout	Endpoint Context Server action to send a user or device logout context to a Juniper SRX server.

Viewing or Modifying Juniper Networks SRX Endpoint Context Server Actions

To view or modify the Juniper Networks SRX endpoint context server actions:

1. Navigate to **Administration > Dictionaries > Context Server Actions**.
The **Endpoint Context Server Actions** page appears.
2. Select the Juniper Networks SRX endpoint context server action of interest.
The **Endpoint Context Server Details** dialog for the selected action is displayed.

Figure 603: *Endpoint Context Server Details for the Juniper SRX Action*

The screenshot shows the 'Endpoint Context Server Details' dialog box with the 'Action' tab selected. The fields are as follows:

Server Type:	Juniper Networks SRX
Action Name:	Juniper Networks SRX Logout
Description:	This is the Endpoint Context Server Action to send user or device logout context to Juniper SRX server
HTTP Method:	POST
Skip HTTP Auth:	☐ Enable to skip HTTP Basic Authentication
URL:	/api/userfw/v1/post-entry

At the bottom right are 'Save' and 'Cancel' buttons.

For descriptions of the parameters in the **Endpoint Context Servers Details** pages, refer to [Configuring Endpoint Context Server Actions on page 563](#).

3. If necessary, modify the parameters in the **Action** page, then click **Save**.
4. To specify a content type and add non-default context server attributes, select the **Content** tab.

[Figure 604](#) shows the content of the Juniper Networks SRX Login action:

Figure 604: *Content for the Juniper Networks SRX Login Action*

The screenshot shows the 'Endpoint Context Server Details' dialog box with the 'Content' tab selected. The fields are as follows:

Content-Type:	XML
Content:	<pre><?xml version="1.0" encoding="UTF-8"?><userfw-entries><userfw-entry><source>Aruba ClearPass</source><timestamp>{%Authorization:Time Source:Now}</timestamp><operation>logon</operation><IP>{%Radius:IETF:Framed-IP-Address}</IP><domain>{%Authentication:NetBIOS-Name}</domain><user>{%Authentication:Username}</user><role-list><role>{%TIPS:Role}</role></role-list><posture>{%posture}</posture><device_category>{%device_category}</device_category><device_family>{%device_family}</device_family><device_name>{%device_name}</device_name></userfw-entry></userfw-entries></pre>

At the bottom right are 'Save' and 'Cancel' buttons.

[Figure 605](#) shows the content of the Juniper Networks SRX Logout action:

Figure 605: Content for the Juniper Networks SRX Logout Action

The screenshot shows a dialog box titled "Endpoint Context Server Details" with a close button in the top right corner. It has four tabs: "Action", "Header", "Content", and "Attributes". The "Content" tab is selected. Inside the tab, there is a "Content-Type:" dropdown menu set to "XML". Below it is a "Content:" text area containing the following XML code:

```
<?xml version="1.0" encoding="UTF-8"?><userfw-entries><userfw-entry>
<source>Aruba ClearPass</source><timestamp>%(Authorization:Time
Source:Now)</timestamp><operation>logoff</operation>
<IP>%(Radius:IETF:Framed-IP-Address)</IP></userfw-entry></userfw-
entries>
```

At the bottom right of the dialog are "Save" and "Cancel" buttons.

5. Make any necessary changes to the **Content** page, then click **Save**.

You return to the **Endpoint Context Servers** page, where the endpoint context server you added is now listed.

Creating a Juniper SRX Enforcement Profile

This section describes how to create a session-notification enforcement profile named "**Juniper SRX Notify**" that acts against the Juniper SRX Login action.

For details on configuring enforcement profiles, see [Configuring Enforcement Profiles on page 345](#).

To create a Juniper SRX enforcement profile:

1. Navigate to **Configuration > Enforcement > Profiles**.

The **Enforcement Profiles** page appears.

Figure 606: Enforcement Profiles Page

Configuration » Enforcement » Profiles

Enforcement Profiles

Add
 Import
 Export All

Filter: Name contains Show records

#	☐	Name ▲	Type	Description
1.	☐	[Aerohive - Terminate Session]	RADIUS_CoA	System-defined profile to disconnect user (Aerohive)
2.	☐	[AirGroup Personal Device]	RADIUS	System-defined profile for an AirGroup personal device request
3.	☐	[AirGroup Response]	RADIUS	System-defined profile for any AirGroup request
4.	☐	[AirGroup Shared Device]	RADIUS	System-defined profile for an AirGroup shared device request
5.	☐	[Allow Access Profile]	RADIUS	System-defined profile to allow network access
6.	☐	[Allow Application Access Profile]	Application	System-defined profile to allow access to application
7.	☐	[Aruba Bounce Host-Port]	RADIUS_CoA	System-defined profile to bounce host-port (Aruba)
8.	☐	[Aruba TACACS read-only Access]	TACACS	System-defined profile for read-only access to Aruba device
9.	☐	[Aruba TACACS root Access]	TACACS	System-defined profile for root access to Aruba device
10.	☐	[Aruba Terminate Session]	RADIUS_CoA	System-defined profile to disconnect user (Aruba)

Showing 1-10 of 36

2. Click **Add**.

The **Add Enforcement Profiles** dialog appears.

Figure 607: Adding the Juniper SRX Enforcement Profile

Configuration » Enforcement » Profiles » Add Enforcement Profile

Enforcement Profiles

Profile	Attributes	Summary
Template:	Session Notification Enforcement	
Name:	Juniper SRX Notify	
Description:	This is an enforcement profile against the Juniper SRX Login and Juniper SRX Logout actions.	
Type:	Post_Authentication	
Action:	☒ Accept ☐ Reject ☐ Drop	
Device Group List:	Remove View Details Modify Add new Device Group	

[Back to Enforcement Profiles](#)
[Next >](#)
[Save](#)
[Cancel](#)

3. Configure the **Add Enforcement Profile** page as follows:

a. **Template:** Select **Session Notification Enforcement**.

For details on configuring session notification enforcement profiles, see [Session Notification Enforcement on page 379](#)

b. **Name:** Enter **Juniper SRX Notify**.

c. **Description:** Optionally, enter a description of this enforcement profile.

d. Click **Next**.

The **Enforcement Profiles Attributes** page appears. In the following steps, you will add the four Session Notify Enforcement attributes illustrated in [Figure 608](#).

Figure 608: Adding Attributes to the Enforcement Profile

Configuration » Enforcement » Profiles » Add Enforcement Profile

Enforcement Profiles

Profile	Attributes	Summary
Type	Name	Value
1. Session-Notify	Server Type	= Juniper Networks SRX
2. Session-Notify	Server IP	= 10.1.1.1
3. Session-Notify	Login Action	= Juniper Networks SRX Login
4. Session-Notify	Logout Action	= Juniper Networks SRX Logout
5. Click to add...		

Server Type

4. Click **Click to add...**

a. **Type:** Select **Session-Notify**.

b. **Name:** Select **Server Type**.

c. **Value:** Select **Juniper Networks SRX**.

Server IP

5. Click **Click to add...**

a. **Type:** Select **Session-Notify**.

b. **Name:** Select **Server IP**.

- c. **Value:** Select the IP address of the Juniper SRX server.

Login Action

6. Click **Click to add...**
 - a. **Type:** Select **Session-Notify**.
 - b. **Name:** Select **Login Action**.
 - c. **Value:** Select **Juniper Networks SRX Login**.

Logout Action

7. Click **Click to add...**
 - a. **Type:** Select **Session-Notify**.
 - b. **Name:** Select **Logout Action**.
 - c. **Value:** Select **Juniper Networks SRX Logout**.

8. Click **Save**.

You return to the **Enforcement Profiles** page, where the Juniper Networks SRX Notify enforcement profile is now listed.

Creating a Juniper SRX Enforcement Policy

This section describes how to create an enforcement policy to act against the "**Juniper SRX Notify**" profile so that external devices can authenticate against this policy.

For details on configuring enforcement policies, see [Configuring Enforcement Policies on page 343](#).

To create a Juniper SRX Enforcement Policy:

1. Navigate to **Configuration > Enforcement > Policies**.

The **Enforcement Policies** page appears.

2. Click **Add**.

The **Add Enforcement Policies** dialog appears.

Figure 609: Adding the Juniper SRX Enforcement Policy

Configuration » Enforcement » Policies » Add

Enforcement Policies

Enforcement	Rules	Summary
Name:	Juniper SRX Enforcement Policy	
Description:	This is an enforcement policy to act against the "Juniper SRX Notify" enforcement profile.	
Enforcement Type:	☒ RADIUS ☐ TACACS+ ☐ WEBAUTH (SNMP/Agent/CLI/CoA) ☐ Application ☐ Event	
Default Profile:	[Allow Access Profile] View Details Modify Add new Enforcement Profile	

3. Enter the following information:
 - a. **Name:** Enter **Juniper SRX Enforcement Policy**.
 - b. **Description:** Optionally, enter a description of this profile.
 - c. **Enforcement Type:** Set by default to **RADIUS**.
 - d. **Default Profile:** Select **Allow Access Profile**.
 - e. Click **Next**.

The **Rules** page opens.

4. Click **Add Rule**.

The Rules Editor dialog opens.

Figure 610: Configuring Juniper SRX Enforcement Policy Rules

The screenshot shows the 'Rules Editor' window. The 'Conditions' panel is active, displaying a table with the following data:

Type	Name	Operator	Value
1. Tips	Role	EQUALS	[User Authenticated]
2. Click to add...			

Below the conditions panel is the 'Enforcement Profiles' panel. It shows a list of profile names with '[Post Authentication] Juniper SRX Notify' selected. To the right of the list are buttons for 'Move Up', 'Move Down', and 'Remove'. At the bottom of the panel is a dropdown menu labeled '--Select to Add--'. The 'Save' and 'Cancel' buttons are at the bottom right of the window.

Specify Conditions

5. In the **Conditions** panel, click **Click to add**, then enter the following information:
 - a. **Type:** Select **Tips**.
 - b. **Name:** Select **Role**.
 - c. **Operator:** Select **EQUALS**.
 - d. **Value:** Select **User Authenticated**.

Specify the Enforcement Profile

6. In the **Enforcement Profiles** panel:
 - a. Click **Select to Add**.
 - b. Select **[Post Authentication] Juniper SRX Notify**.
7. Click **Save**.
8. To view the Juniper SRX enforcement policy summary, click the **Summary** tab.

Figure 611: Summary of the Juniper SRX Enforcement Policy

Configuration » Enforcement » Policies » Edit - Juniper SRX Enforcement Policy
Enforcement Policies - Juniper SRX Enforcement Policy

The screenshot shows the 'Summary' tab of the 'Juniper SRX Enforcement Policy' configuration page. It contains the following information:

Enforcement:

Name:	Juniper SRX Enforcement Policy
Description:	Enforcement policy to act against the "Juniper SRX Notify" profile
Enforcement Type:	RADIUS
Default Profile:	[Allow Access Profile]

Rules:

Rules Evaluation Algorithm: First applicable

Conditions	Actions
1. (Tips:Role EQUALS [User Authenticated])	Juniper SRX Notify

9. Check the summary information to make sure the enforcement policy is correct, make any changes if necessary, then click **Save**.

You return to the Enforcement Policies page where the new **Juniper SRX Policy** is now listed.

Defining a Juniper SRX Wireless Service

This section describes how to create a n 802.1X wireless service named "Juniper SRX Wireless Service" to be applied to the policy "Juniper SRX Policy."

To create the Juniper SRX wireless service:

1. Navigate to **Configuration > Services**.

The Services page appears.

2. Click **Add**.

The Add Services page appears.

Figure 612: Adding a Juniper SRX Wireless Service

Configuration » Services » Add

Services

Service | Authentication | Roles | Enforcement | Summary

Type:	802.1X Wireless
Name:	Juniper SRX Wireless Service
Description:	Juniper 802.1X Wireless Access Service
Monitor Mode:	☐ Enable to monitor network access without enforcement
More Options:	☐ Authorization ☐ Posture Compliance ☐ Audit End-hosts ☐ Profile Endpoints ☐ Accounting Proxy

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...				

3. Specify the following information:
 - a. **Type:** Select **802.1X Wireless**.
 - b. **Name:** Enter **Juniper SRX Wireless Service**.
 - c. **Description:** Optionally, enter a description of this service.
 - d. In the **Service Rule** panel, set **Matches** to **ANY**, then click **Next**.

The **Authentication** page appears.

Figure 613: Specifying the Wireless Service Authentication Settings

Configuration » Services » Add

Services

Service | **Authentication** | Roles | Enforcement | Summary

Authentication Methods:

[EAP MSCHAPv2]
[EAP PEAP]
[EAP FAST]
[EAP TLS]
[EAP TTLS]
--Select to Add--

Move Up

Move Down

Remove

View Details

Modify

Authentication Sources:

[Insight Repository] [Local SQL DB]
--Select to Add--

Move Up

Move Down

Remove

View Details

Modify

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

4. Specify the following information:
 - a. **Authentication Methods:** Select the authentication method.

This example uses **EAP MSCHAPv2** as the authentication method.

- b. **Authentication Sources:** Select the authentication source(s).

This example uses **[Local User Repository] [Local SQL DB]** as the authentication source.

5. Select the **Enforcement** tab.

Figure 614: *Specifying the Enforcement Policy for the Juniper SRX Wireless Service*

Configuration » Services » Add

Services

Service	Authentication	Roles	Enforcement	Summary
Use Cached Results: ☐ Use cached Roles and Posture attributes from previous sessions Enforcement Policy: Juniper SRX Enforcement Policy Modify Add new Enforcement Policy				
Enforcement Policy Details				
Description: Enforcement policy to act against the "Juniper SRX Notify" profile				
Default Profile: [Allow Access Profile]				
Rules Evaluation Algorithm: first-applicable				
Conditions		Enforcement Profiles		
1. (Tips:Role EQUALS [User Authenticated])		Juniper SRX Notify		

6. From the **Enforcement Policy** drop-down, select **Juniper SRX Policy**, then click **Next**.
The **Juniper SRX Wireless Service Summary** is displayed.
7. Check the service summary information to make sure the service is correct, make any changes if necessary, then click **Save**.

You return to the **Services** page where the new **Juniper SRX Wireless Service** is now listed.

Adding a JAMF Endpoint Context Server

Consult the endpoint manufacturer's documentation for information about the parameters that you must enter to configure this endpoint. The following figure displays the **Add Endpoint Context Server - Server (JAMF)** tab:

Figure 615: *Add Endpoint Context Server - Server (JAMF) Tab*

Add Endpoint Context Server

Server

Select Server Type:	JAMF
Server Name:	
Server Base URL:	
Username:	
Password:	Verify Password:
Fetch Computer Records:	☐
Validate Server:	☐ Enable to validate the server certificate
Enable Server:	☐ Enable to fetch endpoints from the server
Bypass Proxy:	☐ Enable to bypass proxy server

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



You can add more than one endpoint context server of the same type. For example, you can add more than one AirWatch endpoint context server.

The following table describes the **Add Endpoint Context Server - Server** (JAMF) tab parameters:

Table 327: *Add Endpoint Context Server - Server (JAMF) Tab Parameters*

Parameter	Description
Select Server Type	Choose JAMF from the drop-down list.
Server Name	Enter a valid server name. You can enter an IP address or hostname.
Server Base URL	Enter the full URL for the server. You can append a custom port, such as for an MDM server: https://yourserver.yourcompany.com:customerportnumber.
Username	Enter the username.
Password	Enter and verify the password.
Verify Password	
Fetch Computer Records	Enable to fetch computer records.
Validate Server	Enable to validate the server certificate. Checking this option enables the Certificate tab.
Enable Server	Enable to fetch endpoints from the server.
Bypass Proxy	Enable to bypass proxy server.

Adding a MaaS360 Endpoint Context Server

Consult the endpoint manufacturer's documentation for information about the parameters that you must enter to configure this endpoint.

Server Tab

The following figure displays the **Add Endpoint Context Server - Server** (MaaS360) tab:

Figure 616: Add Endpoint Context Server - Server (MaaS360) Tab

The screenshot shows a window titled "Add Endpoint Context Server" with a close button in the top right. It has two tabs: "Server" (selected) and "Actions". The "Server" tab contains the following fields:

- Select Server Type: MaaS360 (dropdown)
- Server Name: (text input)
- Server Base URL: (text input)
- Username: (text input)
- Password: (text input) and Verify Password: (text input)
- Application Access Key: (text input)
- Application ID: (text input)
- Application Version: (text input)
- Platform ID: (text input)
- Billing ID: (text input)
- Validate Server: ☐ Enable to validate the server certificate
- Enable Server: ☐ Enable to fetch endpoints from the server
- Bypass Proxy: ☐ Enable to bypass proxy server

At the bottom right of the dialog are "Save" and "Cancel" buttons.



You can add more than one endpoint context server of the same type. For example, you can add more than one AirWatch endpoint context server.

The following table describes the **Add Endpoint Context Server - Server** (MaaS360) tab parameters:

Table 328: Add Endpoint Context Server - Server (MaaS360) Tab Parameters

Parameter	Description
Select Server Type	Choose MaaS360 from the drop-down list.
Server Name	Enter a valid server name. You can enter an IP address or hostname.
Server Base URL	Enter the full URL for the server. You can append a custom port, such as for an MDM server: <code>https://yourserver.yourcompany.com:customerportnumber</code> .
Username	Enter the username.

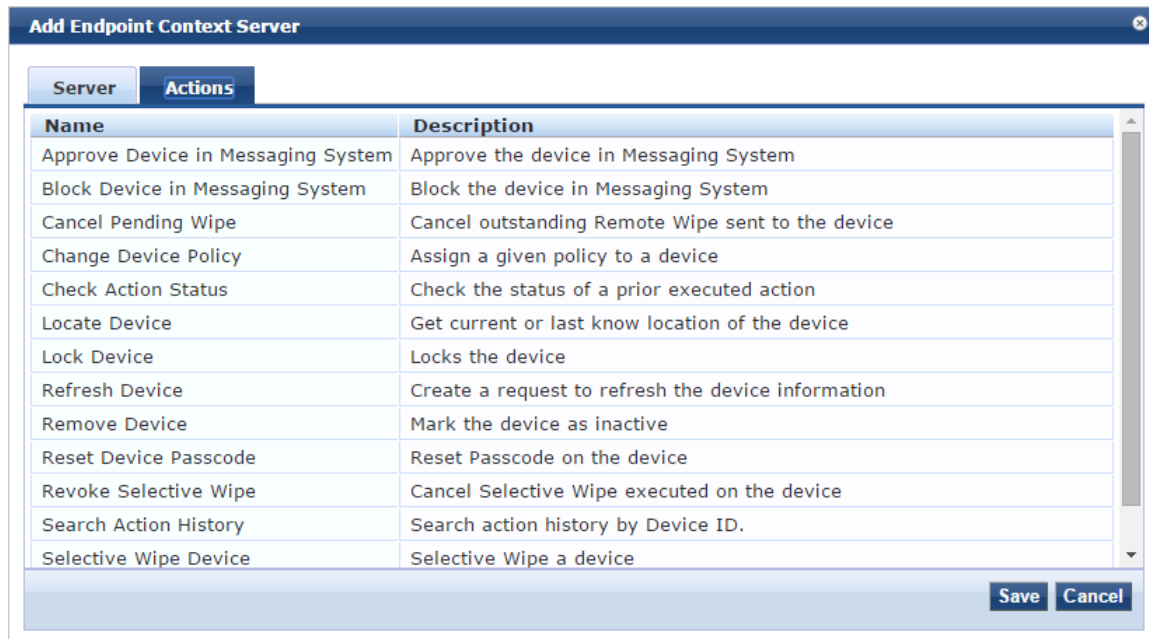
Table 328: Add Endpoint Context Server - Server (MaaS360) Tab Parameters (Continued)

Parameter	Description
Password	Enter and verify the password.
Verify Password	
Application Access Key	Enter the application access key (API key).
Application ID	Enter the application ID.
Application Version	Enter the application version number.
Platform ID	Enter the platform version number.
Billing ID	Enter the billing ID.
Validate Server	Enable to validate the server certificate. Checking this option enables the Certificate tab.
Enable Server	Enable to fetch endpoints from the server.
Bypass Proxy	Enable to bypass proxy server.

Actions Tab

The following figure displays the **Add Endpoint Context Server - Actions** (MaaS360) tab:

Figure 617: Add Endpoint Context Server - Actions (MaaS360) Tab



The following table describes the **Add Endpoint Context Server - Actions** (MaaS360) tab parameters:

Table 329: Add Endpoint Context Server - Actions (MaaS360) Tab Parameters

Parameter	Description
Approve Device in Messaging System	Approve the device in Messaging System.
Block Device in Messaging System	Block the device in Messaging System.
Cancel Pending Wipe	Cancel outstanding Remote Wipe sent to the device.
Change Device Policy	Assign a given policy to a device.
Check Action Status	Check the status of a prior executed action.
Locate Device	Get current or last know location of the device.
Lock Device	Lock the device.
Refresh Device	Create a request to refresh the device information.
Remove Device	Mark the device as inactive.
Reset Device Passcode	Reset the pass code on the device.

Table 329: Add Endpoint Context Server - Actions (MaaS360) Tab Parameters (Continued)

Parameter	Description
Revoke Selective Wipe	Cancel Selective Wipe executed on the device.
Search Action History	Search action history by Device ID.
Selective Wipe Device	Execute a Selective Wipe on a device.
Wipe Device	Delete all information stored on a device.

Adding a MobileIron Endpoint Context Server

Consult MobileIron's documentation for more information about the parameters that you must enter to configure this endpoint context server.

To add a MobileIron Endpoint Context Server:

1. Navigate to **Administration > External Servers > Endpoint Context Servers**.

The **Endpoint Context Servers** page appears.

2. Click **Add**.

The **Add Endpoint Context Server** dialog appears. This dialog opens in the **Server** tab.

3. From the **Select Server Type** drop-down, select **MobileIron**.

Server Page

The following figure displays the **Add Endpoint Context Server - Server** (MobileIron) dialog:

Figure 618: Adding a MobileIron Endpoint Context Server - Server Page

The screenshot shows a dialog box titled "Add Endpoint Context Server" with a close button in the top right corner. The dialog has two tabs: "Server" (selected) and "Actions". The "Server" tab contains the following fields and options:

- Select Server Type:** A dropdown menu with "MobileIron" selected.
- Server Name:** A text input field.
- Server Base URL:** A text input field.
- Username:** A text input field.
- Password:** A text input field.
- Verify Password:** A text input field.
- Validate Server:** A checkbox with the label "Enable to validate the server certificate".
- Enable Server:** A checkbox with the label "Enable to fetch endpoints from the server".
- Bypass Proxy:** A checkbox with the label "Enable to bypass proxy server".

At the bottom right of the dialog, there are two buttons: "Save" and "Cancel".



You can add multiple endpoint context servers of the same type.

4. Enter the appropriate values for each of the MobileIron Add Endpoint Context Server parameters described in [Table 330](#).
5. When satisfied with the settings, click **Save**.

Table 330: Adding a MobileIron Endpoint Context Server - Server Page Parameters

Parameter	Description
Select Server Type	1. Choose MobileIron from the drop-down list.
Server Name	2. Enter a valid server name. You can enter an IP address or host name.
Server Base URL	3. Enter the full URL for the server. You can append a custom port, such as for an MDM server: <i>https://yourserver.yourcompany.com:customerportnumber</i>
Username	4. Enter the username.
Password	5. Enter and verify the password.
Verify Password	
Validate Server	6. Enable to validate the server certificate. Checking this option enables the Certificate tab.
Enable Server	7. Enable to fetch endpoints from the server.
Bypass Proxy	8. Enable to bypass the proxy server.

Actions Page

The following figure displays the **Add Endpoint Context Server - Actions** (MobileIron) page:

Figure 619: Adding a MobileIron Endpoint Context Server - Actions Page

Add Endpoint Context Server	
Server Actions	
Name	Description
Get Labels	Get labels information for the device
Lock Device	Locks the device
Remote Wipe	Delete all information stored
Send Message	Send message to the device
Unlock Device	Unlocks the device

Save Cancel

Table 331 describes the Endpoint Context Server Actions that are available:

Table 331: Adding a MobileIron Endpoint Context Server - Actions Page Parameters

Parameter	Description
Get Labels	Get label information of the device.
Lock Device	Lock the device.
Remote Wipe	Delete all information stored on the device.
Send Message	Send message to the device.
Unlock Device	Unlock the device.

9. When satisfied with the **Action** settings, click **Save**.

Adding a Palo Alto Networks Firewall Endpoint Context Server

Consult Palo Alto Networks' documentation for more information about the parameters that you must enter to configure this endpoint context server.

To add a Palo Alto Networks Firewall Endpoint Context Server:

1. Navigate to **Administration > External Servers > Endpoint Context Servers**.
The **Endpoint Context Servers** page opens.
2. Click **Add**.
The **Add Endpoint Context Server** dialog opens.
3. From the **Select Server Type** drop-down, select **Palo Alto Networks Firewall**.
The following dialog is displayed (see [Figure 620](#)).

Figure 620: Add Endpoint Context Server: Palo Alto Networks Firewall Dialog

Add Endpoint Context Server

Server

Select Server Type: **Palo Alto Networks Firewall**

Server Name:

Server Base URL:

Username:

Password: Verify Password:

Username Transformation: **None**

GlobalProtect: ☐ GlobalProtect Enabled on Palo Alto Networks Firewall

Send Posture Data: ☐ Requires Eager handler polling frequency to be 2 minutes or more

UserID Post URL:

Validate Server: ☐ Enable to validate the server certificate

Bypass Proxy: ☐ Enable to bypass proxy server

Save **Cancel**



You can add multiple endpoint context servers of the same type.

4. Enter the appropriate values for each of the Palo Alto Networks Firewall Add Endpoint Context Server parameters described in [Table 332](#).
5. When satisfied with the settings, click **Save**.

Table 332: Add Endpoint Context Server: Palo Alto Networks Firewall Parameters

Parameter	Description
Select Server Type	Choose Palo Alto Networks Firewall from the drop-down list.
Server Name	Enter a valid server name. You can enter an IP address or a hostname.
Server Base URL	Enter the server base URL in the following format: <code>https://{server_ip}/api/?type=keygen&user={username}&password={password}</code>
Username	Enter the username.
Password	Enter and verify the password.
Verify Password	
Username Transformation	Choose one of the following options: • None: Do not use any username transformation. • Prefix NetBIOS name: Use the Prefix NetBIOS name in UID updates. • Use Full Username: Use the full username in UID updates.
GlobalProtect	Enable this option to send an HIP report to the firewall. You must enable the GlobalProtect license on the firewall for this to work.
Send Posture Data	Enable to send posture data on the Palo Alto Networks firewall after authentication. This option can be resource-intensive. The eager handler-polling interval must be two minutes or more. Enabling this field verifies whether the polling frequency is set to two minutes and then sends the posture data to Palo Alto Networks firewall. You can verify the posture data in the Access Tracker page.
UserID Post URL	Enter the user ID post URL in the following format: <code>https://{server_ip}/api/?type=user-id&action=set&key={key}&cmd={cmd}</code>
Validate Server	Enable to validate the server certificate. Checking this option enables the Certificate tab.
Bypass Proxy	Enable to bypass the proxy server.

Adding a Palo Alto Networks Panorama Endpoint Context Server

Consult the endpoint manufacturer's documentation for information about the parameters that you must enter to configure this endpoint. The following figure displays the **Add Endpoint Context Server - Server** (Palo Alto Networks Panorama) tab:

Figure 621: Add Endpoint Context Server - Server (Palo Alto Networks Panorama) Tab

The screenshot shows the 'Add Endpoint Context Server' window with the 'Server' tab active. The configuration fields are as follows:

- Select Server Type: Palo Alto Networks Panorama
- Server Name: [Empty text box]
- Server Base URL: `https://{server_ip}/api/?type=keygen&user={username}&password={password}`
- Username: [Empty text box]
- Password: [Empty text box]
- Verify Password: [Empty text box]
- Username Transformation: None
- GlobalProtect: ☐ GlobalProtect Enabled on Palo Alto Networks Firewall
- Send Posture Data: ☐ Requires Eager handler polling frequency to be 2 minutes or more
- Palo Alto Firewall Serial Numbers: [Empty text box]
- UserID Post URL: `https://{server_ip}/api/?type=user-id&action=set&key={key}&cmd={cmd}`
- Validate Server: ☐ Enable to validate the server certificate
- Bypass Proxy: ☐ Enable to bypass proxy server

Buttons: Save, Cancel



You can add more than one endpoint context server of the same type. For example, you can add more than one AirWatch endpoint context server.

The following table describes the **Add Endpoint Context Server - Server** (Palo Alto Networks Panorama) tab parameters:

Table 333: Add Endpoint Context Server - Server (Palo Alto Networks Panorama) Tab Parameters

Parameter	Description
Select Server Type	Choose Palo Alto Networks Panorama from the drop-down list.
Server Name	Enter a valid server name. You can enter an IP address or hostname.
Server Base URL	Enter the server base URL in the following format: <code>https://{server_ip}/api/?type=keygen&user={username}&password={password}</code>
Username	Enter the username.
Password	Enter and verify the password.
Verify Password	
Username Transformation	Choose one of the following options: ● None - Do not use any username transformation.

Table 333: Add Endpoint Context Server - Server (Palo Alto Networks Panorama) Tab Parameters (Continued)

Parameter	Description
	● Prefix NETBIOS name - Prefix NETBIOS name in UID updates. ● Use Full Username - Use full username in UID updates.
GlobalProtect	Enable to send HIP report to firewall. GlobalProtect license should be enabled on firewall for this to work.
Send Posture Data	Enable to send posture data on Palo Alto Networks firewall after authentication. This option can be resource-intensive, the eager handler-polling interval must be two minutes or more. Enabling this field verifies whether the polling frequency is set to 2 minutes and then send the posture data to Palo Alto Networks firewall. These posture data can be verified in Access Tracker page.
Palo Alto Firewall Serial Numbers	Enter the Palo Alto firewall serial numbers.
UserID Post URL	Enter the user ID post URL in the following format: https://{server_ip}/api/?type=user-id&action=set&key={key}&cmd={cmd}
Validate Server	Enable to validate the server certificate. Checking this option enables the Certificate tab.
Bypass Proxy	Enable to bypass proxy server.

Adding an SAP Afaria Endpoint Context Server

Consult the endpoint manufacturer's documentation for information about the parameters that you must enter to configure this endpoint.

Server Tab

The following figure displays the **Add Endpoint Context Server - Server** (SAP Afaria) tab:

Figure 622: Add Endpoint Context Server - Server (SAP Afaria) Tab

The screenshot shows a window titled "Add Endpoint Context Server" with a close button in the top right. It has two tabs: "Server" and "Actions". The "Server" tab is active and contains the following fields and options:

- Select Server Type:** A dropdown menu with "SAP Afaria" selected.
- Server Name:** A text input field.
- Server Base URL:** A text input field.
- Username:** A text input field.
- Password:** A text input field.
- Verify Password:** A text input field.
- Validate Server:** A checkbox with the label "Enable to validate the server certificate".
- Enable Server:** A checkbox with the label "Enable to fetch endpoints from the server".
- Bypass Proxy:** A checkbox with the label "Enable to bypass proxy server".

At the bottom right of the dialog are "Save" and "Cancel" buttons.



You can add more than one endpoint context server of the same type. For example, you can add more than one AirWatch endpoint context server.

The following table describes the **Add Endpoint Context Server - Server** (SAP Afaria) tab parameters:

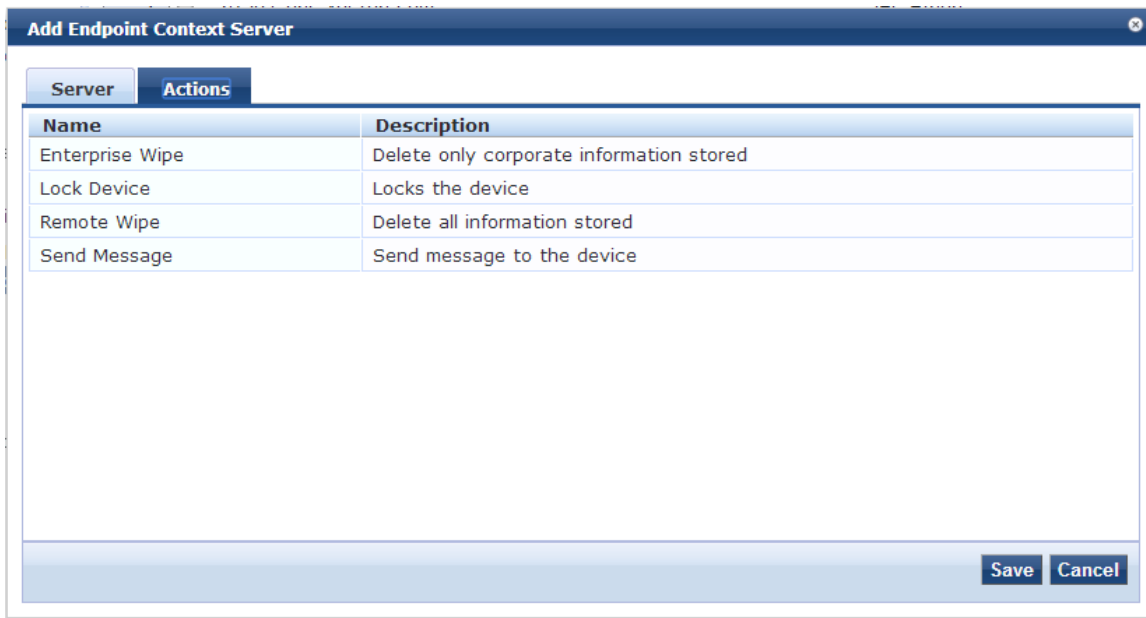
Table 334: Add Endpoint Context Server - Server (SAP Afaria) Tab Parameters

Parameter	Description
Select Server Type	Choose SAP Afaria from the drop-down list.
Server Name	Enter a valid server name. You can enter an IP address or a hostname.
Server Base URL	Enter the full URL for the server. You can append a custom port, such as for an MDM server: <code>https://yourserver.yourcompany.com:customerportnumber</code> .
Username	Enter the username.
Password	Enter and verify the password.
Verify Password	
Validate Server	Enable to validate the server certificate. Checking this option enables the Certificate tab.
Enable Server	Enable to fetch endpoints from the server.
Bypass Proxy	Enable to bypass proxy server.

Actions Tab

The following figure displays the **Add Endpoint Context Server - Actions** (SAP Afaria) tab:

Figure 623: Add Endpoint Context Server - Actions (SAP Afaria) Tab



Name	Description
Enterprise Wipe	Delete only corporate information stored
Lock Device	Locks the device
Remote Wipe	Delete all information stored
Send Message	Send message to the device

The following table describes the **Add Endpoint Context Server - Actions** (SAP Afaria) tab parameters:

Table 335: Add Endpoint Context Server - Actions (SAP Afaria) Tab Parameters

Parameter	Description
Enterprise Wipe	Delete corporate information related data.
Lock Device	Lock the associated device.
Remote Wipe	Delete all stored information.
Send Message	Send message to the device.

Adding a SOTI Endpoint Context Server

Consult the endpoint manufacturer's documentation for information about the parameters that you must enter to configure this endpoint.

The following figure displays the **SOTI Add Endpoint Context Server > Server** dialog:

Figure 624: Adding a SOTI Endpoint Context Server > Server (SOTI) Dialog



You can add more than one endpoint context server of the same type.

The following table describes the **SOTI Add Endpoint Context Server > Server** parameters:

Table 336: Adding a SOTI Endpoint Context Server > Server Parameters

Parameter	Action/Description
Select Server Type	1. Choose SOTI from the Select Server Type drop-down list.
Server Name	2. Enter a valid server name. You can enter an IP address or a hostname.
Server Base URL	3. Enter the complete URL for the SOTI server. You can append a custom port, such as for an MDM server: https://yourserver.yourcompany.com:customerportnumber
Username	4. Enter the username for the SOTI server.
Password	5. Enter the password, then verify it.
Verify Password	
Group ID	6. Enter the group ID. This parameter is optional.
Validate Server	7. Enable Validate Server to validate the server certificate. Enabling this option enables the Certificate tab.

Table 336: Adding a SOTI Endpoint Context Server > Server Parameters (Continued)

Parameter	Action/Description
Enable Server	8. Enable Enable Server to fetch endpoints from the server.
Bypass Proxy	9. Enable Bypass Proxy to bypass the proxy server.
	10. To save your changes, click Save .

Adding a XenMobile Endpoint Context Server

Consult the endpoint manufacturer's documentation for information about the parameters that you must enter to configure this endpoint. The following figure displays the **Add Endpoint Context Server - Server** (XenMobile) tab:

Figure 625: Add Endpoint Context Server - Server (XenMobile) Tab

The screenshot shows a window titled "Add Endpoint Context Server" with a "Server" tab selected. The form contains the following fields and options:

- Select Server Type:** A dropdown menu with "XenMobile" selected.
- Server Name:** A text input field.
- Server Base URL:** A text input field.
- Username:** A text input field.
- Password:** A text input field.
- Verify Password:** A text input field.
- Validate Server:** A checkbox with the label "Enable to validate the server certificate".
- Enable Server:** A checkbox with the label "Enable to fetch endpoints from the server".
- Bypass Proxy:** A checkbox with the label "Enable to bypass proxy server".

At the bottom right of the dialog are "Save" and "Cancel" buttons.



You can add more than one endpoint context server of the same type. For example, you can add more than one AirWatch endpoint context server.

The following table describes the **Add Endpoint Context Server - Server** (XenMobile) tab parameters:

Table 337: Add Endpoint Context Server - Server (XenMobile) Tab Parameters

Parameter	Description
Select Server Type	Choose XenMobile from the drop-down list.
Server Name	Enter a valid server name. You can enter an IP address or hostname.
Server Base URL	Enter the server base URL in the following format: https://{server_ip}

Table 337: Add Endpoint Context Server - Server (XenMobile) Tab Parameters (Continued)

Parameter	Description
	/api/?type=keygen&user={username}&password={password}
Username	Enter the username.
Password	Enter and verify the password.
Verify Password	
Validate Server	Enable to validate the server certificate. Checking this option enables the Certificate tab.
Enable Server	Enable to fetch endpoints from the server.
Bypass Proxy	Enable to bypass proxy server.

File Backup Servers

W-ClearPass Policy Manager provides the ability to push scheduled data securely to an external server. You can push the data using the SFTP and SCP protocols. Navigate to the **Administration > External Servers > File Backup Servers** page and click the **Add** link at the top-right corner. The **Add File Backup Server** page opens.

The following figure displays the **Add File Backup Server** page:

Figure 626: File Backup Servers - Add File Backup Server Page

Add File Backup Server

Host:

Description:

Protocol: ☒ SFTP ☐ SCP

Port:

Username:

Password:

Verify Password:

Timeout:

Remote Directory:

ClearPass Servers: If specified, files will only be backed up from the selected ClearPass servers. Otherwise, it will be backed up from all ClearPass servers in the cluster.

--Select to Add--

The following table describes the **Add File Backup Server** page parameters:

Table 338: Add File Backup Server Page Parameters

Parameter	Description
Host	Enter the name or IP address of the host.
Description	Enter the description that provides additional information about the File Backup server.
Protocol	Specify the protocol to be used to upload the generated reports to an external server. You can select from the following protocols: • SFTP (SSH File Transfer Protocol) • SCP (Session Control Protocol)
Port	Specify the port number. The default port is 22.
Username	Enter the user name and password of the host server.

Table 338: Add File Backup Server Page Parameters (Continued)

Parameter	Description
Password	Enter the user name of the host server.
Verify Password	Enter the password of the host server.
Timeout	Specify the timeout value in seconds. The default value is 30 seconds.
Remote Directory	Specify the location in this field to which the files to be copied. A folder will be automatically created in the file path that you specify based on the selected ClearPass servers in the ClearPass Servers field.
ClearPass Servers	Specify the W-ClearPass servers. If a servers are specified, files will only be backed up from the selected ClearPass servers. Otherwise, it will be backed up from all ClearPass servers in the cluster. You can select the servers from the Select to Add drop-down list.

Server Certificate

The **Server Certificate** page depends if the RADIUS Server Certificate type or the HTTPS Service Certificate type is assigned to the selected server. To configure the server certificate, navigate to **Administration > Certificates > Server Certificate**.

This section describes the following topics:

- [Server Certificate Main Page on page 621](#)
- [Server Certificate Type on page 622](#)

Server Certificate Main Page

The following figure displays the Server Certificate page:

Figure 627: Server Certificate Page

Administration » Certificates » Server Certificate

Server Certificate

Select Server: Select Type:

[Create Self-Signed Certificate](#)
[Create Certificate Signing Request](#)
[Import Server Certificate](#)
[Export Server Certificate](#)

Server Certificate:	
Subject:	L=Sunnyvale, C=US, ST=CA, O=Test Systems, OU=Engineering, CN=qa86.amigopod.arubanetworks.com
Issued by:	L=Sunnyvale, C=US, ST=CA, O=Test Systems, OU=Engineering, CN=qa86.amigopod.arubanetworks.com
Issue Date:	Dec 11, 2013 14:00:31 PST
Expiry Date:	Jun 09, 2014 15:00:31 PDT
Validity Status:	Valid
Details:	View Details

[Delete](#)

The following table describes the **Server Certificate** parameters:

Table 339: *Server Certificate Parameters*

Parameter	Description
Create Self-Signed Certificate	Opens the Create Self-Signed Certificate page where you can create and install a Self-Signed Certificate. For more information, see Creating a Self-Signed Certificate on page 627 .
Create Certificate Signing Request	Opens the Create Certificate Signing Request page where you can create and install a Certificate Signing Request. For more information, see Creating a Certificate Signing Request on page 624 .
Import Server Certificate	Opens the Import Server Certificate page where you can import a certificate that has been exported previously. For more information, see Importing a Server Certificate on page 632 .
Export Server Certificate	On clicking this link, the self-signed certificate is downloaded. For more information, see Exporting a Server Certificate on page 632 .
Select Server	Select a server in the cluster for server certificate operations.
Select Type	Select a certificate type. The options are RADIUS Server Certificate or HTTPS Server Certificate . The availability of two certificate types (internally signed and publicly signed) can provide deployment flexibility.
View Details	Click to view the certificate details.

Server Certificate Type

W-ClearPass Policy Manager provides two types of server certificates.

RADIUS Server Certificate

This page displays the parameters configured when a self-signed certificate with a RADIUS Server Certificate is created and installed. The following figure displays the RADIUS **Server Certificate** page:

Figure 628: *RADIUS Server Certificate Page*

Administration » Certificates » Server Certificate

Server Certificate

Select Server: Select Type:

[Create Self-Signed Certificate](#)
[Create Certificate Signing Request](#)
[Import Server Certificate](#)
[Export Server Certificate](#)

Server Certificate:	
Subject:	L=Sunnyvale, C=US, ST=CA, O=Test Systems, OU=Engineering, CN=qa86.amigopod.arubanetworks.com
Issued by:	L=Sunnyvale, C=US, ST=CA, O=Test Systems, OU=Engineering, CN=qa86.amigopod.arubanetworks.com
Issue Date:	Dec 11, 2013 14:00:31 PST
Expiry Date:	Jun 09, 2014 15:00:31 PDT
Validity Status:	Valid
Details:	View Details

[Delete](#)

The following table describes the RADIUS **Server Certificate** parameters:

Table 340: *RADIUS Server Certificate Parameters*

Parameter	Description
Subject	Displays Organization and Common Name.
Issued by	Displays Organization and Common Name.
Issue Date	Displays the date the self-signed certificate is installed.
Expiry Date	Displays the date (in days) when the self-signed certificate expires.
Validity Status	Displays the validity status of the self-signed certificate.
Details	Click the View Details button to view details about the certificate, such as Signature Algorithm, Subject Public Key Info, and more.

HTTPS Server Certificate

The page displays the parameters configured after a self-signed certificate with an HTTPS Server Certificate is created and installed. The page contains data about the Server Certificate, Intermediate CA Certificate and Root CA Certificate. Click the **View Details** button for each section to see details about Signature Algorithm, Public Key Info, and more. The following figure displays the HTTPS **Server Certificate** page:

Figure 629: *HTTPS Server Certificate Page*

Select Server: Select Type:

Server Certificate:	
Subject:	CN=onboard-lab.arubanetworks.com, OU=InstantSSL Pro, OU=Issued through Aruba Networks E-PKI Manager, O=Aruba Networks, STREET=1344 Crossman Ave, L=Sunnyvale, ST=CA, OID.2.5.4.17=94089, C=US
Issued by:	CN=COMODO High-Assurance Secure Server CA, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB
Issue Date:	Feb 26, 2013 16:00:00 PST
Expiry Date:	Oct 31, 2015 16:59:59 PDT
Validity Status:	Valid
Details:	View Details
Intermediate CA Certificate:	
Subject:	CN=COMODO High-Assurance Secure Server CA, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB
Issued by:	CN=AddTrust External CA Root, OU=AddTrust External TTP Network, O=AddTrust AB, C=SE
Issue Date:	Apr 15, 2010 17:00:00 PDT
Expiry Date:	May 30, 2020 03:48:38 PDT
Validity Status:	Valid
Details:	View Details
Root CA Certificate:	
Subject:	CN=AddTrust External CA Root, OU=AddTrust External TTP Network, O=AddTrust AB, C=SE
Issued by:	CN=AddTrust External CA Root, OU=AddTrust External TTP Network, O=AddTrust AB, C=SE
Issue Date:	May 30, 2000 03:48:38 PDT
Expiry Date:	May 30, 2020 03:48:38 PDT
Validity Status:	Valid
Details:	View Details

[Delete](#)

The following table describes the HTTPS **Server Certificate** parameters:

Table 341: *HTTPS Server Certificate Parameters*

Parameter	Description
Subject	Displays Organization and Common Name.
Issued by	Displays Organization and Common Name.
Issue Date	Displays the date the self-signed certificate is installed.

Table 341: *HTTPS Server Certificate Parameters (Continued)*

Parameter	Description
Expiry Date	Displays the date (in days) when the self-signed certificate expires.
Validity Status	Displays the validity status of the self-signed certificate.
Details	Click the View Details button to view details about the certificate, such as Signature Algorithm, Subject Public Key Info, and more.

Creating a Certificate Signing Request

After you select a server and a certificate type, you can create a certificate signing request. This task creates a self-signed certificate to be signed by a CA. To create a certificate signing request:

1. Navigate to **Administration > Certificates > Server Certificate**.
2. Select a server, for example, localhost.
3. Click the **Create Certificate Signing Request** link. Configure the parameters based on [Table 342](#).
4. Click **Submit**.

The following figure displays the **Create Certificate Signing Request** pop-up:

Figure 630: *Create Certificate Signing Request Pop-up*

Create Certificate Signing Request

Common Name (CN):	Garuda-197
Organization (O):	Acme Systems
Organizational Unit (OU):	Engineering
Location (L):	Sunnyvale
State (ST):	CA
Country (C):	US
Subject Alternate Name (SAN):	email:admin-sunnyvale@acme.com
Private Key Password:	
Verify Private Key Password:	
Private Key Type:	2048-bit RSA
Digest Algorithm:	SHA-512

MD5
SHA-1
SHA-224
SHA-256
SHA-384
SHA-512

Submit **Cancel**

The following figure displays the **Create Certificate Signing Request** page in the FIPS mode pop-up:

Figure 631: *Create Certificate Signing Request - FIPS Mode Pop-up*

The following table describes the **Create Certificate Signing Request** parameters:

Table 342: *Create Certificate Signing Request Parameters*

Parameter	Description
Common Name (CN)	Enter the name associated with this entity. This can be a host name, IP address, or other name. The default is the fully-qualified domain name (FQDN). This field is mandatory.
Organization (O)	Enter the name of the organization. This field is optional.
Organizational Unit (OU)	Enter the name of the department, division, section, or other meaningful name. This field is optional.
Location (L)	Enter the name of the location, state, country, and/or other meaningful name. These fields are optional.
State (ST)	
Country (C)	
Subject Alternate	Enter the alternative names for the specified Common Name. NOTE: Enter the SAN in the following formats:

Table 342: *Create Certificate Signing Request Parameters (Continued)*

Parameter	Description
Name (SAN)	● email: <i>email_address</i> ● URI: <i>uri</i> ● IP: <i>ip_address</i> ● dns: <i>dns_name</i> ● rid: <i>id</i> This field is optional.
Private Key Password	Enter and re-enter the Private Key password.
Verify Private Key Password	
Private Key Type	Select the length for the generated private key types from the following options: ● 1024-bit RSA ● 2048-bit RSA ● 4096-bit RSA ● X9.62/SECG curve over a 256 bit prime field ● NIST/SECG curve over a 384 bit prime field The default private key type is 2048-bit RSA .
Digest Algorithm	Select the message digest algorithm from the following options: ● MD5 ● SHA-1 ● SHA-224 ● SHA-256 ● SHA-384 ● SHA-512 NOTE: The MD5 algorithm is not available in the FIPS mode.

After you create a **Certificate Signing Request** form and click **Submit**, the generated certificate signing request is displayed. Copy the certificate and paste it into the Web form as part of the enrollment process. You can click **Download CSR and Private Key Files** to save the Certificate Signing Request file and the private key password file. The following figure displays the **Create Certificate Signing Request** pop-up:

Create Certificate Signing Request

Contents of the Certificate Signing Request

```
-----BEGIN CERTIFICATE REQUEST-----
MIIDIDCCAggCAQAwYUUKDAMBgNVBAMTH3FhODYuYW1pZ2Z9wb2QuYXJ1YmFuZXR3
b3Jrcy5jb20uZDASBgNVBAstC0VuZ2luZWVyaW5nMRUwEwYDVQQKEWxBY211IFN5
c3RlbXMxCzAJBgNVBAGTAkNBMCswCQYDVQQGEwJVUzESMBAGA1UEBxMJU3Vubnl2
YWxlMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEArTFsqfR1WTksjLK0
/wcjDoPzVYqWhkmMPRtdi/STOBsJ7tcCjvfObrPDclm245tgIOBiqwpJf+aysUlG
OruDez2tkzlnj2JABaQQG105pwBOMGMZXY9JFpn1M1RW1QBcaUfTBnXk97WNPLAT
V4nnaxkwTaoyW+FHsuZIJMITVOj9toa7EbhPONYZzPbi9fSofFabUerjVpE259gd
6iuQNuY8vUu6jghPJYNZp0QWTcaWu7FRW6sd4z2fUukE/8UIgIQwciTqCr/4V/t4
u87LNh56X2sY7/fYCKAs/E74Z/+1wWxW3RG/R6GRmZ9RB8EtZYDBP2CDE8C08imk
zFhfxwIDAQABoFUFUwYJKoZiHvcNAQKOMUYwRDAjBgNVHREEHDAagRhhZG1pbilz
dW5ueXZhbGVAYWNtZS5jb20wHQYDVRO1BBYwFAYIKwYBBQUHAWEGCCSGAQUFBwMD
MA0GCSqGSIb3DQEBBQUAA4IBAQA7mHwUNEaDYHfFjWsmDdi7gB/Qqh3jQqcfN+UR
ErVhYaRhesuPjyttu3ISVo2vMc7IdQ3Yc07MMOTJ9DP9DOQzpWyuEc8FS/udcUPQ
kdpUy+Xmj9LTgnrhHpD2CQG4kZqT2frfZf4q/Y8foQ5WZtF8+shq9c68U94+QbF
rBiwGRH2jDWA8h35iGTzLotZ8ofauyKkPlaUzaRQ/OIULN0vV4yTEdN5VkjOIyho
gxqDz3YQO5EkN3fpJU4gZ63rj/CQEe7tt+cnJVieKgiutkpmXnWjQYJ9zbyMaspvC
PdZapONCyRjKVCqJyqtJ/lezNbLUbnDuNDBS5wvW54BKJoFX
-----END CERTIFICATE REQUEST-----
```

Copy and paste this into the web form in the enrollment process

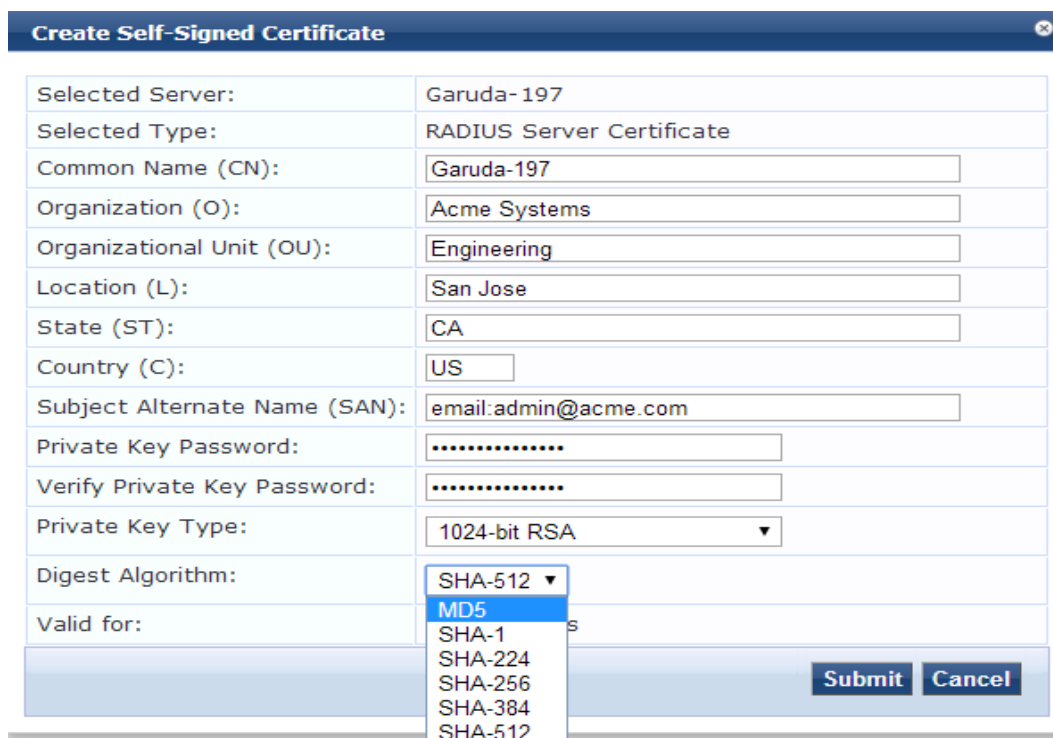
[Download CSR and Private Key Files](#) [Close](#)

After you select a server and a certificate type, you can create and install a self-signed certificate. To create a self-signed certificate:

1. Navigate to **Administration > Certificates > Server Certificate**.
2. Select a server, for example, localhost.
3. Click the **Create Self-Signed Certificate** link. Configure the parameters based on [Table 343](#).
4. Click **Submit**.
5. To install a self-signed certificate, see [Installing a Self-Signed Certificate on page 630](#).

The following figure displays the **Create Self-Signed Certificate** pop-up:

Figure 633: *Create Self-Signed Certificate Pop-up*



The image shows a 'Create Self-Signed Certificate' dialog box. It contains a table of fields for certificate creation. The 'Digest Algorithm' dropdown menu is open, showing options: SHA-512, MD5, SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512. The 'Submit' and 'Cancel' buttons are at the bottom right.

Create Self-Signed Certificate	
Selected Server:	Garuda-197
Selected Type:	RADIUS Server Certificate
Common Name (CN):	Garuda-197
Organization (O):	Acme Systems
Organizational Unit (OU):	Engineering
Location (L):	San Jose
State (ST):	CA
Country (C):	US
Subject Alternate Name (SAN):	email:admin@acme.com
Private Key Password:	
Verify Private Key Password:	
Private Key Type:	1024-bit RSA
Digest Algorithm:	SHA-512 ▼
Valid for:	
Submit Cancel	

The following figure displays the **Create Self-Signed Certificate** page in the FIPS mode pop-up:

Figure 634: *Create Self-Signed Certificate Page - FIPS Mode Pop-up*

Selected Server:	nbalu-79
Selected Type:	RADIUS Server Certificate
Common Name (CN):	nbalu-79
Organization (O):	Acme Systems
Organizational Unit (OU):	Engineering
Location (L):	San Jose
State (ST):	CA
Country (C):	US
Subject Alternate Name (SAN):	email:admin@acme.com
Private Key Password:	
Verify Private Key Password:	
Private Key Type:	1024-bit RSA
Digest Algorithm:	SHA-512
Valid for:	

Submit Cancel

The following table describes the **Create Self-Signed Certificate** parameters:

Table 343: *Create Self-Signed Certificate Parameters*

Parameter	Description
Selected Server	Displays the name of the selected server on the Server Certificate page.
Selected Type	Displays the selected certificate type for the server on the Server Certificate page.
Common Name (CN)	Enter the name associated with this entity. This can be a host name, IP address, or other meaningful name. This field is mandatory.
Organization (O)	Enter the name of the organization. This field is optional.
Organizational Unit (OU)	Enter the name of the department, division, section, or other meaningful name. This field is optional.

Table 343: Create Self-Signed Certificate Parameters (Continued)

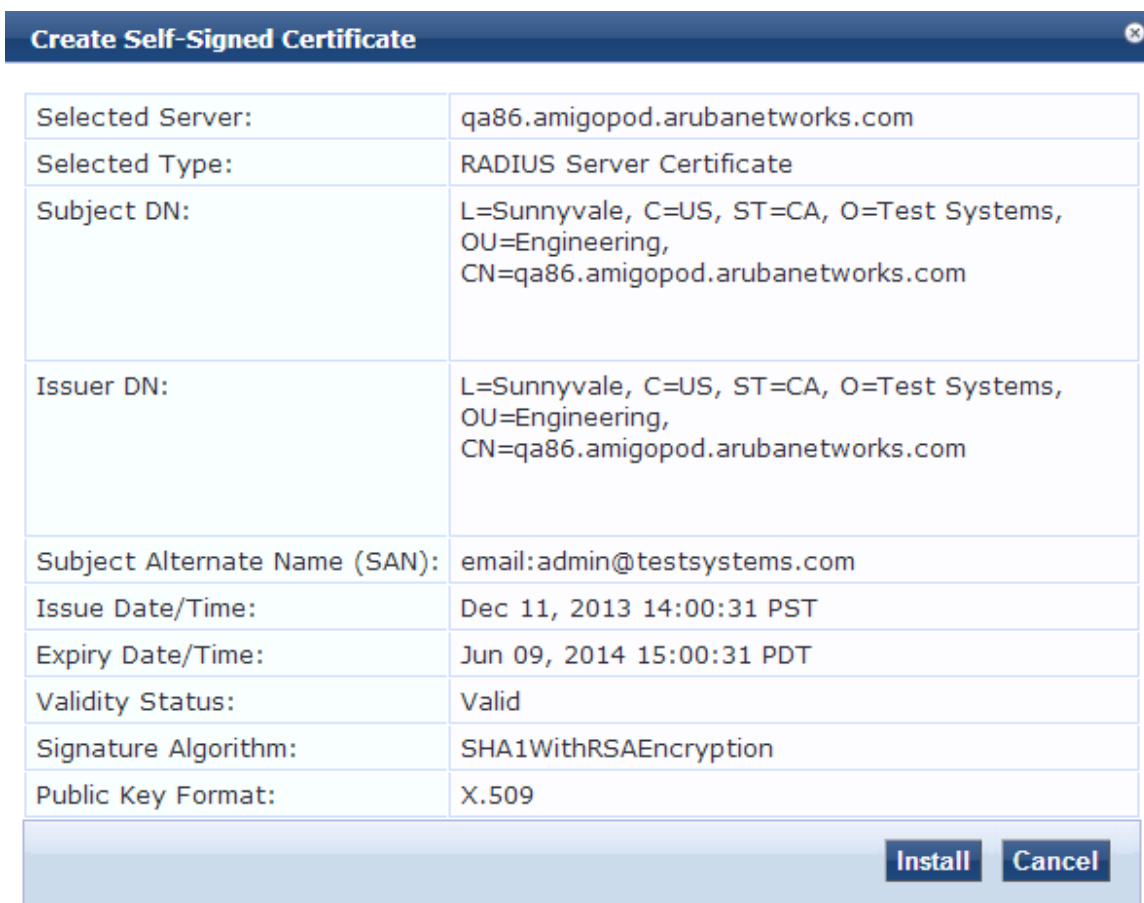
Parameter	Description
Location (L)	Enter the name of the location, state, country, and/or other meaningful name. These fields are optional.
State (ST)	
Country (C)	
Subject Alternate Name (SAN)	Enter the alternative names for the specified Common Name. NOTE: Enter the SAN in the following formats: ● email: <i>email_address</i> ● URI: <i>uri</i> ● IP: <i>ip_address</i> ● dns: <i>dns_name</i> ● rid: <i>id</i> This field is optional.
Private Key Password	Enter and re-enter the Private Key password.
Verify Private Key Password	
Private Key Type	Select the length for the generated private key types from the following options: ● 1024-bit RSA ● 2048-bit RSA ● 4096-bit RSA ● X9.62/SECG curve over a 256 bit prime field ● NIST/SECG curve over a 384 bit prime field The default private key type is 2048-bit RSA .
Digest Algorithm	Select the message digest algorithm from the following options: ● MD5 ● SHA-1 ● SHA-224 ● SHA-256 ● SHA-384 ● SHA-512 NOTE: The MD5 algorithm is not available in the FIPS mode.
Valid for	Enter the duration in number of days.

Installing a Self-Signed Certificate

Once you click **Submit**, you are prompted to install the self-signed certificate. This page displays a summary of the values selected in the **Create Self-Signed Certificate** page. Click **Install** to install the self-signed certificate.

The following figure displays the **Create Self-Signed Certificate** pop-up.

Figure 635: *Create Self-Signed Certificate Pop-up*



Selected Server:	qa86.amigopod.arubanetworks.com
Selected Type:	RADIUS Server Certificate
Subject DN:	L=Sunnyvale, C=US, ST=CA, O=Test Systems, OU=Engineering, CN=qa86.amigopod.arubanetworks.com
Issuer DN:	L=Sunnyvale, C=US, ST=CA, O=Test Systems, OU=Engineering, CN=qa86.amigopod.arubanetworks.com
Subject Alternate Name (SAN):	email:admin@testsystems.com
Issue Date/Time:	Dec 11, 2013 14:00:31 PST
Expiry Date/Time:	Jun 09, 2014 15:00:31 PDT
Validity Status:	Valid
Signature Algorithm:	SHA1WithRSAEncryption
Public Key Format:	X.509

The following table describes the **Create Self-Signed Certificate** parameters configured:

Table 344: *Self-Signed Certificate Parameters*

Parameter	Description
Selected Server	Displays the name of the server selected on the Server Certificate page.
Selected Type	Displays the selected certificate type for the server.
Subject DN	Displays information about the organization, common name, and location of the Subject DN.
Issuer DN	Displays information about the organization, common name, and location of the Subject DN.
Subject Alternate Name (SAN)	Displays the SAN defined during certificate creation.
Issue Date/Time	Displays the certificate issue date and time.
Expire Date/Time	Displays the certificate expiration date and time.

Table 344: *Self-Signed Certificate Parameters (Continued)*

Parameter	Description
Validity Status	Displays the validity status of the certificate.
Signature Algorithm	Displays the Digest Algorithm and Private Key Type selected during certificate configuration.
Public Key Format	Displays the public key format in use for the self-signed server certificate.

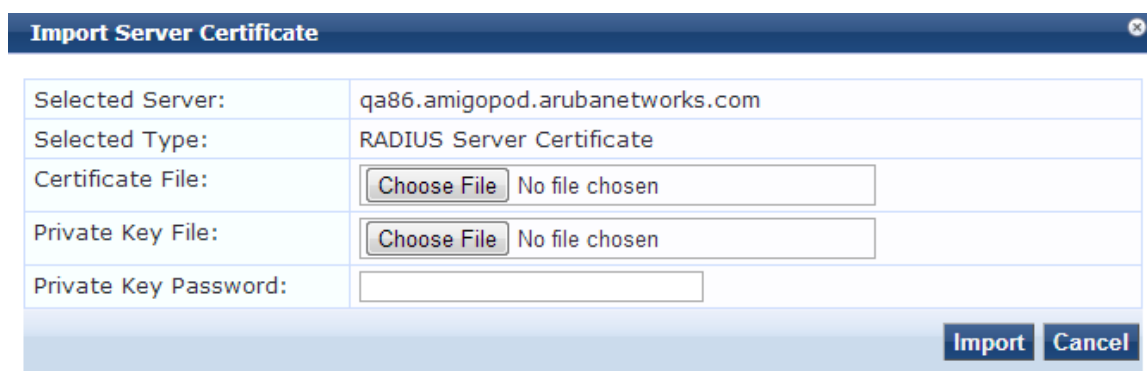
Exporting a Server Certificate

Navigate to **Administration > Certificates > Server Certificates**, and click the **Export Server Certificate** link. The default location for an exported certificate is **C:/<user>/Downloads/<HTTPSServerCertificate.zip> or <RADIUSServerCertificate.zip>**. The zip file has the server certificate (.crt file) and the private key (.pvk file).

Importing a Server Certificate

Navigate to **Administration > Certificates > Server Certificates**, and select the **Import Server Certificate** link. The following figure displays the **Import Server Certificate** pop-up:

Figure 636: *Import Server Certificate Pop-up*



For security reasons, certificate signed using SHA1RSA is not recommended. It is recommended to import certificates signed with stronger keys such as RSA with length more than 1024 bits.

The following table describes the **Import Server Certificate** parameters:

Table 345: *Import Server Certificate Parameters*

Parameter	Description
Selected Server	Displays the name of the selected server on the Server Certificate page.
Selected Type	Displays the selected certificate type for the server on the Server Certificate page.
Certificate File	Browse to the certificate file to be imported.

Table 345: Import Server Certificate Parameters (Continued)

Parameter	Description
Private Key File	Browse to the private key file to be imported.
Private Key Password	Specify the private key password that was entered when the server certificate was configured.

Certificate Trust List

The Certificate Trust List page displays a list of trusted Certificate Authorities (CA). On this page, you can add, view, or delete a certificate.

This section describes the following topics:

- [Certificate Trust List Main Page on page 633](#)
- [Adding a Certificate on page 634](#)
- [Viewing a Certificate Detail on page 634](#)
- [Deleting a Certificate on page 634](#)



You cannot import the certificates that are created with the **MD5** digest algorithm to the **Certificate Trust List** in the **FIPS** mode.

Certificate Trust List Main Page

To display a list of trusted Certificate Authorities (CA), navigate to **Administration > Certificates > Trust List**.

The following figure displays the **Certificate Trust List** page:

Figure 637: Certificate Trust List Main Page

Administration » Certificates » Trust List

Certificate Trust List ➕ Add

Filter: contains Go Clear Filter Show 10 records

#	Subject	Validity	Enabled
1.	☐ CN=AddTrust External CA Root,OU=AddTrust External TTP Network,O=AddTrust AB,C=SE	valid	Disabled
2.	☐ CN=Alcatel Contact Center Solutions,OU=PKI Authority,O=Alcatel,C=FR	valid	Enabled
3.	☐ CN=Alcatel Enterprise Solutions,OU=PKI Authority,O=Alcatel,C=FR	valid	Disabled
4.	☐ CN=Alcatel IP Touch,OU=PKI Authority,O=Alcatel,C=FR	valid	Enabled
5.	☐ CN=Certum CA,O=Unizeto Sp. z o.o.,C=PL	valid	Disabled
6.	☐ CN=COMODO High Assurance Secure Server CA,O=COMODO CA Limited,L=Salford,ST=Greater Manchester,C=GB	valid	Disabled
7.	☐ CN=DigiCert Global Root CA,OU=www.digicert.com,O=DigiCert Inc,C=US	valid	Disabled
8.	☐ CN=DigiCert High Assurance EV Root CA,OU=www.digicert.com,O=DigiCert Inc,C=US	valid	Disabled
9.	☐ CN=DOD CA-25,OU=PKI,OU=DoD,O=U.S. Government,C=US	valid	Disabled
10.	☐ CN=DOD CA-26,OU=PKI,OU=DoD,O=U.S. Government,C=US	valid	Disabled

Showing 1-10 of 58 ▶ Delete

The **Certificate Trust List (Administration > Certificates > Trust List)** page can include the following certificates:

- DoD (Department of Defense) certificates - These are disabled by default. To enable this certificate, select a DoD certificate and click **Enable** in the **View Certificate Details** pop-up. A DoD certificate allows a browser to trust Web sites whose secure communications are authenticated by a DoD agency.
- Alcatel root certificate - These are disabled by default. To enable this certificate, select a DoD certificate and click **Enable** in the **View Certificate Details** pop-up. An Alcatel root certificate allows Alcatel Lucent IP phones to authenticate using EAP-TLS.

The following table describes the **Certificate Trust List** parameters:

Table 346: *Certificate Trust List Parameters*

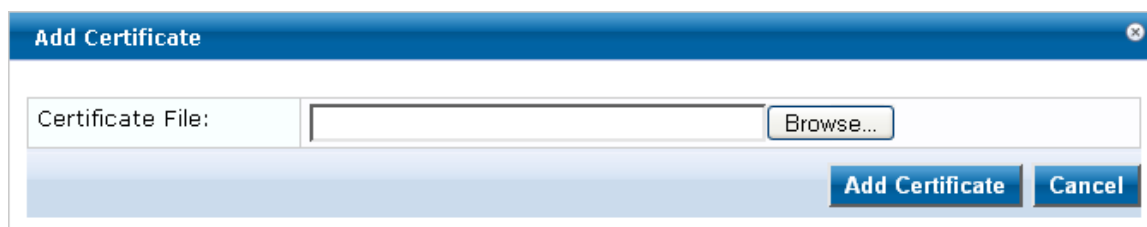
Parameter	Description
Subject	Displays the Distinguished Name (DN) of the subject field in the certificate.
Validity	Indicates whether the CA certificate is valid or expired.
Enabled	Indicates whether the CA certificate is enabled or disabled.

Adding a Certificate

1. Navigate to **Administration > Certificates > Trust List**.
2. Click the **Add** link on the top right section of the page.
3. On the **Add Certificate** pop-up, click **Choose File** to browse the certificate file.
4. Click **Add Certificate**.

The following figure displays the **Add Certificate** pop-up:

Figure 638: *Add Certificate Pop-up*



The following table describes the **Add Certificate** parameters:

Table 347: *Add Certificate Parameters*

Parameter	Description
Certificate File	Click Choose File to browse the certificate file.

Viewing a Certificate Detail

To view the details of a certificate, click any one of the entries from the certificate trust list. From the **View Certificate Details** pop-up, clicking the **Enable** button enables the CA certificate. When you enable a CA certificate, W-Policy Manager considers the entity whose certificate is signed by this CA to be trusted.

Deleting a Certificate

To delete a certificate:

1. Navigate to **Administration > Certificates > Trust List**.
2. Select the check box to the left of the certificate.
3. Click **Delete**.

Certificate Revocation Lists

This section provides the following information:

- [About Certificate Revocation Lists](#)
- [Adding a Certificate Revocation List](#)
- [Deleting a Certificate Revocation List](#)

About Certificate Revocation Lists

A Certificate Revocation List (CRL) is a list of digital certificates that have been revoked by the issuing Certificate Authority (CA) before their scheduled expiration date and should no longer be trusted.

CRLs are a type of blacklist and are used by various endpoints, including Web browsers, to verify whether a certificate is valid and trustworthy.

Digital certificates are used in the encryption process to secure communications, most often by using the TLS/SSL protocol. The certificate, which is signed by the issuing Certificate Authority, also provides proof of the identity of the certificate owner.

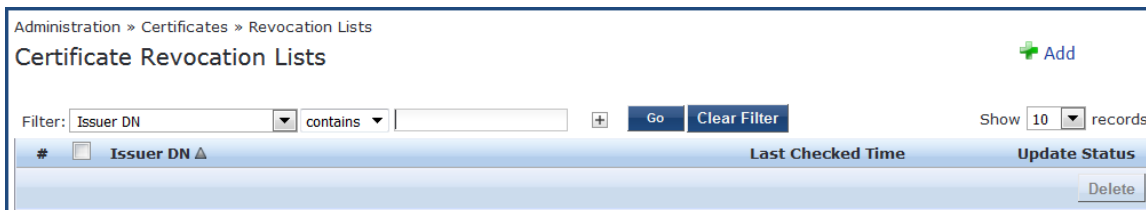
Adding a Certificate Revocation List

To add a certificate revocation list:

1. Navigate to **Administration > Certificates > Revocation Lists**.

The **Certificate Revocation Lists** page opens:

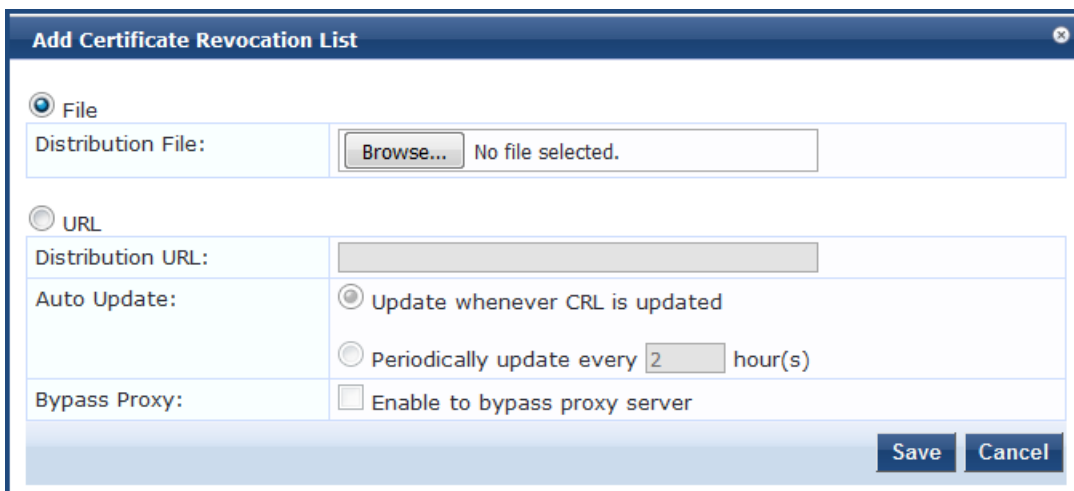
Figure 639: Certificate Revocation Lists Page



2. Click the **Add** link on the top right section of the page.

The Add Certificate Revocation List dialog opens:

Figure 640: Add Certificate Revocation List Dialog



3. Configure the **Add Certificate Revocation List** parameters as described in [Table 348](#), then click **Save**.

Table 348: Add Certificate Revocation List Parameters

Parameter	Action/Description
File	Enable the File button to use a distribution file as the CRL distribution point. File is enabled by default.
Distribution File	To select the distribution file to fetch the certificate revocation list, click Browse and select the CRL distribution file.
URL	Enable the URL button to use a URL as the CRL distribution point. Selecting URL enables the Distribution URL option.
Distribution URL	Specify the distribution URL to fetch the certificate revocation list.
Auto Update	• To update the CRL at intervals specified in the list, select Update whenever CRL is updated. • To check periodically and at the specified frequency (in hours), select Periodically update every _____ hour(s).
Bypass Proxy	To bypass the proxy server, click the Enable to bypass proxy server option.

Deleting a Certificate Revocation List

To delete a certificate revocation list:

1. Navigate to **Administration > Certificates > Revocation Lists**.
2. Select the check box to the left of the certificate revocation list.
3. Click **Delete**.

Using ClearPass Dictionaries

This section provides the following information:

- [RADIUS Dictionary on page 637](#)
- [TACACS+ Services Dictionary on page 638](#)
- [Fingerprints Dictionary on page 640](#)
- [Dictionary Attributes on page 641](#)
- [Applications Dictionaries on page 645](#)
- [Configuring Endpoint Context Server Actions on page 563](#)

RADIUS Dictionary

This page includes the list of available vendor dictionaries. To configure RADIUS dictionaries, navigate to **Administration > Dictionaries > RADIUS**.

The following figure displays the **RADIUS Dictionaries** page:

Figure 641: *RADIUS Dictionaries*

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	true
2.	3GPP	10415	3GPP	false
3.	Acc	5	Acc	false
4.	Acme	9148	Acme	true
5.	ADSL-Forum	3561	ADSL-Forum	true
6.	Aerohive	26928	Aerohive	false
7.	Airespace	14179	Airespace	false
8.	Alcatel	3041	Alcatel	true
9.	Alcatel-Lucent-Service-Router	6527	Alcatel-Lucent-Service-Router	true
10.	Alteon	1872	Alteon	false

Showing 1-10 of 111 ▶▶

Click on a row view the dictionary attributes, to enable or disable the dictionary, and to export the dictionary. For example, click on vendor IETF to see all IETF attributes and their data type. The following figure displays the RADIUS IETF dictionary attributes pop-up:

Figure 642: *RADIUS Attributes Pop-up*

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	

The following table describes the **RADIUS Attributes** parameters:

Table 349: *RADIUS Dictionary Attributes Parameters*

Parameter	Description
Export	Click to save the dictionary file in XML format. You can make modifications to the dictionary and import the file back into W-Policy Manager.
Enable/Disable	Enable or disable this dictionary. Enabling a dictionary makes it appear in the W-Policy Manager rules editors (Service rules, Role mapping rules, etc.).

Import RADIUS Dictionary

You can add additional dictionaries using the Import tool. To add a new vendor dictionary, navigate to **Administration > Dictionaries > RADIUS**, and click the **Import** link. 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**.

The following figure displays the **Import from file** pop-up:

Figure 643: *Import RADIUS Dictionary Pop-up*

The following table describes the **Import from file** parameters:

Table 350: *Import from file Parameters*

Parameter	Description
Select File	Browse to select the file that you want to import.
Enter secret for the file (if any)	If the file that you want to import is password protected, enter the secret here.

TACACS+ Services Dictionary

To view the contents of the TACACS+ service dictionary, navigate to **Administration > Dictionaries > TACACS+ Services** and sort by Name or Display Name. To add a new TACACS+ service dictionary, click the

Import link. 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 W-Policy Manager.

The following figure displays the **TACACS+ Services Dictionaries** page:

Figure 644: TACACS+ Services Dictionaries Page

Administration » Dictionaries » TACACS+ Services

TACACS+ Services Dictionaries

[Import](#)
[Export All](#)

Filter: Name contains [] [Go] [Clear Filter] Show 10 records

#	Name ▲	Display Name
1.	☐ AMP:https	AMP:https
2.	☐ arap	ARAP
3.	☐ Aruba:common	Aruba:Common
4.	☐ ciscowlc:common	CiscoWLC:Common
5.	☐ cpass:http	cpass:HTTP
6.	☐ junos-exec	junos-exec
7.	☐ NCS:HTTP	NCS:HTTP
8.	☐ pixshell	PIX Shell
9.	☐ ppp:ip	PPP:IP
10.	☐ ppp:ipx	PPP:IPX

Showing 1-10 of 13 [▶] [Export] [Delete]

The following table describes the **TACACS+ Services Dictionaries** parameters:

Table 351: TACACS+ Services Dictionaries Parameters

Parameter	Description
Import	Click to open the Import Dictionary pop up. Import the dictionary (XML file).
Export All	Export all TACACS+ services into one XML file containing multiple dictionaries.

To export a specific service dictionary, select a service and click **Export**. To see all the attributes and their data types, click a service row. For example, click shell service to see all shell service attributes and their data type.

The following figure displays the **TACACS+ Service Dictionary Attributes** pop-up:

Figure 645: TACACS+ Service Dictionary Attributes Pop-up

TACACS+ Service Dictionary Attributes				
Display Name:		Shell		
#	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	-
				Close

Fingerprints Dictionary

The **Device Fingerprints** page shows a listing of all the device fingerprints recognized by the Profile module. These fingerprints are updated from the Dell W-ClearPass Update Portal (see [Updating Policy Manager Software on page 646](#) for more information). To view the contents of the fingerprints dictionary, navigate to **Administration > Dictionaries > Fingerprints**. The following figure displays the **Device Fingerprints** page.

Figure 646: Device Fingerprints Page

Administration > Dictionaries > Fingerprints

Device Fingerprints

Filter: Show

#	Category ▲	Family	Name
1.	Access Points	Symbol	Symbol AP
2.	Access Points	Motorola	Motorola AP
3.	Access Points	Cisco	Cisco AP
4.	Access Points	Trendnet	Trendnet AP
5.	Access Points	Enterasys	Enterasys HiPath AP
6.	Access Points	Trapeze	Trapeze AP
7.	Access Points	AeroHive	AeroHive AP
8.	Access Points	Ruckus	Ruckus Wireless
9.	Access Points	Aruba	Aruba RAP
10.	Access Points	Aruba	Aruba AP

Showing 1-10 of 319

You can click on a line in the Device Fingerprints list to drill down and view additional details about the category. The following figure displays the **Device Fingerprint Dictionary Attributes** pop-up.

Figure 647: *Device Fingerprint Dictionary Attributes Pop-up*

Device Fingerprint Dictionary Attributes		
Category:	Computer	
Family:	Linux	
Name:	Fedora	
#	Field	Value
1	DHCP Option55	1,28,2,3,15,6,12,40,41,42 28,2,3,15,6,12,40,41,42 1,28,2,3,15,6,12,40,41,42,26,119 1,28,2,3,15,6,12,40,41,42,26 1,28,2,121,15,6,12,40,41,42,26,119,3,121,249,252,42 1,28,2,121,15,6,12,40,41,42,26,119,3 1,28,2,3,15,6,12,40,41,42,26,119,121,249,252,42
Close		

Dictionary Attributes

This section contains the following information:

- [Introduction](#)
- [Adding a Dictionary Attribute](#)
- [Modifying Dictionary Attributes](#)
- [Importing Dictionary Attributes](#)
- [Exporting All Dictionary Attributes](#)
- [Exporting Selected Dictionary Attributes](#)

Introduction

The **Attributes** dictionary page allows you to specify unique sets of criteria for local users, guest users, endpoints, and devices. This information can then be used with role-based device policies for enabling appropriate network access.

To view the contents of the attributes dictionary, navigate to **Administration > Dictionaries > Attributes**.

The dictionary **Attributes** page appears:

Figure 648: Dictionary Attributes Page

Administration » Dictionaries » Attributes

Attributes

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

Filter: Name contains [] + Go Clear Filter

Show 10 records

#	Name ▲	Entity	Data Type	Is Mandatory	Allow Multiple
1.	☐ AD Membership	Endpoint	String	No	Yes
2.	☐ [airgroup_enable]	GuestUser	String	No	No
3.	☐ [airgroup_shared]	GuestUser	String	No	No
4.	☐ [airgroup_shared_group]	GuestUser	String	No	No
5.	☐ [airgroup_shared_location]	GuestUser	String	No	No
6.	☐ [airgroup_shared_role]	GuestUser	String	No	No
7.	☐ [airgroup_shared_time]	GuestUser	String	No	No
8.	☐ [airgroup_shared_user]	GuestUser	String	No	No
9.	☐ [Blacklisted App]	Endpoint	Boolean	No	No
10.	☐ [Calling-Station-ID]	Endpoint	MACAddress	No	No

Showing 1-10 of 69 ▶▶▶

Export Delete

Table 352 describes the dictionary **Attributes** parameters:

Table 352: Dictionary Attributes Parameters

Parameter	Description
Filter	Use the Filter drop-down list to create a search based on the available Name, Entity, Data Type, Is Mandatory, or Allow Multiple settings.
Name	The name of the attribute.
Entity	Indicates whether the attribute applies to a Local User, Guest User, Device, or Endpoint.
Data Type	Indicates whether the data type is string, integer, boolean, list, text, date, MAC address, or IPv4 address.
Is Mandatory	Indicates whether the attribute is required for a specific entity.
Allow Multiple	Indicates whether multiple attributes are allowed for an entity.

Adding a Dictionary Attribute

To add a dictionary attribute:

1. From the menu on the upper right of the page, click **Add**.
The **Add Attribute** dialog appears.

Figure 649: *Add Attribute Dialog*

The 'Add Attribute' dialog box contains the following fields and values:

Entity	GuestUser
Name	[vendor]
Data Type	String
Is Mandatory	☒ Yes ☐ No
Allow Multiple	☐ Yes ☒ No
Default Value (optional)	conferenceroom (Enter String without special characters e.g., firstfloor)

Buttons: Add, Cancel

2. Enter the information in the fields described in the following table.

The following table describes the **Add Attribute** parameters:

Table 353: *Attribute Setting Parameters*

Parameter	Description
Entity	Specify whether the attribute applies to a Device, Endpoint, Guest User, Local User, or Onboard.
Name	Enter a unique ID for this dictionary attribute.
Data Type	From the drop-down, specify the data type.
Is Mandatory	Specify whether the attribute is required for a specific entity.
Allow Multiple	Specify whether multiple attributes are allowed for an entity. NOTE: Multiple attributes are not permitted if Is Mandatory is specified as Yes .
Default Value (optional)	Specify whether the default value is True or False. This field is optional.

3. When you are done, click **Add**.

Modifying Dictionary Attributes

To modify dictionary attributes in a service dictionary:

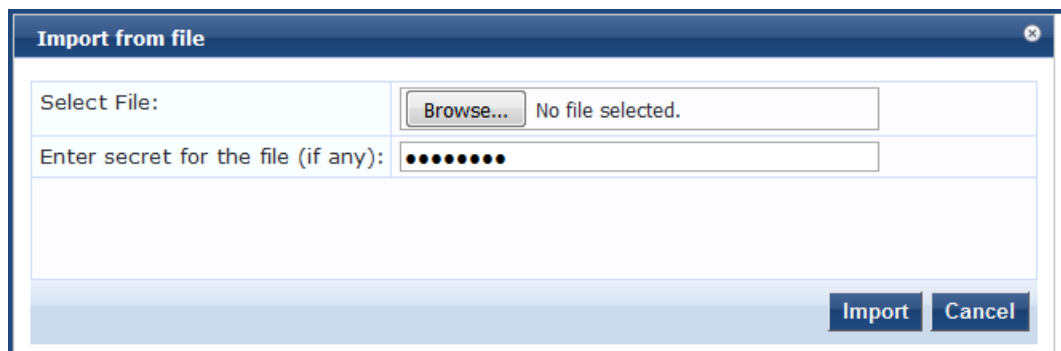
1. Select the dictionary attribute.
2. Make any necessary changes, then click **Save**.

Importing Dictionary Attributes

To import attributes:

1. From the menu at the top right section of the page, click **Import**.
The Import from File dialog appears.

Figure 650: *Importing Dictionary Attributes*

A dialog box titled "Import from file" with a close button (X) in the top right corner. It contains two input fields: "Select File:" with a "Browse..." button and the text "No file selected.", and "Enter secret for the file (if any):" with a password field showing eight dots. At the bottom right are "Import" and "Cancel" buttons.

2. Enter the Import from File parameters as described in [Table 354](#).

Table 354: *Import From File Parameters*

Parameter	Description
Select File	Browse to select the file that you want to import.
Enter secret for the file (if any)	If the file that you want to import is password protected, enter the secret here.

3. When finished, click **Import**.



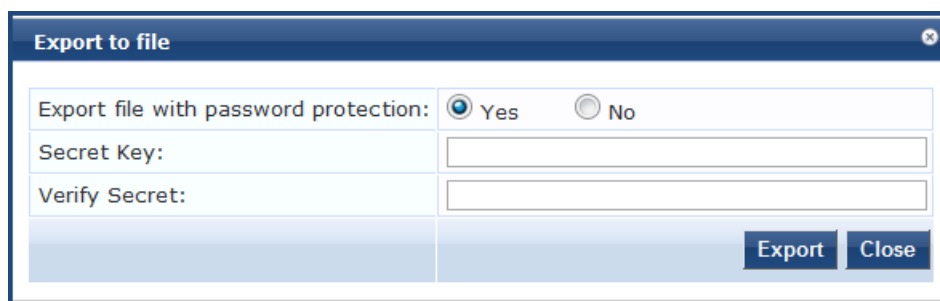
The imported file is in XML format. To view a sample of this XML format, export a dictionary file and open it in an XML viewer.

Exporting All Dictionary Attributes

To export all the dictionary attributes at once:

1. From the menu on the upper right of the pager, select **Export All**.
The **Export to File** dialog appears.

Figure 651: *Exporting Dictionary Attributes*

A dialog box titled "Export to file" with a close button (X) in the top right corner. It contains three input fields: "Export file with password protection:" with radio buttons for "Yes" (selected) and "No", "Secret Key:" with a text field, and "Verify Secret:" with a text field. At the bottom right are "Export" and "Close" buttons.

2. Specify the **Export to File** parameters as described in [Table 355](#).

Table 355: *Export to File Parameters*

Parameter	Description
Export file with password protection	The Yes option is enabled by default. If you wish to disable password protection when exporting a file, select No .
Secret Key	If the file that you want to import is password protected, enter the secret here. Then verify the secret key.

- When finished, click **Export**.
The **TagDictionary.xml** file is created.
- Download the file.

Exporting Selected Dictionary Attributes

To export selected dictionary attributes:

- On the **Attributes** dictionary page, select one or more attribute entries.
The **Export** and **Delete** buttons on the lower right are now enabled.
- Click **Export**.
The **Export to File** dialog appears.
- Specify the Export to File parameters as described in [Table 355](#).
- When finished, click **Export**.
The **TagDictionary.xml** file is created.
- Download the file.

Applications Dictionaries

Application dictionaries define the attributes of the Onboard W-Policy Manager application and the type of each attribute.

When W-Policy Manager is used as the Policy Definition Point (PDP), it uses the information in these dictionaries to validate the attributes and data types sent in a WEB-AUTH request.

Viewing an Application Dictionary

To view the contents of the application dictionary:

- Navigate to **Administration > Dictionaries > Applications**.
The **Applications Dictionaries** page appears.

Figure 652: *Applications Dictionaries Page*

Administration » Dictionaries » Applications

Applications Dictionaries

 [Import](#)
 [Export All](#)

Filter: contains

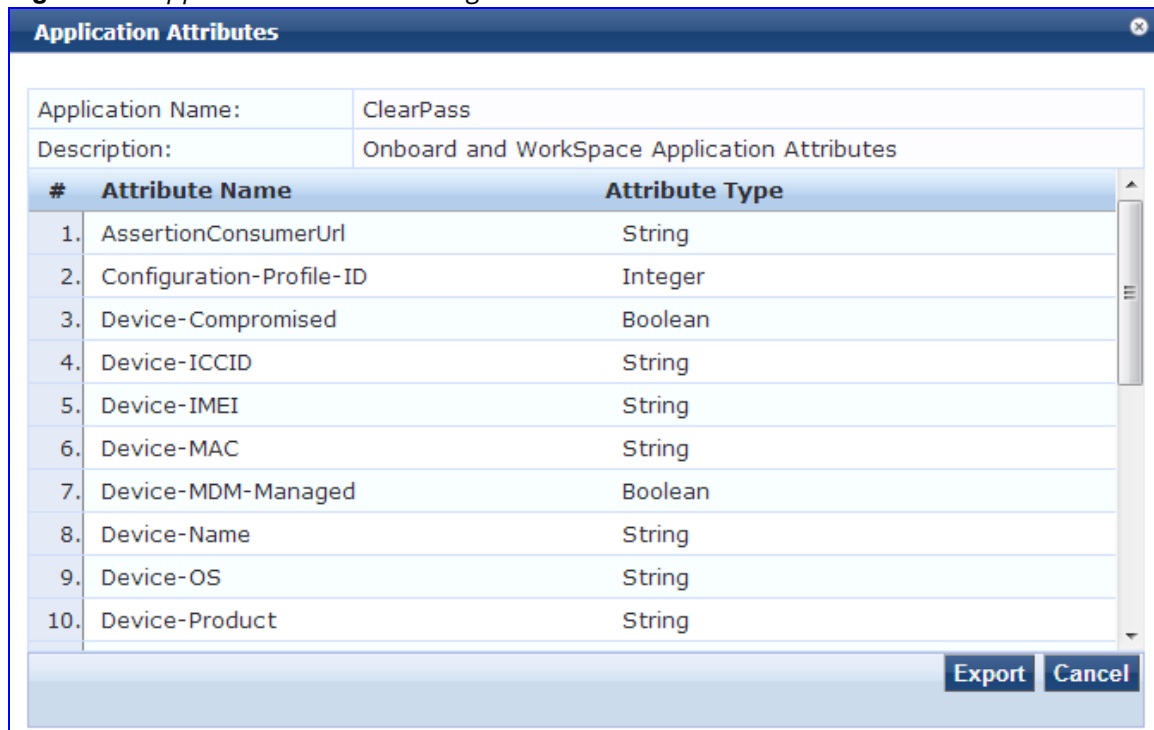
Show records

#	Application Name ▲	Description
1.	☐ ClearPass	ClearPass Application Attributes
2.	☐ SSO	SSO Application Attributes

Showing 1-2 of 2

2. To see the application attributes, click the name of an application.
The **Application Attributes** dialog box appears.

Figure 653: *Application Attributes Dialog*



#	Attribute Name	Attribute Type
1.	AssertionConsumerUrl	String
2.	Configuration-Profile-ID	Integer
3.	Device-Compromised	Boolean
4.	Device-ICCID	String
5.	Device-IMEI	String
6.	Device-MAC	String
7.	Device-MDM-Managed	Boolean
8.	Device-Name	String
9.	Device-OS	String
10.	Device-Product	String

Deleting an Application Dictionary

In general, there is no need to delete an application dictionary. They have no effect on W-Policy Manager performance.

To delete an application dictionary:

1. Navigate to **Administration > Dictionaries > Applications**.
2. Click the check box next to an application name.
3. Click **Delete**.

Updating Policy Manager Software

This section provides the following information:

- [Introduction](#)
- [Software Updates Page on page 647](#)
- [Install Update Dialog Box on page 649](#)
- [Reinstalling a Patch on page 651](#)
- [Uninstalling a Skin, Translation, or Plug-in on page 651](#)
- [Updating the Software on page 1](#)
- [OnGuard Settings on page 651](#)
- [OnGuard Global Agent Settings on page 654](#)

Introduction

This section describes the W-ClearPass Policy Manager server software update process.

Use the **Software Updates** page to register for and receive live updates for:

- Posture updates, including antivirus, antispyware, and Windows updates
- Profile data updates, including Fingerprint
- Software upgrades for the W-ClearPass family of products
 - Patch binaries, including Onboard, Guest Plug-ins, and Skins

You can also:

- Reinstall a patch in the event the previous installation attempt fails.
- Uninstall a skin, translation, or plug-in.

The W-ClearPass Policy Manager checks for available updates to the W-ClearPass Webservice server. The administrator can download and install these updates directly from the **Software Updates** page. The first time the Subscription ID is saved, W-ClearPass Policy Manager performs the following:

- Contacts the Webservice to download the latest Posture & Profile Data updates.
- Checks for any available firmware and patch updates.

Software Updates Page

To update the software on the current W-ClearPass server:

1. Navigate to **Administration > Agents and Software Updates > Software Updates**.

Figure 654 displays the **Software Updates** page:

Figure 654: *Software Updates Page*

Administration » Agents and Software Updates » Software Updates

Software Updates

 Cluster Upgrade
 Cluster Update

You are not signed up for live updates; enter your Subscription ID and save.

Subscription ID

Subscription ID:

Posture & Profile Data Updates

Update Type	Data Version	Data Created	Last Update	Last Updated	Update Status
AntiVirus & AntiSpyware Updates	-	-	-	-	Needs Update
Windows Hotfixes Updates	1.1530	2016/01/20 12:16:16	File	2016/01/23 09:51:02	Updated 2 days ago
Endpoint Profile Fingerprints	2.342	2016/01/14 10:00:09	File	2016/01/23 09:51:08	Updated 2 days ago
User-Agents Updates	-	-	-	-	Needs Update

To manually import Posture & Profile Data Updates, refer to Help for this page.

Firmware & Patch Updates

Update Type	Name	Version	Size (MB)	Update Released	Last Checked	Status	Delete

* Needs Restart
+ Restarts Administration UI
! Last Installed, available for Re-Install

Table 356 describes the **Software Updates** parameters:

Table 356: *Software Updates Parameters*

Parameter	Description
Subscription ID	
Subscription ID	1. Enter the Subscription ID provided to you. This text box is enabled only on a Publisher node. You can opt out of automatic downloads at any time by saving an empty Subscription ID.
Save	2. To save the Subscription ID , click Save . This button is enabled only on a Publisher node.
Reset	Performs an "undo" of any unsaved changes you have made in the Subscription ID field. NOTE: Reset does not clear the text box.
Posture & Profile Data Updates	
Import Updates	If this W-ClearPass Policy Manager server is not able to reach the Webservice server, use Import Updates to import (upload) the Posture and Profile Data into this server. You can download the data from the Webservice server by accessing the following URL: https://clearpass.dell-pcw.com/cppm/appupdate/cppm_apps_updates.zip When prompted, enter the provided Subscription ID for the username and the password. NOTE: In a cluster, the Import Updates option is available on the Publisher node only.
Firmware & Patch Updates	
Import Updates	3. If the server is not able to reach the Webservice server, click Import Updates to import the latest signed Firmware and Update patch binaries (obtained via support or other means) into this server. These patch binaries will appear in the table and can be installed by clicking the Install button. When logged in as <i>appadmin</i> , you can manually install the Upgrade and Patch binaries imported via the CLI using the following commands: ■ system update (for patches) ■ system upgrade (for upgrades) If a patch requires a prerequisite patch, that patch's Install button will not be enabled until the prerequisite patch is installed.
Install	The Install button appears after the update has been downloaded. 4. Click Install . When you click Install , the installation of the update starts and the Install Update dialog box appears, showing the log messages that are generated.
Re-Install	5. Click Re-Install to reinstall a patch in the event the previous attempt to install fails. Reinstalling a patch is available only for the last installed patch.
Uninstall	6. Click Uninstall to uninstall a skin, translation, or plugin.

Table 356: *Software Updates Parameters (Continued)*

Parameter	Description
Needs Restart	The Needs Restart link appears when an update needs a reboot of the server in order to complete the installation. Clicking this link displays the Install Update dialog box, which shows the log messages generated during the installation.
Installed	The Installed link appears when an update has been successfully installed. Clicking this link displays the Install Update dialog box, which shows the log messages generated during the installation.
Install Error	This link appears when an update install encounters an error. Clicking this link displays the Install Update dialog box, which shows the log messages generated during the install.
Other	
Check Status Now	Click this button to perform an on-demand check for available updates. Check Status Now applies to updates only on a publisher node, as well as Firmware & Patch Updates.
Delete	Use this option to delete a downloaded update.

The Firmware & Patch Updates table shows only the data that is known to webservice or imported using the **Import Updates** button.

Install Update Dialog Box

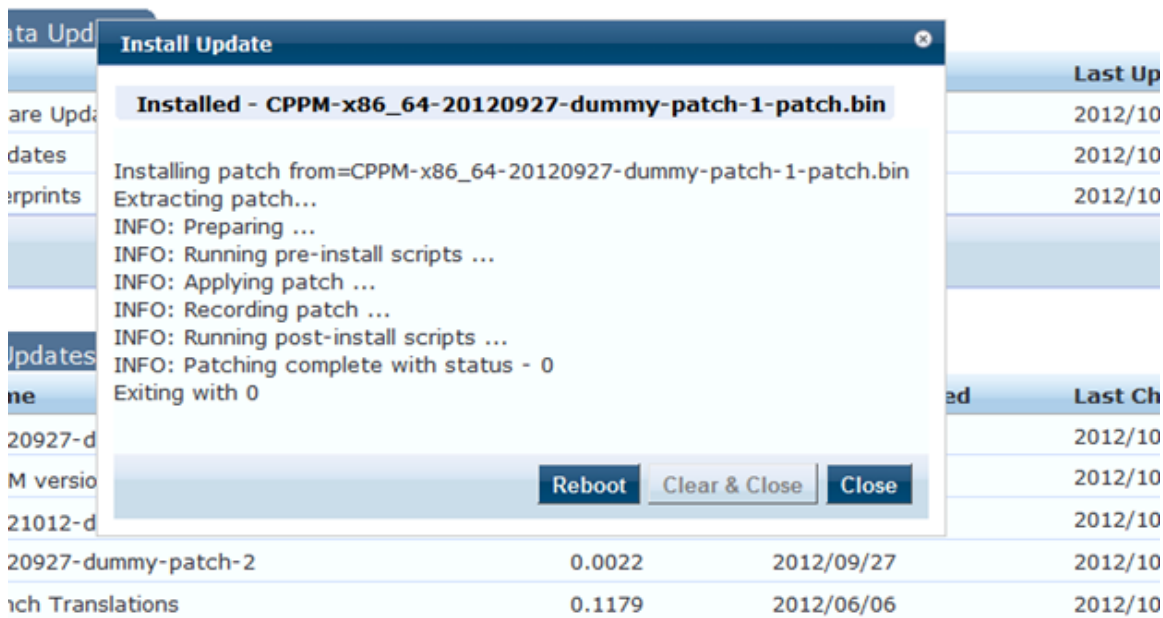
The **Install Update** dialog box shows the log messages generated during the installation of an update. This dialog appears when you click the **Install** button.

If the dialog is closed, you can bring it up again by any one of the three following methods:

- Clicking the **Install in progress...** link while the installation is in progress.
- Clicking the **Installed, Install Error** link.
- Clicking the **Needs Restart** link when the installation is completed.

The following figure displays the **Install Update** pop-up:

Figure 655: *Install Update Pop-up*



The following table describes the **Install Update** parameters:

Table 357: *Install Update Parameters*

Parameter	Action/Description
Reboot	1. To initiate a reboot of the server, click Reboot . The Reboot button appears only for updates that require a reboot to complete the installation.
Clear & Close	2. To delete the log messages and close the dialog, click Clear & Close . Clear & Close also removes the corresponding row from the Firmware & Patch Updates table. To delete the log messages from a failed installation, use the Clear & Close button. After the log messages are cleared, attempt the installation again.
Close	3. To close the dialog box, click this button.

Webservice Operations

System Events (as seen on the **Monitoring > Event Viewer** page) show records for events, such as communication failures with Webservice, successful or failed download of updates, and successful or failed installation of updates.

The W-ClearPass Policy Manager server contacts the Webservice server every hour in the background to download any newly available Posture & Profile Data updates. The current list of firmware and patch updates is queried from Webservice every day at a random minute between 4:00 a.m and 5:00 a.m.

Any new list of firmware and update patches that are available are noted by the W-Policy Manager server automatically and shown in the UI that they are available for download and installation.

The Webservice itself is refreshed with the Antivirus and Antispyware data hourly, with Windows Updates daily. Fingerprint data and Firmware & Patches are refreshed as and when new ones are available.

An event is generated and displayed in the **Event Viewer** with the list of new updates that are available. If the event affects an SMTP server, Alert Notification email addresses are configured, and an email from the Publisher is sent with the list of downloaded images.

Reinstalling a Patch

The **Reinstall Patch** feature allows the administrator to reinstall a patch in the event the previous attempt to install fails.

You can only reinstall the last installed patch, which is indicated by a "!" symbol next to it in the Firmware & Patch Updates table on the **Administration > Agents and Software Updates > Software Updates** page.

To reinstall a patch or software update:

1. Navigate to **Administration > Agents and Software Updates > Software Updates**.
2. In the **Firmware & Patch Updates** section, observe the **Status** column.
3. To bring up the dialog that shows the logs, click the **Installed**, **Install Error**, or **Needs Restart** link.
4. To reinstall the patch or software update, click **Re-Install**.

The **Install Update** screen closes and the re-installation process begins. A pop-up displays, showing the installation progress via log messages.

Uninstalling a Skin, Translation, or Plug-in

To uninstall a skin, translation, or plug-in:

1. Navigate to **Administration > Agents and Software Updates > Software Updates**.
2. In the **Firmware & Patch Updates** section, observe the **Status** column.
3. To bring up the dialog that shows the logs, click the **Installed** link.
4. To uninstall the patch or software update, click **Uninstall**.

The **Install Update** screen closes and the software is uninstalled.

OnGuard Settings

This section provides the following information:

- [Introduction](#)
- [Accessing OnGuard Agent Support Charts](#)
- [Configuring OnGuard Settings](#)

Introduction

Use the **OnGuard Settings** page to configure the agent deployment packages.

When you save the OnGuard configuration, W-ClearPass creates agent deployment packages for the Windows and Macintosh OS X operating systems and provides the packages at a fixed URL on the W-ClearPass Policy Manager hardware or virtual appliance.

You can then publish this URL to the user community. You can also download the agent deployment packages to another location.

Accessing OnGuard Agent Support Charts

For information about the OnGuard Agent Support Charts that are included with W-ClearPass Policy Manager, navigate to **Administration > Support > Documentation > OnGuard Agent Support Charts**.

Configuring OnGuard Settings

To configure the OnGuard settings:

1. Navigate to **Administration > Agents and Software Updates > OnGuard Settings**.

The OnGuard Settings main page appears:

Figure 656: *OnGuard Settings Main Page*

Administration » Agents and Software Updates » OnGuard Settings -

OnGuard Settings -

Agent Version: 6.6.0.79050

[Global Agent Settings](#)
[Policy Manager Zones](#)

Agent Installers

Agent Installers updated at Jan 22, 2016 16:20:54 PST

Installer Mode:

Agent will be used only to authenticate/perform health checks for client machines. This setting will not install the Aruba VIA component. If already installed, then the VIA component will be disabled on the client machine.
Note - This WILL remove any existing/installed Aruba VIA client

	Windows	http://10.2.50.199/agent/installer/windows/ClearPassOnGuardInstall.exe	(Full Install - EXE)	24MB
		http://10.2.50.199/agent/installer/windows/ClearPassOnGuardInstall.msi	(Full Install - MSI)	24MB
	Mac OS X	http://10.2.50.199/agent/installer/mac/ClearPassOnGuardInstall.dmg	(Full Install)	14MB
	Ubuntu	http://10.2.50.199/agent/installer/ubuntu/ClearPassOnGuardInstall.tar.gz	(Full Install)	19MB

Native Dissolvable Agent Apps

	Windows	http://10.2.50.199/agent/webagent/windows/OnGuard_Windows_Health_Checker.exe		12MB
	Mac OS X	http://10.2.50.199/agent/webagent/mac/OnGuard_Mac_Health_Checker.dmg		7MB
	Ubuntu	http://10.2.50.199/agent/webagent/ubuntu/OnGuard_Ubuntu_Health_Checker-x86.tar.gz	(32-bit)	4MB
		http://10.2.50.199/agent/webagent/ubuntu/OnGuard_Ubuntu_Health_Checker.tar.gz	(64-bit)	4MB

Agent Customization

Managed Interfaces: ☒ Wired ☒ Wireless ☒ VPN ☐ Other

Mode:

Authenticate with health checks

Username Text:

Password Text:

Agent action when an update is available:

Ignore

Native Dissolvable Agent Customization

Managed Interfaces: ☒ Wired ☒ Wireless ☐ VPN ☐ Other

2. Configure the OnGuard Settings parameters as described in [Table 358](#), then click **Save**.

Table 358: *OnGuard Settings Parameters*

Parameter	Action/Description
Global Agent Settings	1. Configure the global agent settings parameters for OnGuard agents. For more information, see OnGuard Global Agent Settings on page 654 .
W-Policy Manager Zones	2. Configure the network (subnet) for a W-Policy Manager Zone. For more information on configuring W-Policy Manager zones, see Manage Policy Manager Zones on page 500 .
Agent Version	Indicates the current version of the OnGuard agent.
Agent Installers	
Installer Mode	3. Specify the action to be taken from the following options when the Dell VIA component is used to provide VPN-based access: ■ Do not install/enable Aruba VIA component

Table 358: OnGuard Settings Parameters (Continued)

Parameter	Action/Description
	■ Install and enable Aruba VIA component
Windows	4. Use the download link to download OnGuard Agent for Windows. This binary file is provided in .exe and .msi formats.
Mac OS X	5. Use the download link to download OnGuard Agent for Mac OS X. This binary file is in .DMG format.
Ubuntu	6. Use the download link to download Ubuntu Agent for Linux. This binary file is in .tar.gz format.
Native Dissolvable Agent Apps	
Windows	7. Click the URL to download Native Dissolvable Agent for Windows.
Mac OS X	8. Click the URL to download Native Dissolvable Agent for Mac OS X.
Ubuntu	9. Click the URL to download Native Dissolvable Agent for Ubuntu. You can download the .tar.gz files specific to 32-bit and 64-bit systems.
Agent Customization	
Managed Interfaces	10. Select the type(s) of interfaces that OnGuard will manage on the endpoint. Select from the following options: ■ Wired ■ Wireless ■ VPN ■ Other
Mode	11. Select one of the following options: ■ Authenticate - no health checks: OnGuard collects username/password but does not perform health checks on the endpoint. ■ 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 and Password fields on the OnGuard agent. ■ This setting is not valid for the Check health - no authentication mode.
Username Text	The label for the Username field on the OnGuard agent. This setting is not valid for the Check health - no authentication mode.
Password Text	The label for the Password field on the OnGuard agent. This setting is not valid for the Check health - no authentication mode.

Table 358: *OnGuard Settings Parameters (Continued)*

Parameter	Action/Description
Agent action when an update is available	Determines what the agent does when an update is available. 12. Select one of the following options: ■ Ignore: W-ClearPass Policy Manager ignores the available update. ■ Notify User: W-ClearPass Policy Manager notifies the user that an update is available. ■ Download and Install: W-ClearPass Policy Manager automatically downloads and installs an update when it is available.
Native Dissolvable Agent Customization	
Managed Interfaces	This feature ensures that, if both wired and wireless interfaces are connected, the OnGuard Agent will send health requests through the correct interface. 13. Select the type(s) of managed interfaces that are supported for the Native Dissolvable Agent. The Native Dissolvable Agent performs health checks for one of the selected interfaces. Select from the following options: ■ Wired ■ Wireless ■ VPN ■ Other

OnGuard Global Agent Settings

This section provides the following information:

- [About Global Agent Settings](#)
- [Global Settings Parameters for OnGuard Agents](#)
- [Global Agent Settings: Run OnGuard As Parameter](#)

About Global Agent Settings

Use the **Global Agent Settings** page to configure the global parameters for OnGuard agents.

1. Navigate to the **Administration > Agents and Software Updates > OnGuard Settings** page.
2. Click the **Global Agent Settings** link at the top-right corner.
The **Configure Global Agent Settings** page opens.

Figure 657: *Configure Global Agent Settings Page*

Name	Value	
1. Cache Credentials Interval(in days)	= 15	
2. Enable to install VPN component	= true	
3. Click to add...		

Save Cancel

3. To add additional Global Agent Settings parameters, click **Click to add...**

4. **Name:** Select the desired Global Agent Setting (see [Table 359](#)).
5. **Value:** Specify the appropriate value.
6. Repeat these steps as necessary for each additional setting, then click **Save**.

Global Settings Parameters for OnGuard Agents

[Table 359](#) describes the Global Settings parameters for OnGuard agents:

Table 359: *Configure Global Settings Parameters*

Parameter	Action/Description
Name	Allowed Subnets for Wired access: Add a comma-separated list of IP addresses or subnet addresses.
	Allowed Subnets for Wireless access: Add a comma-separated list of IP addresses or subnet addresses.
	Cache Credentials Interval (in days): Select the number of days the user credentials should be cached on OnGuard agents.
	Delay to bounce after Logout (in minutes): Specify the number of minutes that should elapse before OnGuard bounces the interface if OnGuard remains disconnected.
	Enable OnGuard requests load-balancing: Enable this option to balance the load of OnGuard authentication requests across W-ClearPass Policy Manager servers in a cluster.
	Enable access over Remote Desktop Session: Enable this option to allow OnGuard access through a Remote Desktop session.
	Enable to hide Logout button: Enable this option to hide the Logout button on OnGuard agent.
	Enable to install VPN component: Enable this option to install the OnGuard VPN component.
	Enable to use Windows Single-Sign On: Enable this option to allow use of a user's Windows credentials for authentication.
	Keep-alive Interval (in seconds): Specify a keep-alive interval for OnGuard agents. The connected OnGuard Agents periodically send heart-beat (Keep-Alive) messages to W-ClearPass Policy Manager. This interval is defined by the Keep-alive Interval (in seconds) parameter. The default value is 60 seconds. W-ClearPass uses Keep-Alive messages to: • Update the status of OnGuard Agents regarding OnGuard Activity. • Issue CoA (Change of Authorization) for a Session Restrictions Enforcement Profile if OnGuard Agent is disconnected: ■ Session-Check > Agent-Connection = Down ■ Post-Auth-Check > Action = Disconnect For related information, see Session Restrictions Enforcement on page 381.
	OnGuard Health Check Interval (in hours): Specify the number of hours that OnGuard will skip health checks for healthy clients. NOTE: Note the following information when you set the OnGuard Health Check Interval parameter: ■ You can set this parameter if OnGuard mode is set to health only.

Table 359: *Configure Global Settings Parameters (Continued)*

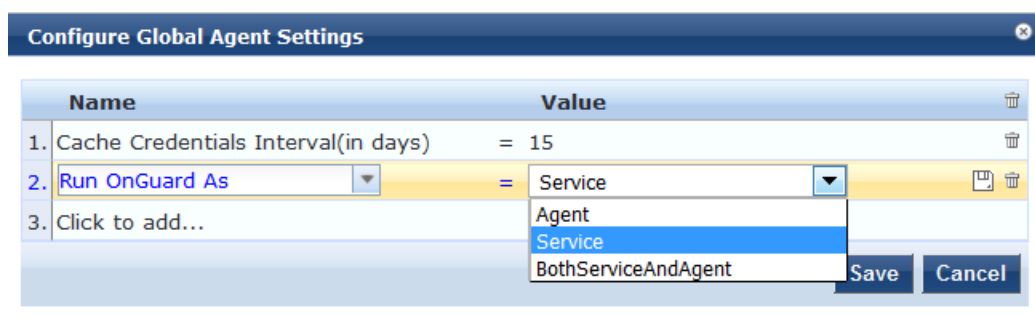
Parameter	Action/Description
	- This parameter is valid only for wired and wireless interface types. - This parameter is not applicable for the OnGuard Dissolvable Agent, VPN, and Other interface types. You can also specify the health check interval in the Agent enforcement (Configuration > Agent enforcement > New attribute) profile to create different Agent Enforcement Profiles for different users.
	Run OnGuard As: For details, see the next section, Global Agent Settings: Run OnGuard As Parameter.
	Support Team Email Address: Enter an email address that automatically populates the To field in the user's email client when they send logs.
Value	Enter the value for the parameters selected in the Name drop-down.

Global Agent Settings: Run OnGuard As Parameter

You can configure OnGuard to run health checks even if a user is not logged in.

1. Navigate to **Administration > Agents and Software Updates > OnGuard Settings**.
The OnGuard Settings page appears.
2. Click **Global Agent Settings**.
The Global Agent Settings dialog appears.

Figure 658: *Global Agent Settings Dialog*



3. Click **Click to add....**
4. **Name:** Select **Run OnGuard As**.
5. **Value:** Select the appropriate option as described in [Table 360](#).
[Table 360](#) describes the available values for the **Run OnGuard As** parameter.
6. Click **Save**.

Table 360: *Global Agent Settings: Run OnGuard As Parameters*

Value	Description
Agent	Health checks are performed by the OnGuard Agent after the user logs in to the client.
Service	OnGuard Agent performs health checks as soon as the client boots up, that is, even before the user logs in to the client. When a user logs in to the client, the user can view the most recent health check results via the OnGuard Agent user interface. The user can perform health checks again by clicking the Retry button. For details, see the next section, Limitations for the Run OnGuard As Parameter .
BothService AndAgent	When the user is not logged in to the client, the ClearPass OnGuard Agent service performs health checks. As soon as the user logs in to the client, the W-ClearPass OnGuard Agent service stops health checks and the OnGuard Agent user interface initiates health checks.

Limitations for the Run OnGuard As Parameter

When the **Run OnGuard As** parameter is set to **Service**, the following limitations pertain:

1. In **Service** mode, OnGuard always runs in **Health Only** mode; that is, OnGuard always sends the client's MAC Address as User Name.
2. If a user is not logged in, some of the health checks and auto-remediation may fail in **Service** mode. These health checks are user-level checks, such as Registry Keys (HKCU), Processes, and Installed Applications (per user applications).
3. When OnGuard Agent is running in **Service** mode, the OnGuard user interface is used only to display messages and provide the **Retry** button (to perform health checks).
4. The **Enable to Hide Quit Option** does not have any effect in **Service** mode as the **Quit** button is only for exiting the OnGuard user interface.

Contact Support

The **Administration > Support > Contact Support** page provides you with information on how to contact Dell Support.

The following figure displays the **Contact Support** page:

Figure 659: *Contact Support Page*

Company:											
Contact Details:	Contacting Dell <table><tr><th>Website Name</th><th>Address</th></tr><tr><td>Main Website</td><td>dell.com</td></tr><tr><td>Support Website</td><td>dell.com/support</td></tr><tr><td>Documentation Website</td><td>dell.com/support/manuals</td></tr><tr><td>Software Download Website</td><td>download.dell-pcw.com</td></tr></table>	Website Name	Address	Main Website	dell.com	Support Website	dell.com/support	Documentation Website	dell.com/support/manuals	Software Download Website	download.dell-pcw.com
Website Name	Address										
Main Website	dell.com										
Support Website	dell.com/support										
Documentation Website	dell.com/support/manuals										
Software Download Website	download.dell-pcw.com										

Remote Assistance

This section provides the following information:

- [Remote Assistance Process Flow](#)
- [Adding a Remote Assistance Session](#)

The **Remote Assistance** feature enables the W-ClearPass Policy Manager administrator to allow a support engineer to remotely log in using Secured Shell (SSH) to the W-ClearPass Policy Manager server and perform the following tasks:

- View the W-ClearPass Policy Manager user interface to debug any issues the customer is experiencing.
- Perform proactive monitoring of the W-ClearPass server.

Remote Assistance Process Flow

The Remote Assistance process flow is as follows:

1. Administrator schedules a Remote Assistance session for a specific duration.
2. The support contact receives an email with instructions and credentials to log in to the remote system.
3. The session is terminated at the end of the specified duration.
4. You can terminate a session before its stipulated duration.
5. The support contact can terminate the session before the time expires.



You can configure a Remote Assistance session through the CLI if the W-ClearPass Policy Manager user interface at the customer site is inaccessible. For details, refer to [System Commands on page 769](#). The relevant commands are: **system start-rasession**, **system status-rasession**, and **system terminate-rasession**.

The following figure displays the **Remote Assistance** page:

Figure 660: Remote Assistance Page

The screenshot shows the 'Remote Assistance' page in the W-ClearPass Policy Manager. At the top, there's a breadcrumb 'Administration » Support » Remote Assistance' and a title 'Remote Assistance'. On the right, there's a '+ Add Session' button and a 'Select Server:' dropdown menu with '10.' selected. Below this is a filter section with 'Filter: Name' and a 'contains' dropdown, followed by a search input field, a '+ Go' button, and a 'Clear Filter' button. To the right of the filter is a 'Show 10 records' dropdown. The main content is a table with columns: '#', 'Name', 'Type', 'Support Contact', 'Status', and 'Timestamp'. There is one row with the following data: '# 1.', 'Name Customer_Session', 'Type One Time Now', 'Support Contact manishas', 'Status Saving', and 'Timestamp -'. At the bottom right of the table, there are 'Delete' and 'Terminate' buttons.

The following table describes the **Remote Assistance** session parameters:

Table 361: Remote Assistance Session Parameters

Parameter	Description
Name	Name of the session.
Type	Indicates if the session is a one-time session or a periodic session. Move the cursor over the entry to view the schedule of the session.
Support Contact	The email address of the support contact.
Status	Provides the session state. Available states are:

Table 361: Remote Assistance Session Parameters (Continued)

Parameter	Description
	• Saving • Scheduled • Initiated • Running • Terminated • Failed NOTE: You can edit and save a session in Scheduled, Terminated, and Failed states. Only a session in Running state can be terminated by selecting that session and clicking Terminate. You can delete a session in Scheduled, Terminated, and Failed states by selecting that session and clicking Delete. If a session fails, the Event Viewer indicates the cause of the failure.
Timestamp	Displays the server time when the Remote Assistance session status was last updated.

Adding a Remote Assistance Session

To create a session on a W-ClearPass Policy Manager server in the cluster, the administrator can click the **Add Session** link.

Sessions can only be saved and deleted from the cluster Publisher node. Sessions can be terminated from the Publisher or from Subscribers nodes.

To set up a Remote Assistance session:

1. Navigate to **Administration > Support > Remote Assistance**.

The **Remote Assistance** page opens (see [Figure 660](#)).

2. Click the **Add Session** link.

The **Add Session** dialog opens:

Table 362: Remote Assistance > Add Session Dialog

Add Session	
Session Name:	sample_session
Session Type:	One Time Now
Duration:	Hours: 00 Minutes: 00
Aruba Support Contact:	[text field]@arubanetworks.com
Save Cancel	

3. Specify the **Add Session** parameters as described in [Table 363](#):

Table 363: *Add Session Parameters*

Parameter	Action/Description
Session Name	1. Enter the name of the Remote Assistance session.
Session Type	2. Specify the Session Type : ● One Time Now ● One Time Future: Initiates a session at a specified date and time. ● Weekly: Initiates a session on a specified weekday at the selected time. ● Monthly: Initiates a session on a specified day of every month at the selected time.
Duration	3. Specify the duration of the Remote Assistance session in hours and minutes. The "session begin" time is the time relative to the W-ClearPass server's time, and is specified in a 24-hour clock format.
Dell Support Website	4. For support, navigate to the Dell Support Website. The Dell Support Website is: dell.com/support .
	5. To save your changes, click Save .

This chapter contains the following information:

- [Cluster Update Tool](#)
- [Cluster Upgrade Tool](#)

Cluster Update Tool

This section provides instructions for updating a W-ClearPass cluster with Patch and Skin releases using the Cluster Update feature.

The Cluster Update feature automates the process of updating your W-ClearPass cluster. The cluster Publisher is updated first. You can select one or more Subscriber nodes to be updated automatically after the Publisher update is complete.

After you initiate the Cluster Update, no manual actions are required until the Publisher and all the selected Subscriber nodes have been updated.

This section includes the following information:

- [About the Cluster Update Feature](#)
- [Before Updating the Cluster](#)
- [Updating the Cluster](#)
- [Viewing Update Status](#)

About the Cluster Update Feature

The Cluster Update feature performs the following actions:

- Copies the update image to the selected Subscriber nodes.
Subscriber nodes copy the update image over a HTTPS connection to the Publisher.
If you want to avoid the copy on one or more Subscriber nodes, log in to the subscriber and trigger a download of the update image in the Update portal or upload the update image through the Update Portal before initiating the cluster update.
- The Publisher is updated and rebooted (reboot is initiated only if it is mandatory).
- After the Publisher update completes, the Update utility will be accessible again to review progress and log messages.
- Update is now initiated on the selected Subscriber nodes; after completion, the Subscriber nodes are rebooted (reboot is initiated only if it is mandatory).
- Where possible, multiple Subscriber nodes are updated in parallel.
- After all selected Subscriber nodes have been updated, you may select and trigger Cluster Update for any additional Subscriber nodes.

The time required for subscriber update depends on multiple factors:

- Hardware or Virtual Appliance model. In the case of Virtual Machine installations, update times vary significantly based on the IOPS (I/O per second) performance of your Virtual Machine infrastructure.
- For Subscriber nodes, bandwidth and latency of the network link between subscriber and Publisher.

Before Updating the Cluster

- Confirm that Relevant Patch updates are available under software updates before starting the cluster update. Please download the patches either from Webservice or by uploading directly to Software Updates.
- Only patches listed under Software Updates will be shown in Cluster Update.
- Confirm that your Cluster sync and replications are fine before starting the Cluster Update.
- When a particular node's version information is set to "UNKNOWN", it means the Publisher is not able to contact the remote node. (If a Node has been disabled and gone out of sync, Cluster Update Interface might not detect the status until the patch failure has occurred, after which the failed/inaccessible node is marked as UNKNOWN).

Please confirm the status of the cluster sync and service status of "Async network services" in such cases.

- In VM environments, W-ClearPass Policy Manager Virtual Machine host date/time settings should be in sync with that of the ESX or Hyper-V server, which is hosting the instance. Otherwise, you might see inconsistent data in "Time Taken" columns of the Update Interface.

Updating the Cluster

Plan for sufficient downtime and review the Release Notes before starting the Cluster Update.

To update the cluster:

1. Navigate to **Administration > Agents and Software Updates > Software Updates > Cluster Update**.

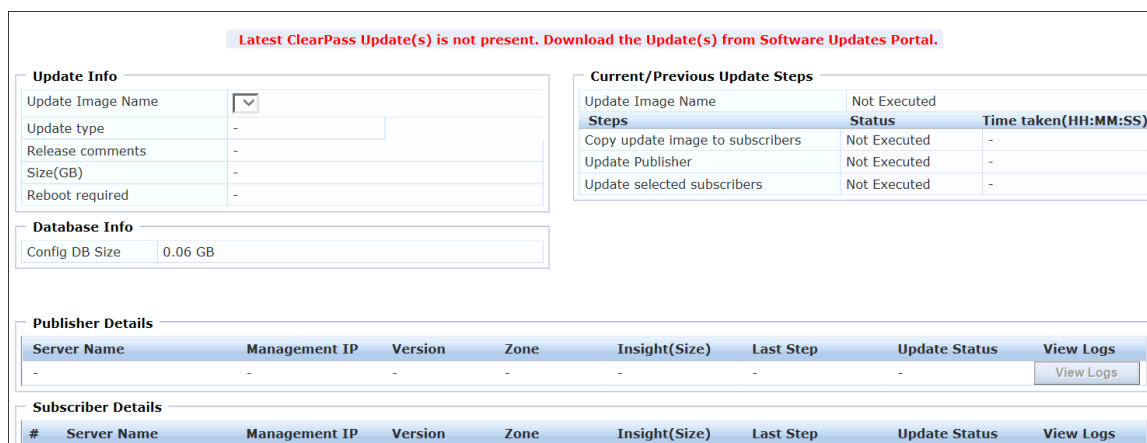
Figure 661: *Navigate to Cluster Update*



2. Before you start the update, verify that the W-ClearPass update is downloaded and available in the Software Updates portal.

If the update is not available, the Cluster Update page displays a message advising you to download it.

Figure 662: *The Message Advising that the Update Must Be Downloaded*



Latest ClearPass Update(s) is not present. Download the Update(s) from Software Updates Portal.							
Update Info				Current/Previous Update Steps			
Update Image Name				Update Image Name	Not Executed		
Update type				Steps	Status	Time taken(HH:MM:SS)	
Release comments				Copy update image to subscribers	Not Executed	-	
Size(GB)				Update Publisher	Not Executed	-	
Reboot required				Update selected subscribers	Not Executed	-	
Database Info							
Config DB Size	0.06 GB						
Publisher Details							
Server Name	Management IP	Version	Zone	Insight(Size)	Last Step	Update Status	View Logs
-	-	-	-	-	-	-	View Logs
Subscriber Details							
#	Server Name	Management IP	Version	Zone	Insight(Size)	Last Step	Update Status
View Logs							

3. If you are prompted to log in, use your W-ClearPass Policy Manager administrator credentials. The Cluster Update page opens.

Figure 663: *Cluster Update Page*

Update Info	
Update Image Name	Dummy Patch 3 for ClearPass 6.6.0 with services restart
Update type	Patch Release Notes
Release comments	Dummy Patch 3 for ClearPass 6.6.0, with restart of services
Size(GB)	0.00 GB
Reboot required	No

Database Info	
Config DB Size	0.04 GB

Publisher Details							
Server Name	Management IP	Version	Zone	Insight(Size)	Last Step	Update Status	View Logs
vm-655	10.17.6.55	6.6.0.79478	default	Enabled (0.01 GB)	-	-	View Logs

Subscriber Details							
#	Server Name	Management IP	Version	Zone	Insight(Size)	Last Step	Update Status
1.	VM-654	10.17.6.54	6.6.0.79478	default	Disabled (0.01 GB)	-	-

Current/Previous Update Steps		
Update Image Name	Dummy Patch 1 for ClearPass 6.6., No Reboot enabled	
Steps	Status	Time taken(HH:MM:SS)
Copy update image to subscribers	Completed	00:00:17
Update Publisher	Completed	00:01:02
Update selected subscribers	Completed	00:02:02

This page includes the information described below in [Table 364](#).

Table 364: *Information on the Cluster Update Page*

Field	Description
Update Info	Describes the patch update details, provides a link to the Release Notes, includes release-specific comments, and specifies if a reboot is required for the patch.
Database Info	Shows the size of the Configuration database.
Publisher Details	Information for the Publisher and for all Subscriber nodes in the cluster. Information includes the management IP address, version number, zone, Insight database size, last update step completed, and update status.
Subscriber Details	
Update Steps	During the cluster update, this area shows the status of each stage in the process. As each stage completes, it shows how long it took to complete.
View Logs	In each Publisher and Subscriber row, this link provides detailed status and log messages for each update stage.

- Select the **Update Image Name** from the drop-down list.
When the update is available locally and all Subscriber nodes have been patched, the **Start Update** link is available in the upper-right corner.
- Click **Start Update**.
The **Start Cluster Update** window opens.

Figure 664: *The Start Cluster Update Window*

Start Cluster Update

Publisher Details

Management IP	Server Name	Version	Zone
10.17.6.55	vm-655	6.6.0.79478	default

Note: Publisher has not been updated; it will be updated with any selected subscribers

Subscriber Details

Select subscribers to update:

#	☐	Management IP	Server Name	Version	Zone
1.	☐	10.17.6.55	VM-654	6.6.0.79478	default

Install Option

Force install patch update: ☐

Update **Close**



You can update the entire cluster or just a subset of Subscriber nodes.

6. In the **Start Cluster Update** window, use the check boxes to select the Subscriber nodes to update.
7. To force the update, select **Force install patch update** under **Install Option**.
8. Click **Update**.

This initiates the automated update process. No further manual steps are required until all selected Subscriber nodes have been updated. The Publisher is always updated and rebooted first.

The Cluster Update page will not be available while the Publisher is rebooted. When the Publisher update is complete, you can use the Cluster Update page to monitor update progress.

Viewing Update Status

After the Publisher Update is complete, you can monitor the Update status of the Subscriber nodes at **Administration > Agents and Software Updates > Software Updates > Cluster Update**.

There are two ways to monitor the update's progress:

1. On the **Cluster Update** page, progress indicators in the **Update Steps** area show the status of some of the main steps.

Indicators in the **Publisher Details** and **Subscriber Details** areas also show when the Publisher or each subscriber is in progress or completed.

When the update is complete, these areas should show a successful update status for the Publisher and every subscriber.

Figure 665: Status Indicators in the Update Steps Area

Administration » Agents and Software Updates » Software Updates » Cluster Update

Cluster Update

Update in progress for 2 node(s)

Update Info

Update Image Name	MySQL driver updates	Release Notes
Update type	Patch	
Release comments	MySQL driver updates	
Size(GB)	0.00 GB	
Reboot required	Yes	

Current/Previous Update Steps

Update Image Name: MySQL driver updates		
Steps	Status	Time taken(HH:MM:SS)
Copy update image to subscribers	Completed	00:00:17
Update Publisher	In Progress	-
Update selected subscribers	Not Executed	-

Database Info

Config DB Size	0.03 GB

Publisher Details

Server Name	Management IP	Version	Zone	Insight(Size)	Last Step	Update Status	View Logs
VM-206	10.17.4.206	6.6.0.79829	default	Disabled (0.01 GB)	Update	In Progress	View Logs

Subscriber Details

#	Server Name	Management IP	Version	Zone	Insight(Size)	Last Step	Update Status	View Logs
1.	VM-212	10.17.4.212	6.6.0.79829	default	Disabled (0.01 GB)	Upload	In Progress	View Logs

[Back to Software Updates](#)

If you navigate to another page, and then navigate back to the Software Updates page, a status link will be provided.

Figure 666: In Progress Status Link

⚠ One or more node in cluster is under upgrade/update

Administration » Agents and Software Updates » Software Updates

Software Updates

[Cluster Upgrade](#)
[Cluster Update](#)

You are not signed up for live updates; enter your Subscription ID and save.

Subscription ID

Subscription ID:

[Save](#) [Reset](#)

Clicking the link takes you back to the **Cluster Update** page.

- For detailed progress information, click the **View Logs** button in the Publisher's or subscriber's row.

The **Logs** window opens. This window includes tabs for the **Download**, **Upgrade**, **Reboot**, and **Onboot** logs.

You can view detailed status in these logs during and after the update.



This option is not available while the Publisher is rebooted and data migration is in progress. It is available again when the Publisher update is complete.

Figure 667: Details Displayed on the Logs Window

Logs

Server

Server Name:	VM-206
Management IP:	10.17.4.206
Version:	6.6.0.79829
Cluster Role:	Publisher
Zone:	default
Insight(Size):	Disabled (0.01 GB)

MySQL driver updates Update Steps

Name	Status	Time taken(HH:MM:SS)
Download	Completed	00:00:02
Update	Completed	00:01:03
Reboot	In Progress	-
Onboot	-	-

Download Update Reboot Onboot

Log Filename:

1-Update-2016-02-23-18-03-46.log

```

Node is reachable.

Installing patch from=CPPM-x86_64-20140821-mysql-support-66-patch.bin
Extracting patch...
INFO: Preparing ...
INFO: Running pre-install scripts ...
INFO: Applying patch ...
INFO: Recording patch ...
INFO: Running post-install scripts ...
INFO: Patching complete with status - 0
Time taken to install this patch is 0 minute(s) and 1 second(s).
Exiting with 0

```

Close

Logs

Server

Server Name:	VM-206
Management IP:	10.17.4.206
Version:	6.6.0.79829
Cluster Role:	Publisher
Zone:	default
Insight(Size):	Disabled (0.01 GB)

MySQL driver updates Update Steps

Name	Status	Time taken(HH:MM:SS)
Download	Completed	00:00:02
Update	Completed	00:01:03
Reboot	Completed	00:05:40
Onboot	Completed	00:07:03

Download Update Reboot Onboot

Log Filename:

1-Upload-2016-02-23-18-03-29.log

```

Node is reachable.

Publisher Node: Backup of executables started.
Publisher Node: Backup of executables completed.

Update image download started.

Update image download completed.

```

Close

Cluster Upgrade Tool

This section includes the following information:

- [Cluster Upgrade Process Overview](#)
- [Before You Upgrade](#)
- [Installing the Cluster Upgrade Tool](#)

- [Opening the Cluster Upgrade Tool](#)
- [Upgrading the W-ClearPass Cluster](#)
- [Viewing Upgrade Status](#)
- [Steps in the Upgrade Tool's Automated Workflow](#)
- [Troubleshooting](#)

Introduction

This section provides instructions for upgrading a W-ClearPass cluster using the Cluster Upgrade Tool.

The Cluster Upgrade Tool is a simple user interface that automates the upgrade procedure for a W-ClearPass cluster. When the Upgrade is initiated, no manual actions are required until the publisher and all selected Subscribers have been upgraded.

This release of the tool can be used to upgrade W-ClearPass 6.3.6, 6.4.7, and 6.5.x systems to W-ClearPass 6.6. It cannot be used to upgrade to an earlier version of the Cluster Upgrade Tool.

If you have an earlier version of the Cluster Upgrade Tool already installed, you can install this version directly over the earlier version of the tool; no cleanup steps are needed.

Cluster Upgrade Process Overview

These tasks summarize the Cluster Upgrade process:

1. Download the upgrade image to the **Software Updates Portal**.
2. Install the Cluster Upgrade Tool.
3. Launch the Cluster Upgrade Tool and specify the Subscriber nodes to be upgraded.
4. Click the **Upgrade** button.
The Cluster Upgrade tool automatically performs the upgrade.
5. After the upgrade, verify that the Publisher and all Subscriber nodes in the cluster are back in sync and all services are accessible.



Cloning a virtual machine to facilitate a W-ClearPass deployment is not recommended or supported.

Before You Upgrade

- Review this section and the latest Release Notes for W-ClearPass 6.6.
- Plan for adequate downtime for the upgrade.
Use the upgrade time estimates in [Sample Times Required for Upgrade on page 675](#) as a guide.
- Install the Cluster Upgrade Tool on the Publisher of your 6.3.6, 6.4.7, and 6.5.* version.
- Before installing the Cluster Upgrade Tool on the Publisher, verify that W-ClearPass services are up and running on both the Publisher and all Subscriber nodes. Verify again after installing the tool.
- If the cluster password contains special characters, change it temporarily to only use alphanumeric characters (letters and numbers) before installing this patch.
You can change the cluster password back to the old password after the cluster upgrade completes.
- HTTP/HTTPS and SSH port traffic must be allowed between the cluster nodes. This is required in order for the tool to be able to communicate between nodes.
Verify that the following ports are in an open state between the cluster nodes:
 - Port 80 (HTTP)
 - Port 443 (HTTPS)

- Port 22 (SSH)
- Confirm that the Publisher and all Subscriber nodes in the cluster are in sync before starting the upgrade.
- On the Publisher, download the W-ClearPass 6.6 upgrade image from the **Software Updates** portal (see [Updating Policy Manager Software on page 646](#)).

The Upgrade tool automates the process of copying over the upgrade image to the selected subscribers in the cluster.

- If you are upgrading on a reverted system (retrying an upgrade), you will need to replace the contents of certain directories first before triggering the new upgrade. Please contact Support (see [Contact Support on page 657](#)), who will assist you with the following tasks:
 1. Copying the contents of the `/var/avenda/platform/store/updates/backup/*` directory to the `/var/avenda/platform/store/updates/` directory.
 2. Clearing the contents of the `/var/avenda/tips/upgrade/db/*` directory.
 3. Restarting the **cpass-admin-server** on the Publisher.
- When a particular node's version information is set to "UNKNOWN," it means the publisher is not able to contact the remote node.
 If a node has been disabled and gone out of sync, the Cluster Upgrade Interface might not detect the status until the patch failure has occurred, after which the failed/inaccessible node is marked as UNKNOWN.
 In such cases, confirm the status of the cluster sync and service status of "Async network services."
- In Virtual Machine environments, W-ClearPass Policy Manager VM host date/time settings should be in sync with that of the ESX server or Hyper-V server, which is hosting the instance. Otherwise, you might see inconsistent data in "Time Taken" columns of the Upgrade interface.

Installing the Cluster Upgrade Tool

The Cluster Upgrade Tool is released as separate patches for each of the W-ClearPass 6.3.6, 6.4.7 and 6.5.* versions. It can be downloaded and installed either through W-Policy Manager's Software Updates portal or from the Dell Support Center (<https://download.dell-pcw.com>).



The Upgrade Tool can only be installed on the Publisher node.

To install the Upgrade Tool through the Software Updates Portal:

1. Log in to W-ClearPass Policy Manager on the Publisher and navigate to **Administration > Agents and Software Updates > Software Updates**.
2. In the row for the W-ClearPass Cluster Upgrade Tool patch, click the **Install** button.
 When the installation is complete, the Admin service will be restarted. You do not need to reboot.
3. To review the Release Notes for the tool, click the patch's row.
 The **More Information** window opens.
4. Click the **Release Notes URL** link.
 The Support Center's **Release Notes** page opens in a new tab.

Figure 668: The Link to the Cluster Upgrade Tool Release Notes

Firmware & Patch Updates							
Update Type	Name	Version	Size (MB)	Update Released	Last Checked	Status	Delete
Upgrade	W-ClearPass Upgrade version 6.5.0.71095*	More Information Update: Cluster Upgrade Tool for W-ClearPass 6.5.0 Upgrades Version 2 Description: This tool automates the process of upgrading nodes in a ClearPass cluster. Install this patch on the Publisher and launch the Upgrade Tool to upgrade your cluster. Release Notes URL: Click Here Close			/08/18 12:51:07	Download	-
Upgrade	W-ClearPass Upgrade version 6.4.0.66756*				/08/18 12:51:07	Download	-
Patch	Dell Leap second Fix Patch*				/08/18 12:51:07	Download	-
Patch	W-ClearPass Patch - Support DER format upgrade and update images in CLI				/08/18 12:51:07	Download	-
Patch	Cluster Upgrade Tool for W-ClearPass 6.4.0 Upgrades*				/08/18 12:51:07	Download	-
Patch	Cluster Upgrade Tool for W-ClearPass 6.5.0 Upgrades Version 2*				/08/18 12:51:07	Install	Delete
							Import Updates

* Needs Restart
+ Restarts Administration UI

If the Publisher Is Not Set Up

To install the Upgrade Tool if the publisher is not set up to display available updates:

1. On the Dell Support Site (<https://download.dell-pcw.com>), manually download the Cluster Upgrade Tool.
2. On the Publisher's **Software Updates** portal, use the **Import Updates** link to upload it.
3. Install the Upgrade Tool as described above.

Opening the Cluster Upgrade Tool

After the Cluster Update Tool is installed, you can open the Cluster Upgrade tool either from the Software Updates portal or through your Web browser.

To open the Cluster Upgrade Tool from the Software Updates portal:

1. In W-ClearPass Policy Manager, navigate to **Administration > Agents and Software Updates > Software Updates**.
2. In the upper-right of the page, click **Cluster Upgrade**.
The **Cluster Upgrade** page opens.

An Alternative Way to Open the Tool

An alternative way to open the tool is as follows:

1. In W-ClearPass Policy Manager, navigate to **Administration > Agents and Software Updates > Software Updates**.
2. In the **Firmware & Patch Updates** area, click the row of the W-ClearPass Cluster Upgrade Tool patch.
3. In the **More Information** window that opens, click the **Upgrade Tool** link.

Figure 669: The Link to the Cluster Upgrade Tool

Firmware & Patch Updates							
Update Type	Name	Version	Size (MB)	Update Released	Last Checked	Status	Delete
Upgrade	W-ClearPass Upgrade version 6.5.0.71095*	More Information Update: Cluster Upgrade Tool for W-ClearPass 6.5.0 Upgrades Version 2 Description: This tool automates the process of upgrading nodes in a ClearPass cluster. Install this patch on the Publisher and launch the Upgrade Tool to upgrade your cluster. Release Notes URL: Click Here Close			/08/18 12:51:07	Download	-
Upgrade	W-ClearPass Upgrade version 6.4.0.66756*				/08/18 12:51:07	Download	-
Patch	Dell Leap second Fix Patch*				/08/18 12:51:07	Download	-
Patch	W-ClearPass Patch - Support DER format upgrade and update images in CLI				/08/18 12:51:07	Download	-
Patch	Cluster Upgrade Tool for W-ClearPass 6.4.0 Upgrades*				/08/18 12:51:07	Download	-
Patch	Cluster Upgrade Tool for W-ClearPass 6.5.0 Upgrades Version 2*				/08/18 12:51:07	Install	Delete
							Import Updates

* Needs Restart
+ Restarts Administration UI

Opening the Tool Via Your Web Browser

To open the Cluster Upgrade Tool directly through your Web browser:

1. Enter **https://<W-ClearPass-Publisher-IP-address>/upgrade** in your browser's address bar.
2. If you are prompted to log in, use your W-ClearPass Policy Manager administrator credentials.

The **Cluster Upgrade Utility** page opens.

Figure 670: *The Cluster Upgrade Utility Page*

Cluster Upgrade Utility

Upgrade Info

Upgrade Image Name	-
Release comments	-
Size(GB)	-

Database Info

Config DB Size	0.27 GB

Upgrade Steps

Steps	Status	Time taken(HH-MM-SS)
Prepare subscribers	Completed	00:01:10
Copy upgrade image to subscribers	Not Executed	-
Upgrade Publisher	Not Executed	-
Upgrade selected subscribers	Not Executed	-

Publisher Details

Server Name	Management IP	Version	Zone	Insight(Size)	Last Step	Upgrade Status	View Logs
VM-206	10.17.4.206	6.3.5.66826	default	Disabled (0.03 GB)	-	-	View Logs

Subscriber Details

#	Server Name	Management IP	Version	Zone	Insight(Size)	Last Step	Upgrade Status	View Logs
1.	VM-207	10.17.4.207	6.3.5.66826	default	Enabled (0.01 GB)	-	-	View Logs
2.	VM-209	10.17.4.209	6.3.5.66826	default	Disabled (0.01 GB)	-	-	View Logs

This page includes the information described below in [Table 365](#).

Table 365: *Information on the Cluster Upgrade Utility Page*

Field	Description
Upgrade Info	Describes the upgrade image's name and size, provides a link to the Cluster Upgrade Tool Release Notes, and includes release-specific comments.
Publisher Details	Information for the Publisher and for all Subscriber nodes in the cluster. Information includes the management IP address, version number, zone, Insight database size, last upgrade step completed, and upgrade status.
Subscriber Details	
Database Info	Shows the size of the Configuration database.
Upgrade Steps	During the cluster upgrade, this area shows the status of each stage in the process. As each stage completes, it shows how long it took to complete.
View Logs	In each Publisher and Subscriber row, this link provides detailed status and log messages for each upgrade stage.
Help	Briefly describes the actions performed by the tool.

3. If the cluster password contains special characters, change it temporarily to only use alphanumeric characters (letters and numbers) before installing this patch.

The cluster password can be changed back to the old password after the cluster upgrade completes.

Figure 671: Special Characters Note

Cluster Upgrade Utility

Please make sure Cluster Password doesn't contain special characters like (@ : /) before starting Upgrade from Cluster Upgrade Tool.

Upgrade Info	
Upgrade Image Name	-
Release comments	-
Size(GB)	-

Database Info	
Config DB Size	0.04 GB

Upgrade Steps							
Steps	Status	Time taken(HH:MM:SS)					
Prepare subscribers	Completed	00:01:18					
Copy upgrade image to subscribers	Not Executed	-					
Upgrade Publisher	Not Executed	-					
Upgrade selected subscribers	Not Executed	-					

Publisher Details							
Server Name	Management IP	Version	Zone	Insight(Size)	Last Step	Upgrade Status	View Logs
VM-6-56	10.17.6.56	6.5.5.78974	default	Disabled (0.01 GB)	-	-	View Logs

Subscriber Details								
#	Server Name	Management IP	Version	Zone	Insight(Size)	Last Step	Upgrade Status	View Logs
1.	VM-6-57	10.17.6.57	6.5.5.78974	default	Disabled (0.01 GB)	-	-	View Logs

Figure 672: More Information > Special Characters Note

Firmware & Patch Updates	
Update Type	Name
Upgrade	ClearPass Upgrade version 6.6.0.79478*
Patch	ClearPass Cluster Upgrade Tool for 6.6.0 Upgrades.+!

* Needs Restart
+ Restarts Administration UI
! Last Installed, available for Re-Install

More Information

Update: ClearPass Cluster Upgrade Tool for 6.6.0 Upgrades.

Description: This tool automates the process of upgrading nodes in a ClearPass cluster. Install this patch on the Publisher and launch the [Upgrade Tool](#) to upgrade your cluster.

Note - If the cluster password contains special characters, please change it temporarily to only use alpha-numeric characters (letters and numbers) before installing this patch. The cluster password can be changed back to the old password after the cluster upgrade completes.

Release Notes URL: [Click Here](#)

[Close](#)

Upgrading the W-ClearPass Cluster

To upgrade the W-ClearPass cluster:

1. Navigate to **Administration > Agents and Software Updates > Software Updates > Cluster Upgrade**.
2. Before you start the upgrade, verify that the W-ClearPass 6.6 Upgrade Image is downloaded and available in the Software Updates portal.

If the upgrade image is not available, the **Cluster Upgrade** page displays a message advising you to download it.

Figure 673: The Message Advising that the Upgrade Image Must Be Downloaded

Latest ClearPass Upgrade image is not present. Download the image from Software Updates Portal.

Upgrade Info	
Image Name	-
Release comments	-
Size(GB)	-

Database Info	
Config DB Size	0.06 GB

Upgrade Steps							
Steps	Status	Time taken(HH:MM:SS)					
Prepare subscribers	Not Executed	-					
Copy upgrade image to subscribers	Not Executed	-					
Upgrade Publisher	Not Executed	-					
Upgrade selected subscribers	Not Executed	-					

Publisher Details							
Server Name	Management IP	Version	Zone	Insight(Size)	Last Step	Upgrade Status	View Logs
-	-	-	-	-	-	-	View Logs

Subscriber Details								
#	Server Name	Management IP	Version	Zone	Insight(Size)	Last Step	Upgrade Status	View Logs

- When you open the Cluster Upgrade Tool, it immediately prepares the subscribers for upgrade by automatically installing the required additional API support.
This is a background process and does not require any actions from the user. A progress indicator is shown during this stage.



To install the patch for API support on the subscribers, subscribers must be able to access the publisher over HTTP, or they must be able to access the publisher over HTTPS using its hostname and validate the certificate that is presented (trust the issuer and match the hostname in the certificate CN).

When the 6.6 upgrade image is available locally and all Subscriber nodes have been patched, the **Start Upgrade** link is available (in the upper-right corner).

- Click **Start Upgrade**.

The **Start Cluster Upgrade** window opens.

Figure 674: *The Start Cluster Upgrade Window*

Start Cluster Upgrade

Publisher Details

Management IP	Server Name	Version	Zone
10.17.4.210	HW-210	6.3.6.67943	default

Note: Publisher has not been upgraded; it will be upgraded with any selected subscribers

Subscriber Details

Select subscribers to upgrade:

#	☐	Management IP	Server Name	Version	Zone
1.	☐	10.17.5.227	HW-500-227	6.3.6.67943	default
2.	☐	10.17.5.235	VM-5235	6.3.6.67943	default
3.	☐	10.17.5.241	VM-5241	6.3.6.67943	default
4.	☐	10.17.5.242	VM-5242	6.3.6.67943	default
5.	☐	10.17.6.63	VM-6-63	6.3.6.67943	default
6.	☐	10.17.6.64	VM-6-64	6.3.6.67943	default
7.	☐	10.17.6.65	VM-6-65	6.3.6.67943	default

Database options

LogDB backup and restore options: Access tracker records are backed up but will not be restored

Access tracker records are backed up but will not be restored

Do not backup access tracker records

lose

You can upgrade the entire cluster or just a subset of Subscriber nodes.

- In the **Start Cluster Upgrade** window, use the check boxes to select the Subscriber nodes to upgrade.
- In the **LogDB backup and restore options** drop-down list:
 - If you need a backup of the Access Tracker records to potentially restore after upgrade, select **Access tracker records are backed up but will not be restored**.
This option will increase the overall upgrade time.
 - If you do not need a backup of the Access Tracker records, select **Do not back up access tracker records**.
- Click **Upgrade**.
The Upgrade Tool begins the automated upgrade process.

No further manual steps are required until all selected subscribers have been upgraded. For information on the automated process, see [Steps in the Upgrade Tool's Automated Workflow on page 674](#).

The Publisher is always upgraded and rebooted first. The Upgrade Tool will not be available while the publisher is rebooted and data migration is in progress.

8. When the Publisher upgrade is complete, navigate to the **Cluster Upgrade Utility** page to monitor upgrade progress, as described in [Viewing Upgrade Status on page 673](#).
9. After a successful upgrade, confirm that all the Subscriber nodes in the cluster are back in sync and all the services are accessible.
10. Verify that any preexisting Standby Publisher settings are restored:
 Navigate to: **Administration > Server Manager > Server Configuration > Cluster-Wide Parameters** link > **Standby Publisher** tab.

Viewing Upgrade Status

After the Publisher Upgrade is complete, you can monitor the Upgrade status of the subscribers at **Administration > Agents and Software Updates > Software Updates > Cluster Upgrade**.

The tool provides two ways to monitor the upgrade's progress:

1. On the **Cluster Upgrade** page, progress indicators in the **Upgrade Steps** area show the status of some of the main steps.

Indicators in the **Publisher Details** and **Subscriber Details** areas also show when the Publisher or each Subscriber is in progress or completed.

When the upgrade is complete, these areas should show a successful upgrade status for the Publisher and every Subscriber node.

Figure 675: Status Indicators in the Upgrade Steps Area

Upgrade in progress for 1 node(s)

Please Note:
New features

Upgrade Steps		
Steps	Status	Time taken(HH:MM:SS)
Prepare subscribers	Completed	00:00:00
Copy upgrade image to subscribers	Completed	00:00:02
Upgrade Publisher	In Progress	-
Upgrade selected subscribers	Not Executed	-

Zone	Insight(Size)	Last Step	Upgrade Status	View Logs
default	Disabled (0.01 GB)	Upgrade	In Progress	View Logs

If you navigate to another page, and then navigate back to the Software Updates page, a status link will be provided.

Figure 676: In Progress Status Link

⚠ One or more node in cluster is under upgrade/update

Administration » Agents and Software Updates » Software Updates

Software Updates

You are not signed up for live updates; enter your Subscription ID and save.

Cluster Upgrade
Cluster Update

Subscription ID

Subscription ID:

Save Reset

Clicking the link takes you back to the Cluster Upgrade page.

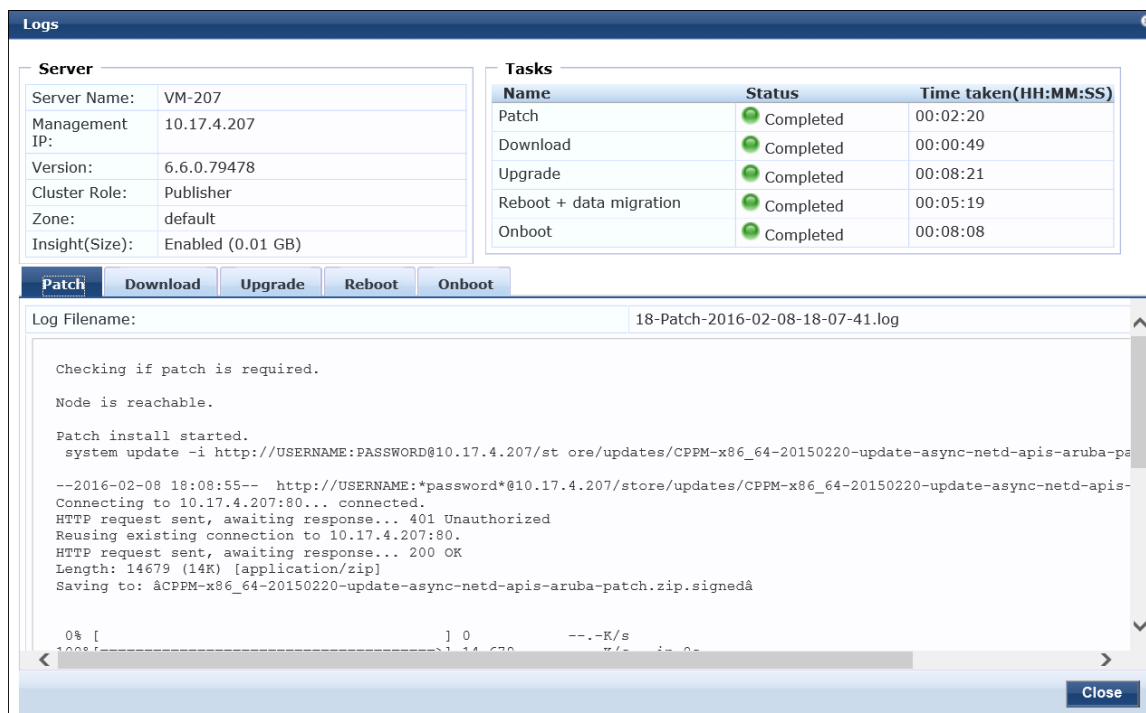
- For detailed progress information, click the **View Logs** button in the Publisher's or Subscriber's row. The **Logs** window opens. This window includes tabs for the **Patch**, **Download**, **Upgrade**, **Reboot**, and **Onboot** logs.

You can view detailed status in these logs during and after the upgrade.



This option is not available while the Publisher is rebooted and data migration is in progress. It is available again when the Publisher upgrade is complete.

Figure 677: Details Displayed on the Logs Window



Steps in the Upgrade Tool's Automated Workflow

This section describes the steps that are automatically completed by the Cluster Upgrade Tool.

- To prepare the Subscriber nodes for upgrade, a patch that provides required API support is automatically installed by the Upgrade Tool on every Subscriber.

The Cluster Upgrade Tool uses remote API calls to control and monitor upgrade progress on the subscribers.



To install the patch for API support on the subscribers, subscribers must be able to access the publisher over HTTP, or they must be able to access the publisher over HTTPS using its hostname and validate the certificate that is presented (trust the issuer and match the hostname in the certificate CN).

- After you select the Subscriber nodes and click **Upgrade**, the upgrade image is copied to the Subscribers you selected.

The Subscriber nodes copy the upgrade image over an HTTPS connection to the Publisher.

If the upgrade image is already present on a Subscriber node (you have downloaded it from the Software Updates portal, or uploaded it in the Software Updates portal), the existing upgrade image on the subscriber will be used for the upgrade.

- If the Standby Publisher settings were configured, they are temporarily disabled. This setting is restored after all subscribers have been upgraded.

4. The Publisher is the first to be upgraded and rebooted. Configuration database and Insight database migration is performed on reboot.
5. When the Publisher upgrade is complete, you can use the **Cluster Upgrade Utility** page to review log messages.
6. When the Publisher upgrade is complete, upgrade is initiated on each selected Subscriber node. When possible, multiple Subscribers are upgraded in parallel. When each Subscriber node is complete, the Subscriber is rebooted.
7. During the parallel upgrade process, upgrade of the first Subscriber node begins five minutes after the Publisher upgrade is completed.
8. Upgrade of the second Subscriber node begins five minutes after the upgrade of the first Subscriber begins. This pattern continues sequentially for all Subscriber nodes in the cluster, with a five-minute delay between each start time.
9. When each Subscriber is rebooted, it is added back into the cluster. Insight data is migrated and restored.
10. When all selected Subscriber nodes have been upgraded, you can select and trigger the upgrade operation for any additional Subscriber nodes.
11. When all the Subscriber nodes in the cluster have been upgraded, the Standby Publisher settings are restored.

Detailed information for each of these steps is available in the Logs window during and after upgrade.

Sample Times Required for Upgrade

To help you estimate how much time the upgrade might take, [Table 366](#) shows representative numbers for upgrade times under test conditions. Keep in mind that the figures here are only examples. The actual time required for your upgrade depends on several factors:

- Your hardware or virtual appliance model. In the case of virtual machine installations, upgrade times vary significantly based on the IOPS performance of your virtual machine infrastructure.
- The size of the configuration database to be migrated.
- For W-ClearPass Insight nodes, the size of the Insight database.
- For Subscriber nodes, the bandwidth and latency of the network link between the Subscriber and the Publisher.

Table 366: *Sample Times Required for Upgrade*

Hardware Model	Config DB Size	Insight DB Size	Publisher Upgrade Time	Subscriber Upgrade Time	Insight Restoration Time in Publisher or Subscriber
CP-500	100 MB	5 GB	50 minutes	50 minutes	20 minutes
	200 MB	5 GB	60 minutes	60 minutes	20 minutes
CP-5K	100 MB	5 GB	50 minutes	50 minutes	15 minutes
	200 MB	5 GB	60 minutes	60 minutes	15 minutes
CP-25K	200 MB	5 GB	30 minutes	30 minutes	15 minutes
	500 MB	10 GB	40 minutes	40 minutes	20 minutes

Troubleshooting

Troubleshooting tips:

- If you encounter errors while upgrading a Subscriber, use a manual upgrade procedure to upgrade the Subscriber after the root cause for the upgrade failure has been fixed.
- If you need to revert to the previous version of W-ClearPass, you can do so manually from the CLI for individual Subscribers.

Be aware that all status and progress information will be reset when the Publisher is reverted to a previous version. You can initiate the upgrade again from the Cluster Upgrade Tool.

This chapter includes the following information:

- Enabling Ingress Event Dictionaries
- Configuring the Ingress Event Sources
- Configuring an Event-Based Enforcement Service
- Configuring the Ingress Receiving Ports
- Enabling Ingress Events Processing

Overview

This chapter provides the procedures for configuring W-ClearPass Policy Manager to process ingress threat-related events.

The W-ClearPass Ingress Event Engine processes inbound threat-related events—which are Syslog events received from any third-party vendor device—and performs enforcements and actions based on defined policies.

Enabling Ingress Event Dictionaries

By default, a set of ingress event dictionaries are available and initially set to disabled. You must enable the ingress event dictionaries before you proceed.

To enable an ingress event dictionary:

1. Navigate to **Administration > Dictionaries > Ingress Events**.

The Ingress **Events Dictionaries** page opens, where the set of ingress event dictionaries are displayed. By default, they are disabled.

Figure 678: Viewing Ingress Event Dictionaries

Administration » Dictionaries » Ingress Events

Ingress Events Dictionaries

Filter: Vendor contains + Go Clear Filter

Show 10 records

#	Vendor	Format Name	Prefix	Status
1.	☒ Check Point	CheckPoint-Log	CheckPoint-Log	Disabled
2.	☒ Infoblox	Infoblox-Log	Infoblox-Log	Disabled
3.	☐ Juniper Networks	Juniper-SRX-Traditional-Syslog-RT_SCREEN_TCP_SRC_IP	Juniper-SRX-TS	Enabled
4.	☐ Juniper Networks	Juniper-SRX-Traditional-Syslog-RT_SCREEN_IP	Juniper-SRX-TS	Enabled
5.	☐ Juniper Networks	Juniper-SRX-Traditional-Syslog-RT_SCREEN_TCP	Juniper-SRX-TS	Enabled
6.	☐ Juniper Networks	Juniper-SRX-Structured-Syslog	Juniper-SRX-SS	Enabled
7.	☐ Juniper Networks	Juniper-SRX-Traditional-Syslog-IDP_ATTACK_LOG_EVENT	Juniper-SRX-TS	Enabled
8.	☐ Juniper Networks	Juniper-SRX-Traditional-Syslog-ANTISPAM_SPAM_DETECTED_MT	Juniper-SRX-TS	Enabled
9.	☐ Juniper Networks	Juniper-SRX-Traditional-Syslog-AV_VIRUS_DETECTED_MT	Juniper-SRX-TS	Enabled
10.	☐ Palo Alto Networks	PANW-Traffic-Syslog	PANW-Traffic	Disabled

Showing 1-10 of 11

Export Delete

2. To enable a dictionary, select the Ingress Events Dictionary for the appropriate vendor.
The **Events Attributes** dialog opens.

Figure 679: *Enabling an Ingress Events Dictionary*

Vendor:	Check Point
Format Name:	CheckPoint-Log
Prefix:	CheckPoint-Log
Description:	Check Point log message
Format:	TIME LOG_TYPE ORIGIN SERVICE PID ACTION SRC_INTERFACE MESSAGE

#	Attribute Name	Type
1.	time	Time
2.	log_type	String
3.	origin	String
4.	pid	String
5.	action	String
6.	service	String
7.	src_interface	String
8.	web_client_type	String
9.	resource	String
10.	src	String
11.	dst	String
12.	proto	String
13.	session_id	String

Enable **Export** **Close**

3. To enable the selected ingress events dictionary, click **Enable**.

You return to the Ingress Events Dictionaries page. The dictionary information is no longer displayed in red and the **Enabled** column is set to **True**.

Configuring the Ingress Event Sources

The Event Source is the device that sends Syslog events to W-ClearPass. Any events sent that are not from configured event sources are ignored.

To configure the Event Source (in this example, a Juniper Networks SRX gateway):

1. Navigate to **Configuration > Network > Event Sources**.

The **Event Sources** page appears.

2. To add the Event Source for the desired vendor, click **Add**.

The **Add Events Source** dialog appears.

Figure 680: Adding an Event Source

Name:	192.0.2.100
Description:	Juniper Networks SRX device that sends events to ClearPass
IP Address:	192.0.2.100
Type:	Syslog
Vendor:	Juniper Networks
Enable:	☒

3. Populate the **Add Event Source** parameters as described in Table 367.

Table 367: Configuring the Event Source Parameters

Parameter	Action/Description
Name	1. Enter the IP address of the device that will send Syslog events to W-ClearPass.
Description	Optionally, enter a description of this Event Source.
IP Address	2. Enter the IP address of the device that will send Syslog events to W-ClearPass.
Type	3. From the drop-down, select the Event Source Type .
Vendor	4. From the drop-down, select the Event Source Vendor .
Enable	5. Select this check box to enable the device as an Event Source.

6. When finished, click **Add**.

The **Event Sources** page now displays the new Event Sources (see Figure 681).

Figure 681: Event Sources Page

Configuration » Network » Event Sources

Event Sources

Event Source 192.0.2.100 added successfully

Filter: Name contains Go Clear Filter

Show 10 records

#	Name	Description	IP Address	Type	Vendor	Enabled
1.	192.0.2.100	Juniper Networks SRX device that sends events to ClearPass	192.0.2.100	Syslog	Juniper Networks	true

Showing 1-1 of 1

Export Delete

The IP address displayed in Figure 681 is the IP address and host name of the Juniper SRX gateway that sends Syslog events to W-ClearPass.

Configuring the Ingress Receiving Ports

The ingress receiving ports are the TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) ports on the W-ClearPass server where the events source sends threat-related events.

By default, the ingress receiving port is **514** for both TCP and UDP. You can modify the ingress receiving ports to a custom value as necessary.

To confirm or change the ingress receiving ports on the W-ClearPass server:

1. Navigate to **Administration > Server Manager > Server Configuration**.
2. From the list of W-ClearPass servers, select the appropriate server.
The Server Configuration page appears.
3. Select the **Service Parameters** tab.
4. From the **Select Service** drop-down, choose **Ingress syslog service** as shown in [Figure 682](#).

Figure 682: *Selecting the Ingress Syslog Service*

Administration » Server Manager » Server Configuration - VM-6-54
Server Configuration - VM-6-54 (.54)

System	Services Control	Service Parameters	System Monitoring	Network	FIPS
Select Service: Ingress syslog service ▼					
Parameter Name		Parameter Value			
Syslog Configuration		Default Value			
Allowed Values					
TCP Port	Ingress syslog service	514	514	1-65535	
UDP Port	Policy server	514	514	1-65535	
	Radius server				
	Stats collection service				
	System monitor service				
	Tacacs server				

As you can see in [Figure 682](#), the parameter value for both the TCP and UDP receiving ports is set to the default value of **514**.

5. If you wish to modify the parameter values for one or both of the receiving ports, enter the new value(s).
6. When satisfied with the settings, click **Save**.

Configuring an Event-Based Enforcement Service

This section provides the following information:

- [Introduction](#)
- [Adding an Event-Based Enforcement Service](#)
- [Associating the Enforcement Service with an Enforcement Policy](#)

Introduction

This section describes how to add the **Event-Based Enforcement** service that manages enforcement actions in response to threat-event processing.

When there is a suspicious user, this user could represent a common DOS attack or some other threat. When a threat is detected, W-ClearPass performs enforcement operations as configured, for example, executing a change of authorization (COA) to disconnect a suspicious user from the network.

Adding an Event-Based Enforcement Service

To add an event-based enforcement service:

1. Navigate to **Configuration > Services**.

The **Services** page opens. The **Services** page provides options to add, modify, and remove a service.

2. To add the event-based enforcement service, click **Add**.

The **Add Services** dialog opens.

3. From the **Type** drop-down list, select **Event-based Enforcement** (see [Figure 683](#)).

Figure 683: Specifying Event-Based Enforcement

Configuration » Services » Add

Services

Enforcement policy "Event-based enforcement policy" has been added

Service Enforcement Summary

Type: Event-based Enforcement

Name: Event-based Enforcement Service

Description: Service for ingress events based enforcement

Monitor Mode: ☒ Enable to monitor network access without enforcement

More Options:

Service Rule

Matches ☐ ANY or ☒ ALL of the following conditions:

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

For configuration information for each of the available service types, see [Policy Manager Service Types on page 70](#).

4. Enter the name or label of the event-based enforcement service.
5. Enter the values for any other parameters, including service rules, required for this service.
For a description of all the parameters in the **Service** page, see [Adding Services on page 1](#).
6. Click **Next**.

The **Add Services > Enforcement** tab opens.

Associating the Enforcement Service with an Enforcement Policy

After you create the event-based enforcement service, you must associate the service with an enforcement policy.

To associate an event-based enforcement server with an enforcement policy:

1. When finished with the parameter settings on the **Add Services > Service** page, click **Next**.

The **Add Services > Enforcement** page opens.

Figure 684: Specifying the Event-Based Enforcement Policy

Configuration » Services » Add

Services

Enforcement policy "Event-based enforcement policy" has been added

Service Enforcement Summary

Use Cached Results: ☐ Use cached Roles and Posture attributes from previous sessions

Enforcement Policy: Event-based enforcement policy [Modify](#)

Enforcement Policy Details

Description:

Default Profile: [HPE Bounce Host-Port]

Rules Evaluation Algorithm: first-applicable

Conditions	Enforcement Profiles
1. (Date:Day-of-Week BELONGS_TO Wednesday)	[HPE Bounce Host-Port]

From the **Add Services > Enforcement** page, you can either select an existing enforcement policy or create a new one.

2. From the **Enforcement Policy** drop-down list, select the appropriate Event Enforcement policy.
3. If you have not configured Event-type Enforcement policies, click **Add New Enforcement Policy** to create a new enforcement policy.
4. Specify the values for the remaining parameters as described in [Table 368](#), then click **Save**.

Table 368: Service Enforcement Page Parameters

Parameter	Description
Use Cached Results	1. Select this check box to use cached roles and posture attributes from previous sessions.
Enforcement Policy	2. From the drop-down list, select the preconfigured enforcement policy. This is mandatory.
Enforcement Policy Details	
Description	Displays additional information about the selected enforcement policy.
Default Profile	Displays a default profile applied by .
Rules Evaluation Algorithm	Shows first matched rule and return the role or select all matched rules and return a set of roles.

Enabling Ingress Events Processing

The final task is to enable ingress events processing.

To enable ingress events processing on the W-ClearPass server:

1. Navigate to **Administration > Server Manager > Server Configuration**.
2. From the list of W-ClearPass servers, select the appropriate server.
The Server Configuration page appears.
3. Select the appropriate server.
The Server Configuration dialog appears.

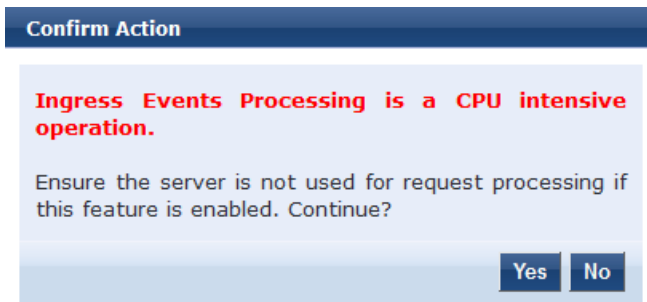
Figure 685: Enabling Ingress Event Processing

The screenshot shows the 'Service Parameters' tab of the Server Configuration dialog. The 'Enable Ingress Events Processing' checkbox is checked and highlighted with a red box. Other visible settings include Hostname: manisha-183, FQDN: (empty), Policy Manager Zone: default, and various other checkboxes for enabling features like endpoint classification, performance monitoring, and insight.

4. Click the **Enable Ingress Events Processing** check box.

The following warning dialog is displayed, alerting you to the impact on system performance that may occur when you enable ingress events processing.

Figure 686: *Warning Dialog for Enabling Ingress Events Processing*



5. To proceed with ingress events processing on this server, click **Yes**.
For details on the **Server Configuration > System Tab** parameters, see [System Tab on page 462](#).

This chapter describes how to use the W-ClearPass 6.6 Insight Reporting tool.

This chapter includes the following information:

- [About W-ClearPass Insight](#)
- [About the Insight Dashboard](#)
- [Searching the Insight Database](#)
- [Creating Alerts](#)
- [Creating Reports](#)
- [Insight Report Categories Reference](#)
- [Administration Operations](#)
- [Managing Insight Admin Privileges](#)

About W-ClearPass Insight

This section presents an overview of W-ClearPass Insight. It provides the following information:

- [Introduction](#)
- [Enabling Insight and Specifying a Master Insight Node](#)
- [Launching Insight](#)

Introduction

W-ClearPass Insight is an application for use with W-ClearPass Policy Manager that is capable of aggregating data from multiple W-Policy Manager appliances that contain archived network access logs.

You can access each application within the W-ClearPass suite with a single login. You need only sign in once for access to W-ClearPass W-Policy Manager, Insight, Onboard, and Guest. For more information, see [Launching Insight](#) below.

- Insight makes it easy to add many different types of report "widgets" that will produce reports that provide the specific kinds of information you need to monitor and understand what is occurring on the network. You can create customized reports to track detailed authentication records, audit trails, and details on network-access trends (see [About the Insight Dashboard on page 688](#)).
- The Insight Search feature allows you to search for clients, users, W-ClearPass servers, and network access devices (see [Searching the Insight Database on page 698](#)).
- This chapter illustrates how to generate customized reports that analyze authentication information, device profiling, client health and posture data, as well as guest and BYOD use cases (for details, see [Creating Reports on page 706](#) and [Insight Report Categories Reference on page 713](#)).
- This chapter also describes how to configure alerts that allow you to receive near-real-time messages regarding anomalous network activity. Alerts can be delivered via SMS or email notification to multiple recipients.

You can also set up a User Watchlist (a list of VIPs, executives or devices that warrant special tracking) that you can monitor for authentication failures or other key events (see [Creating Alerts on page 699](#)).

- Finally, this chapter provides information on how to configure operational elements about file transfers, as well as database and report data retention (see [Administration Operations on page 727](#)).

Browsers Supported

W-ClearPass Insight uses a Web-based management interface. The following browsers are supported:

- Apple Safari 6.2.x, 7.1.x, 8.0
- Google Chrome 47.x, 48.x
- Microsoft Edge 25.x
- Microsoft Internet Explorer 11.0
- Mozilla Firefox 43, 44

Enabling Insight and Specifying a Master Insight Node

Before you can use Insight, you must enable it on the current W-ClearPass server.

If multiple nodes in a cluster have Insight enabled, one node should be configured as an Insight Master.



Insight Reports, Alerts, and Administration settings can be configured on a Master Insight node only. To be able to generate a report, enabling the node as an Insight Master (even in a single-node cluster) is mandatory.

To enable Insight :

1. Navigate to **Administration > Server Manager > Server Configuration**.
2. From the list of W-ClearPass servers, click the server on which you want to enable Insight.
The **Server Configuration > System** page opens.

Figure 687: *Server Configuration > System Page*

Administration » Server Manager » Server Configuration - NIGHTLY-CPPM-31
Server Configuration - NIGHTLY-CPPM-31 (10.2.51.31)

System Services Control Service Parameters System Monitoring Network FIPS

Hostname: NIGHTLY-CPPM-31
FQDN:
Policy Manager Zone: default [Manage Policy Manager Zones](#)
Enable Profile: ☒ Enable this server for endpoint classification
Enable Performance Monitoring Display: ☒ Enable this server for performance monitoring display
Insight Setting: ☒ Enable Insight ☒ Enable as Insight Master Current Master: NIGHTLY-CPPM-31(10.2.51.31)
Enable Ingress Events Processing: ☒ Enable Ingress Events processing on this server
Span Port: -- None --

	IPv4	IPv6	Action
Management Port	IP Address	10.2.51.31	Configure
	Subnet Mask	255.255.255.0	
	Default Gateway	10.2.51.1	
Data/External Port	IP Address		Configure
	Subnet Mask		
	Default Gateway		
DNS Settings	Primary	10.2.51.18	Configure
	Secondary		
	Tertiary		

AD Domains: [Join AD Domain](#)

Domain Controller	NetBIOS Name	Password Servers	Action
1. CPATS.AVENDASYS.COM	CPATS	-	Leave AD Domain

3. Insight Setting:

- a. **Enable Insight:** Select this check box to enable W-ClearPass Insight on the current server.
- b. **Enable as Insight Master:** Select this check box to specify this server as an Insight Master.



To enable replication of Insight configurations across a cluster, you must configure one W-ClearPass server in the cluster as an Insight Master node.

4. Click **Save**.

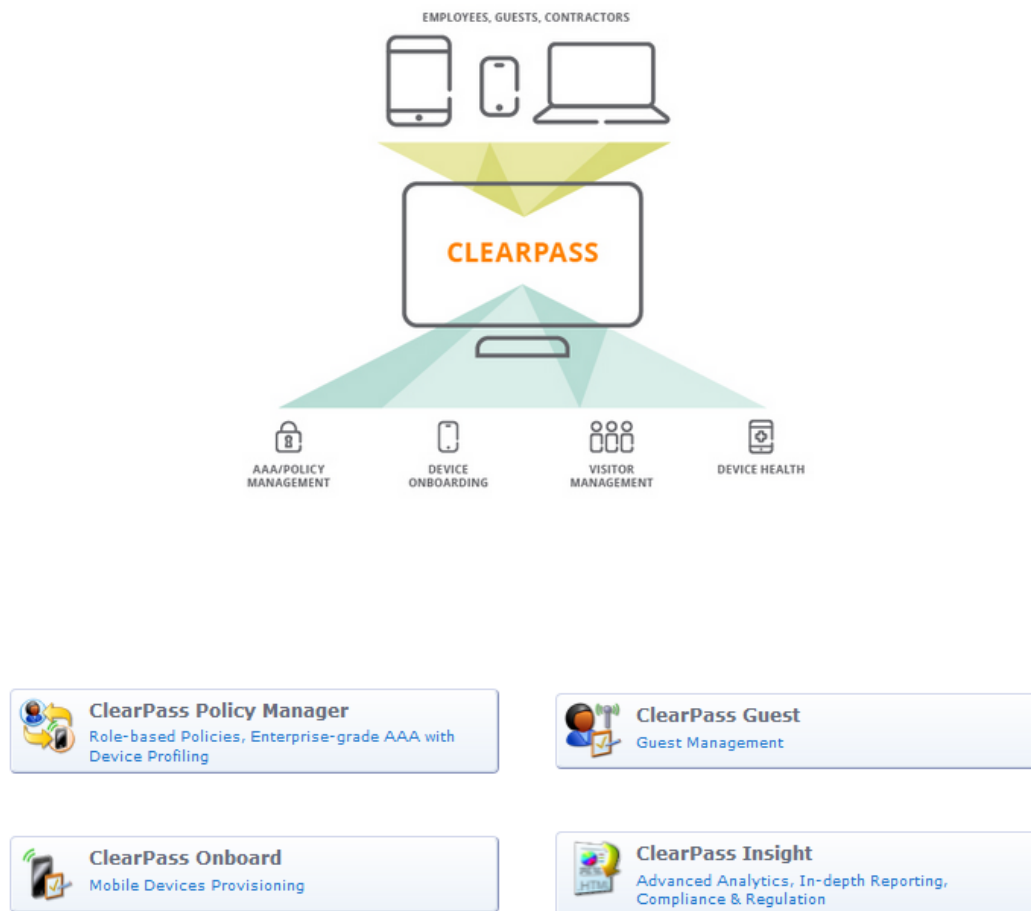
Launching Insight

To launch W-ClearPass Insight:

1. Use one of the following methods to launch W-ClearPass Insight.
 - Log in to W-Policy Manager, and then select **Insight** in the **Dashboard > Applications** widget. This opens Insight in a new tab.
 - Access W-Policy Manager by pointing the browser to <https://<W-ClearPass-host-name>/tips>, then select the **ClearPass Insight** link (see Figure 688).
 - Point the browser to <https://<W-ClearPass-host-name>/insight>.
2. Enter the default username and password, then click **Login** to launch Insight.

Figure 688 displays the W-ClearPass Access page:

Figure 688: W-ClearPass Access Page



About the Insight Dashboard

This section provides the following information:

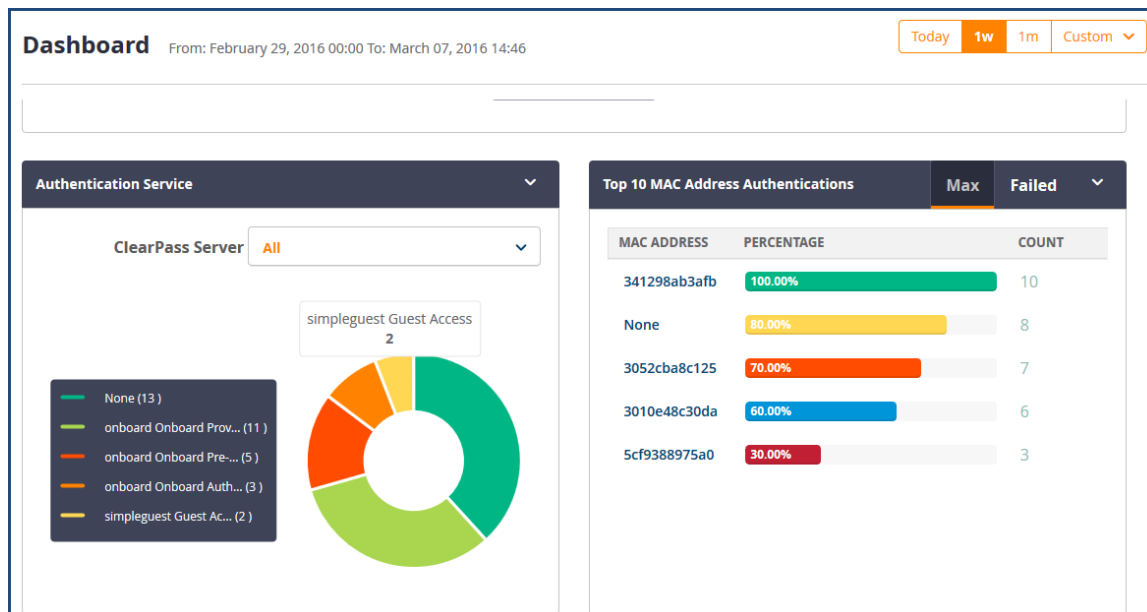
- [Dashboard Overview](#)
- [Adding a Report Widget to the Dashboard Landing Page](#)
- [Removing a Report Widget from the Dashboard Landing Page](#)
- [Creating a Report or Alert From the Dashboard](#)
- [Specifying the Date Range for Data Collection](#)
- [Authentication Dashboard](#)
- [Endpoints Dashboard](#)
- [Guest Dashboard](#)
- [Network Dashboard](#)
- [Posture Dashboard](#)
- [System Dashboard](#)
- [System Monitor Dashboard](#)

Dashboard Overview

The **Dashboard Landing Page** opens immediately when you successfully log in to W-ClearPass Insight. The Dashboard includes report widgets that provide a summarized and graphical view of your network analytics.

- You can customize the Dashboard to display the report widgets that you use most often by adding widgets to the Dashboard Landing Page; you can also remove any report widget from the Dashboard Landing Page as needed.
- You can create reports and alerts from any of the Dashboard pages.

Figure 689: *Insight Dashboard Landing Page*



The following report widgets are included by default on the **Dashboard Landing** page:

- Authentication Trend
- Authentication Distribution
- Authentication Service

- Top 10 MAC Address Authentications

Adding a Report Widget to the Dashboard Landing Page

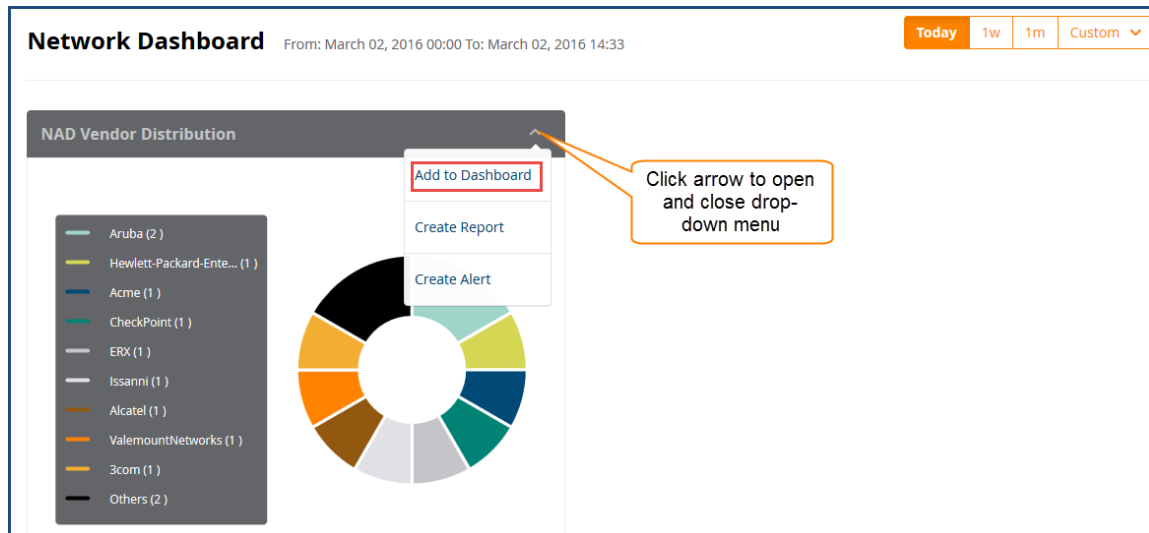
When you add a report widget to the Dashboard Landing page, that widget will appear in the Landing page, and the widget will also continue to be available on its Dashboard category page (for example, if you added the **Top 10 Restarted Services** widget from the System Dashboard, the **Top 10 Restarted Services** widget would be present in both the Dashboard Landing page and the System Dashboard).

To add a report widget to the Dashboard Landing page:

1. From any of the Dashboard category pages, click the arrow icon in the right corner of the widget title bar.
2. Select **Add to Dashboard** (see Figure 690).

That report widget will appear when you return to the Dashboard Landing page.

Figure 690: Adding a Widget to the Dashboard Landing Page



3. To view the newly-added widget, return to the Dashboard Landing page.

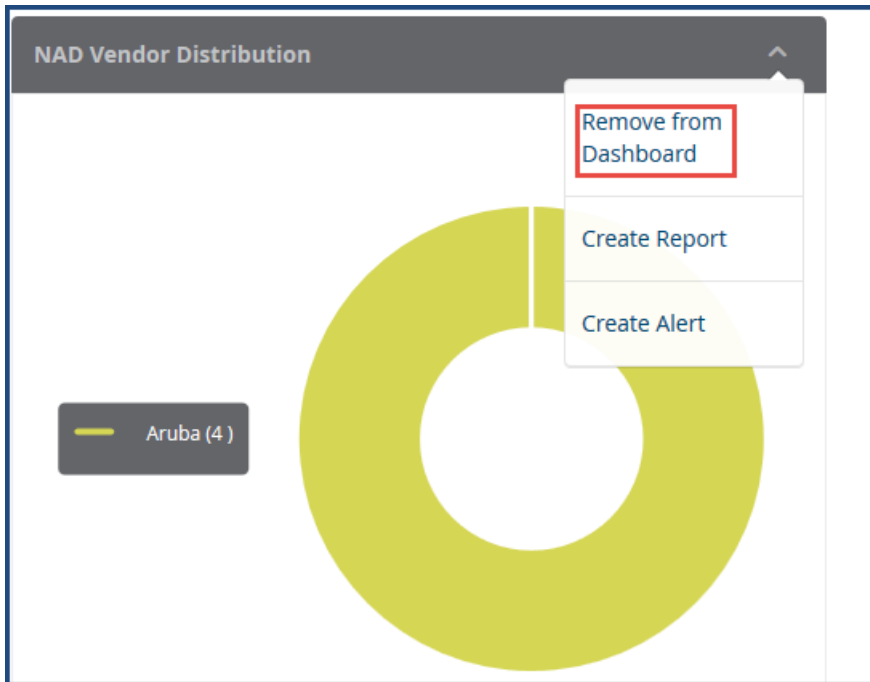
Removing a Report Widget from the Dashboard Landing Page

You can only remove a report widget from the **Dashboard Landing Page**. Report widgets cannot be deleted from Dashboard category pages (for example, if you choose to remove the Top 10 MAC Address Authentications widget from the Landing page, it will remain in the set of report widgets provided in the Authentication Dashboard).

To remove a report widget from the Dashboard Landing page:

1. From the **Dashboard Landing Page**, locate the widget you want to remove.
2. Click the arrow icon in the right corner of the widget title bar.
3. From the menu, select **Remove from Dashboard** (see Figure 691).

Figure 691: *Removing a Widget From the Dashboard*



When you refresh the page, that widget will disappear from the Dashboard.

Creating a Report or Alert From the Dashboard

The widgets on the **Dashboard** include links to the **Creat Reports** and **Create Alerts** pages.

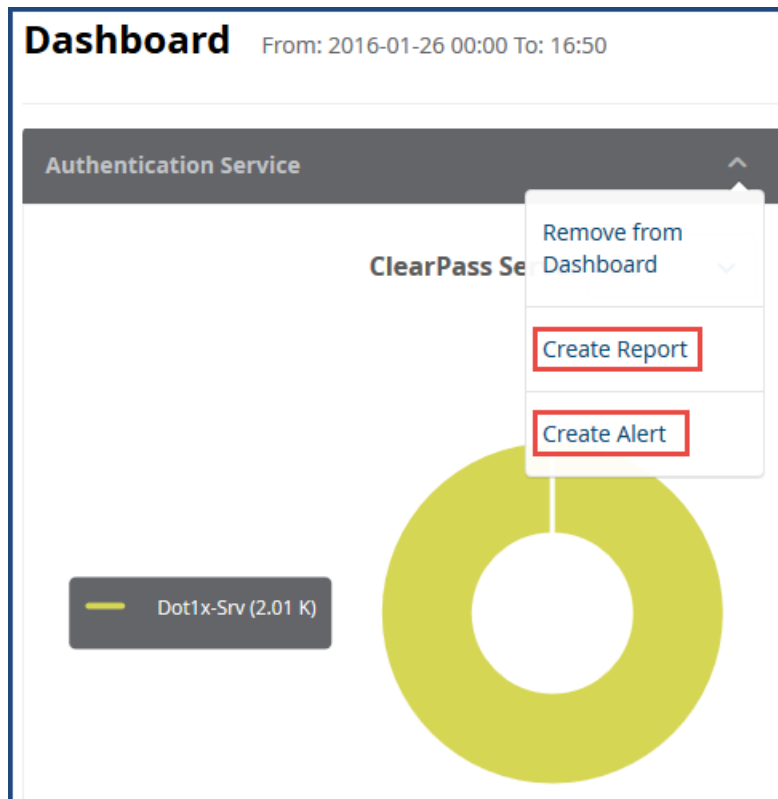
To define and to receive a regular report of data for that Dashboard:

- To open the **Create Reports** wizard from the Dashboard, click the down-arrow icon in the widget title bar and select **Create Report**.

To define and to receive alerts when customized thresholds are reached:

- To open the **Creat Alerts** wizard from the Dashboard, click the down-arrow icon in the widget title bar and select **Create Alert**.

Figure 692: Opening the Reports or Alerts Wizard from the Dashboard



For detailed procedures to create reports and alerts, see [Creating Reports on page 706](#) and [Creating Alerts on page 699](#).

Specifying the Date Range for Data Collection

By default, the Insight widgets, including those on the **Dashboard** page as well as all the other Insight widgets, such as Endpoints, Guest, Posture, and so on, display information collected over the previous seven days. The **System Monitor** widget is an exception as it displays data for the previous two hours.

You can modify the Authentication, Endpoints, Guest, Posture, and System widgets to display widget data for today, one week, one month, or a custom date and time range.

To specify the date range to have data collected for a Dashboard widget:

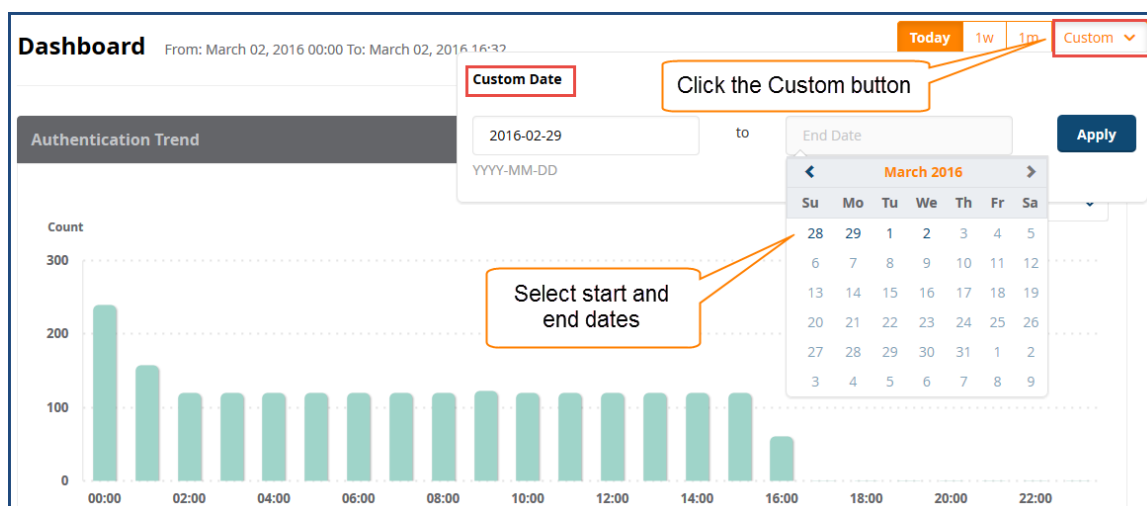
1. To specify data collection for today, one week, or one month, from the upper right corner of the Dashboard, select **Today**, **1w** (for one week), or **1m** (for one month) as desired.

The Dashboard widgets then display the information for the specified number of days.

2. To specify a customized period for Insight data collection, click the **Custom** button.

You are prompted to specify the start and end dates for your date range, as shown in [Figure 693](#).

Figure 693: Specifying a Custom Date Range



3. Select the **Start Date** and **End Date** from the calendar, then click **Apply**.

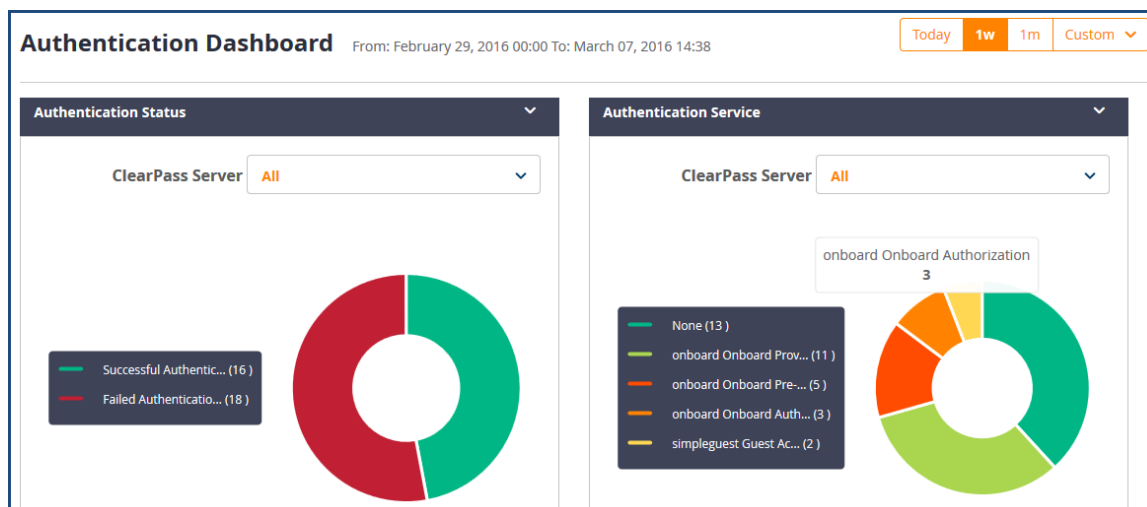
The Dashboard widgets then display the information for the specified range of dates.

Authentication Dashboard

Authentication Dashboard widgets focus on authentication analytics and include widgets on trends, distribution, status, service, alerts, and statistics.

To access the Authentication Dashboard, navigate to **Dashboard > Authentication**.

Figure 694: Authentication Dashboard



The following widgets are included by default on the **Authentication Dashboard**:

- Authentication Trend
- Authentication Distribution
- Authentication Service
- Authentication Status
- Top 10 MAC Address Authentications
- Top 20 NAD Authentications
- Top 10 Authentication Errors
- Latest 10 Authentication Alerts

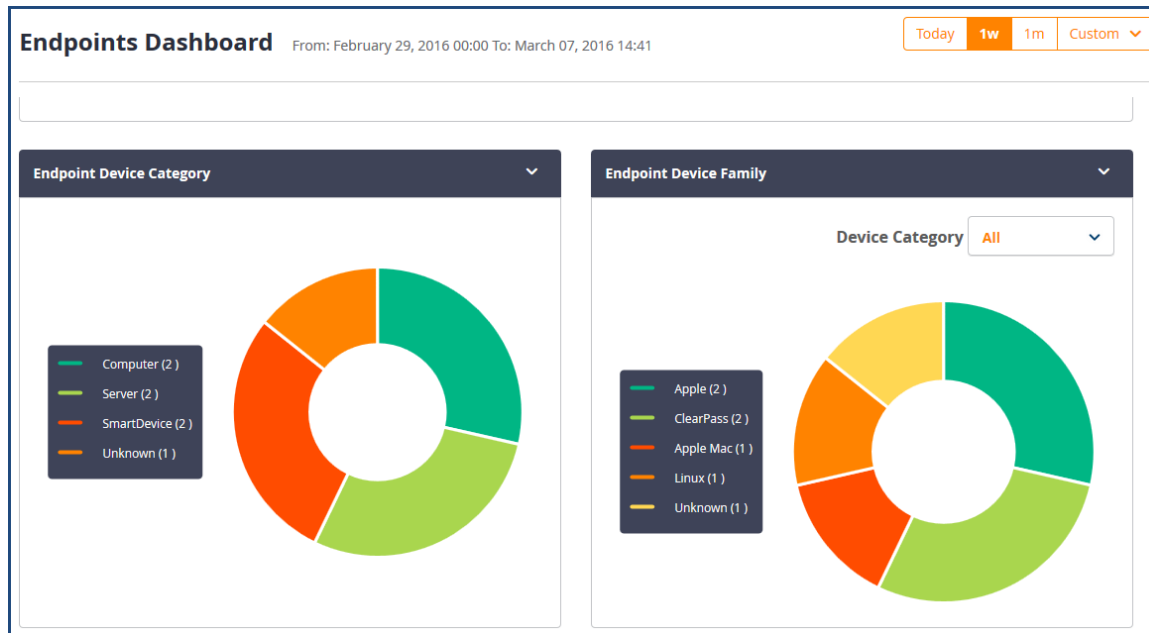
For more information about the Authentication reports and the widgets provided for each report, see [Authentication Category Reports on page 714](#).

Endpoints Dashboard

The Endpoints Dashboard widgets provide analytics that focus on Endpoint trends, distribution, device profile, and bandwidth usage.

To access the Authentication Dashboard, navigate to **Dashboard > Endpoints**.

Figure 695: *Endpoints Dashboard*



The following widgets are included by default on the **Endpoints Dashboard**:

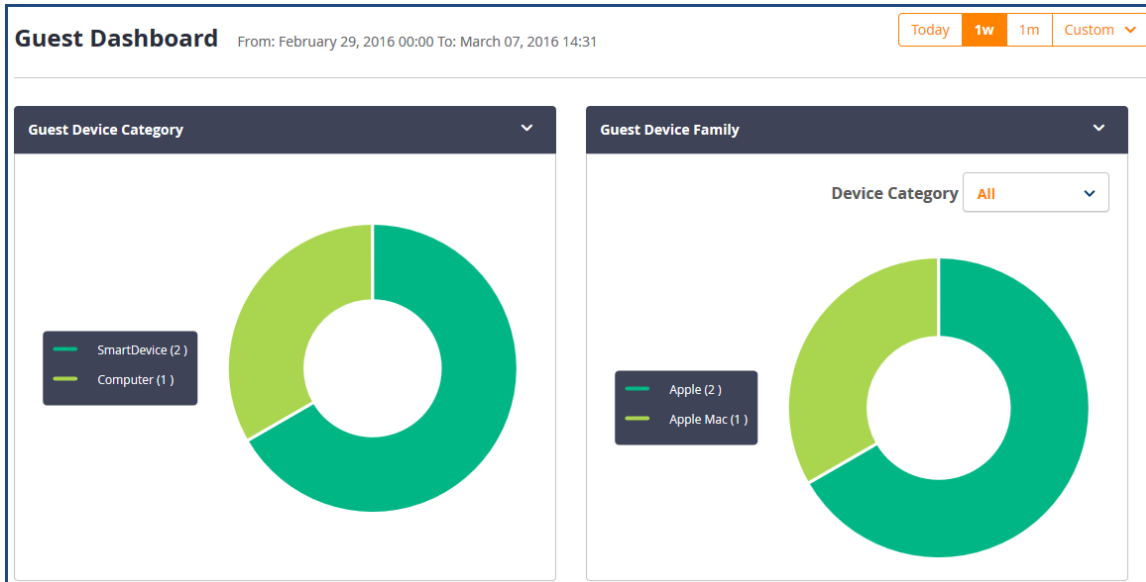
- Endpoint Unique Trend
- Endpoint Device Profiling
- Endpoint Device Category
- Endpoint Device Family
- Endpoint Device Name
- Top 20 Bandwidth Users

For more information about the Endpoints reports and the widgets provided for each report, see [Endpoint Category Reports on page 717](#).

Guest Dashboard

To access the Guest Dashboard, navigate to **Dashboard > Guest**.

Figure 696: *Guest Dashboard*



The following widgets are included by default on the **Guest Dashboard**:

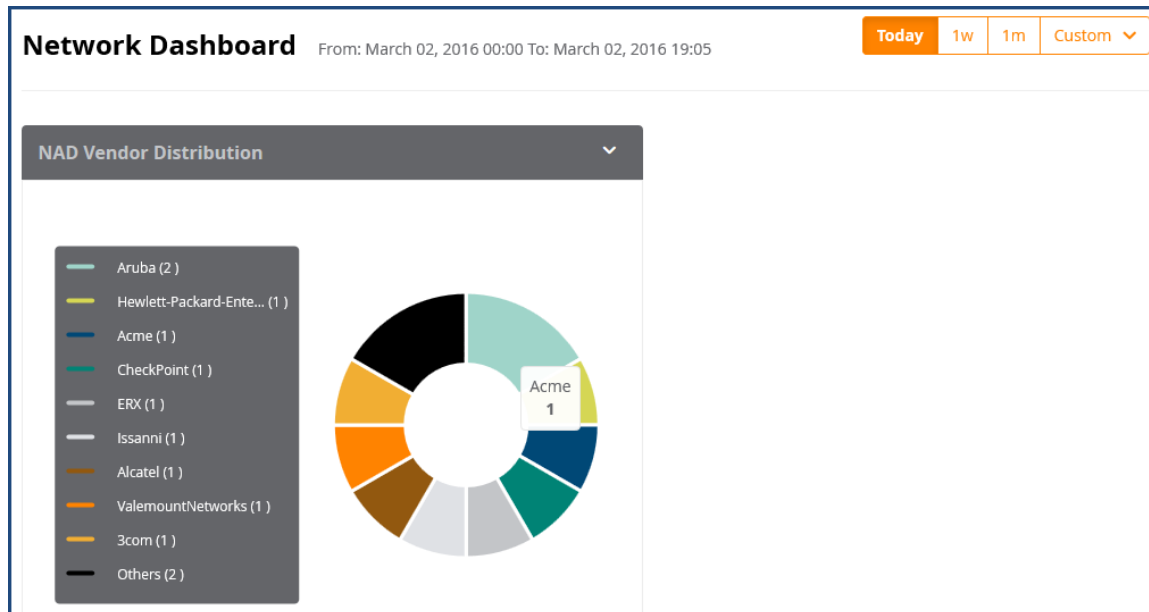
- Guests Authentication Trend
- Unique Guest Authentication
- Guests Provisioned
- Guest Device Category
- Guest Device Family
- Guest Device Name
- Top 20 Bandwidth Guest Users

For more information about the Guest reports and the widgets provided for each report, see [Guest Authentication Category Reports on page 718](#).

Network Dashboard

To access the Network Dashboard, navigate to **Dashboard > Network**.

Figure 697: *Network Dashboard: NAD Vendor Distribution*



The following widget is included on the **Network Dashboard**:

- NAD Vendor Distribution

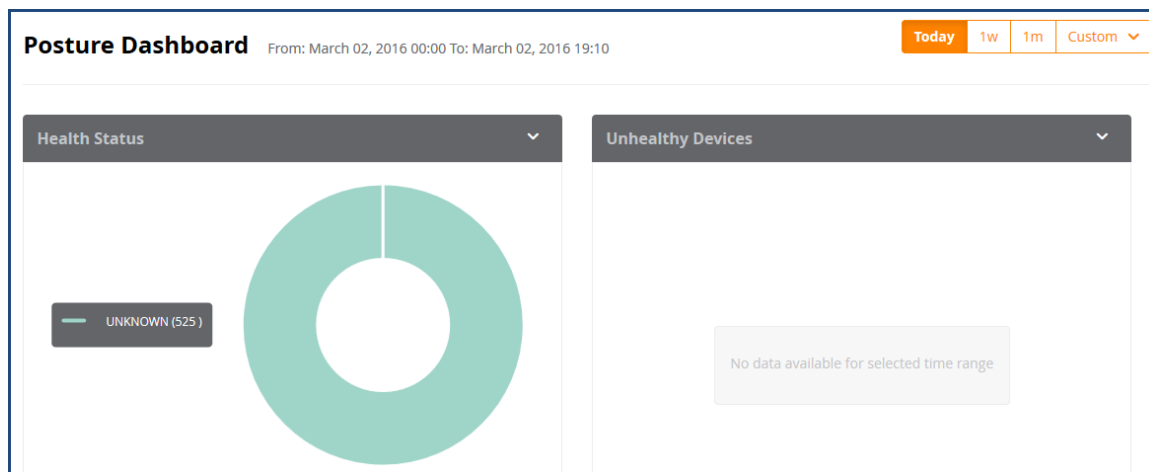
This widget displays the list of all the NAD (Network Access Device) vendors, including the number of NADs by each vendor. Each vendor is associated with a unique color, and those colors are reflected in the circle graph that displays the distribution percentage each NAD vendor represents.

For more information about the Network reports, see [Network Category Reports on page 720](#).

Posture Dashboard

The Posture Dashboard widgets focus on device health status and device profiles. To access the Posture Dashboard, navigate to **Dashboard > Posture**.

Figure 698: *Posture Dashboard*



The following widgets are included by default on the **Posture Dashboard**:

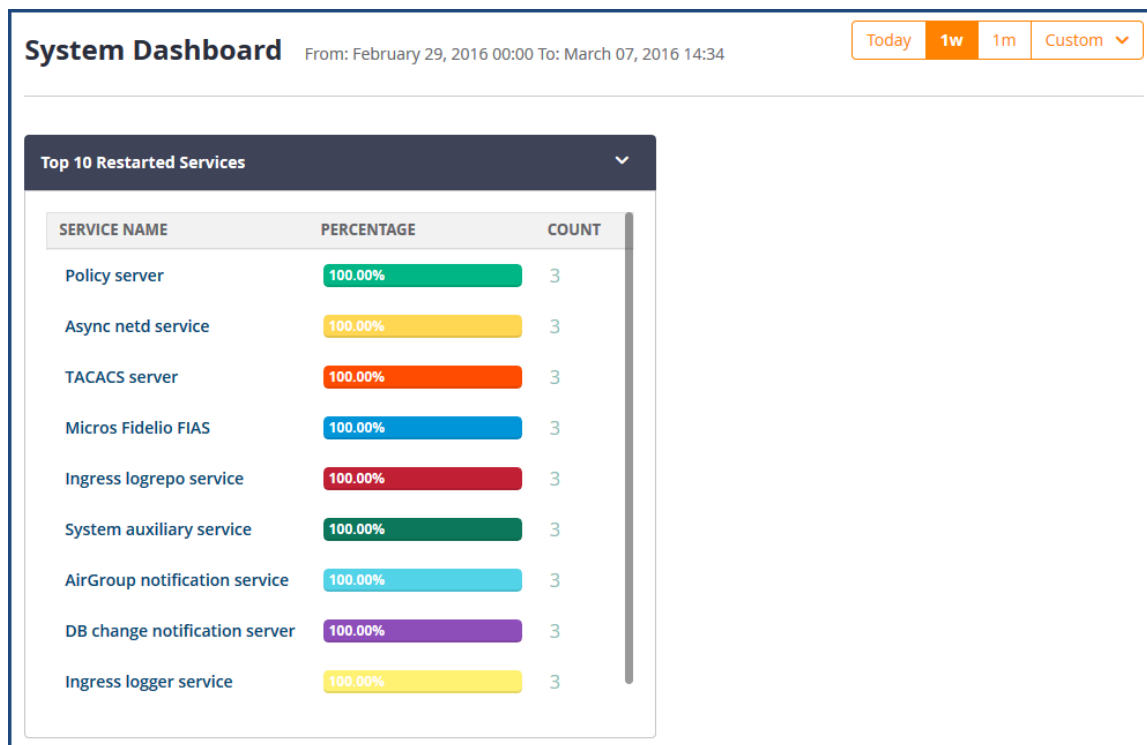
- Health Status
- Unhealthy Devices

For more information about the Posture-related reports, see [OnGuard Category Reports on page 721](#).

System Dashboard

To access the System Dashboard, navigate to **Dashboard > System**.

Figure 699: *System Dashboard*



The following widgets are included by default on the **System Dashboard**:

- Cluster-Wide License Summary
- W-Policy Manager License Usage
- Guest License Usage Trend
- Top 10 Restarted Services

For more information about the System-related reports, see [System Category Reports on page 726](#).

System Monitor Dashboard

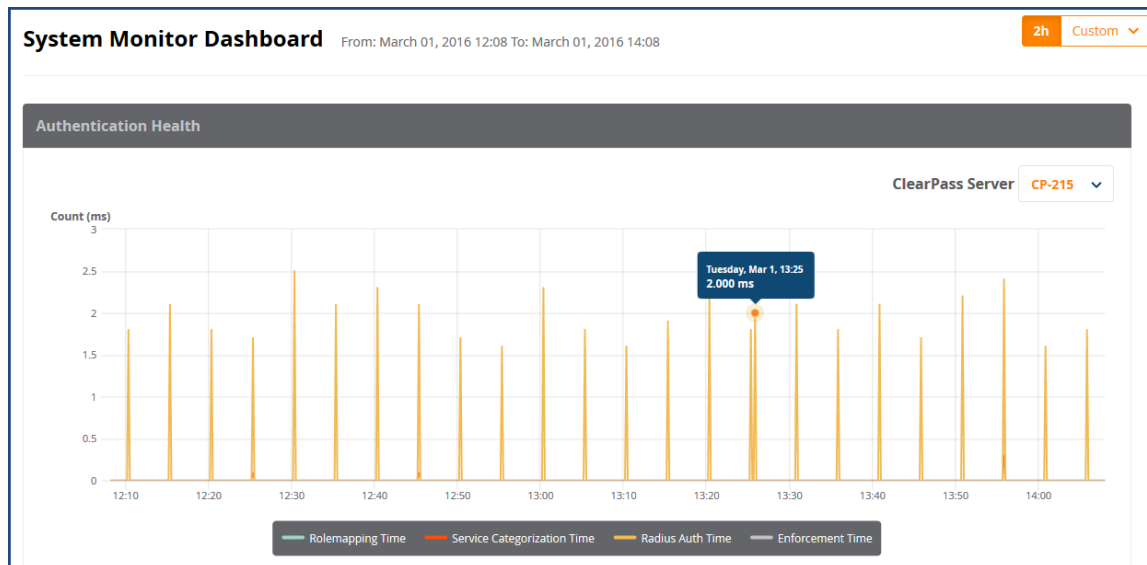
The System Monitor Dashboard widgets focus on health, including Authentication health, processing time, and CPU, memory, and disk usage.



You cannot pin System Monitor widgets to the Dashboard.

To access the System Monitor Dashboard, navigate to **Dashboard > System Monitor**.

Figure 700: System Monitor Dashboard



The following widgets are included by default on the **System Monitor Dashboard**:

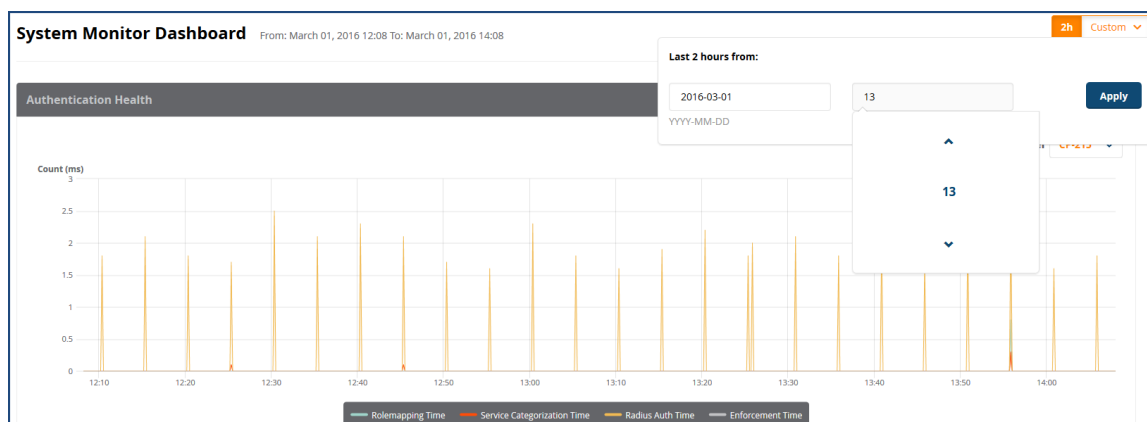
- Authentication Health
- End-to-End Request Processing Time
- Memory Usage
- Swap Memory Usage
- Disk Usage
- CPU Usage
- CPU Load

The **System Monitor** Dashboard differs from the other Dashboard pages in that it can show data for two hours only (**2h**).

To define a custom two-hour time slot:

1. Click the **Custom** drop-down list.

Figure 701: Specifying the Hour to Start System Monitor Scan



2. Select the starting date.
3. Click the **HH** field, then use the up- and down-arrows to specify the hour to start the system monitor scan.
For example, specifying **13** in the **HH** field indicates that the start time for the two-hour period is **1:00 p.m.**
4. Click **Apply**.

Searching the Insight Database

This section provides the following information:

- [About Insight Search](#)
- [Search Example](#)

About Insight Search

Use the **Insight Search** feature to query the Insight database.

You can search for the following entities:

- Clients by MAC address, hostname, or IP address
- Usernames
- W-ClearPass servers by name or IP address
- Network access devices by name or IP address

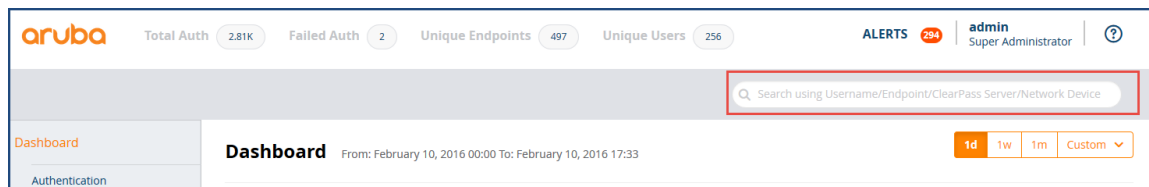
You can add clients and users to the Watchlist from Search results. For details, see [Adding or Removing Users from the Watchlist on page 704](#).

The Insight Search window is always available at the top of every page.



Search works on all pages except the Report Configuration and Alert Configuration pages.

Figure 702: Search Window



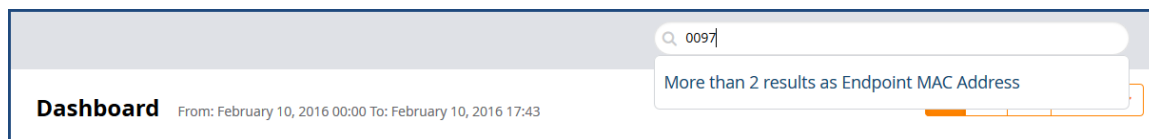
Search Example

Let's take the example of searching for a MAC address:

1. Start entering the MAC address into the Search window.

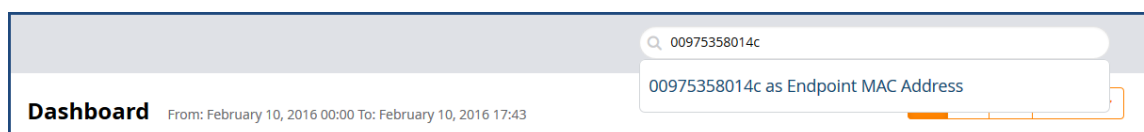
As you type in the MAC address in this example, Search discovers that there are two MAC addresses with the same initial characters:

Figure 703: Search Locating Matching Entities



2. To locate the desired MAC address:
 - a. Click on the suggestion and see which MAC address you are looking for from the list displayed.
 - b. Or refine your search by typing more characters to further specify the search entity.In this example, the MAC address is identified as an Endpoint.

Figure 704: *Locating and Identifying the Search Object*

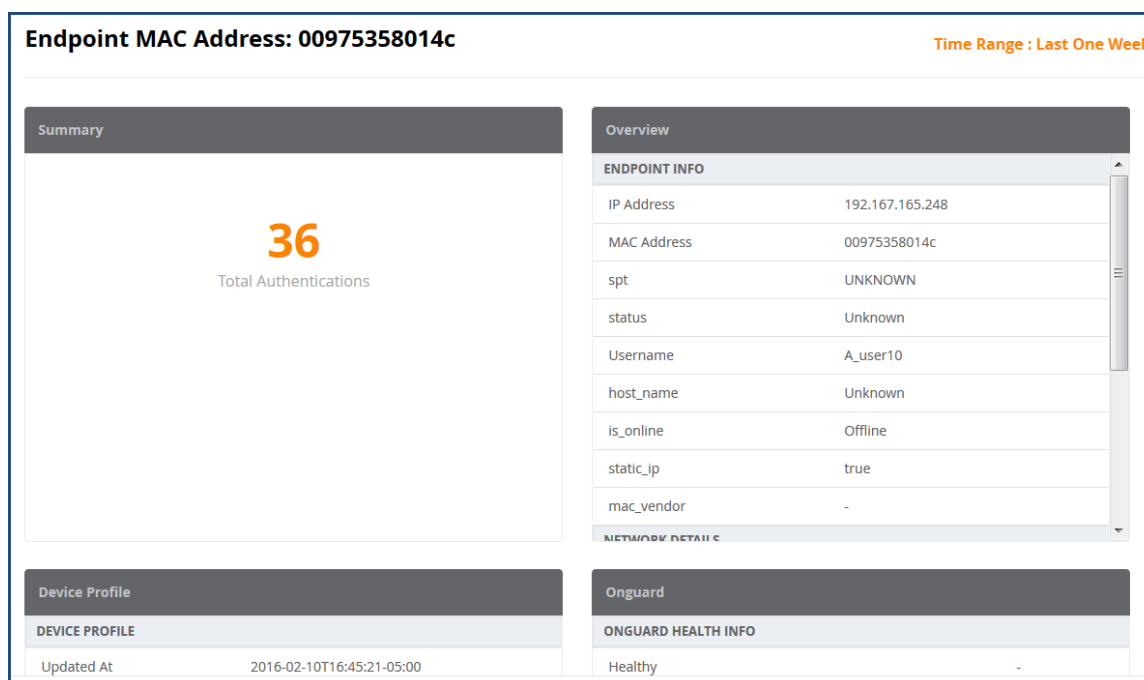


3. Select the search object.

The Endpoint MAC Address report is automatically displayed (see [Figure 705](#)). It includes the following information about the Endpoint:

- Summary
- Overview
- Device Profile
- OnGuard Health Information
- Authentication Status Trend

Figure 705: *Report of Search Result*



Creating Alerts

This section provides the following information:

- [Introduction](#)
- [Creating New Alerts](#)
- [Modifying the User Watchlist](#)
- [Adding or Removing Users from the Watchlist](#)

Introduction

Alerts provide network managers with near-real-time messages on anomalous network activity. Such activity could consist of:

- Irregular authentication activity

- Irregular network device access activity
- Users attempting privileged commands on network devices
- Irregular activity on the W-ClearPass servers

Reports and alerts include templates for easy configuration. These templates allow you to quickly configure and monitor network activity. In addition to email notifications, you can also send alerts to mobile devices via SMS, providing the capability to receive mission-critical information on the go.



Any Error-level System Event/Event Viewer entries in W-ClearPass servers are notified with a System Alert Notification.

Creating New Alerts

To create a new alert:

1. Navigate to the **Alerts** page.

Figure 706: Alerts Configuration Page

The screenshot shows the 'Alerts Configuration' page. On the left is a sidebar with navigation links: Dashboard, Reports, Alerts, Configuration (highlighted), Watchlist, and Administration. The main content area is titled 'Alerts Configuration' and has a 'Create New Alert' button in the top right. Below the title is a 'Configuration' tab. Under this tab is a section 'MY CONFIGURED ALERTS' which contains a table with columns: #, NAME, TEMPLATE, DESCRIPTION, NOTIFICATION, ENABLE, and MUTE. There is one row for 'User WatchList'. At the bottom of the table are controls for 'per page' (set to 5), a severity filter (set to Critical), and a 'Page: 1' indicator with 'Go' and navigation buttons.

- **Enable** button: From the switch, you can enable or disable the selected alert.
- **Mute** button: Allows you to mute alert output while you work to address the alert.

2. Click **Create New Alert**.

Figure 707: Creating a New Alert

The screenshot shows the 'Create New Alert' form. It has a header 'Create New Alert' and a sub-header 'Create New Alert'. The form is divided into three main sections: 'Settings', 'Category', and 'Notifications'. The 'Settings' section includes 'Alert Name' (with a 'Name' input field) and 'Description' (with a 'Description' input field). The 'Category' section has a 'Category' dropdown set to 'Authentication' and two radio buttons: 'Failed Authentication' and 'Total Authentication'. The 'Notifications' section has two checkboxes: 'Notify by Email' and 'Notify by SMS'. Below these are two large text areas for email and SMS templates. A red note at the bottom says 'Configure Messaging Setup in Policy Manager to enable Notifications'. At the bottom of the form is a 'Trigger' section with 'Severity' (set to Critical), 'Threshold' (set to #), 'Interval' (set to #), and 'Minutes' (set to Minutes). There is also an 'Alert Summary' link at the bottom left.

3. Enter the information for each Alert parameter as described in [Table 369](#).

Table 369: *Create New Alert Parameters*

Alert Field	Action/Description
Alert Name	1. Enter the name of the alert.
Description	2. Optionally, enter a summary description of the alert.
Category	3. Select the alert Category , then specify the desired alert type in the selected category: ■ Authentication a. Failed Authentication b. Total Authentication ■ System a. TACACS Commands b. TACACS Failures
Notifications	4. Specify report notifications. ■ Notify by Email. When you select this option, enter the list of email addresses to be notified. The alert notification is sent whenever the trigger threshold is met. NOTE: Enabling Notify by Email is mandatory. ■ Notify by SMS. When you select this option, enter the phone numbers of each recipient. The alert notification is sent whenever the trigger threshold is met. NOTE: A warning message appears if you have not configured the SMTP mail server for email notifications. To do so, from the W-Policy Manager, navigate to Administration > External Servers > Messaging Setup.
Trigger Severity	5. From the Trigger Severity drop-down, select one of the following: ■ Critical ■ Warning
Trigger Threshold	6. Specify Threshold and Interval values as criteria for determining whether an alert is necessary. For example, if you specify the threshold as 25 and the interval as 15 minutes , once the threshold of 25 is met within 15 minutes, an alert is triggered.
Trigger Interval	7. Specify the Interval , then select Minutes or Hours .
Alert Summary	When you have configured the alert settings, the Alert Summary displays the settings for your review.
	8. Click Save .

Modifying the User Watchlist

A Watchlist is a list of VIPs, executives, and devices known to be problematic that are monitored for authentication failures. W-ClearPass collects all user authentication status.

When W-ClearPass finds a user defined in the Watchlist that both fails to authenticate and also matches the Watchlist triggers (severity, threshold, and interval), an alert notification is sent to the notification list via email

or to mobile devices via SMS. This allows the authentication failure to be resolved proactively before the problem is reported by the user.

The Watchlist generates an alert only when an unsuccessful authentication for a specific device occurs.

Default Watchlist Trigger Settings

The default Watchlist trigger settings are as follows:

- **Severity** = Critical
- **Threshold** = 1
- **Interval** = 30 seconds



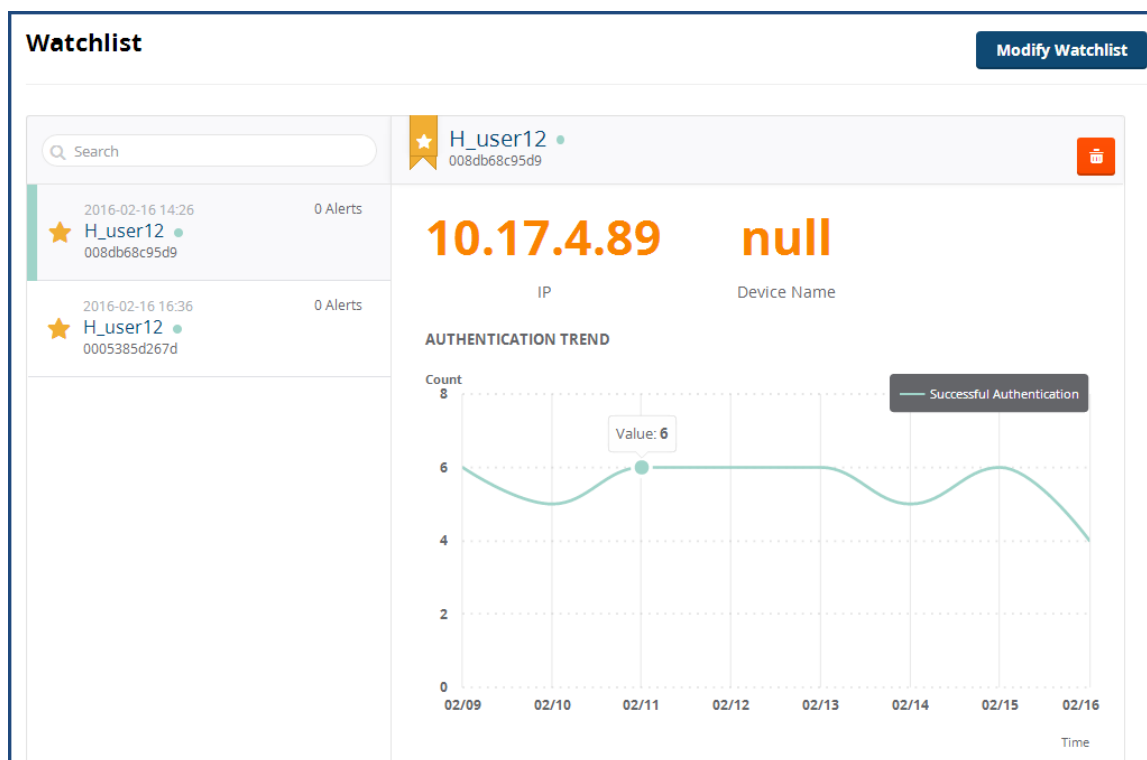
You cannot edit the The Watchlist trigger settings.

To modify the User Watchlist:

1. From the Insight navigation panel, choose **Alerts**, then select **Watchlist**.

The **User Watchlist** opens (see [Figure 708](#)).

Figure 708: *User Watchlist*



The users who are currently on the Watchlist are displayed. By default, the User Watchlist includes the **Authentication Trend** report widget.

2. Click **Modify Watchlist**.

The **Edit Alert** page appears.

Figure 709: Modifying the User Watchlist

Edit Alert

Create New Alert

Settings

Alert Name
User WatchList

Description
List of users who are monitored for authentication failures

Category
WatchList > User WatchList

Notifications

☐ Notify by Email

☐ Notify by SMS

Configure Messaging Setup in Policy Manager to enable Notifications

Filter

Username ▼

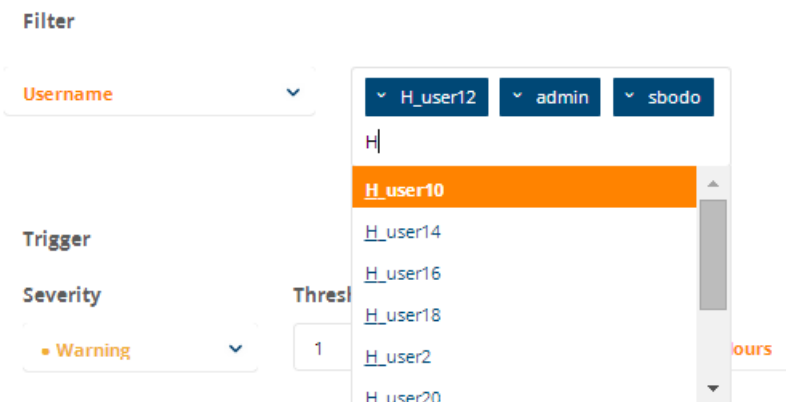
Alert Summary

3. Enter the desired settings for each **User Watchlist** parameter as described in [Table 370](#).

Table 370: Modify User Watchlist Parameters

Alert Field	Action/Description
Alert Name	1. Optionally, you can modify the name of the User Watchlist.
Description	2. Optionally (and recommended), enter a summary description of the User Watchlist.
Category	The Category is set to Alert > User Watchlist . This is not an editable field.
Notifications	3. Specify Watchlist notifications. ■ Notify by Email. When you select this option, enter the list of email addresses to be notified. The alert notification is sent whenever the threshold is met. ■ Notify by SMS. When you select this option, enter the phone numbers of each recipient. An SMS message is sent with an alert notification whenever threshold is met. NOTE: A warning message appears if you have not configured the SMTP mail server for email notifications. To do so, navigate to Administration > External Servers > Messaging Setup.
Filter: Username	The User Watchlist has only one filter: Username. 4. From the Username drop-down, select one or more users to add to the Watchlist.

Table 370: Modify User Watchlist Parameters (Continued)

Alert Field	Action/Description
	
Alert Summary	When you have configured the Watchlist settings, the Alert Summary displays the settings for your review.
Save your changes	5. Click Save .

Adding or Removing Users from the Watchlist

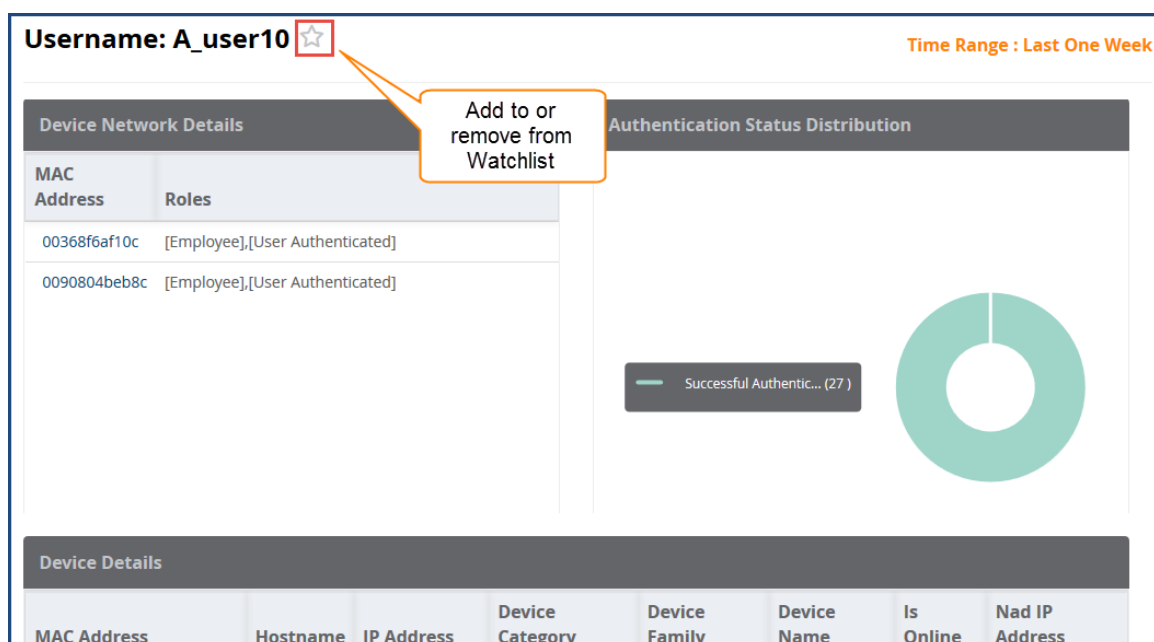
You can use the Insight Search function to add users to or remove users from the Watchlist.

Adding a User to the Watchlist

To add a user to the Watchlist:

1. In the Insight Search window, enter the name of the user.
The Insight **User Information** page for the selected user is displayed.

Figure 710: Insight User Information Page



2. To add a user to the Watchlist, click the star icon next to the username as shown in Figure 710. The **User Information** page now displays the following information:

Figure 711: User Successfully Added to Watchlist

A screenshot of the 'User Information' page for 'A_user10'. At the top, a yellow banner with an information icon states: 'A_user10 added to user watchlist successfully. Please configure sms/email notifications.' Below this, a sidebar on the left contains links for 'Dashboard', 'Reports', 'Alerts', and 'Administration'. The main content area shows the 'Username: A_user10' with an orange star icon. Underneath is a 'Device Network Details' table with two columns: 'MAC Address' and 'Roles'.

MAC Address	Roles
00368f6af10c	[Employee],[User Authenticated]
0090804beb8c	[Employee],[User Authenticated]

The star icon color is now set to orange, indicating the user has been added to the Watchlist.

The following message is displayed:

<User> added to User Watchlist successfully. Please configure SMS and email notifications.

Removing a User from the Watchlist

To remove a user from the Watchlist:

1. In the Insight Search window, enter the name of the user.
The Insight **User Information** page for the selected user opens.

Figure 712: Removing a User from the Watchlist

A screenshot of the 'User Information' page for 'A_user10'. The orange star icon next to the username is highlighted with an orange box and a callout bubble that says 'Click star icon to remove user from Watchlist'. Below the username is a 'Summary' section with two large orange numbers: '2' for 'Unique Devices' and '28.46GB' for 'Total Bandwidth'.

2. Click the orange star icon next to the username.
The user is removed from the Watchlist. The star icon is now white. You receive the following message:
<User> removed from User Watchlist successfully.

Creating Reports

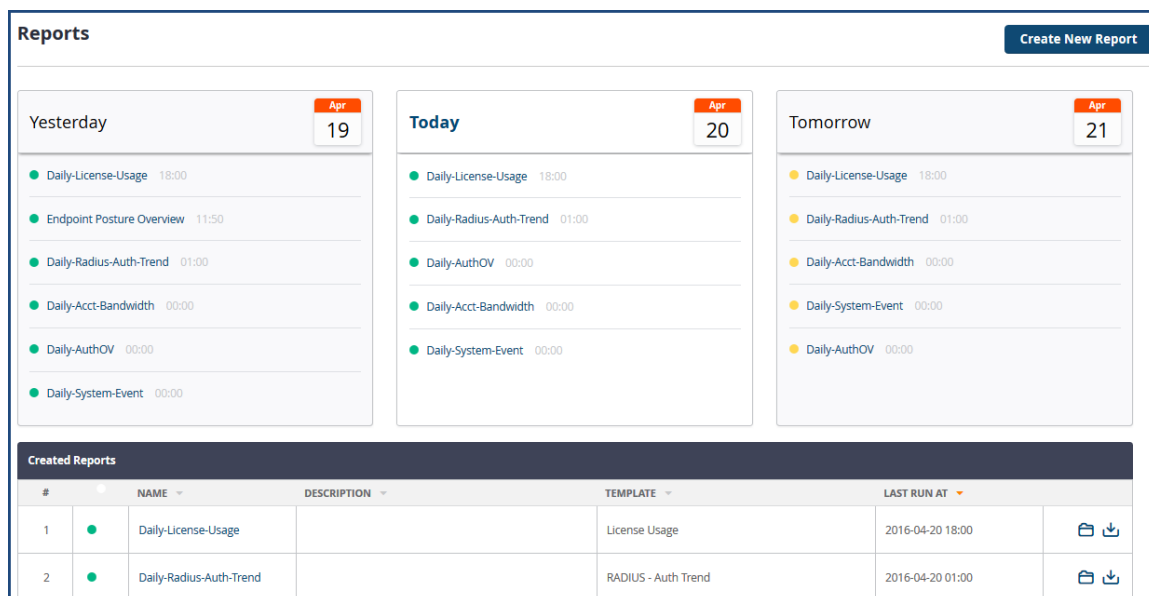
This section provides the following information:

- [Overview](#)
- [Settings Configuration](#)
- [Report Filters Configuration](#)
- [Specifying the Logo and Branding](#)
- [Report Summary Page](#)
- [Configured Reports Page](#)
- [Viewing Reports](#)

Overview

The **Reports** page provides a method for creating reports with data filters and customized time ranges up to the previous two months.

Figure 713: *Reports Page*



Run Reports Now or on a Specified Schedule

You can set up reports to run immediately or you can schedule a report to run on a daily, weekly, or monthly basis. Although Insight reports show data over the previous two-month period, Insight can retain data for up to two years.

Select Report Filters

Many reports allow you to select filters that include a simple AND condition. For example, you can use filters to create a report that displays data for RADIUS Authentications from the Active Directory AND the Guest User Repository source.

PDF, CSV, and HTML Report Formats Are Available

After a report is configured and run, the report is available for download in PDF and CSV formats. You can also open a report and view it in HTML format.



Deleting a configured report deletes both the report configuration and all related report output.

Settings Configuration

To create a new report:

1. From the Insight navigation panel, click **Reports**.
2. Select **Create New Report**.

The **Settings** page of the **Create New Report Wizard** appears.

Figure 714: *Create New Report Wizard: Settings*

3. Enter the appropriate information as described in [Table 371](#).

Table 371: *Specifying the Report Settings Parameters*

Report Parameter	Action/Description
Report Name	1. Enter the name of the report.
Description	2. Optionally, enter a summary description of the report.
Category	3. Select the report Category , then specify the desired report type in the selected category: ■ Authentication ■ Endpoint ■ Guest Authentication ■ Network ■ OnGuard ■ Onboard ■ RADIUS Authentication

Table 371: *Specifying the Report Settings Parameters (Continued)*

Report Parameter	Action/Description
	■ System ■ TACACS NOTE: For detailed information about what report types are provided for each report category, see Insight Report Categories Reference on page 713.
Notifications	4. Optionally, specify report notifications. ■ Notify by Email. When you select this option, enter the list of email addresses to be notified. ■ Notify by SMS. When you select this option, enter the phone numbers of each recipient (separated by commas). NOTE: A warning message appears if you have not configured the SMTP mail server for email notifications. To do so, from the W-Policy Manager, navigate to Administration > External Servers > Messaging Setup. For details, see Messaging Setup on page 553.
Options	NOTE: Before you can enable one or both of these two options, you must configure the File Transfer Settings (including the Remote Directory) in the Administration section. For more information, see File Transfer Settings Configuration on page 728. ● Include raw data in output A full set of raw data is customizable in the CSV reports only. ● Enable remote copy This option lets you copy reports to the location specified in the Administration > Remote Directory setting.
Repeat Scheduled Report	5. Specify whether you want to generate this report Daily, Weekly, or Monthly. The default is No Repeat. ■ To rerun a No Repeat report or a static report, edit and save the report. Insight will then automatically run the report. ■ When you create a report with the No Repeat option selected, the report runs when you click Save. ■ When you create a periodic report (Daily, Weekly, or Monthly), the report is run according to the specified schedule.

Table 371: *Specifying the Report Settings Parameters (Continued)*

Report Parameter	Action/Description
Preset Date Range	6. You can choose to specify a Preset Date Range for this report: ■ Custom Date When you select Custom Date, specify the Start Date and Time and the End Date and Time. ■ Today ■ Since Yesterday ■ This Week ■ Within Last Week ■ Within Last 2 Weeks ■ This Month ■ Within Last Month When you select one of these date range options (with the exception of Custom Date), Insight automatically populates the Start Date/Time and End Date/Time settings.
Report Summary	When you have configured the report settings, the Report Summary displays them for your review.
	7. Click Next .

Report Filters Configuration

When you complete the **Settings** page in the **Create New Report** wizard and click **Next**, the page that opens allows you to configure the filters for your report. Each type of report has a specific set of filters available.

Report filters apply the data fetched from the database, then Insight displays the result in the report. The filters that are available depend on the report category you specify.

If you don't apply a filter, Insight includes all the data in the generated report that matches the report category.

Figure 715: *Specifying a Report Filter*

The screenshot shows the 'Create New Report' wizard interface. At the top right is a 'Sample Report' button. Below it is a progress bar with four steps: '« Prev: Settings', 'Step 2: Filters, Raw Data, Branding' (highlighted with an orange dot), and 'Next: Report Summary »'. The main content area is titled 'Filters' and contains the text 'What would you like to see in your new Report?'. Below this text are two input fields: 'Field' and 'Value'. The 'Field' field has a dropdown menu with 'NAD IP' selected. The 'Value' field has a dropdown menu with '104.36.248.113' selected.

To specify a report filter:

1. **Field:** From the **Field** drop-down, select the parameter you wish to filter on.
2. **Value:** From the **Value** drop-down, select the appropriate value.
As you enter characters in the **Value** field, Insight searches for the matching value.

Specifying the Logo and Branding

When you complete the report filters configuration, scroll to the **Logo and Branding** section on the same page.

Figure 716: *Logo and Branding Section*

Create New Report Sample Report

Logo and Branding

Select your Logo and Branding template for the export.

Select Template

Default Logo and Branding

Page Title

Authentication by NAD: Sales Dept.

Top Section

Aruba Header

Logo Image Replace Image

Bottom Section

Footer

Copyright

Copyright NewSales, Inc. 2016

Save Template

Next

To specify the logo and branding information:

1. Enter the information as described in [Table 372](#), then click **Next**.

Table 372: *Specifying Logo and Branding Parameters*

Report Parameter	Action/Description
Select Template	1. From the drop-down, select the logo and branding template.
Page Title	2. Enter the page title.
Top Section	3. Enter the header for the top of the page.

Table 372: Specifying Logo and Branding Parameters (Continued)

Report Parameter	Action/Description
Logo Image	4. To browse to the appropriate logo image, click Replace Image .
Bottom Section	5. Enter the footer text.
Copyright	6. Enter the copyright information. For example, "Copyright 2016 NewSales, Inc."
Save Template	7. To save the new branding and logo settings, click Save Template .
	8. Click Next .

Report Summary Page

When you complete the **Logo and Branding** section, the **Report Summary** is displayed.

Figure 717: Report Summary

Report Summary [Sample Report](#)

« Prev: [Filters](#), [Raw Data](#), [Branding](#) **Step 3: Report Summary**

Report Summary [Edit Report](#)

Report Name Auth by NAD-Sales

Description

Category Network > Auth by NAD

Notifications Notify by Email: james.jones@newsales.com
Notify by SMS:

Schedule Report contains data from 2016-04-20 8:00 PM to 2016-04-21 5:14 PM

Filters 1. NAD IP: 104.36.248.113

Raw Data Columns None

Logo & Branding Default Logo and Branding

1. Review the Report Summary.
 - a. If you wish to change any aspect of the report, click **Edit Report**.

The **Report Summary** dialog opens. You can edit the current report settings as needed.
 - b. Make any necessary changes, then click **Save**.
2. When the report settings are satisfactory, click **Save**.

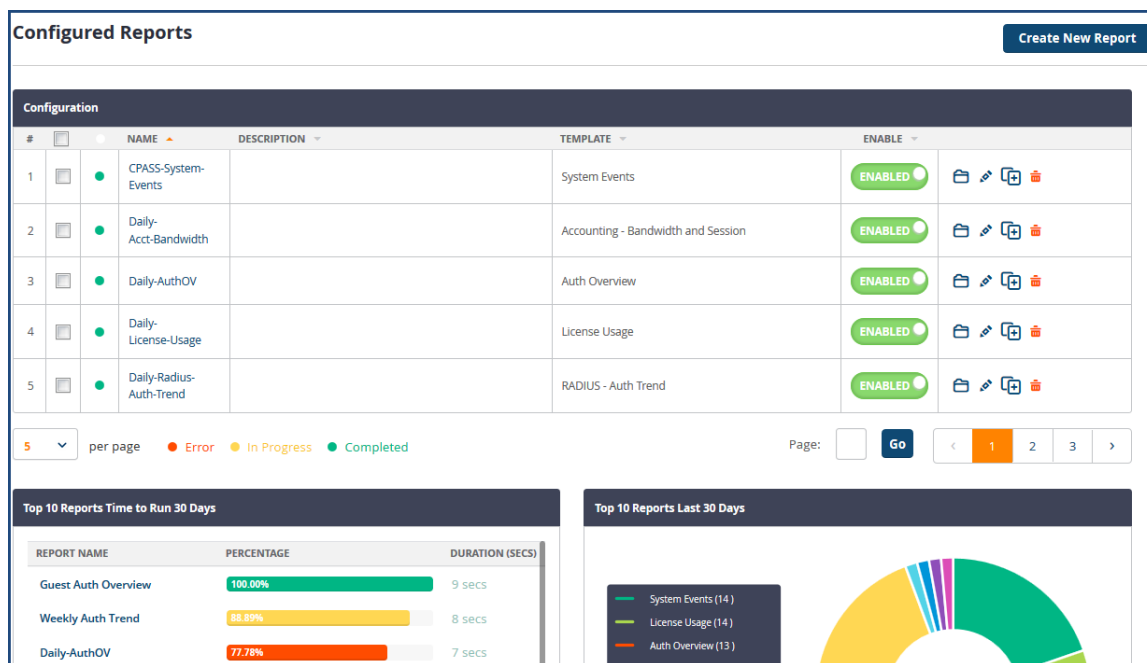
Insight generates the report. You return to the **Configured Reports** page.

Configured Reports Page

To see the set of configured reports, select **Reports > Configuration**.

The **Configured Reports** page opens.

Figure 718: *Configured Reports Page*



The blue dot next to a report name indicates that the report generation is complete.

From this view, you can edit, copy, or delete a configured report.

This page also provides two report widgets:

- **Top 10 Reports Time to Run 30 Days**
This widget lists the ten reports that took the longest (in seconds) to run over the last 30 days.
- **Top 10 Reports Last 30 Days**
This widget lists the ten most frequently run reports over the last 30 days.

Viewing Reports

To view a generated report:

1. From the navigation panel, click **Reports**.
2. Scroll to the **Created Reports** section.

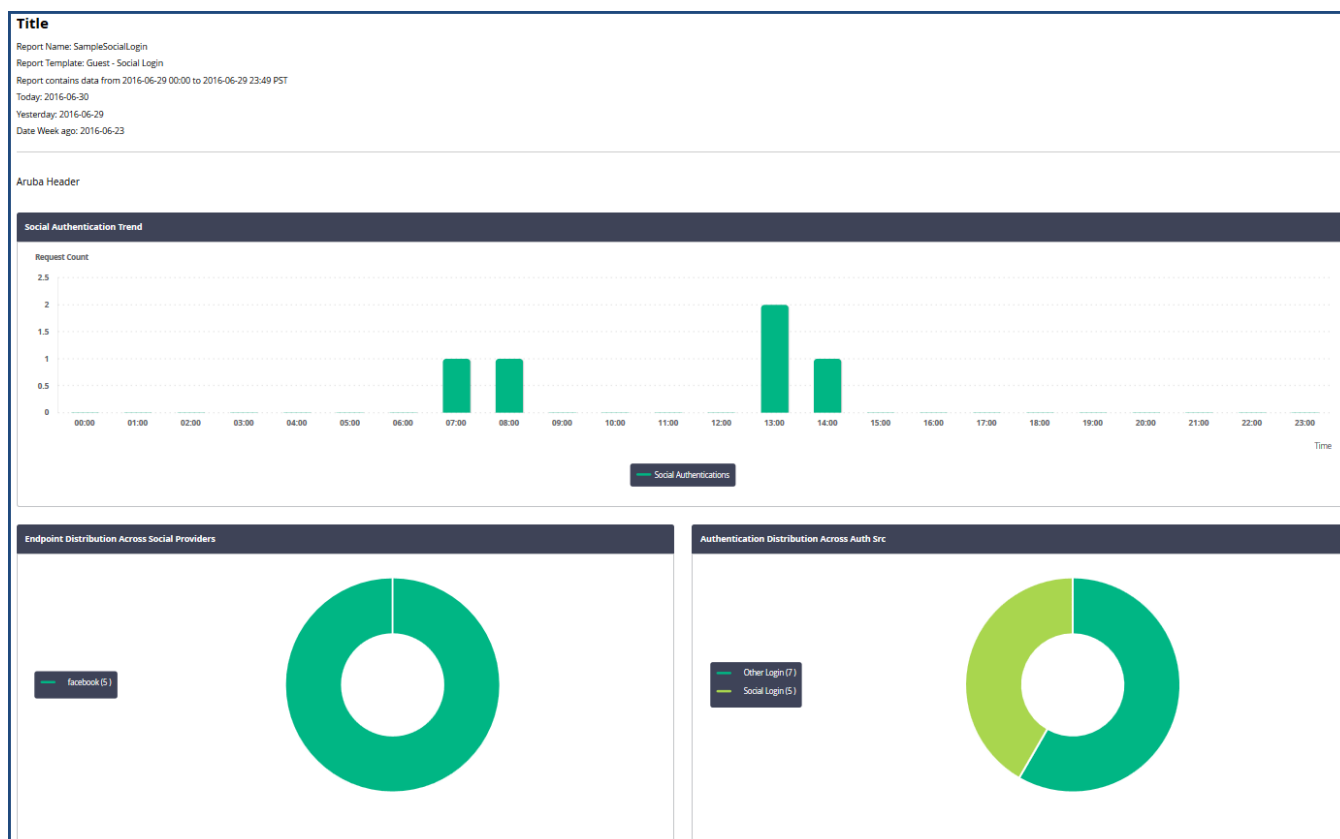
Figure 719: Created Reports

Reports						Create New Report
Created Reports						
#	NAME	DESCRIPTION	TEMPLATE	LAST RUN AT		
1	atrend		Auth Trend	2016-03-01 12:31		
2	overview		Endpoint Posture Overview	2016-03-01 11:16		
3	mac-ong		Apple Mac Endpoint Posture			
4	windows		Windows Endpoint Posture			
5	win-ong		Windows Endpoint Posture	2016-02-29 19:18		

5 per page ● Error ● In Progress ● Completed Page: Go < 1 2 >

- To download the zip file that contains the reports in PDF and CSV formats, click the **Download** icon (as shown in Figure 719).
- To view the desired report in HTML format (which opens in new tab), click the name of the report. The generated report is displayed (see Figure 720).

Figure 720: Report Displayed in HTML Format



Insight Report Categories Reference

This section provides the following information:

- [Introduction](#)
- [Authentication Category Reports](#)
- [Endpoint Category Reports](#)
- [Guest Authentication Category Reports](#)
- [Network Category Reports](#)
- [OnGuard Category Reports](#)
- [Onboard Category Report](#)
- [RADIUS Authentication Category Reports](#)
- [System Category Reports](#)
- [TACACS Category Reports](#)

Introduction

This section provides detailed information about each of the report types and their associated widgets available for each Insight Report category. The Insight report templates are organized into categories, where each category has multiple report types that each contain a unique set of report data.

The following sections describe each report category, including the available reports within each category, and the contents of each report.

Authentication Category Reports

The reports available in the Authentication category described in [Table 373](#) provide the list of authentications that occurred during the report duration.

Additional authentication statistics are displayed on the **Authentication Dashboard**. For more information, see [Authentication Dashboard on page 692](#).

Table 373: Authentication Category Reports

Report Type	Report Widgets
Accounting—Bandwidth and Session Provides the statistics using the accounting data generated during report duration.	This report type includes the following bandwidth and session information: • Bandwidth Statistics • Upstream Bandwidth and Downstream Bandwidth Trend • Total Bandwidth and Average Bandwidth Trend • Average Session Time Trend • Unique Session Trend • Top 10 Device Categories with Most Bandwidth Consumed • Top 10 Device Categories with Most Sessions • Top 10 Device Categories with Most Duration • Top 10 Device Families with Most Bandwidth Consumed • Top 10 Device Families with Most Sessions • Top 10 Device Families with Most Duration • Top 10 Endpoints with Most Bandwidth Consumed • Top 10 Endpoints with Most Sessions • Top 10 Endpoints with Most Duration • Top 20 Users with Most Bandwidth Consumed • Top 10 Users with Most Sessions • Top 10 Users with Most Duration NOTE: This report allows you to filter the report data by W-ClearPass Policy Manager server, Network Access Device (NAD) IP address, SSID, and Error Code.
Authentication by Authentication Source Provides the statistics for successful and failed authentications per authentication source.	This report type includes the following information: • Authentication Statistics • Total Authentication Trend • Failed Authentication Trend • Authentication Distribution Across Authentication Source • Authentication Distribution Across Authorization Source • Authentication Distribution Across Authentication Source NOTE: This report allows you to filter the report data by authentication source.
Authentication by W-ClearPass Provides the statistics for successful and failed authentications per W-ClearPass servers in a cluster.	This report type includes the following information: • Authentication Statistics • Total Authentication Trend • Failed Authentication Trend • Authentication Distribution—Error Types • Authentication Distribution Across Service • Top 10 W-ClearPass with Most Authentications • Top 10 W-ClearPass with Most Failed Authentications • Top 10 W-ClearPass with Most MAC Address Authentications • Top 10 W-ClearPass with Most Users NOTE: This report allows you to filter the report data by W-ClearPass Policy Manager server.
Authentication Overview	This report type includes the following information: • Authentication Statistics

Table 373: Authentication Category Reports (Continued)

Report Type	Report Widgets
Provides statistics in general for the report duration, such as total authentications per day, unique devices authentications trend by day, unique users authentication trend by day, authentication distribution based on authentication status, service, W-ClearPass server, SSID, VLAN, enforcement profile, authentication source, and top 10 users with most authentications, and so on.	• Total Authentication Trend • Authentication Status Trend • Unique Devices Authentication Trend • Unique Users Authentication Trend • Authentication Distribution Across Auth Status • Authentication Distribution Across Cluster • Authentication Distribution Across Service • Authentication Distribution Across VLAN • Authentication Distribution Across SSID • Authentication Distribution Across Enforcement Profiles • Authentication Distribution Across Role • Authentication Distribution Across Authentication Source • Top 10 Users with Most Authentications • Top 10 MAC Addresses with Most Authentications • Top 10 Services with Most Authentications • Top 10 Auth Sources with Most Authentications • Top 10 W-ClearPass Roles Assigned • Top 10 Authorization Sources • Top 20 NADs with Most Authentications • Top 10 Enforcement Profiles Users NOTE: This report allows you to filter the report data by W-ClearPass Policy Manager host name, Network Attached Device (NAD) IP address, SSID, and Error Code.
Authentication Trend Provides authentication trend statistics for today and yesterday, today and the same day a week ago, and so on.	This report type includes the following information: • Authentication Statistics • Total Authentication Trend • Authentication Trend for Today and Yesterday • Authentication Trend for Today and Same Day Week Ago • Total Authentication for 1 Month (per month) NOTE: This report allows you to filter the report data by W-ClearPass Policy Manager host name, Network Access Device (NAD) IP address, and SSID.
Failed Authentication Provides statistics based on failed authentications.	This report type includes the following information: • Error Statistics • Failed Authentication Trend • Authentication Distribution—Error Types • Failed Authentication Distribution across Service • Failed Authentication Distribution across Authentication Source • Top 10 Errors with Most Failed Authentications • Top 20 NADs with Most Failed Authentications • Top 10 W-ClearPass Servers with Most Failed Authentications • Top 10 Users with Most Failed Authentications • Top 10 Endpoints with Most Failed Authentications • Top 10 Services with Most Failed Authentications

Table 373: Authentication Category Reports (Continued)

Report Type	Report Widgets
	NOTE: This report allows you to filter the report data by W-ClearPass Policy Manager host name, Network Access Device (NAD) IP address, SSID, and Error Code.

Endpoint Category Reports

The Endpoint category provides information on endpoints discovered during the report duration.

The reports available in the Endpoint category described in [Table 374](#) contain data that can also be found in the Endpoints widgets on the **Endpoints Dashboard**.

For additional information about the Endpoints Dashboard, see [Endpoints Dashboard on page 693](#).

Table 374: Endpoint Category Reports

Report Type	Report Widgets
Endpoint Authentication Overview	This report type includes the following information for all endpoint types: - Endpoint Statistics - Endpoints Distribution Across Device Category - Endpoints Distribution Across Device Family - Endpoints Distribution Across Device Name - Top 10 Users with Most Endpoints - Top 10 Device Categories with Most Endpoints - Top 10 Device Names with Most Endpoints - Top 10 Device Families with Most Endpoints NOTE: This report also allows you to filter the report data by Network Access Device (NAD) IP address, Device Category, Device Family, Device name, and SSID.
Guest—Endpoint Overview	This report type includes the following information for endpoints using Guest Authentication: - Endpoint Statistics - Endpoints Distribution Across Device Category - Endpoints Distribution Across Device Family - Endpoints Distribution Across Device Name - Top 10 Users with Most Endpoints - Top 10 Device Categories with Most Endpoints - Top 10 Device Names with Most Endpoints - Top 10 Device Families with Most Endpoints NOTE: This report also allows you to filter the report data by Network Access Device (NAD) IP address, Device Category, Device Family, Device name, and SSID.
RADIUS—Endpoint Overview	This report type includes the following information for endpoints using RADIUS authentication: - Endpoint Statistics - Endpoints Distribution Across Device Category - Endpoints Distribution Across Device Family - Endpoints Distribution Across Device Name

Table 374: *Endpoint Category Reports (Continued)*

Report Type	Report Widgets
	• Top 10 Users with Most Endpoints • Top 10 Device Categories with Most Endpoints • Top 10 Device Names with Most Endpoints • Top 10 Device Families with Most Endpoints NOTE: This report also allows you to filter the report data by Network Access Device (NAD) IP address, Device Category, Device Family, Device name, and SSID.

Guest Authentication Category Reports

The reports available in the Guest Authentication category described in [Table 375](#) provide statistics based on Guest authentications from the Guest database. The statistics for authentication trend and usage for guest users are drawn from the accounting data.

Additional authentication statistics are displayed on the **Guest Dashboard**. For additional information about the Guest Dashboard, see [Guest Dashboard on page 694](#).

Table 375: *Guest Authentication Category Reports*

Report Type	Report Widgets
Guest—Authentication by W-ClearPass	This report type includes the following information guest authentication by W-ClearPass: • Authentication Statistics • Total Authentication Trend • Failed Authentication Trend • Authentication Distribution—Error Types • Authentication Distribution Across Service • Top 10 W-ClearPass with Most Authentications • Top 10 W-ClearPass with Most Failed Authentications • Top 10 W-ClearPass with Most MAC Authentications • Top 10 W-ClearPass with Most Guests NOTE: This report also allows you to filter the report data by W-ClearPass Policy Manager host name.
Guest—Authentication Overview	This report type includes the following information for guest authentication: • Authentication Statistics • Total Authentication Trend • Authentication Status Trend • Unique Devices Authentication Trend • Unique Guests Authentication Trend • Authentication Distribution Across Authentication Status • Authentication Distribution Across Cluster • Authentication Distribution Across Service • Authentication Distribution Across VLAN • Authentication Distribution Across SSID • Authentication Distribution Across Enforcement Profiles • Authentication Distribution Across Role • Authentication Distribution Across Authentication Sources • Top 10 Guests with Most Authentications • Top 10 MAC Addresses with Most Authentications • Top 10 IP Addresses with Most Authentications • Top 10 Services with Most Authentications • Top 10 Authentication Sources with Most Authentications • Top 10 W-ClearPass Roles Assigned • Top 10 Authorization Source • Top 20 NADs with Most Authentications • Top 10 Enforcement Profiles Used NOTE: This report also allows you to filter the report data by W-ClearPass Policy Manager host name and Network Access Device (NAD) IP address.
Guest—Authentication Trend	This report type includes the following information for guest authentication trends: • Authentication Statistics • Total Authentication Trend • Authentication Trend for Yesterday and Today • Authentication Trend for Today and Same Day Week Ago

Table 375: *Guest Authentication Category Reports (Continued)*

Report Type	Report Widgets
	• Total Authentication for 1 Month • Sponsor List NOTE: This report also allows you to filter the report data by W-ClearPass Policy Manager host name and Network Access Device (NAD) IP address.
Guest—Social Login	This report type includes the following information for guest authentication for Social Logins: • Social Authentication Trend • Endpoint Distribution Across Social Providers • Authentication Distribution Across Authentication Source NOTE: This report also allows you to filter the report data by W-ClearPass Policy Manager host name and Network Access Device (NAD) IP address.
Guest Accounting—Bandwidth and Session	This report type includes the following bandwidth and session information: • Bandwidth Statistics • Upstream Bandwidth and Downstream Bandwidth Trend • Total Bandwidth and Average Bandwidth Trend • Average Session Time Trend • Unique Session Trend • Top 10 Device Categories with Most Bandwidth Consumed • Top 10 Device Categories with Most Sessions • Top 10 Device Categories with Most Duration • Top 10 Device Families With Most Bandwidth Consumed • Top 10 Device Families With Most Sessions • Top 10 Device Families With Most Duration • Top 10 Endpoints with Most Bandwidth Consumed • Top 10 Endpoints with Most Sessions • Top 10 Endpoints with Most Duration • Top 20 Users with Most Bandwidth Consumed • Top 10 Users with Most Sessions • Top 10 Users with Most Duration NOTE: This report also allows you to filter the report data by W-ClearPass Policy Manager host name, NAD IP address, Device Category, Device Family, Device Name, and SSID.

Network Category Reports

The reports available in the Network category described in [Table 376](#) contain data about network access devices and ives details on authentication trends such as successful and failed authentications on a per-day basis.

Similar information can also be found in the Network widgets on the **Network Dashboard**. For additional information, see [Network Dashboard on page 695](#).

Table 376: *Network Category Reports*

Report Type	Report Widgets
Authentication by NAD	This report type includes the following information for Network Access Devices (NADs) using guest authentication. • Authentication Statistics • Total Authentication Trend • Failed Authentication Trend • Authentication Distribution Across NAD Ports • Top 20 NADs with Most Authentication • Top 10 Services with Most Authentications • Top 20 NADs with Most Failed Authentications • Top 20 NADs with Most MAC Addresses • Top 20 NADs with Most Users NOTE: This report also allows you to filter the report data by NAD IP address.
Guest—Authentication by NAD	This report type includes the following information for Network Access Devices (NADs) using guest authentication • Authentication Statistics • Total Authentication Trend • Failed Authentication Trend • Authentication Distribution Across NAD Ports • Top 20 NADs with Most Authentication • Top 10 Services with Most Authentications • Top 20 NADs with Most Failed Authentications • Top 20 NADs with Most MAC Addresses • Top 20 NADs with Most Guests NOTE: This report also allows you to filter the report data by NAD IP address.
RADIUS—Auth by NAD	This report type includes the following information for Network Access Devices (NADs) using guest authentication: • Authentication Statistics • Authentication Distribution Across NAD Ports • Top 20 NADs with Most Authentication • Top 10 Services with Most Authentications • Top 20 NADs with Most Failed Authentications • Top 20 NADs with Most MACs • Top 20 NADs with Most Users NOTE: This report also allows you to filter the report data by NAD IP address.

OnGuard Category Reports

The reports available in the OnGuard category provide analysis on the devices' posture and health status.

These widgets contain data that can also be found in the Posture widgets on the **Posture Dashboard**. For additional information, see [Posture Dashboard on page 695](#).

Table 377: OnGuard Category Reports

Report Type	Report Widgets
Apple Mac Endpoint Posture	This report type includes the following posture information for Apple/Macintosh endpoints: • OnGuard Statistics • OnGuard Device Authentication Trend • OnGuard Device Distribution Across Health Status • Antispyware Product Name • Antispyware Dat File Version • Antispyware Engine Version • OnGuard Device Distribution Across Antispyware Real-Time Protection Status • Antispyware Version • Antivirus Product Name • Antivirus Dat File Version • Antivirus Engine Version • OnGuard Device Distribution Across Antivirus RealTimeProtection Status • Antivirus Version • Disk Encryption Product Name • Disk Encryption Version • Firewall Product Name • OnGuard Device Distribution Across Firewall Status • Firewall Version • OnGuard Device Distribution Across Network Connection Type • OnGuard Device Distribution Across P2P Application Name • OnGuard Device Distribution Across P2P Status • OnGuard Device Distribution Across Patch Agent Name • Missing Patches Count • OnGuard Device Distribution Across Patch Agent Status • OnGuard Device Distribution Across Client Operating System • OnGuard Device Distribution Across Client Running as VM NOTE: This report also allows you to filter the report data by System Posture Token (SPT).
Endpoint Posture Overview	This report type includes the following endpoint posture information: • OnGuard Statistics • OnGuard Device Distribution Across Health Status • Unhealthy OnGuard Device Distribution Across Device Family • OnGuard Device Distribution Across Agent Type • OnGuard Device Distribution Across Agent Version • Health Class • Missing Hotfixes NOTE: This report also allows you to filter the report data by System Posture Token (SPT).
Linux Endpoint Posture	This report type includes the following posture information for endpoints using a Linux operating system: • OnGuard Statistics • OnGuard Device Authentication Trend

Table 377: OnGuard Category Reports (Continued)

Report Type	Report Widgets
	- OnGuard Device Distribution Across Health Status - Antivirus Product Name - Antivirus Dat File Version - Antivirus Engine Version - OnGuard Device Distribution Across Antivirus RealTimeProtection Status - Antivirus Version NOTE: This report also allows you to filter the report data by System Posture Token (SPT).
Windows Endpoint Posture	This report type includes the following posture information for endpoints using a Windows operating system: - OnGuard Statistics - OnGuard Device Authentication Trend - OnGuard Device Distribution Across Health Status - Antispyware Product Name - Antispyware Dat File Version - Antispyware Engine Version - OnGuard Device Distribution Across Antispyware Real-Time Protection Status - Antispyware Version - Antivirus Product Name - Antivirus Dat File Version - Antivirus Engine Version - OnGuard Device Distribution Across Antivirus RealTimeProtection Status - Antivirus Version - Disk Encryption Product Name - Disk Encryption Version - Firewall Product Name - OnGuard Device Distribution Across Firewall Status - Firewall Version - OnGuard Device Distribution Across Network Connection Type - OnGuard Device Distribution Across P2P Application Name - OnGuard Device Distribution Across P2P Status - OnGuard Device Distribution Across Patch Agent Name - Missing Patches Count - OnGuard Device Distribution Across Patch Agent Status - OnGuard Device Distribution Across Client Operating System - OnGuard Device Distribution Across Client Running as VM NOTE: This report also allows you to filter the report data by System Posture Token (SPT).

Onboard Category Report

The report available in the Onboard category provides analysis on onboarded devices during the report period, such as the active users/devices count, revoked devices count, and onboarded devices distribution based on device type.

Table 378: *Onboard Report Content*

Report Type	Report Widgets
Onboard Certificate	This report type includes the following certificate information: - Onboard statistics for numbers of revoked devices, active devices, and users - Latest Onboard Device Distribution - Active Onboard Device Distribution - Top 10 Users with Most Active Devices

RADIUS Authentication Category Reports

The reports available in the RADIUS Authentication provide detailed analysis on authentication trends on successful and failed RADIUS authentication.

Additional authentication statistics are displayed on the **Authentication Dashboard**. For additional information, see [Authentication Dashboard on page 692](#).

Table 379: *RADIUS Authentication Category Reports*

Report Type	Report Widgets
RADIUS—Authentication by Authentication Source	This report type includes the following information for RADIUS authentication: - Authentication statistics for numbers and percentages of authentications successes and failures - Total Authentication Trend - Failed Authentication Trend - Authentication Distribution Across Authentication Source - Authentication Distribution Across Authorization Source - Failed Authentication Distribution Across Authentication Source NOTE: This report also allows you to filter the report data by W-ClearPass Policy Manager host name.
RADIUS—Authentication by W-ClearPass	This report type includes the following information for RADIUS authentication: - Authentication Statistics, including numbers and percentages of authentications successes and failures - Total Authentication Trend - Failed Authentication Trend - Authentication Distribution Error Types - Authentication Distribution Across Service - Top 10 W-ClearPass with Most Authentications - Top 10 W-ClearPass with Most Failed Authentications - Top 10 W-ClearPass with Most MAC Addresses - Top 10 W-ClearPass with Most Users NOTE: This report also allows you to filter the report data by authentication source.
RADIUS—Authentication Overview	This report type includes the following information for RADIUS authentication:

Table 379: RADIUS Authentication Category Reports (Continued)

Report Type	Report Widgets
	• Authentication statistics, including numbers and percentages of authentications successes and failures, and numbers of users, endpoints, network devices, roles, W-ClearPass servers and enforcement profiles • Total Authentication Trend • Authentication Status Trend • Unique Devices Authentication Trend • Unique Users Authentication Trend • Authentication Distribution Across Auth Status • Authentication Distribution Across Cluster • Authentication Distribution Across Service • Authentication Distribution Across VLAN • Authentication Distribution Across SSID • Authentication Distribution Across Enforcement Profiles • Authentication Distribution Across Role • Authentication Distribution Across Auth Source • Top 10 Users with Most Authentications • Top 10 MACs with Most Authentications • Top 10 Services with Most Authentications • Top 10 W-ClearPass Roles Assigned • Top 10 Authorization Sources • Top 20 NADs with Most Authentications • Top 10 Enforcement Profiles Used NOTE: This report also allows you to filter the report data by W-ClearPass Policy Manager host name, Network Access Device (NAD) IP address, SSID and authentication service name.
RADIUS—Authentication Trend	This report type includes the following information: • Authentication Statistics, including authentication data for the previous day and week • Total Authentication Trend • Authentication Trend for Today and Yesterday • Authentication Trend for Today and Same Day Week Ago • Total Authentication for 1 Month (per month) NOTE: This report also allows you to filter the report data by W-ClearPass Policy Manager name, Network Access Device (NAD) IP address, and SSID.
RADIUS—Failed Authentication	This report type includes the following information: • Error Statistics • Failed Authentication Trend • Authentication Distribution—Error Types • Failed Authentication Distribution Across Service • Failed Authentication Distribution Across Authentication Sources • Top 10 Errors with Most Failed Authentications • Top 10 W-ClearPass Servers with Most Failed Authentications • Top 20 NADs with Most Failed Authentications

Table 379: *RADIUS Authentication Category Reports (Continued)*

Report Type	Report Widgets
	• Top 10 Users with Most Failed Authentications • Top 10 Endpoints with Most Failed Authentications • Top 10 Services with Most Failed Authentications NOTE: This report also allows you to filter the report data by W-ClearPass Policy Manager host name, Network Access Device (NAD) IP, SSID, and Error Code.

System Category Reports

The reports available in the **System** category provide information about system-level events, such as configuration changes performed on the W-ClearPass server (configuration audit), license usage, and system events.

Additional system statistics are displayed on the **System Dashboard**. For additional information about the System Dashboard, see [System Dashboard on page 696](#).

Table 380: *System Category Reports*

Report Type	Report Widgets
Configuration Audit	This report type includes the following information for each configuration audit record: • Name of change • Action (for example, modify, add, or delete) • Category • Updated by • Update timestamp
License Usage	This report type includes the following licensing information: • License Statistics, including the total licenses and used licenses for W-Policy Manager, Guest, W-ClearPass Enterprise, Onboard, and OnGuard • Endpoints Trend • Policy Manager License Usage Trend • Guest License Usage Trend • W-Policy Manager License Distribution • W-Policy Manager License Usage • Guest License Usage Distribution Across Cluster • Onboard License Usage Distribution Across Cluster • OnGuard License Usage Distribution Across Cluster • W-ClearPass Enterprise License Usage Distribution Across Cluster NOTE: This report also allows you to filter the report data by W-ClearPass Policy Manager host name.
System Events	This report type includes the following information for each system event : • W-ClearPass host name • Source of Event • Event Category

Table 380: *System Category Reports (Continued)*

Report Type	Report Widgets
	• Event Level • Timestamp • Description NOTE: This report also allows you to filter the report data by W-ClearPass Policy Manager host name.

TACACS Category Reports

The reports available in the TACACS category provide TACACS authentication trends such as successful and failed TACACS authentication and command authorizations.

Table 381: *TACACS Reports Content*

Report Type	Report Widgets
TACACS—Authentication	This report type includes the following licensing information • TACACS statistics, including the numbers and percentages of successful and failed authentications, and the numbers of users, W-ClearPass servers, and network devices. • Total Authentication Trend • Authentication Status Trend • Authentication Trend For Today and Yesterday • Command List • Authentication Distribution Across Authentication Status • Authentication Distribution Across Cluster • Top 10 Errors with Most Failed Authentications • Top 20 NADs with Most Authentication • Top 10 Users with Most Authentications NOTE: This report also allows you to filter the report data by W-ClearPass server and NAD IP address.

Administration Operations

This section provides the following information:

- [Overview](#)
- [File Transfer Settings Configuration](#)
- [Database Settings Configuration](#)

Overview

You can use the **Administration** page to do the following tasks:

- Specify the number of days to retain information in the database.
- Test the new notification settings to review Insight log files.
- Store reports offline using SCP or SFTP.

To access the **Administration** page:

1. From the Insight navigation pane, click **Administration**.

The **Administration** page appears.

Figure 721: *Administration Page*

The screenshot shows the 'Administration' page with a sidebar on the left containing links to 'Dashboard', 'Reports', 'Alerts', and 'Administration' (which is highlighted in orange). The main content area is titled 'Administration' and contains two sections: 'Settings' and 'Database Settings'. The 'Settings' section is further divided into 'File Transfer Settings' and 'Database Settings'. The 'File Transfer Settings' section includes fields for 'Host' (with a placeholder 'Host'), 'Protocol' (with radio buttons for 'SCP' and 'SFTP'), 'Port' (with a value of '22'), 'Username' (with a value of 'admin'), and 'Password' (with a masked field). There is also a 'Timeout' field with a value of '30' and a unit of 'seconds', and a 'Remote Directory' field. A 'Test' button is located below these fields. The 'Database Settings' section includes fields for 'Database Retention' (with a value of '30' and a unit of 'Days'), 'Report Retention' (with a value of '60' and a unit of 'Days'), and 'CSV Report Limit' (with a value of '50000' and a unit of 'Rows').

Support Information

- Insight database migration is supported.
- Configuration migration is not supported.
- Database retention default: 30 days
- Report retention default: 60 days
- CSV report limit: 50,000 rows

File Transfer Settings Configuration

You can specify the file transfer settings for uploading generated Insight reports to a FileStore.

To configure the File Transfer settings:

1. Navigate to the **Administration** page.

Figure 722: *Specifying the Insight File Transfer Settings*

The screenshot shows the 'File Transfer Settings' configuration form. It includes fields for 'Host' (with a value of '192.0.2.50'), 'Protocol' (with radio buttons for 'SCP' and 'SFTP'), 'Port' (with a value of '22'), 'Username' (with a value of 'admin'), and 'Password' (with a masked field). There is also a 'Timeout' field with a value of '30' and a unit of 'seconds', and a 'Remote Directory' field with a value of '\\reports\\insight'. A 'Test' button is located at the bottom left of the form.

2. In the **File Transfer Settings** section, enter the appropriate values as described in [Table 382](#).

- When finished, click **Save**.

Table 382: *Insight File Transfer Parameters*

Parameter	Action/Description
Host	1. Specify the IP address of the destination host FTP server.
Protocol	2. Specify the protocol to be used to upload the generated reports to a FileStore. You can select from the following protocols: ■ SCP (Session Control Protocol) ■ SFTP (SSH File Transfer Protocol)
Port	3. Specify the destination port number. The default destination port is 22 .
Username/Password	4. Enter the username and password of the host FTP server.
Timeout	5. Specify the timeout value in seconds. The default value is 30 seconds .
Remote Directory	6. Specify the location where the generated reports are to be copied. If the remote directory location is same as default root of FTP, you can leave this field blank. NOTE: To copy reports to a remote directory, you must enable the Reports > Create New Report > Enable remote copy option.

Testing File Transfer Configuration

When you have configured the Insight file transfer settings, you can then test to see if file transfer is operational.

To test the Insight file transfer configuration:

- Review the File Transfer Settings to ensure they are correct.
- Click the **Test** button.

You see the message: *File Transfer Settings testing in progress...*

Then the following screen appears:

Figure 723: *Successful File Transfer Test*

The screenshot shows the 'File Transfer Settings' form. At the top, there are five input fields: 'Host' (containing '10.1...'), 'Protocol' (with radio buttons for 'SCP' and 'SFTP', where 'SCP' is selected), 'Port' (containing '22'), 'Username' (containing 'root'), and 'Password' (containing masked characters). Below these are 'Timeout' (a numeric field with '30' and a 'seconds' label) and 'Remote Directory' (containing '/tmp/test'). At the bottom left is a blue 'Test' button. To the right of the button, a message states: 'Test tgz file has been copied to 'test' folder in remote directory'.

You are now ready to commence transferring Insight files to the FTP server as needed.

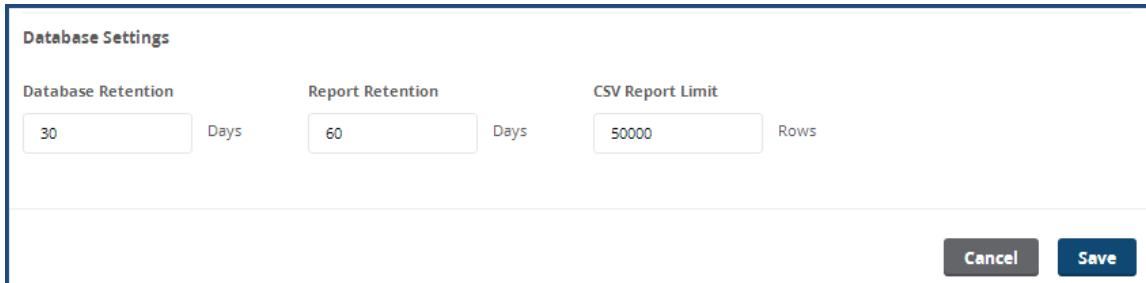
Database Settings Configuration

To configure the Insight database parameters:

1. Navigate to the **Administration** page.

The **Database Settings** section is at the bottom of the **Administration** page.

Figure 724: Specifying the Insight Database Settings



The screenshot shows a 'Database Settings' form. It contains three input fields with labels: 'Database Retention' (value: 30, unit: Days), 'Report Retention' (value: 60, unit: Days), and 'CSV Report Limit' (value: 50000, unit: Rows). At the bottom right, there are two buttons: 'Cancel' and 'Save'.

2. In the **Database Settings** section, enter the appropriate values as described in [Table 383](#).
3. When finished, click **Save**.

Table 383: Insight Database Parameters

Parameter	Action/Description
Database Retention	1. Specify the number of days to retain the database. The supported range is from 1 to 730 days. The default value is 30 days .
Report Retention	2. Specify the number of days to retain the generated reports. The supported range is from 1 to 365 days. The default value is 60 days .
CSV Report Limit	3. Specify the number of rows for a CSV report. The supported range is from 1 to 50,000 rows. The default value is 50000 rows.

Managing Insight Admin Privileges

This section provides the following information:

- [Overview](#)
- [Viewing the Default Insight Admin Privileges](#)
- [Defining Custom Insight Admin Privileges](#)
- [Insight UI Differences for Read-Only Users](#)

Overview

W-ClearPass supports multilevel Insight administrators, each with a different level of administrative access to Insight.

W-ClearPass provides a default Admin Privileges Read-only Administrator. The default sets of admin privileges cannot be modified.

Each of the Insight modules (Dashboard, Reports, Alerts, and Administration) can have three privilege levels or no privileges:

- Read-only
- Read and Write

- Read, Write, and Delete

In the case of a user with no Insight admin privileges, the navigation panel on the left side of the Insight user interface is not visible.

Viewing the Default Insight Admin Privileges

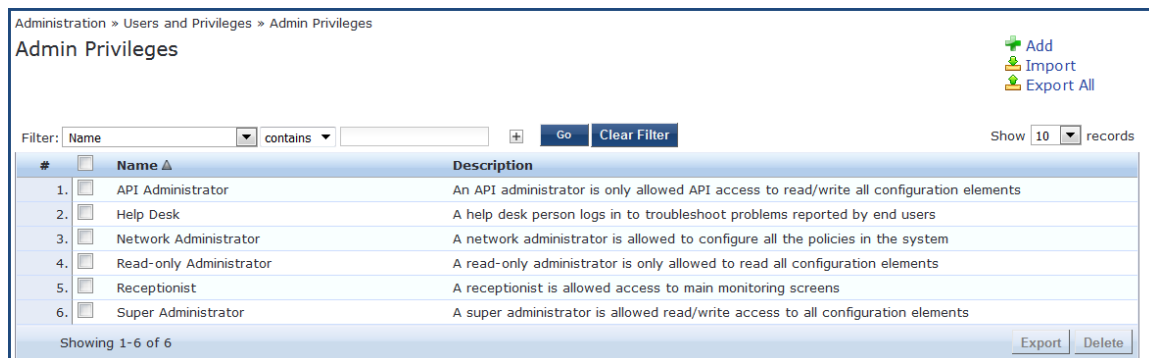
The settings for the default admin privileges cannot be modified.

To view the default Insight admin privileges defined in W-ClearPass:

1. Navigate to **Administration > Users and Privileges > Admin Privileges**.

The **Admin Privileges** page opens.

Figure 725: *Admin Privileges Page*



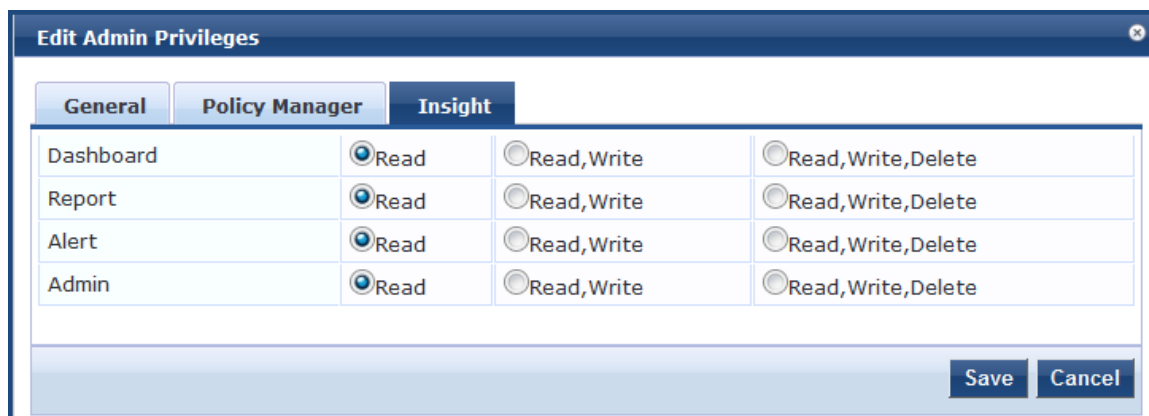
2. To view the Read-only admin privileges for Insight, select **Read-only Administrator**.

The **Edit Admin Privileges** dialog opens.

3. Select the **Insight** tab.

The default Insight admin privileges for the Read-only Administrator are displayed.

Figure 726: *Insight Read-Only Administrator Admin Privileges*



As shown in [Figure 726](#), the default admin privileges for the Insight Read-only Administrator specifies Read-only access to all of the Insight modules—Dashboard, Reports, Alerts, and Administration.

Defining Custom Insight Admin Privileges

As described above, W-ClearPass provides a default Read-only Administrator. The default sets of admin privileges cannot be modified.

When a different set of admin privileges is needed (for example, if you require different admin privileges for the Report module than the admin privileges defined for the other Insight modules), you must create a new admin privileges administrator.

Insight privileges can be defined from two locations:

- Operator Profiles in W-ClearPass Guest
- Admin Privileges in W-ClearPass

To define custom admin privileges for Insight:

1. Navigate to **Administration > Users and Privileges > Admin Privileges**.

The **Admin Privileges** page opens.

2. Click the **Add** link.

The **Add Admin Privileges** dialog opens.

Figure 727: Add Admin Privileges Dialog: Basic Information Tab

The screenshot shows a dialog box titled "Add Admin Privileges". It has three tabs: "Basic Information", "Policy Manager", and "Insight". The "Basic Information" tab is selected. The form contains the following fields:

- Name:** A text input field.
- Description:** A large text area.
- Access Type:** A dropdown menu with the option "Give full access to the Admin" selected.
- Allow Passwords:** A checkbox.

At the bottom right of the dialog are "Save" and "Cancel" buttons.

3. Specify the parameters in the **Basic Information** tab as described in [Table 384](#).

Table 384: Add Admin Privileges Parameters: Basic Information Tab

Parameter	Action/Description
Name	1. Enter the name of the Admin Privileges administrator.
Description	2. Provide a description of this new admin privileges administrator.
Access Type	3. Select one of the following Access Types: ■ Give full access to the Admin ■ Give UI access to the Admin ■ Give API access to the Admin
Allow Passwords	4. Select this check box if you want to allow password access.

Specifying Insight Admin Privileges

To specify the Insight admin privileges for the new administrator:

1. When you complete the **Basic Information** parameters, select the **Insight** tab.
The **Add Admin Privileges > Insight** dialog opens.

Figure 728: Add Admin Privileges > Insight Dialog

	Read	Read, Write	Read, Write, Delete
Dashboard	☐	☒	☐
Report	☐	☒	☐
Alert	☐	☒	☐
Admin	☒	☐	☐



You must configure the admin privileges for W-Policy Manager also, otherwise the changes to the Insight admin privileges cannot be saved.

2. Specify the desired admin privileges for each of the Insight modules, then click **Save**.

Insight UI Differences for Read-Only Users

When Insight is accessed by a user who has Read-only privileges for all four Insight modules (Dashboard, Reports, Alerts, and Administration), that user is not allowed to create or delete reports.

As shown in [Figure 729](#), when a Read-only administrator logs in to Insight, the **Create New Report** button is not visible.

Likewise, the **Delete** icon on the **Configured Reports** table is not visible for a Read-only administrator.

Figure 729: Create New Report Button Not Present for Read-Only User

Various action buttons, icons, and so on throughout the Insight user interface are shown only to users who are allowed to execute the actions provided by their admin privilege level.

Refer to the following sections to perform various tasks using the Command Line Interface (CLI):

- [Cluster Commands on page 735](#)
- [Configure Commands on page 738](#)
- [Miscellaneous Commands on page 750](#)
- [Network Commands on page 743](#)
- [Service Commands on page 758](#)
- [Show Commands on page 760](#)
- [SSH Timed Account Lockout](#)
- [System Commands on page 769](#)

Cluster Commands

The Policy Manager command line interface includes the following cluster commands:

- `cluster drop-subscriber`
- `cluster list`
- `cluster make-publisher`
- `cluster make-subscriber`
- `cluster reset-database`
- `cluster set-cluster-passwd`
- `cluster sync-cluster-passwd`

cluster drop-subscriber

Use the **drop-subscriber** command to remove a specific subscriber node from the cluster.

Syntax

```
cluster drop-subscriber [-f] [-i <IP address>] -s
```

[Table 385](#) describes the required and optional parameters for the **drop-subscriber** command:

Table 385: Drop-Subscriber Command Parameters

Parameter/Flag	Description
-f	Forces to drop even the nodes that are down.
-i <IP Address>	Specifies the Management IP address of the node. If this IP address is not specified and the current node is a subscriber, then W-Policy Manager drops the current node.
-s	Restricts resetting the database on the dropped node. By default, W-Policy Manager drops the current node—if it's a subscriber—from the cluster.

Example

The following example removes the IP address 192.xxx.1.1 from the cluster:

```
[appadmin]# cluster drop-subscriber -f -i 192.xxx.1.1 -s
```

cluster list

Use the **cluster list** command to list all the nodes in the cluster.

Syntax

```
cluster list
```

Example

The following example lists all the nodes in a cluster:

```
[appadmin]# cluster list
```

cluster make-publisher

Use the **cluster make-publisher** command to promote a specific subscriber node to be the publisher node in the same cluster.



When running this command, do not close the shell or interrupt the command execution.

Example

The following example promotes a subscriber node to publisher node status:

```
[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
```

To continue the **make-publisher** operation, enter **y**.

cluster make-subscriber

Run the **cluster make-subscriber** command on a standalone publisher to make the standalone node a subscriber and add it to the cluster.

Syntax

```
cluster make-subscriber -b -i <IP address> [-l]
```

Table 386 describes the required and optional parameters for the **make-subscriber** command:

Table 386: Cluster Make-Subscriber Command Parameters

Parameter/Flag	Description
-b	Generates a backup of the publisher before you make it a subscriber in the event the make-subscriber process fails and you need to restore the publisher.
-i <IP address>	Specifies the publisher's IP address. This field is mandatory.
-l	Restores the local log database after this operation. This field is optional.

Example

The following example converts the node with IP address 192.xxx.1.1 to a subscriber node:

```
[appadmin]# cluster make-subscriber -i 192.xxx.1.1 -l
```

cluster reset-database

Use the **reset-database** command to reset the local database and erase its configuration.



Running this command erases the W-Policy Manager configuration and resets the database to its default configuration—all the configured data will be lost.

When running this command, do not close the shell or interrupt the command execution.

Syntax

cluster reset-database

Example

The following example reset the database:

```
[appadmin]# cluster reset-database
*****
* WARNING: Running this command will erase the Policy Manager *
* 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
```

To continue the **reset-database** operation, enter **y**.

cluster set-cluster-passwd

Use the **cluster set-cluster-passwd** command to change the cluster password on all nodes in the cluster. You may only issue this command from the publisher node.



Setting the cluster password changes the **appadmin** password for all the nodes in the cluster

Syntax

cluster set-cluster-passwd

Example

The following example changes the cluster password on publisher nodes:

```
[appadmin]# cluster set-cluster-passwd
cluster set-cluster-passwd
```

```
Continue? [y|n]: y
```

```
Enter Cluster Passwd: college.162
```

```
Re-enter Cluster Passwd: college.162
```

INFO - Password changed on local (publisher) node
Cluster password changed

cluster sync-cluster-passwd

Use the **cluster sync-cluster-passwd** command to synchronize the cluster (**appadmin**) password currently set on the publisher with all the subscriber nodes in the cluster.



Synchronizing the cluster password changes the **appadmin** password for all the nodes in the cluster

Syntax

```
cluster sync-cluster-passwd
```

Example

The following example synchronizes the cluster password:

```
[appadmin]# cluster sync-cluster-passwd
```

```
Continue? [y|n]: y
```

```
Enter Password: college.205
```

```
Re-enter Password: college.205
```

Configure Commands

The W-Policy Manager command line interface includes the following **configure** commands:

- `configure date`
- `configure dns`
- `configure fips-mode`
- `configure hostname`
- `configure ip`
- `configure ip6`
- `configure mtu`
- `configure timezone`

configure date

Use the **configure date** command to set the system date, time, and time zone.

Syntax

```
configure date -d <date> [-t <time> ] [-z <timezone>]
```

or

```
configure date -s <ntpserver> [-z <timezone>]
```

The following table describes the required and optional parameters for the **configure date** command:

Table 387: *Configure Date Command Parameters*

Flag/Parameter	Description
-s <ntpserver>	Synchronizes time with the specified NTP server name (see <i>Example 2</i> below). This field is optional. NOTE: You can specify a destination node with an IPv6 address enabled.
-d <date>	Specifies the date with the syntax: yyyy-mm-dd . This field is mandatory.
-t <time>	Specifies the time with the syntax: hh:mm:ss . This field is optional.
-z <timezone>	Specifies the time zone syntax. To view the list of supported time zone values, enter show all-timezones . This field is optional.

Example 1

The following example configures the date, time, and the time zone:

```
[appadmin]# configure date -d 2007-06-22 -t 12:00:31 -z America/Los_Angeles
```

Example 2

The following example synchronizes with a specified NTP server:

```
[appadmin]# configure date -s pool.ntp.org
```

configure dns

Use the **configure dns** command to configure DNS servers. You must specify a minimum of one DNS server; you can specify a maximum of three DNS servers.

Syntax

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

Example 1: DNS Server

The following example configures a DNS server:

```
[appadmin]# configure dns 192.168.xx.1
```

Example 2: Primary and Secondary DNS Servers

The following example configures the primary and secondary DNS servers. You can configure IPv6 address as described in this example.

```
[appadmin]# configure dns 192.168.xx.1 2001:4860:4860::8888
```

Example 3: Primary, Secondary, and Tertiary DNS Servers

The following example configures primary, secondary, and tertiary DNS servers:

```
[appadmin]# configure dns 192.168.xx.1 2001:4860:4860::8888 192.168.xx.2
```

configure fips-mode

Use the **configure fips-mode** command to enable or disable **FIPS** (Federal Information Processing Standard) mode.



Running this command erases the ClearPass Policy Manager configuration settings and returns the database to the default configuration. All configured data will be lost. This command also shuts down all running applications and reboots the system.

Syntax

```
configure fips-mode [0|1]
```

The following table describes the required and optional parameters for the **configure fips-mode** command:

Table 388: *Configure fips-mode Command Parameters*

Flag/Parameter	Description
0	To disable FIPS mode, enter 0 . Read the warning message carefully before enabling or disabling FIPS mode.
1	To enable FIPS mode, enter 1 .

Example 1

The following example disables **FIPS** mode:

```
[appadmin]# configure fips-mode 0
*****
*                                     *
* WARNING: Running this command will erase the Policy Manager *
* configuration and leave the database with default          *
* configuration. You will lose all the configured data.      *
*                                     *
* This command will also shutdown all applications and reboot *
* the system.                                                *
*                                     *
* Do not close the shell or interrupt this command execution. *
*                                     *
*****
Continue? [y|n]: y
```

Clicking **y** in this example disables **FIPS** mode.

configure hostname

Use the **configure hostname** command to configure the hostname.

Syntax

```
configure hostname <hostname>
```

Example

The following example configures a hostname:

```
[appadmin]# configure hostname sun.us.dellnetworks.com
```

configure ip

Use the **configure ip** command to configure the IPv4 address of the management interface or the data interface, netmask, and gateway address.

Syntax

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

The following table describes the parameters used in the **configure ip** command:

Table 389: *Configure IP Command Parameters*

Flag/Parameter	Description
ip <mgmt data> <ip address>	Specifies the network interface type: management port interface or data port interface. <ip address> specifies the IPv4 address of the host.
netmask <netmask>	Specifies the netmask for the IP address.
gateway <gateway address>	Specifies the IP address for the network gateway.

Example

The following example configures the IP address for the data interface, the netmask for that address, and the gateway address:

```
[appadmin]# configure ip data 192.168.xx.12 netmask 255.255.255.0 gateway 192.168.xx.1
```

configure ip6

Use the **configure ip6** command to configure the IPv6 address, netmask, and gateway address of the host.

Syntax

```
configure ip6 <mgmt|data> <IPv6 address/PrefixLen> gateway <gateway address>
```

```
configure ip6 <mgmt|data> <IPv6 address> netmask <netmask> gateway <gateway address>
```

The following table describes the parameters used in the **ip6** command:

Table 390: *Configure ip6 Command Parameters*

Flag/Parameter	Description
ip6 <mgmt data> <ip address>	Specifies the network interface type: management interface or data interface.
netmask <netmask>	Specifies the netmask. For example, ffff:ffff:ffff:ffff:0000:0000:0000:0000.
gateway <gateway address>	Specifies the gateway address. For example, fe90:0000:0000:0000:020c:29ff:fe7e:d3a2.

Example

The following example configures the IPv6 management interface, netmask, and gateway address:

```
[appadmin]# configure ip6 mgmt fe90:0000:0000:0000:020c:29ff:fe7e:d3e1 netmask  
ffff:ffff:ffff:ffff:0000:0000:0000:0000 gateway fe90:0000:0000:0000:020c:29ff:fe7e:d3a1
```

configure mtu

Use the **configure mtu** command to set the MTU (Maximum Transmission Unit) for the management and data port interfaces.



Running this command might cause the W-ClearPass server to lose network connectivity.

Syntax

```
configure mtu <mgmt|data> <mtu-value>
```

The following table describes the **configure mtu** command parameters:

Table 391: *Configure mtu Command Parameters*

Flag/Parameter	Description
mtu <mgmt data>	Specifies the network interface types: management port interface or data port interface.
<mtu-value>	Specify the MTU value in bytes. The default value is 1500 bytes.

Example 1

The following example configures the MTU management interface:

```
[appadmin] # configure mtu mgmt 1498
*****
*
* WARNING: Running this command might cause system
* to lose network connectivity and may require relogin.*
*
*****
Continue? [y|Y]: y
INFO: Restarting network services
INFO: Successfully applied MTU settings
```

Example 2

The following example configures the MTU data port value:

```
[appadmin] # configure mtu data 1498
*****
*
* WARNING: Running this command might cause system
* to lose network connectivity and may require relogin.*
*
*****
Continue? [y|Y]: y
INFO: Restarting network services
INFO: Successfully applied MTU settings
```

Example 3

Use the **show ip** command to display the settings of the MTU management and data port interfaces:

```
[appadmin] # show ip
=====
Device Type      : Management Port
-----
```

```

IPv4 Address      :   10.2.xx.86

Subnet Mask       :   255.255.255.0
Gateway          :   10.2.xx.1

IPv6 Address      :   2607:f0d0:1002:0011:0000:0000:0000:0002
Subnet Mask       :   ffff:ffff:ffff:ffff:0000:0000:0000:0000
Gateway          :   2607:f0d0:1002:0011:0000:0000:0000:0001
Hardware Address  :   00:0C:29:70:27:40
MTU              :   1499
=====
Device Type       :   Data Port
-----
IPv4 Address      :   <not configured>
Subnet Mask       :   <not configured>
Gateway          :   <not configured>
IPv6 Address      :   fe80:0000:0000:0000:020c:29ff:fe70:274a
Subnet Mask       :   ffff:ffff:ffff:ffff:0000:0000:0000:0000
Gateway          :   fe80:0000:0000:0000:020c:29ff:fe70:2741
Hardware Address  :   00:0C:29:70:27:4A
MTU              :   1498
=====
DNS Information
-----
Primary   DNS    :   10.2.xx.3

Secondary DNS    :   10.1.xx.50

Tertiary   DNS   :   10.1.xx.200

=====

```

configure timezone

Use the **configure timezone** command to interactively configure the time zone.

Syntax

```
configure timezone
```

Example

The following example configures the time zone interactively:

```

[appadmin]# configure timezone
configure timezone
*****
* WARNING: When the command is completed Policy Manager services *
* are restarted to reflect the changes.                          *
*****
Continue? [y|Y]: y

```

Network Commands

The W-ClearPass Policy Manager command line interface includes the following **network** commands:

- [network ip6](#)
- [network ip](#)

- [nslookup](#)
- [Network Commands on page 743](#)
- [network ping6](#)
- [network reset](#)
- [network traceroute6](#)
- [network traceroute](#)

network ip6

Use the **network ip6** command to add, delete, or list custom routes to the data or management interface routing table in IPv6 networks.

Syntax: network ip6 add

```
network ip6 add <mgmt|data> [-i <id>] <[-s <SrcAddr>] [-d <DestAddr>]> [-g <ViaAddr>]
```

The following table describes the required and optional parameters for the **network ip6** command:

Table 392: Network IP6 Add Command Parameters

Flag/Parameter	Description
<mgmt data>	Specifies the management or the data interface.
-i <id>	Specifies the ID of the network IP rule. If this ID is not specified, the system generates an ID automatically. NOTE: This ID determines the priority in the ordered list of rules in the routing table.
-s <SrcAddr>	Specifies the source interface IPv6 address or netmask from where the network IPv6 rule is specified. For example, fe82::20c:29ff:fe7e:d3e1. A valid IPv6 address or a netmask or 0/0 values are allowed. This parameter is optional.
-d <DestAddr>	Specifies the destination interface IPv6 address or netmask where the network IPv6 rule is specified. A valid IPv6 address or a netmask or 0/0 values are allowed. This parameter is optional.
-g <ViaAddr>	Specifies the via or gateway IPv6 address through which the network traffic should flow. A valid IPv6 address is allowed. This parameter is optional.

Example: Adding an IPv6 Custom Route

You can use an IPv6 address when adding a custom route.

The following example adds a custom route:

```
[appadmin]# network ip6 add data -s fe82::20c:29ff:fe7e:d3e1/d3e24
```

Syntax: network ip6 del

This command deletes an IPv6 custom route.

```
network ip6 del <-i <id>>
```

Syntax: network ip6 list

This command lists all custom routing rules.

```
network ip6 list
```

Example: Listing All IPv6 Custom Routing Rules

The following example lists all custom routing rules:

```
[appadmin]# network ip6 list
```

```
=====
IP Rule Information
-----
0:   from all lookup local
13000: from all to fe82::20c:99ff:fe7e:d3e1 lookup mgmt
13001: from all to fe82::20c:99ff:fe7e:d3e4 lookup mgmt
13002: from all to fe82::20c:99ff:fe7e:d3e7 lookup mgmt
13003: from all to fe82::20c:99ff:fe7e:d3e8 lookup mgmt
13004: from all to fe82::20c:99ff:fe7e:d3e9 lookup mgmt
13005: from all to fe82::20c:99ff:fe7e:d3ea lookup static
32766: from all lookup main
=====
```

Syntax: network ip6 reset

```
network ip6 reset
```

This command resets the routing table to the factory default settings and all custom routes are removed.

network ip

Use the **network ip** command to add, delete, or list custom routes to the data or management interface routing table.

Syntax: network ip add

```
network ip add <mgmt|data|greN|vlanN> [-i <id>] <[-s <SrcAddr>] [-d <DestAddr>]> [-g <ViaAddr>]
```

The following table describes the required and optional parameters for the **network ip add** command:

Table 393: Network IP Add Command Parameters

Flag/Parameter	Description
<mgmt data greN vlanN>	Configures the management interface, data interface, the name of the GRE tunnel, or the VLAN number. <greN>: N specifies the GRE tunnel number ranging from 1,2,3...N. <vlanN>: N specifies the VLAN number.
-i <id>	Specifies the ID of the network IP rule. If this ID is not specified, the system generates an ID automatically. NOTE: This ID determines the priority in the ordered list of rules in the routing table.
-s <SrcAddr>	Specifies the IP address or network. For example, 192.168.xx.0/24 or 0/0 (for all traffic) of traffic originator. You must specify only one source IP address. This parameter is optional.

Table 393: *Network IP Add Command Parameters (Continued)*

Flag/Parameter	Description
-d <DestAddr>	Specifies the destination IP address or network. For example, 192.168.xx.0/24 or 0/0 (for all traffic). You must specify only one destination IP address. This parameter is optional.
-g <ViaAddr>	Specifies the via or gateway IP address through which the network traffic should flow. A valid IP address is allowed. This parameter is optional.

Syntax: network ip del

```
network ip del <-i <id>>
```

The following table describes the parameter for the **network ip del** command:

Table 394: *Network IP Del Command Parameters*

Flag/Parameter	Description
-i <id>	Specifies the ID of the rule to delete.

Syntax: network ip list

```
network ip list
```

This command lists all routing rules.

Example: Adding a Custom Route

The following example adds a custom route:

```
[appadmin]# network ip add data -s 192.168.xx.0/24
```

Example: Listing All Custom Routes

The following example lists all custom routes:

```
[appadmin]# network ip list
=====
      IP Rule Information
-----
0:   from all lookup local
10020: from all to 10.xx.4.0/24 lookup mgmt
10040: from 10.xx.4.200 lookup mgmt
10060: from 10.xx.5.200 lookup data
32766: from all lookup main
32767: from all lookup default
=====
```

Syntax: network ip reset

```
network ip reset
```

This command resets the routing table to the factory default settings. All custom routes are removed.

nslookup

Use the **network nslookup** command to get the IP address of the host using DNS.

Syntax: network nslookup

```
network nslookup -q <record-type> <host>
```

The following table describes the required and optional parameters for the `nslookup` command:

Table 395: *Network Nslookup Command Parameters*

Flag/Parameter	Description
<record-type>	Specifies the type of DNS record. The record types available are: • A • AAAA • CNAME • PTR • SRV
<host>	Specifies the host or domain name to be queried.

Example: Obtaining Address of Host or Domain

The following examples obtain the IPv4 and IPv6 addresses of the host or domain using DNS:

```
[appadmin]# nslookup sun.us.dellnetworks.com
[appadmin]# network nslookup 2001:4860:4860::8888
```

Example: Querying for SRV Records

The following example queries a host or domain for SRV records:

```
[appadmin]# nslookup -q SRV dellnetworks.com
```

Syntax

Use the **AAAA** flag with the **-q** option to perform network nslookup with IPv6 destinations.

```
nslookup -q AAAA <IPv6_addr>
```

Example: Nslookup for IPv6 Address

The following example performs network nslookup for the destination with an IPv6 address:

[illegible]

network ping6

Use the **network ping6** command to test the reachability of the network host.

Syntax: network ping6

```
network ping6 [-i <SrcIPv6Addr>] [-t] <host>
```

The following table describes the required and optional parameters for the **network ping6** command:

Table 396: Network Ping6 Command Parameters

Flag/Parameter	Description
-i <SrcIPv6Addr>	Specifies the originating IPv6 address for the ping. This field is optional.
-t	Use this parameter to ping indefinitely. This field is optional.
<host>	Specifies the host to be pinged.

Example

The following example pings an IPv6 network host to test its reachability:

```
[appadmin]# network ping6 -i fe82::20c:29ff:fe7e:d3e1 -t sun.us.  
dellnetworks  
.com
```

network ping

Use the **network ping** command to test the reachability of the network host.

Syntax: network ping

```
network ping [-i <SrcIpAddr>] [-t] <host>
```

The following table describes the required and optional parameters for the **network ping** command:

Table 397: Network Ping Command Parameters

Flag/Parameter	Description
-i <SrcIpAddr>	Specifies the originating IP address for the ping. This field is optional.
-t	Use this parameter to ping indefinitely. This field is optional.
<host>	Specifies the host to be pinged.

Example: Testing Reachability

The following example pings a network host to test the reachability:

```
[appadmin]# network ping -i 192.168.xx.10 -t sun.us.dellnetworks.com
```

network reset

Use the **network reset** command to reset the network data and management ports. You can use this command to reset both IPv4 and IPv6 addresses.

Syntax: network reset

```
network reset <data[v4|v6]/mgmt>
```

The following table describes the required and optional parameters for the **network reset** command:

Table 398: *Network Reset Command Parameters*

Flag/Parameter	Description
data [v4 v6]	Specifies the name of network data port to reset, as well as whether it is an IPv4 or IPv6 address. This parameter is mandatory.
mgmt	Specifies the name of network management port to reset.

Example

The following example resets the IPv6 network data port:

```
[appadmin]# network reset data v6
```

network traceroute6

Use the **network traceroute6** command to print the route taken to reach the IPv6 network host.

Syntax: network traceroute6

```
network traceroute6 <host>
```

The following table describes the required and optional parameters for the **network traceroute6** command:

Table 399: *Network Traceroute6 Command Parameters*

Flag/Parameter	Description
<host>	Specifies the name of network host. You can specify the host with an IPv6 address.

Example

The following example prints the route taken to reach the network host:

```
[appadmin]# network traceroute6 sun.us.dellnetworks.com
```

network traceroute

Use the **network traceroute** command to print the route taken to reach the network host.

Syntax: network traceroute

```
network traceroute <host>
```

The following table describes the required parameter for the **network traceroute** command:

Table 400: *Network Traceroute Command Parameters*

Flag/Parameter	Description
<host>	Specifies the name of the network host.

Example

The following example prints the route taken to reach the network host:

```
[appadmin]# network traceroute sun.us.dellnetworks.com
```

Miscellaneous Commands

The W-Policy Manager command line interface includes the following miscellaneous commands:

- [ad auth on page 750](#)
- [ad netjoin on page 751](#)
- [ad netleave on page 751](#)
- [ad passwd-server](#)
- [ad testjoin on page 752](#)
- [alias on page 753](#)
- [backup on page 753](#)
- [cli session idle timeout](#)
- [dump certchain on page 754](#)
- [dump logs on page 754](#)
- [dump servercert on page 755](#)
- [exit on page 755](#)
- [help on page 756](#)
- [krb auth on page 756](#)
- [krb list on page 756](#)
- [ldapsearch on page 757](#)
- [quit on page 757](#)
- [restore on page 757](#)

ad auth

Use the **ad auth** command to authenticate the user against Active Directory.

Syntax

```
ad auth <username> -n <domain NetBIOS name>
```

The following table describes the parameters for the **ad auth** command:

Table 401: AD Auth Command Parameter

Flag/Parameter	Description
<username>	Specifies the username of the authenticating user. This is a mandatory parameter.
<domain NetBIOS name>	Specifies the domain name. This field is optional.

Example

The following example authenticates the user against Active Directory:

```
[appadmin]# ad auth jbrown -n cppm.sanfran1
```

ad netjoin

Use the **ad netjoin** command to join the host to the domain.

Syntax

```
ad netjoin <domain-controller.domain-name> [domain NetBIOS name] [domain REALM name]
[ou=<object container>]
```

The following table describes the parameters for the **ad netjoin** command:

Table 402: AD Netjoin Command Parameters

Parameter	Action/Description
<domain-controller.domain-name>	Specify the complete Fully Qualified Domain Name (FQDN) of the domain controller, including its hostname. For example, if atlas.org is the Domain FQDN and DC01.atlas.org is one of its domain controllers, then this argument would be correctly expressed as DC01.atlas.org This field is mandatory.
[domain NetBIOS name]	Specify the NetBIOS name of the domain (optional argument). You can specify this argument if the derived NetBIOS name is different from the actual name. This is an optional argument.
[domain REALM name]	You can specify this argument if the derived REALM is different from the actual. This is an optional argument.
[ou=<object container>]	If the computer account must be created in a different OU, this argument specifies the Object Container . For example 'ou=Domain Computer' OR 'ou=Domain Computer+Linux Hosts'. Note the usage of the separator '+' to specify the OU hierarchy.

Example

The following example joins the host to the domain:

```
[appadmin]# ad netjoin DC01.atlas.org.dellnetworks.com
```

ad netleave

Use the **ad netleave** command to remove the host from the domain.

Syntax

```
ad netleave <domain NetBIOS name> [-f]
```

Table 403: AD Netleave Command Parameters

Flag/Parameter	Description
<domain NetBIOS name>	Specifies the host to be joined to the domain. This field is mandatory.
-f	Forces the removal of Active Directory domain membership even if the operation fails.

Example

The following example removes the host from the domain:

```
[appadmin]# ad netleave balsamcollege.edu -f
```

ad passwd-server

Use the **ad passwd-server** command to do the following tasks:

- Set the password servers.
- List the configured password servers.
- Reset the password servers.

Syntax

```
ad passwd-server <server> <list> <reset>
```

Table 404: *AD passwd-server Command Parameters*

Flag/Parameter	Description
set • -n <domain NetBIOS name> • -s <Server1> [Server2 Server3 Server4 ...]	Sets the password servers. The -n parameter specifies the domain name. The -s parameter specifies one or more password server names.
list -n <domain NetBIOS name>	Lists the configured password servers.
reset -n <domain NetBIOS name>	Resets the password servers.

Example

The following example sets the configured password servers:

```
[appadmin]# ad passwd-server set -n balsamcollege.edu -s cppm.campus1
```

ad testjoin

Use the **ad testjoin** command to test if the **ad netjoin** command succeeded. This command also tests whether W-Policy Manager is a member of the Active Directory domain.

Syntax

```
ad testjoin <domain NetBIOS name>
```

Table 405: *AD Netjoin Command Parameter*

Flag/Parameter	Description
<domain NetBIOS name>	Specifies the host to be joined to the domain. This field is mandatory.

Example

The following example tests if the **ad testjoin** command succeeded:

```
[appadmin]# ad testjoin balsamcollege.edu
```

alias

Use the **alias** command to create or remove aliases.

Syntax

```
alias <name>=<command>
```

The following table describes the required and optional parameters for **alias** command:

Table 406: Alias Command Parameters

Flag/Parameter	Description
<name>=<command>	Sets <name> as the alias for <command>.
<name>=	Removes the association.

Example 1

This example set the alias "**sh**" for the **show** command:

```
[appadmin]# alias sh=show
```

Example 2

This example removes the alias "**sh**":

```
[appadmin]# alias sh=
```

backup

Use the **backup** command to create backup of W-Policy Manager configuration data. If no arguments are entered, the system automatically generates a filename and backs up the configuration to this file.

Syntax

```
backup [-f <filename>] [-c] [-l] [-r] [-w] [-P]
```

The following table describes the required and optional parameters for the **backup** command:

Table 407: Backup Command Parameters

Flag/Parameter	Description
[-f <filename>]	Specifies the backup target. If not specified, W-Policy Manager automatically generates a filename. This field is optional.
-c	Backs up W-ClearPass W-Policy Manager configuration data.
-l	Backs up W-ClearPass W-Policy Manager session log data.
-r	Backs up Insight data.
-P	Does not backup password fields from the configuration database. This field is optional.
-w	Backs up only the most recent records from the log database (the last one week).

Example

```
[appadmin]# backup -f PolicyManager-data.tar.gz
Continue? [y|Y]: y
```

cli session idle timeout

Use the **cli session idle timeout** command to configure the amount of Idle time allowed before a CLI session timeout occurs.

Syntax

```
cli session idle timeout <minutes>
```

Table 408: CLI Session Idle Time Command Parameters

Flag/Parameter	Description
<time>	Specifies the time in minutes a session may be idle before a timeout.

Changes to the CLI session idle timeout will take effect only after the session is ended and a new session opened.

dump certchain

Use the **dump certchain** command to remove the certificate chain of any SSL-secured server.

Syntax

```
dump certchain <hostname:port-number>
```

The following table describes the required and optional parameters for the **dump certchain** command:

Table 409: Dump Certchain Command Parameters

Flag/Parameter	Description
<hostname:port-number>	Specifies the hostname and SSL port number.

Example 1

The following example dumps certificate chain of a SSL secured server:

```
[appadmin]# dump certchain ldap.acme.com:636
```

dump logs

Use the **dump logs** command to remove W-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]
```

The following table describes the required and optional parameters for the **dump logs** command:

Table 410: *Dump Logs Command Parameters*

Flag/Parameter	Description
-f <output-file-name>	Specifies the target for concatenated logs.
-s yyyy-mm-dd	Specifies the start date range. The default value is today's date. This field is optional.
-e yyyy-mm-dd	Specifies the end date range. The default value is today's date. This field is optional.
-n <days>	Specifies the duration in days (from today). This field is optional.
-t <log-type>	Specifies the type of log to collect. This field is optional.
-h	Specifies the print help for available log types.

Example 1

The following example dumps W-Policy Manager application log files:

```
[appadmin]# dump logs -f tips-system-logs.tgz -s 2007-10-06 -e 2007-10-17 -t SystemLogs
```

Example 2

The following example prints help for available log types:

```
[appadmin]# dump logs -h
```

dump servercert

Use the **dump servercert** command to remove the server certificate of an SSL-secured server.

Syntax

```
dump servercert <hostname:port-number>
```

The following table describes the required and optional parameters for the **dump servercert** command:

Table 411: *Dump Servercert Command Parameters*

Flag/Parameter	Description
<hostname:port-number>	Specifies the hostname and SSL port number.

Example

The following example removes the server certificate of the specified SSL-secured server:

```
[appadmin]# dump servercert ldap.acme.com:636
```

exit

Use the **exit** command to exit the shell.

Syntax

```
exit
```

Example

The following example exits the shell:

```
[appadmin]# exit
```

help

Use the **help** command to display the list of supported commands:

Syntax

```
help <command>
```

Example

The following example displays the list of supported commands:

```
[appadmin]# help
help
alias          Create aliases
backup         Backup Policy Manager data
cluster       Policy Manager cluster related commands
configure     Configure the system parameters
dump          Dump Policy Manager information
exit          Exit the shell
help          Display the list of supported commands
netjoin       Join host to the domain
netleave      Remove host from the domain
network       Network troubleshooting commands
quit          Exit the shell
restore       Restore Policy Manager database
service       Control Policy Manager services
show          Show configuration details
system       System commands
```

krb auth

User the **krb auth** command to perform a Kerberos authentication against a Kerberos server (such as Microsoft Active Directory).

Syntax

```
krb auth <user@domain>
```

The following table describes the parameter for the **krb auth** command:

Table 412: Kerberos Authentication Command Parameter

Flag/Parameter	Description
<user@domain>	Specifies the username and domain.

Example

The following example performs a kerberos authentication against a kerberos server:

```
[appadmin]# krb auth mike@corp-ad.acme.com
```

krb list

Use the **krb list** command to list the cached Kerberos tickets.

Syntax

```
krb list
```

Example

The following example lists the cached Kerberos tickets:

```
[appadmin]# krb list
```

ldapsearch

Use the Linux **ldapsearch** command to find objects in an LDAP directory. Note that only the W-Policy Manager-specific command line arguments are listed. For other command line arguments, refer to **ldapsearch** man pages on the Internet.

Syntax

```
ldapsearch -B <user@hostname>
```

The following table describes the parameters for the **ldapsearch** command:

Table 413: LDAP Search Command Parameter

Flag/Parameter	Description
-B	Finds the bind DN (Distinguished Name) of the LDAP directory.
<user@hostname>	Specifies the username and the full qualified domain name of the host.

Example

The following example finds objects in an LDAP directory:

```
[appadmin]# ldapsearch -B admin@corp-ad.acme.com
```

quit

Use the **quit** command to exit the shell.

Syntax

```
quit
```

Example

The following command quits the shell:

```
[appadmin]# quit
```

restore

Use the **restore** command to restore W-Policy Manager configuration data from the backup file.

Syntax 1

```
restore user@hostname:/<backup-filename> [-l] [-i] [-b] [-c] [-r] [-n|-N] [-s]
```

Syntax 2

```
restore http://hostname/<backup-filename>[-l] [-i] [-b] [-c] [-e] [-n|-N] [-s]
```

Syntax 3

```
restore <backup-filename>[-l] [-i] [-b] [-c] [-e] [-n|-N] [-s]
```

The following table describes the parameters for the **restore** command:

Table 414: *Restore Command Parameters*

Flag/Parameter	Description
• user@hostname:/<backup-filename> • http://hostname/<backup-filename> • <backup-filename>	Specifies the filepath of the the restore source.
-b	Does not backup the current configuration data before the restore operation starts.
-c	Restores W-ClearPass W-Policy Manager configuration data.
-l	If it exists in the backup file, restores the W-ClearPass W-Policy Manager log database. This field is optional.
-i	Ignores version mismatch errors and attempts data migration. This field is optional.
-n	Retains local node configuration data, such as certificates, after the restore operation (default).
-N	Does not retain local node configuration data after the restore operation.
-r	Restores Insight data if it exists in the backup.
-s	Restores cluster server/node entries from the backup file. Node entries are in a disabled state upon restore. This field is optional.

Example

The following example restores W-Policy Manager configuration data from the backup file:

```
[appadmin]# restore user@hostname:/tmp/cppm1-backup.tgz -l -i -c -s
```

Service Commands

The W-Policy Manager CLI includes the following **service** <action> commands:

- service list
- service restart
- service start
- service status
- service stop

service <action> <service-name>

Use the **service** <action> <service-name> command to control the specified W-Policy Manager service.

Syntax

service <action> <service-name>

Table 415: Service Action Command Parameters

Service Parameter	Description
action	1. Choose an action: ■ <i>list</i> ■ <i>restart</i> ■ <i>start</i> ■ <i>status</i> ■ <i>stop</i>
service-name	2. Choose a service: ■ <i>cpass-policy-server</i> ■ <i>cpass-tacacs-server</i> ■ <i>cpass-radius-server</i> ■ <i>cpass-admin-server</i> ■ <i>cpass-dbwrite-server</i> ■ <i>cpass-dbcn-server</i> ■ <i>cpass-repl-server</i> ■ <i>cpass-system-auxiliary-server</i> ■ <i>cpass-sysmon-server</i> ■ <i>cpass-domain-server_<NetBIOS_name></i> ■ <i>airgroup-notify</i> ■ <i>fias_server</i> ■ <i>cpass-ipsec-service</i> ■ <i>cpass-vip-service</i> ■ <i>cpass-async-netd</i> ■ <i>cpass-statsd-server</i> ■ <i>cpass-igssyslog-server</i> ■ <i>cpass-igslogger-server</i> ■ <i>cpass-igslogrepo-server</i> ■ <i>cpass-carbon-server</i> ■ <i>cpass-multi-master-cache-server</i>

Example

```
[appadmin]# service list all
```

```
Policy server [ cpass-policy-server ]
Admin UI service [ cpass-admin-server ]
System auxiliary services [ cpass-system-auxiliary-server ]
Radius server [ cpass-radius-server ]
Tacacs server [ cpass-tacacs-server ]
Async DB write service [ cpass-dbwrite-server ]
DB change notification server [ cpass-dbcn-server ]
DB replication service [ cpass-repl-server ]

System monitor service [ cpass-sysmon-server ]
Async network services [ cpass-async-netd ]
Multi-master cache [ cpass-multi-master-cache-server ]
Virtual IP service [ cpass-vip-service ]
Stats collection service [ cpass-statsd-server ]
```

```
Stats aggregation service [ cpass-carbon-server ]
ClearPass IPsec service [ cpass-ipsec-service ]
AirGroup notification service [ airgroup-notify ]
Micros Fidelio FIAS [ fias_server ]
Ingress logger service [ cpass-igslogger-server ]
Ingress syslog service [ cpass-igssyslog-server ]
```

Show Commands

The W-Policy Manager command line interface includes the following **show** commands:

- [show all-timezones](#)
- [show date](#)
- [show dns](#)
- [show domain](#)
- [show fipsmode](#)
- [show fipsmode](#)
- [show hostname](#)
- [show ip](#)
- [show license](#)
- [show ntp](#)
- [show sysinfo](#)
- [show timezone](#)
- [show version](#)

show all-timezones

Use the **show all-timezones** command to view all available time zones.

Syntax

```
show all-timezones
```

Example

The following displays an example of the **show all-timezones** command output:

```
[appadmin]# show all-timezones
America/Aruba
America/Barbados
America/Belem
America/Belize
[More]
```

show date

Use the **show date** command to view the system date, time, and time zone information.

Syntax

```
show date
```

Example

The following displays an example of the **show date** command output:

```
[appadmin]# show date
```

```
Wed Jan 27 14:33:39 UTC 2016
```

show dns

Use the **show dns** command to view DNS (Domain Name System) servers.

Syntax

```
show dns
```

Example

The following example of **show dns** command output displays the DNS servers configured for the current W-ClearPass server:

```
[appadmin]# show dns
```

```
=====
DNS Information
-----
Primary   DNS   :   192.xxx.5.3
Secondary DNS :   <not configured>

Tertiary  DNS   :   <not configured>
=====
```

show domain

Use the **show domain** command to view the Active Directory Domain controller information.



The **show domain** command is operational only when the current W-ClearPass server is joined to an Active Directory domain.

Syntax

```
show domain
```

Example

The following displays an example of the **show domain** command output:

```
[appadmin]# show domain
```

```
=====
Domain Information
-----
Domain Name           : COLLEGE152.COM
Domain NETBIOS Name   : COLLEGE152
Domain Server IP Address : 10.xx.110

Domain Server Name     : balsam.college152.com
Domain Status          : online
-----
=====
```

show fipsmode

Use the **show fipsmode** command to find whether **FIPS** (Federal Information Processing Standard) mode is enabled or disabled.

Example

The following example shows that **FIPS** mode is enabled:

```
[appadmin]# show fipsmode
FIPS Mode: Enabled
```

show hostname

Use the **show hostname** command to view the hostname of the current W-ClearPass server.

Syntax

```
show hostname
```

Example

The following displays an example of the **show hostname** command:

```
[appadmin]# show hostname
cpm.chicago.1
```

show ip

Use the **show ip** command to view the IPv4, IPv6, and DNS information of the host.

Syntax

```
show ip
```

Example

The following example of the **show ip** command displays the IPv4, IPv6, and DNS information of the host:

```
[appadmin]# show ip
=====
Device Type      :   Management Port
-----
IPv4 Address     :   10.2.xx.86

Subnet Mask      :   255.255.255.0
Gateway          :   10.2.xx.1
IPv6 Address     :   2607:f0d0:1002:0011:0000:0000:0000:0002
Subnet Mask      :   ffff:ffff:ffff:ffff:0000:0000:0000:0000
Gateway          :   2607:f0d0:1002:0011:0000:0000:0000:0001
Hardware Address :   00:0C:29:70:27:40
MTU              :   1499
=====
Device Type      :   Data Port
-----
IPv4 Address     :   <not configured>
Subnet Mask      :   <not configured>
Gateway          :   <not configured>
IPv6 Address     :   fe80:0000:0000:0000:020c:29ff:fe70:274a
Subnet Mask      :   ffff:ffff:ffff:ffff:0000:0000:0000:0000
Gateway          :   fe80:0000:0000:0000:020c:29ff:fe70:2741
```

```

Hardware Address : 00:0C:29:70:27:4A
MTU              : 1498
=====
DNS Information
-----
Primary   DNS : 10.2.xx.30

Secondary DNS : 10.1.xx.50

Tertiary  DNS : 10.1.xx.200
=====

```

show license

Use the **show license** command to view the W-Policy Manager license information.

Syntax

```
show license
```

Example

The following displays an example of the **show license** command output:

```
[appadmin]# show license
```

```

-----
Application           : PolicyManager
License key           : VKQO-MW62AB-VMVF-B7GNJX-OHUABC-IAAM-RTQUPQ-WODIFNJI-CD7N-I1325A

License key type      : Permanent
License added on      : 2016-01-11 10:16:38

Validity              : <not applicable>
Issued for            : 5000 users
Customer id           : JCC

Licensed features      : <not applicable>

-----
Application           : PolicyManager
License key           : VKQO-MW62AB-VMVF-B7GNJX-OHUABC-IAAM-RTQUPQ-WODIFNJI-CD7N-I1325A
License key type      : Permanent
License added on      : 2016-01-11 10:16:38

Validity              : <not applicable>
Issued for            : 5000 users
Customer id           : JCC

Licensed features      : <not applicable>

=====

```

show ntp

Use the **show ntp** command to view the IP addresses of the primary and secondary Network Time Protocol (NTP) servers configured for the current W-ClearPass server.

Syntax

```
show ntp
```

Example

The following displays an example of the **show ntp** command output:

```
[appadmin]# show ntp

=====

NTP Server Information
-----
Primary   NTP   :    10.xx.x.1
Secondary NTP   :    <not configured>

=====
```

show sysinfo

Use the **show sysinfo** command to view the node uptime, disk utilization, and memory utilization information:

Syntax

```
show sysinfo
```

Example

The following displays an example of the **show sysinfo** command output:

```
[appadmin]# show sysinfo
System Uptime :  1 day, 23:29:15.510000

=====

Disk Utilization
-----
Total          :    115.48 GB
Free           :    5.42 GB (6%)

=====

Memory Utilization
-----
Total          :    4.00 GB
Free           :    1.36 GB (36%)

=====
```

show timezone

Use the **show timezone** command to view the current system time zone.

Syntax

```
show timezone
```

Example

The following displays an example of the **show timezone** command output:

```
[appadmin]# show timezone

Timezone is set to 'Asia/Kolkata'
```


show version

Use the **show version** command to view the W-Policy Manager software version and the hardware model.

Syntax

```
show version
```

Example

The following displays an example of the **show version** command output:

```
[appadmin]# show version
=====
Policy Manager software version : 6.6(1).6649
Policy Manager model number    : ET-5010
=====
```

SSH Timed Account Lockout

This section provides the following information:

- [Introduction](#)
- [SSH Account Lockout Configuration](#)
- [SSH Account Lockout Alerts](#)
- [SSH Account Lockout Behavior](#)

Introduction

The **SSH Timed Account Lockout** feature provides an administrator with the ability to configure the number of successive unsuccessful authentication attempts for administrators attempting to authenticate remotely.

When the defined number of unsuccessful authentication attempts has occurred, the CLI account is locked and administrators cannot log in to the system via the CLI until one of the following conditions are met:

- Prevent the offending remote administrator from successfully authenticating until an action is taken by a local administrator.
- Prevent the offending remote administrator from successfully authenticating until time period defined by the administrator has elapsed.

Node-Specific

This feature is node-specific. In a cluster with multiple nodes, SSH timed account lockout must be configured on each node in the cluster.

Cluster Reset-Database Command

The **cluster reset-database** command does not impact this feature.

Account Lockout Persistence

- The SSH timed account lockout feature configuration persists across reboots, updates and upgrades.
- The account lock status persists across reboots.

SSH Account Lockout Configuration

The **SSH Timed Lockout** options are exposed as a part of the **ssh** command set.

Figure 730: *SSH Command Set*

```
[appadmin@123]# ssh
lockout      SSH lockout configuration options
unlock      Unlock the SSH locked out account
```

SSH Lockout

The **ssh lockout** command set provides ability to configure SSH lockout configuration options. This command exposes three options :

- count
- duration
- reset

Figure 731: *SSH Lockout Command Set*

```
[appadmin@123]# ssh lockout
Usage:
count      Lockout attempts
duration   Lockout duration
reset      Reset SSH lockout configuration
```

SSH Lockout Count

Sets the maximum number of failed login attempts before the account is locked out. The default is **5**.

Figure 732: *SSH Lockout Count Command*

```
[appadmin@123]# ssh lockout count
Usage:
ssh lockout count <N>
Where
N      -- Maximum failed SSH password login attempts prior to
account lockout. Allowed values are 1-1000. If
ssh lockout duration is non-zero, this value
(when not configured) defaults to 5.

[appadmin@123]# ssh lockout count 3
INFO: SSH lockout details updated to - Lockout count = 3, Unlock time = 900 secs
```

Syntax

```
ssh lockout count <N>
```

Example

```
ssh lockout count 3
```

SSH Lockout Duration

Sets the amount of time in minutes that the account will remain locked after the number of SSH password login attempts exceeds the SSH lockout count.

Figure 733: *SSH Lockout Duration Command*

```
[appadmin@123]# ssh lockout duration
Usage:
    ssh lockout duration <N mins>
Where
    N          -- Amount of time (in mins) the account will remain locked after the
                  maximum failed SSH password login attempts. Allowed values
                  are 1-10080. If ssh lockout count is non-zero, this value
                  (when not configured) defaults to 15.

[appadmin@123]# ssh lockout duration 3
INFO: SSH lockout details updated to - Lockout count = 3, Unlock time = 180 secs
[appadmin@123]#
```

Syntax

```
ssh lockout duration <N minutes>
```

Example

```
ssh lockout duration 3
```

SSH Lockout Reset

Resets the SSH lockout count and duration to factory defaults and disables this feature.



The SSH timed account lockout feature is disabled by default.

Figure 734: *SSH Lockout Reset Command*

```
[appadmin@123]# ssh lockout reset
INFO: SSH lockout reset for the user appadmin
```

SSH Unlock

Unlocks any SSH locked accounts.

When the account is locked, you can perform this operation by logging into the system via the console or from a host that is enabled for SSH public key authentication with W-ClearPass.

Figure 735: *SSH Unlock Command*

```
[appadmin@123]# ssh unlock
INFO: Unlocked SSH lockout for the user appadmin
```

Show SSH

Shows the SSH lockout configuration settings and the active SSH client sessions.

Figure 736: *Show SSH Command*

```
[appadmin@123]# show ssh
=====
SSH lockout details
-----
SSH lockout count      : 7 attempts
SSH lockout duration   : 900 secs
-----
SSH sessions
-----
Client IP Address = 10. [REDACTED] : Session Count = 3
Client IP Address = 10. [REDACTED] : Session Count = 2
Client IP Address = 10. [REDACTED] : Session Count = 1
=====
```

SSH Account Lockout Alerts

Alerts for SSH lockout events are logged in to the Event Viewer when any of the following conditions are present:

- SSH lockout configurations are performed
- Account is locked
- Account is unlocked
- Failed SSH login attempts

SSH Account Lockout Behavior

The SSH account lockout feature is disabled by default.

1. To enable SSH account lockout:
 - Perform the **ssh lockout count** or **ssh lockout duration** configuration options.
2. To disable the feature, perform **ssh lockout reset**.
3. If the SSH account lockout feature is configured with **failed attempts=3** and **unlock time = 5 minutes**:
 - CLI access via SSH (password-based) authentication is locked on three consecutive failed login attempts.
 - If the failed password attempt continues (even after the account is locked), the unlock time shifts for the next five minutes (as in this example) from the current time from the last failed login attempt.
 - Successful password-based SSH logins are rejected during the lockout period.
 - Console-based logins are allowed during the lockout period.
 - SSH logins via public key methods are allowed during the lockout period.
4. Administrators can use any of the above options to reset the SSH account lockout. This can be done via **ssh unlock**.
5. After the lockout period, successful SSH logins are accepted and the account is unlocked.

System Commands

The W-Policy Manager command line interface (CLI) includes the following **system** commands:

- `system apps-access-reset`
- `system boot-image`
- `system cleanup`
- `system create-api-client`
- `system gen-recovery-key`
- `system gen-support-key`
- `system install-license`
- `system morph-vm`
- `system refresh-license`
- `system reset-server-certificate`
- `system restart`
- `system shutdown`
- `system sso-reset`
- `system start-rasession`
- `system status-rasession`
- `system terminate-rasession`
- `system update`
- `system upgrade`

system apps-access-reset

Use the **system apps-access-reset** command to reset the access control restrictions for W-Policy Manager.

Syntax

```
system apps-access-reset
```

Example

The following example reset the access control restrictions for W-Policy Manager:

```
[appadmin]# system apps-access-reset  
Policy Manager application access is restored
```

system boot-image

Use the **system boot-image** command to set system boot image control options.

Syntax

```
system boot-image [-l] [-a <version>]
```

The following table describes the required and optional parameters for the **system boot-image** command:

Table 416: *Boot-Image Command Parameters*

Flag/Parameter	Description
-l	Lists the boot images installed on the system.
-a <version>	Sets the active boot image version in <i>A.B.C.D</i> syntax. This field is optional.

Example

The following example sets the system boot image control options:

```
[appadmin]# system boot-image -l
```

system cleanup

Use the **system cleanup** command to perform a system cleanup operation that purges the following records:

- System and application log files
- Past authentication records
- Audit records
- Expired guest accounts
- Past auto and manual backups
- Stored reports

Syntax

```
system cleanup <num_days>
```

The following table describes the required parameter for the **system cleanup** command:

Table 417: *System Cleanup Command Parameter*

Flag/Parameter	Description
<num_days>	This is the cleanup interval that specifies the number of days to retain the data. This field is mandatory.

Example

The following example performs a system cleanup operation that retains records for four days:

```
[appadmin]# system cleanup 4
```

```
*****
*                                     *
* WARNING: This command will perform system cleanup   *
* operation that will result in purging of:           *
* [*] system and application log files                 *
* [*] past authentication records                     *
* [*] audit records                                  *
* [*] expired guest accounts                          *
* [*] past auto and manual backups                    *
* [*] stored reports etc...                          *
*                                     *
*****
Are you sure you want to continue? [y|n]: y
INFO - Starting system cleanup
```

INFO - Purging diagnostic dumps
INFO - Detected empty core directory
INFO - Performing system cleanup tasks
INFO - Purging platform logs
INFO - Purging application logs
INFO - Performing database cleanup tasks
INFO - Completed system cleanup

system create-api-client

Use the **system create-api-client** command create a new API client.

Syntax

```
system create-api-client <Client_ID> <Client_Secret>
```

Example

The following example creates an API client and specifies the client ID and client secret:

```
system create-api-client Win.139 college52
```

system gen-recovery-key

Use the **system gen-recovery-key** command to generate the recovery key for the system.

Example

The following example generates the recovery key for the system:

```
[appadmin]# system gen-recovery-key  
Recovery key='04U2FsdGVkX18To8NDWayziQ17LzKA17DW5y+AZvGj41c='
```

system gen-support-key

Use the **system gen-support-key** command to generate the support key for the system.

Syntax

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

Example

The following example generates the support key for the system:

```
[appadmin]# system gen-support-key  
system gen-support-key  
Support key='01U2FsdGVkX1+/WS9jZKQajERyzXhM8mF6zAKrzzrHvaM='
```

system install-license

Use the **system install-license** command to replace the current license key with a new one.

Syntax

```
system install-license <license-key>
```

The following table describes the required parameter for the **system install-license** command:

Table 418: *System Install-License Command Parameter*

Flag/Parameter	Description
<license-key>	Specifies the newly issued license key. This field is mandatory.

Example

The following example replaces the current license key with a new one:

```
[appadmin]# system install-license API111-3117-90982-007
```

system morph-vm

Use the **system morph-vm** command to convert an evaluation virtual machine (VM) to a production virtual machine .

With this command, licenses are still required to be installed after the morph operation is completed.

To convert an evaluation virtual machine to a production virtual machine:

1. Determine the type of the appliance to which you want to morph your evaluation virtual machine .
2. Procure the license for the target virtual appliance.
3. Shut down the virtual machine.
4. Determine the required capacity of an additional hard disk and attach it to the target virtual appliance.
5. Adjust the CPU and Memory settings for the evaluation virtual machine to match the target virtual appliance.
6. Boot the virtual machine.
7. Execute the **system morph-vm** command.

The configuration data from the evaluation virtual machine will be migrated to the newly-attached disk. The node will reboot as a virtual machine of the selected appliance model.

8. Log in to the user interface and enter the permanent license.

The evaluation virtual machine is now a production virtual machine .

Syntax

```
system morph-vm <CP-VA-500 | CP-VA-5K | CP-VA-25K>
```

The following table describes the parameters for the **system morph-vm** command:

Table 419: *System Morph-VM Command*

Flag/Parameter	Description
<vm-version>	This is the updated W-ClearPass version of the virtual appliances. The following options are available: • CP-VA-500 • CP-VA-5K • CP-VA-25K This field is mandatory.

Example

The following example converts an evaluation virtual machine to a production CP-25K virtual appliance:


```
[appadmin]# system morph-vm CP-VA-25K
```

system refresh-license

Use the **system refresh-license** command to refresh the license count information.

Syntax

```
system refresh-license
```

Example

The following example refreshes the license count information:

```
[appadmin]# system refresh-license
```

INFO: Refreshing license count information

INFO: Successfully refreshed license count information

system reset-server-certificate

Use the **system reset-server-certificate** command to reset the HTTP server certificate or RADIUS server certificate or both.

After executing the command, the W-Policy Manager services are restarted to reflect the changes.

Syntax

```
System reset-server-certificate
```

Example

The following example resets both HTTP and RADIUS server certificates:

```
[appadmin]# system reset-server-certificate
```

```
*****
*                                     *
* WARNING: When the command is completed Policy Manager services *
* are restarted to reflect the changes.                               *
*                                     *
*****
```

Continue? [y | n]: **y**

0: Reset Http and Radius Server Certificates

1: Reset Radius Server Certificate

2: Reset Http Server Certificate

3: Quit

2

Updating the server certificate...

Updation of server certificate complete

system restart

Use the **system restart** command to restart the system.



Executing this command shuts down all running applications and reboots the system.

Syntax

```
system restart
```

Example

The following example restarts the system with a confirmation before proceeding:

```
[appadmin]# system restart
system restart
*****
* WARNING: This command will shut down all applications *
*
* and reboot the system *
*****
Are you sure you want to continue? [y|Y]: y
```

system shutdown

Use the **system shutdown** command to shut down the current W-ClearPass server.



Executing this command shuts down all running applications and powers off the system.

Syntax

```
system shutdown
```

Example

The following example shuts down the system with a confirmation before proceeding:

```
[appadmin]# system shutdown
*****
* WARNING: This command will shut down all applications *
*
* and power off the system *
*****
Are you sure you want to continue? [y|Y]: y
```

system sso-reset

Use the **system sso-reset** command to reset the Single Sign-On (SSO) configuration.

Syntax

```
system sso-reset
```

system start-rasession

Use the **system start-rasession** command to start a Remote Assistance (RA) session.

Syntax

```
system start-rasession [duration_hours | duration_mins | contact_id | cppm_server_ip]
```

The following table describes the parameters for the **system start-rasession** command:

Table 420: *System Start Remote Assistance Session Command Parameters*

Flag/Parameter	Action/Description
duration_hours	1. Specify the session duration in hours. You can specify values from 0 to 12.
duration_mins	2. Specify the session duration in minutes. You can specify values from 0 to 59.
contact_id	3. Enter the username ID part of the Dell TAC or Engineering contact.
cppm_server_ip	4. Specify the W-ClearPass W-Policy Manager server IP address.

system status-rasession

Use the **system status-rasession** command to view the status of a Remote Assistance session.

Syntax

```
system status-rasession <session_id>
```

Example

The following example displays the status of a Remote Assistance session 3001:

```
[appadmin]# system status-rasession 3001
```

system terminate-rasession

Use the **system terminate-rasession** command to terminate a running Remote Assistance session.

Syntax

```
system terminate-rasession <session_id>
```

Example

The following example terminates a running RemoteAssist session 3001:

```
[appadmin]# system terminate-rasession 3001
```

system update

The **system update** command provides options to manage system patch updates.

Syntax

```
system update [-i [-f] <user@hostname:/<filename> | http://hostname/<filename>>>]
```

```
system update [-f]
```

```
system update [-l]
```

The following table describes the required and optional parameters for the **system update** command:

Table 421: *System Update Command Parameters*

Flag/Parameter	Description
-i user@hostname:<filename> http://hostname/<filename>	Installs the specified patch on the system. This field is optional.
-f	Reinstalls the patch in the event of a problem with the initial installation attempt. This field is optional.
-l	Lists the patches installed on the system. This field is optional.



This command supports Secure Copy (SCP), HTTPS, HTTP, and local uploads.

Example

The following example of the system update command will reinstall the patch if necessary and list the patches currently installed on the W-ClearPass server:

```
[appadmin]# system update -f -l
```

system upgrade

The **system upgrade** command upgrades the system. This command provides you with the following system upgrade options:

- From a Linux server
- From a Web server
- Performing an offline upgrade

Syntax

- **Upgrading from a Linux server**

```
system upgrade user@hostname:<filepath> [-w] [-l] [-L]
```

See [Example 1: Upgrading from a Linux Server](#).

- **Upgrading from a Web server**

```
system upgrade http://hostname/<filepath> [-w] [-l] [-L]
```

See [Example 2: Upgrading from a Web Server](#).

- **Performing an offline upgrade**

```
system upgrade <filepath> [-w] [-l] [-L]
```

See [Example 3: Performing an Offline Upgrade](#).

Table 422: *System Upgrade Command Parameters*

Flag/Parameter	Description
-w	Restores last (one) week of access tracker records after the upgrade.
-l	Restores all access tracker records from this version.
-L	Does not backup or restore access tracker records from this version.

Table 422: *System Upgrade Command Parameters (Continued)*

Flag/Parameter	Description
<filepath>	Enter the filepath using the syntax provided in the two examples below. This field is mandatory.



This command supports Secure Copy (SCP), HTTPS, HTTP, and local uploads.



If none of these **system upgrade** command options are specified, Access Tracker records are backed up, but they are not restored by default.

Example 1: Upgrading from a Linux Server

To upgrade the W-Policy Manager image from a Linux server:

1. Upload the upgrade image to a Linux server.
2. Use the following syntax to upload the upgrade image:

```
system upgrade user@hostname:/<filepath> [-w] [-l] [-L]
```

For example:

```
[appadmin]# system upgrade admin@sun.us.dellnetworks.com:/tmp/PolicyManager-x86-64-upgrade-71.tgz
```

Example 2: Upgrading from a Web Server

To upgrade the W-Policy Manager image from a Web server:

1. Upload the upgrade image to a Web server.
2. Use the following syntax to upload the upgrade image:

```
system upgrade http://hostname/<filepath> [-w] [-l] [-L]
```

For example:

```
[appadmin]# system upgrade http://sun.us.dellnetworks.com/downloads/PolicyManager-x86-64-upgrade-71.tgz
```

Example 3: Performing an Offline Upgrade

To perform an offline upgrade:

1. Log in to the Dell Download site: download.dell-pcw.com.
2. Navigate to the **ClearPass > Policy Manager > Current Release > Upgrade** folder.
3. In the **Description Remarks** section, click the link for the appropriate upgrade.
The upgrade file is uploaded to your local system.
4. Navigate to the W-ClearPass W-Policy Manager **Software Updates** page at **Administration > Agents and Software Updates > Software Updates**.
5. In the **Firmware & Patch Updates** section of the **Software Updates** page, click the **Import Updates** button.
The **Import from File** dialog appears.
6. Browse to the location of the upgrade file on your system, then click **Import**.
The selected upgrade file is uploaded to the W-ClearPass Policy Manager.
7. Log in to the W-Policy Manager command line interface (CLI) with the following user name: *appadmin*.

8. Initiate the upgrade process by entering the following command:

```
system upgrade <filepath> [-w] [-l] [-L]
```

For example:

```
[appadmin]# system upgrade CPPM-upgradeimage.bin
```

9. After the upgrade process is complete, restart the machine by issuing the following command in the CLI:

```
system restart
```

The W-Policy Manager restarts and boots up to the most recent version of W-ClearPass Policy Manager.

This appendix contains the following information:

- [W-ClearPass SNMP Private MIB](#)
- [SNMP Trap Details](#)
- [Important System Events](#)
- [Error Codes](#)

W-ClearPass SNMP Private MIB

This section contains the following information:

- [Introduction](#)
- [System MIB Entries](#)
- [RADIUS Server MIB Entries](#)
- [Policy Server MIB Entries](#)
- [Web Authentication Server MIB Entries](#)
- [TACACS+ Server MIB Entries](#)
- [Network Traffic MIB Entries](#)

Introduction

A MIB (Management Information Base) is a collection of definitions that define the properties of the managed object within the device to be managed. The various pieces of information are accessed by a protocol such as SNMP.

This section describes the MIB objects exposed and traps sent through the W-ClearPass Policy Manager Private SNMP MIB.

System MIB Entries

[Table 423](#) describes the *CPPMSystemTableEntry* MIB objects.

Table 423: *CPPMSystemTableEntry* System MIB Objects

MIB Object	Description
cppmClusterNodeType	W-ClearPass cluster node type indicating whether the node is a Publisher or Subscriber
cppmNwDataPortIPAddress	W-ClearPass server data port IP address
cppmNwDataPortMACAddress	W-ClearPass server data port MAC address
cppmNwMgmtPortIPAddress	W-ClearPass server management port IP address

Table 423: *CPPMSystemTableEntry* System MIB Objects (Continued)

MIB Object	Description
cppmNwMgmtPortMACAddress	W-ClearPass server management port MAC address
cppmSystemDiskSpaceFree	Amount of disk space free (in bytes) in the W-ClearPass server
cppmSystemDiskSpaceTotal	Total amount of disk space available (in bytes) in the W-ClearPass server
cppmSystemHostname	W-ClearPass server host name
cppmSystemMemoryFree	Amount of memory free (in bytes) in the W-ClearPass server
cppmSystemMemoryTotal	Total amount of memory available (in bytes) in the W-ClearPass server
cppmSystemModel	Model of the W-ClearPass server
cppmSystemNumCPUs	Total number of CPUs in the W-ClearPass server
cppmSystemSerialNumber	Serial number of the W-ClearPass server
cppmSystemUptime	Amount of time the W-ClearPass server has been up
cppmSystemVersion	Product version of the W-ClearPass server

RADIUS Server MIB Entries

RadiusServerTableEntry

Table 424 describes the *RadiusServerTableEntry* objects.

Table 424: *RadiusServerTableEntry* Objects

MIB Object	Description
radAuthRequestTime	Total time taken for an end-to-end RADIUS request
radPolicyEvalTime	Time taken for policy evaluation from the RADIUS server perspective
radServerCounterCounts	Total number of successful RADIUS authentications
radServerCounterFailure	Total number of failed RADIUS authentications
radServerCounterSuccess	Total number of successful RADIUS authentications

RadiusServerAuthTableEntry

RadiusServerAuthTableEntry exposes the following counters that refer to *authSourceName* wherever applicable (see [Table 425](#)). Counters and delays reflect details that are logged into Graphite.

Table 425: *RadiusServerAuthEntry MIB MIB Objects*

MIB Object	Description
radAuthCounterCount	Total number of RADIUS authentications
radAuthCounterFailure	Total number of failed RADIUS authentications
radAuthCounterSuccess	Total number of successful RADIUS authentications
radAuthCounterTime	Time taken to perform RADIUS authentications
radAuthSourceName	Name of the RADIUS server authentication source

Policy Server MIB Entries

PolicyServerTableEntry

PolicyServerTableEntry exposes the following MIB objects (see [Table 426](#)). Counters and delays reflect details logged into Graphite.

Table 426: *PolicyServerTableEntry Objects*

MIB Object	Description
psAuditPolicyEvalCount	Audit policy evaluation count
psAuditPolicyEvalTime	Audit policy evaluation time
psAuthCounterFailure	Number of failed Policy Server authentications
psAuthCounterSuccess	Number of successful Policy Server authentications
psAuthCounterTotal	Total number of Policy Server authentications
psEnforcementPolicyEvalCount	Enforcement policy evaluation count
psEnforcementPolicyEvalTime	Enforcement policy evaluation time
psPosturePolicyEvalCount	Posture policy evaluation count
psRestrictionPolicyEvalCount	Authorization restriction policy evaluation count
psRolemappingPolicyEvalCount	Role mapping policy evaluation count

Table 426: *PolicyServerTableEntry Objects (Continued)*

MIB Object	Description
psRolemappingPolicyEvalTime	Role mapping policy evaluation time
psPosturePolicyEvalTime	Posture policy evaluation time
psRestrictionPolicyEvalTime	Restriction policy evaluation time
psServicePolicyEvalCount	Service policy evaluation count
psServicePolicyEvalTime	Service policy evaluation time
psSessionlogTime	Policy Server session logging time

PolicyServerProtoTableEntry

PolicyServerProtoTableEntry exposes MIB objects for the counter values for the RADIUS, TACACS, WEBAUTH, and APPLICATION protocols.

Table 427: *PolicyServerProtoTableEntry MIB Objects*

MIB Object	Description
psPolicyEvalTime	Policy evaluation time for the protocol
psProtocolName	Name of the protocol

PolicyServerAutzTableEntry

PolicyServerAutzTableEntry exposes MIB objects for authorization counters (see [Table 428](#)).

Table 428: *PolicyServerAutzTableEntry MIB Objects*

MIB Object	Description
psAutzCounterCount	Total number of Policy Server authorizations
psAutzCounterFailure	Number of failed Policy Server authorizations
psAutzCounterSuccess	Number of successful Policy Server authorizations
psAutzCounterTime	Time taken to perform Policy Server authorizations
psAutzAuthSourceName	Name of the Policy Server authorization source

Web Authentication Server MIB Entries

WebAuthProtoTableEntry exposes MIB objects for the WebLogin, AppLogin, SamlIdp, and SamlSp web authentication protocols.

Table 429: *WebAuthProtoTableEntry* MIB Objects

MIB Object	Description
waAuthCounterAuthTime	Time taken for web authentication
waAuthCounterCount	Total number of web authentications
pwaAuthCounterFailure	Number of failed web authentications
waAuthCounterSuccess	Number of successful web authentications
waAuthCounterTime	Total time taken for web login
waPolicyEvalTime	Time taken to perform policy evaluation
waProtocolName	Name of the protocol
pwaServicePolicyEvalTime	Time taken to perform service policy evaluation

TACACS+ Server MIB Entries

TacacsAuthTableEntry

TacacsAuthTableEntry exposes MIB objects for TACACS+ authentication counters.

Table 430: *TacacsAuthTableEntry* Objects

MIB Object	Description
tacAuthCounterAuthTime	Time taken for TACACS+ authentications
tacAuthCounterCount	Total number of TACACS+ server authentications
tacAuthCounterFailure	Number of failed TACACS+ server authentications
tacAuthCounterSuccess	Number of successful TACACS+ server authentications
tacAuthCounterTime	Total time taken for TACACS+ login
tacPolicyEvalTime	Time taken to perform policy evaluation
tacServicePolicyEvalTime	Time taken to perform service policy evaluation

TacacsAutzTableEntry

TacacsAutzTableEntry exposes MIB objects for TACACS+ authorization counters.

Table 431: *TacacsAuthTableEntry Objects*

MIB Object	Description
tacAutzCounterCount	Total number of TACACS+ server authorizations
tacAutzCounterFailure	Number of failed TACACS+ server authorizations
tacAutzCounterSuccess	Number of successful TACACS+ server authorizations
tacAutzCounterTime	Total time taken for TACACS+ authorizations

Network Traffic MIB Entries

NetworkTrafficTableEntry exposes MIB objects for network protocol and applications. These MIB objects cover the following:

- agent_controller (6658)
- db (5432)
- http (80)
- https (443)
- ntp (123)
- radius (1645, 1646, 1812, 1813)
- ssh (22)
- tacacs (49)

Table 432: *TacacsAuthTableEntry Objects*

MIB Object	Description
nwAppPort	Application port
nwAppName	Application name
nwTrafficTotal	Total network traffic in bytes

W-ClearPass SNMP Traps and OIDs

This section provides the following information:

- [Introduction](#)
- [W-ClearPass SNMP Traps](#)

Introduction

This section describes the traps that W-ClearPass Policy Manager supports as part of the W-ClearPass SNMP Private MIB.

[Table 433](#) provides the description and OID (Object Identifier) for each W-ClearPass SNMP trap. OIDs uniquely identify managed objects in a MIB hierarchy.

W-ClearPass SNMP Traps

Table 433: *SNMP Traps Supported by the SNMP Private MIB*

SNMP Trap	Description and OID
cppmLicenseExpiry	- Indicates that one or more licenses associated with a W-ClearPass application <i><cppmNodeApplicationName></i> on the W-ClearPass server will expire in <i><cppmLicenseDaysRemaining></i> days. OID: .1.3.6.1.4.1.14823.1.6.1.1.200.1001
cppmActivationExpiry	- Indicates that one or more licensing activations associated with the <i><cppmNodeApplicationName></i> on the ClearPass Server will expire in <i><cppmActivationDaysRemaining></i> days. OID: .1.3.6.1.4.1.14823.1.6.1.1.200.1002
cppmNodeCertExpiry	- Indicates that a server certificate associated with the <i><cppmNodeCertApplicationName></i> on the ClearPass Server will expire in <i><cppmCertDaysRemaining></i> days. OID: .1.3.6.1.4.1.14823.1.6.1.1.200.1003
cppmLowDiskSpace	- Indicates that the system is running low on disk space as indicated by <i><cppmDiskSpaceRemaining></i> with the units specified in <i><cppmResourceUnit></i>. OID: .1.3.6.1.4.1.14823.1.6.1.1.200.1004
cppmLowMemory	- Indicates that the system is running low on memory as indicated by <i><cppmMemoryRemaining></i> with the units specified in <i><cppmResourceUnit></i>. OID: .1.3.6.1.4.1.14823.1.6.1.1.200.1005
cppmClusterNodeAddNotification	- Indicates the addition of a W-ClearPass node to the cluster. <i><cppmClusterServerIp></i> indicates the IP address of the node added to the cluster. OID: .1.3.6.1.4.1.14823.1.6.1.1.200.1006
cppmClusterNodeDelNotification	- Indicates that a W-ClearPass node has been deleted from the cluster. <i><cppmClusterServerIp></i> indicates the IP address of the node removed from the cluster. OID: .1.3.6.1.4.1.14823.1.6.1.1.200.1007
cppmClusterNodePromNotification	- Indicates the promotion of a W-ClearPass node to Publisher status. <i><cppmClusterServerIp></i> indicates the IP address of the node promoted to Publisher. OID: .1.3.6.1.4.1.14823.1.6.1.1.200.1008
cppmClusterNodeDbldNotification	Indicates that a W-ClearPass node in the cluster has been disabled.

Table 433: SNMP Traps Supported by the SNMP Private MIB (Continued)

SNMP Trap	Description and OID
	■ <i><cppmClusterServerIp></i> indicates the IP address of the disabled node. ● OID: .1.3.6.1.4.1.14823.1.6.1.1.200.1009
cppmClusterNodeNSyncNotification	● Indicates the W-ClearPass node in the cluster that is in the out-of-sync state. ■ <i><cppmClusterServerIp></i> indicates the IP address of the out-of-sync node. ■ <i><cppmClusterOutOfSyncMinutes></i> indicates the number of minutes that the node has been out-of-sync. ● OID: .1.3.6.1.4.1.14823.1.6.1.1.200.1010
cppmClusterPwdChangedNotification	● Indicates that the cluster password has been changed. ● OID: .1.3.6.1.4.1.14823.1.6.1.1.200.1011
cppmConfigReset	● Indicates that the W-ClearPass node's configuration has been reset. ● OID: .1.3.6.1.4.1.14823.1.6.1.1.200.1012
cppmConfigRestore	● Indicates that the W-ClearPass node's configuration has been restored. ● OID: .1.3.6.1.4.1.14823.1.6.1.1.200.1013
cppmUpdateNotification	● Indicates that the CPPM node's installation has been updated. ● OID: .1.3.6.1.4.1.14823.1.6.1.1.200.1014
cppmUpgradeNotification	● Indicates that the CPPM node's installation has been upgraded. ● OID: .1.3.6.1.4.1.14823.1.6.1.1.200.1015
cppmClusterLicenseUsage	● Indicates the W-ClearPass cluster license utilization details. ■ <i><clearpassServerApplicationName></i> indicates the name of the application. ■ <i><clearpassClusterLicenseTotalCount></i> indicates the application's total cluster-wide license count. ■ <i><clearpassClusterLicenseUsageCount></i> indicates the count of the application's used cluster-wide licenses. ● OID: .1.3.6.1.4.1.14823.1.6.1.1.200.1016

SNMP Trap Details

W-ClearPass Policy Manager leverages native SNMP support from the UC Davis 'net-SNMP' MIB package to send trap notifications for the following events.

In these trap OIDs, the value of X varies from 1 through N, depending on the number of process states that are being checked. Details about specific OIDs associated with the processes are listed in this section.

For more information, see:

- [SNMP Daemon Trap Events on page 787](#)

- [W-ClearPass Processes Stop and Start Events on page 788](#)
- [Network Interface up and Down Events on page 787](#)
- [Disk Utilization Threshold Exceed Events on page 788](#)
- [CPU Load Average Exceed Events for 1, 5, and 15 Minute Thresholds on page 796](#)
- [SNMP Daemon Traps on page 787](#)
- [Process Status Traps on page 788](#)
- [Network Interface Status Traps on page 787](#)
- [Disk Space Threshold Traps on page 788](#)
- [CPU Load Average Traps on page 796](#)

SNMP Daemon Traps

This section contains OIDs for various trap events that are sent from W-ClearPass Policy Manager.

.1.3.6.1.6.3.1.1.5.1 ==> Coldstart trap indicating the reinitialization of the **netsnmp** daemon and its configuration file may have been altered.

.1.3.6.1.6.3.1.1.5.2 ==> Warmstart trap indicating the reinitialization of the **netsnmp** daemon and its configuration file is not altered.

Figure 737: *SNMP daemon traps example*

25-Mar-13 04:09 PM	10.162.111.30	public	1.3.6.1.4.1.8072.3.2.10	1.3.6.1.2.1.1.3.0 = 26 1.3.6.1.6.3.1.1.4.1.0 = 1.3.6.1.6.3.1.1.5.1

SNMP Daemon Trap Events

OIDs:

.1.3.6.1.6.3.1.1.5.1 ==> Cold Start

.1.3.6.1.6.3.1.1.5.2 ==> Warm Start

Network Interface up and Down Events

OIDs:

.1.3.6.1.6.3.1.1.5.3 ==> Link Down

.1.3.6.1.6.3.1.1.5.4 ==> Link Up

Network Interface Status Traps

.1.3.6.1.6.3.1.1.5.3 ==> Indicates the linkdown trap with the 'ifAdminStatus' and 'ifOperStatus' values set to 2.

.1.3.6.1.6.3.1.1.5.4 ==> Indicates the linkup trap with the 'ifAdminStatus' and 'ifOperStatus' values set to 1.

In each case, the 'ifIndex' value is set to 2 for management interface and 3 for the data port interface.

Figure 738: *Network interface status traps example*

25-Mar-13 01:57 PM	10.162.111.30	public	1.3.6.1.4.1.8072.3.2.10	1.3.6.1.2.1.1.3.0 = 44 1.3.6.1.6.3.1.1.4.1.0 = 1.3.6.1.6.3.1.1.5.3 1.3.6.1.2.1.2.2.1.1.3 = 3 1.3.6.1.2.1.2.2.1.7.3 = 2 1.3.6.1.2.1.2.2.1.8.3 = 2
25-Mar-13 01:57 PM	10.162.111.30	public	1.3.6.1.4.1.8072.3.2.10	1.3.6.1.2.1.1.3.0 = 44 1.3.6.1.6.3.1.1.4.1.0 = 1.3.6.1.6.3.1.1.5.4 1.3.6.1.2.1.2.2.1.1.2 = 2 1.3.6.1.2.1.2.2.1.7.2 = 1 1.3.6.1.2.1.2.2.1.8.2 = 1

W-ClearPass Processes Stop and Start Events

OIDs:

.1.3.6.1.4.1.2021.8.1.2.X ==> Process Name

.1.3.6.1.4.1.2021.2.1.101.X ==> Process Status Message

Disk Space Threshold Traps

.1.3.6.1.4.1.2021.9.1.100.1 ==> Error flag indicating the disk or partition is under the minimum required space configured for it. Value of 1 indicates the system has reached the threshold and 0 indicates otherwise.

.1.3.6.1.4.1.2021.9.1.2.1 ==> Name of the partition which has met the above condition.

Figure 739: *Disk Space Threshold Traps Example*

25-Mar-13 01:57 PM	10.162.111.30	public	1.3.6.1.2.1.1.3.0 = 44 1.3.6.1.6.3.1.1.4.1.0 = 1.3.6.1.2.1.88.2.0.2 1.3.6.1.2.1.88.2.1.1.0 = diskTable 1.3.6.1.2.1.88.2.1.2.0 = 1.3.6.1.2.1.88.2.1.3.0 = 1.3.6.1.2.1.88.2.1.4.0 = 1.3.6.1.4.1.2021.9.1.100.1 1.3.6.1.2.1.88.2.1.5.0 = 1 1.3.6.1.4.1.2021.9.1.2.1 = / 1.3.6.1.4.1.2021.9.1.101.1 = /: less than 99% free (= 13%)
25-Mar-13 01:57 PM	10.162.111.30	public	1.3.6.1.2.1.1.3.0 = 43 1.3.6.1.6.3.1.1.4.1.0 = 1.3.6.1.2.1.88.2.0.3 1.3.6.1.2.1.88.2.1.1.0 = memory 1.3.6.1.2.1.88.2.1.2.0 = 1.3.6.1.2.1.88.2.1.3.0 = 1.3.6.1.2.1.88.2.1.4.0 = 1.3.6.1.4.1.2021.4.100.0 1.3.6.1.2.1.88.2.1.5.0 = 0 1.3.6.1.4.1.2021.4.2.0 = swap 1.3.6.1.4.1.2021.4.101.0 =

Disk Utilization Threshold Exceed Events

OIDs:

.1.3.6.1.4.1.2021.9.1.100.1 ==> Error flag for disk partition

.1.3.6.1.4.1.2021.9.1.2.1 ==> Name of the partition

Process Status Traps

RADIUS server stop SNMP trap

snmpTrapOID: .1.3.6.1.2.1.88.2.0.2

.1.3.6.1.2.1.88.2.1.1.0: extTable

.1.3.6.1.2.1.88.2.1.2.0:

.1.3.6.1.2.1.88.2.1.3.0:

.1.3.6.1.2.1.88.2.1.4.0: .1.3.6.1.4.1.2021.8.1.100.5

.1.3.6.1.2.1.88.2.1.5.0: 3

.1.3.6.1.4.1.2021.8.1.2.5: cpass-radius-server

.1.3.6.1.4.1.2021.8.1.101.5: Radius server [cpass-radius-server] is stopped

RADIUS server start SNMP trap

snmpTrapOID: .1.3.6.1.2.1.88.2.0.3

.1.3.6.1.2.1.88.2.1.1.0: extTable

.1.3.6.1.2.1.88.2.1.2.0:

.1.3.6.1.2.1.88.2.1.3.0:
.1.3.6.1.2.1.88.2.1.4.0: .1.3.6.1.4.1.2021.8.1.100.5
.1.3.6.1.2.1.88.2.1.5.0: 0
.1.3.6.1.4.1.2021.8.1.2.5: cpass-radius-server
.1.3.6.1.4.1.2021.8.1.101.5: Radius server [cpass-radius-server] is running

Admin Server stop SNMP trap

snmpTrapOID: .1.3.6.1.2.1.88.2.0.2
.1.3.6.1.2.1.88.2.1.1.0: extTable
.1.3.6.1.2.1.88.2.1.2.0:
.1.3.6.1.2.1.88.2.1.3.0:
.1.3.6.1.2.1.88.2.1.4.0: .1.3.6.1.4.1.2021.8.1.100.1
.1.3.6.1.2.1.88.2.1.5.0: 3
.1.3.6.1.4.1.2021.8.1.2.1: cpass-admin-server
.1.3.6.1.4.1.2021.8.1.101.1: Admin server [cpass-admin-server] is stopped

Admin Server start SNMP trap

snmpTrapOID: .1.3.6.1.2.1.88.2.0.3
.1.3.6.1.2.1.88.2.1.1.0: extTable
.1.3.6.1.2.1.88.2.1.2.0:
.1.3.6.1.2.1.88.2.1.3.0:
.1.3.6.1.2.1.88.2.1.4.0: .1.3.6.1.4.1.2021.8.1.100.1
.1.3.6.1.2.1.88.2.1.5.0: 0
.1.3.6.1.4.1.2021.8.1.2.1: cpass-admin-server
.1.3.6.1.4.1.2021.8.1.101.1: Admin server [cpass-admin-server] is running

System Auxiliary server stop SNMP trap

snmpTrapOID: .1.3.6.1.2.1.88.2.0.2
.1.3.6.1.2.1.88.2.1.1.0: extTable
.1.3.6.1.2.1.88.2.1.2.0:
.1.3.6.1.2.1.88.2.1.3.0:
.1.3.6.1.2.1.88.2.1.4.0: .1.3.6.1.4.1.2021.8.1.100.2
.1.3.6.1.2.1.88.2.1.5.0: 3
.1.3.6.1.4.1.2021.8.1.2.2: cpass-system-auxiliary-server
.1.3.6.1.4.1.2021.8.1.101.2: System auxiliary service [cpass-system-auxiliary-server] is stopped

System Auxiliary server start SNMP trap

snmpTrapOID: .1.3.6.1.2.1.88.2.0.3
.1.3.6.1.2.1.88.2.1.1.0: extTable
.1.3.6.1.2.1.88.2.1.2.0:

.1.3.6.1.2.1.88.2.1.3.0:
.1.3.6.1.2.1.88.2.1.4.0: .1.3.6.1.4.1.2021.8.1.100.2
.1.3.6.1.2.1.88.2.1.5.0: 0
.1.3.6.1.4.1.2021.8.1.2.2: cpass-system-auxiliary-server
.1.3.6.1.4.1.2021.8.1.101.2: System auxiliary service [cpass-system-auxiliary-server] is running

Policy server stop SNMP trap

snmpTrapOID: .1.3.6.1.2.1.88.2.0.2
.1.3.6.1.2.1.88.2.1.1.0: extTable
.1.3.6.1.2.1.88.2.1.2.0:
.1.3.6.1.2.1.88.2.1.3.0:
.1.3.6.1.2.1.88.2.1.4.0: .1.3.6.1.4.1.2021.8.1.100.3
.1.3.6.1.2.1.88.2.1.5.0: 3
.1.3.6.1.4.1.2021.8.1.2.3: cpass-policy-server
.1.3.6.1.4.1.2021.8.1.101.3: Policy server [cpass-policy-server] is stopped

Policy server start SNMP trap

snmpTrapOID: .1.3.6.1.2.1.88.2.0.3
.1.3.6.1.2.1.88.2.1.1.0: extTable
.1.3.6.1.2.1.88.2.1.2.0:
.1.3.6.1.2.1.88.2.1.3.0:
.1.3.6.1.2.1.88.2.1.4.0: .1.3.6.1.4.1.2021.8.1.100.3
.1.3.6.1.2.1.88.2.1.5.0: 0
.1.3.6.1.4.1.2021.8.1.2.3: cpass-policy-server
.1.3.6.1.4.1.2021.8.1.101.3: Policy server [cpass-policy-server] is running

Async DB write service stop SNMP trap

snmpTrapOID: .1.3.6.1.2.1.88.2.0.2
.1.3.6.1.2.1.88.2.1.1.0: extTable
.1.3.6.1.2.1.88.2.1.2.0:
.1.3.6.1.2.1.88.2.1.3.0:
.1.3.6.1.2.1.88.2.1.4.0: .1.3.6.1.4.1.2021.8.1.100.6
.1.3.6.1.2.1.88.2.1.5.0: 1
.1.3.6.1.4.1.2021.8.1.2.6: cpass-dbwrite-server
.1.3.6.1.4.1.2021.8.1.101.6: Async DB write service [cpass-dbwrite-server] is stopped

Async DB write service start SNMP trap

snmpTrapOID: .1.3.6.1.2.1.88.2.0.3
.1.3.6.1.2.1.88.2.1.1.0: extTable
.1.3.6.1.2.1.88.2.1.2.0:

.1.3.6.1.2.1.88.2.1.3.0:
.1.3.6.1.2.1.88.2.1.4.0: .1.3.6.1.4.1.2021.8.1.100.6
.1.3.6.1.2.1.88.2.1.5.0: 0
.1.3.6.1.4.1.2021.8.1.2.6: cpass-dbwrite-server
.1.3.6.1.4.1.2021.8.1.101.6: Async DB write service [cpass-dbwrite-server] is running

DB replication service stop SNMP trap

snmpTrapOID: .1.3.6.1.2.1.88.2.0.2
.1.3.6.1.2.1.88.2.1.1.0: extTable
.1.3.6.1.2.1.88.2.1.2.0:
.1.3.6.1.2.1.88.2.1.3.0:
.1.3.6.1.2.1.88.2.1.4.0: .1.3.6.1.4.1.2021.8.1.100.7
.1.3.6.1.2.1.88.2.1.5.0: 1
.1.3.6.1.4.1.2021.8.1.2.7: cpass-repl-server
.1.3.6.1.4.1.2021.8.1.101.7: DB replication service [cpass-repl-server] is stopped

DB replication service start SNMP trap

snmpTrapOID: .1.3.6.1.2.1.88.2.0.3
.1.3.6.1.2.1.88.2.1.1.0: extTable
.1.3.6.1.2.1.88.2.1.2.0:
.1.3.6.1.2.1.88.2.1.3.0:
.1.3.6.1.2.1.88.2.1.4.0: .1.3.6.1.4.1.2021.8.1.100.7
.1.3.6.1.2.1.88.2.1.5.0: 0
.1.3.6.1.4.1.2021.8.1.2.7: cpass-repl-server
.1.3.6.1.4.1.2021.8.1.101.7: DB replication service [cpass-repl-server] is running

DB Change Notification server stop SNMP trap

snmpTrapOID: .1.3.6.1.2.1.88.2.0.2
.1.3.6.1.2.1.88.2.1.1.0: extTable
.1.3.6.1.2.1.88.2.1.2.0:
.1.3.6.1.2.1.88.2.1.3.0:
.1.3.6.1.2.1.88.2.1.4.0: .1.3.6.1.4.1.2021.8.1.100.8
.1.3.6.1.2.1.88.2.1.5.0: 3
.1.3.6.1.4.1.2021.8.1.2.8: cpass-dbcn-server
.1.3.6.1.4.1.2021.8.1.101.8: DB change notification server [cpass-dbcn-server] is stopped

DB Change Notification server start SNMP trap

snmpTrapOID: .1.3.6.1.2.1.88.2.0.3
.1.3.6.1.2.1.88.2.1.1.0: extTable
.1.3.6.1.2.1.88.2.1.2.0:

.1.3.6.1.2.1.88.2.1.3.0:
.1.3.6.1.2.1.88.2.1.4.0: .1.3.6.1.4.1.2021.8.1.100.8
.1.3.6.1.2.1.88.2.1.5.0: 0
.1.3.6.1.4.1.2021.8.1.2.8: cpass-dbcn-server
.1.3.6.1.4.1.2021.8.1.101.8: DB change notification server [cpass-dbcn-server] is running

Async netd service stop SNMP trap

snmpTrapOID: .1.3.6.1.2.1.88.2.0.2
.1.3.6.1.2.1.88.2.1.1.0: extTable
.1.3.6.1.2.1.88.2.1.2.0:
.1.3.6.1.2.1.88.2.1.3.0:
.1.3.6.1.2.1.88.2.1.4.0: .1.3.6.1.4.1.2021.8.1.100.9
.1.3.6.1.2.1.88.2.1.5.0: 3
.1.3.6.1.4.1.2021.8.1.2.9: cpass-async-netd
.1.3.6.1.4.1.2021.8.1.101.9: Async netd service [cpass-async-netd] is stopped

Async netd service start SNMP trap

snmpTrapOID: .1.3.6.1.2.1.88.2.0.3
.1.3.6.1.2.1.88.2.1.1.0: extTable
.1.3.6.1.2.1.88.2.1.2.0:
.1.3.6.1.2.1.88.2.1.3.0:
.1.3.6.1.2.1.88.2.1.4.0: .1.3.6.1.4.1.2021.8.1.100.9
.1.3.6.1.2.1.88.2.1.5.0: 0
.1.3.6.1.4.1.2021.8.1.2.9: cpass-async-netd
.1.3.6.1.4.1.2021.8.1.101.9: Async netd service [cpass-async-netd] is running

Multi-master Cache service stop SNMP trap

snmpTrapOID: .1.3.6.1.2.1.88.2.0.2
.1.3.6.1.2.1.88.2.1.1.0: extTable
.1.3.6.1.2.1.88.2.1.2.0:
.1.3.6.1.2.1.88.2.1.3.0:
.1.3.6.1.2.1.88.2.1.4.0: .1.3.6.1.4.1.2021.8.1.100.10
.1.3.6.1.2.1.88.2.1.5.0: 3
.1.3.6.1.4.1.2021.8.1.2.10: cpass-multi-master-cache-server
.1.3.6.1.4.1.2021.8.1.101.10: Multi-master cache [cpass-multi-master-cache-server] is stopped

Multi-master Cache service start SNMP trap

snmpTrapOID: .1.3.6.1.2.1.88.2.0.3
.1.3.6.1.2.1.88.2.1.1.0: extTable
.1.3.6.1.2.1.88.2.1.2.0:

.1.3.6.1.2.1.88.2.1.3.0:
.1.3.6.1.2.1.88.2.1.4.0: .1.3.6.1.4.1.2021.8.1.100.10
.1.3.6.1.2.1.88.2.1.5.0: 0
.1.3.6.1.4.1.2021.8.1.2.10: cpass-multi-master-cache-server
.1.3.6.1.4.1.2021.8.1.101.10: Multi-master cache [cpass-multi-master-cache-server] is running

AirGroup Notification service stop SNMP trap

snmpTrapOID: .1.3.6.1.2.1.88.2.0.2
.1.3.6.1.2.1.88.2.1.1.0: extTable
.1.3.6.1.2.1.88.2.1.2.0:
.1.3.6.1.2.1.88.2.1.3.0:
.1.3.6.1.2.1.88.2.1.4.0: .1.3.6.1.4.1.2021.8.1.100.11
.1.3.6.1.2.1.88.2.1.5.0: 3
.1.3.6.1.4.1.2021.8.1.2.11: airgroup-notify
.1.3.6.1.4.1.2021.8.1.101.11: AirGroup notification service [airgroup-notify] is stopped

AirGroup Notification service start SNMP trap

snmpTrapOID: .1.3.6.1.2.1.88.2.0.3
.1.3.6.1.2.1.88.2.1.1.0: extTable
.1.3.6.1.2.1.88.2.1.2.0:
.1.3.6.1.2.1.88.2.1.3.0:
.1.3.6.1.2.1.88.2.1.4.0: .1.3.6.1.4.1.2021.8.1.100.11
.1.3.6.1.2.1.88.2.1.5.0: 0
.1.3.6.1.4.1.2021.8.1.2.11: airgroup-notify
.1.3.6.1.4.1.2021.8.1.101.11: AirGroup notification service [airgroup-notify] is running

Micros Fidelio FIAS service stop SNMP trap

snmpTrapOID: .1.3.6.1.2.1.88.2.0.2
.1.3.6.1.2.1.88.2.1.1.0: extTable
.1.3.6.1.2.1.88.2.1.2.0:
.1.3.6.1.2.1.88.2.1.3.0:
.1.3.6.1.2.1.88.2.1.4.0: .1.3.6.1.4.1.2021.8.1.100.12
.1.3.6.1.2.1.88.2.1.5.0: 3
.1.3.6.1.4.1.2021.8.1.2.12: fias_server
.1.3.6.1.4.1.2021.8.1.101.12: Micros Fidelio FIAS [fias_server] is stopped

Micros Fidelio FIAS service start SNMP trap

snmpTrapOID: .1.3.6.1.2.1.88.2.0.3
.1.3.6.1.2.1.88.2.1.1.0: extTable
.1.3.6.1.2.1.88.2.1.2.0:

.1.3.6.1.2.1.88.2.1.3.0:
.1.3.6.1.2.1.88.2.1.4.0: .1.3.6.1.4.1.2021.8.1.100.12
.1.3.6.1.2.1.88.2.1.5.0: 0
.1.3.6.1.4.1.2021.8.1.2.12: fias_server
.1.3.6.1.4.1.2021.8.1.101.12: Micros Fidelio FIAS [fias_server] is running

TACACS server stop SNMP trap

snmpTrapOID: .1.3.6.1.2.1.88.2.0.2
.1.3.6.1.2.1.88.2.1.1.0: extTable
.1.3.6.1.2.1.88.2.1.2.0:
.1.3.6.1.2.1.88.2.1.3.0:
.1.3.6.1.2.1.88.2.1.4.0: .1.3.6.1.4.1.2021.8.1.100.4
.1.3.6.1.2.1.88.2.1.5.0: 3
.1.3.6.1.4.1.2021.8.1.2.4: cpass-tacacs-server
.1.3.6.1.4.1.2021.8.1.101.4: TACACS server [cpass-tacacs-server] is stopped

TACACS server start SNMP trap

snmpTrapOID: .1.3.6.1.2.1.88.2.0.3
.1.3.6.1.2.1.88.2.1.1.0: extTable
.1.3.6.1.2.1.88.2.1.2.0:
.1.3.6.1.2.1.88.2.1.3.0:
.1.3.6.1.2.1.88.2.1.4.0: .1.3.6.1.4.1.2021.8.1.100.4
.1.3.6.1.2.1.88.2.1.5.0: 0
.1.3.6.1.4.1.2021.8.1.2.4: cpass-tacacs-server
.1.3.6.1.4.1.2021.8.1.101.4: TACACS server [cpass-tacacs-server] is running

Virtual IP service stop SNMP trap

snmpTrapOID: .1.3.6.1.2.1.88.2.0.2
.1.3.6.1.2.1.88.2.1.1.0: extTable
.1.3.6.1.2.1.88.2.1.2.0:
.1.3.6.1.2.1.88.2.1.3.0:
.1.3.6.1.2.1.88.2.1.4.0: .1.3.6.1.4.1.2021.8.1.100.13
.1.3.6.1.2.1.88.2.1.5.0: 1
.1.3.6.1.4.1.2021.8.1.2.13: cpass-vip-service
.1.3.6.1.4.1.2021.8.1.101.13: ClearPass Virtual IP service [cpass-vip-service] is stopped

Virtual IP service start SNMP trap

snmpTrapOID: .1.3.6.1.2.1.88.2.0.3
.1.3.6.1.2.1.88.2.1.1.0: extTable
.1.3.6.1.2.1.88.2.1.2.0:

.1.3.6.1.2.1.88.2.1.3.0:
.1.3.6.1.2.1.88.2.1.4.0: .1.3.6.1.4.1.2021.8.1.100.13
.1.3.6.1.2.1.88.2.1.5.0: 0
.1.3.6.1.4.1.2021.8.1.2.13: cpass-vip-service
.1.3.6.1.4.1.2021.8.1.101.13: ClearPass Virtual IP service [cpass-vip-service] is running

Stats Collection service stop SNMP trap

snmpTrapOID: .1.3.6.1.2.1.88.2.0.2
.1.3.6.1.2.1.88.2.1.1.0: extTable
.1.3.6.1.2.1.88.2.1.2.0
.1.3.6.1.2.1.88.2.1.3.0
.1.3.6.1.2.1.88.2.1.4.0: .1.3.6.1.4.1.2021.8.1.100.15
.1.3.6.1.2.1.88.2.1.5.0: 3
.1.3.6.1.4.1.2021.8.1.2.15: cpass-statsd-server
.1.3.6.1.4.1.2021.8.1.101.15: Stats collection service [cpass-statsd-server] is stopped

Stats Collection service start SNMP trap

snmpTrapOID: .1.3.6.1.2.1.88.2.0.3
.1.3.6.1.2.1.88.2.1.1.0: extTable
.1.3.6.1.2.1.88.2.1.2.0
.1.3.6.1.2.1.88.2.1.3.0
.1.3.6.1.2.1.88.2.1.4.0: .1.3.6.1.4.1.2021.8.1.100.15
.1.3.6.1.2.1.88.2.1.5.0: 0
.1.3.6.1.4.1.2021.8.1.2.15: cpass-statsd-server
.1.3.6.1.4.1.2021.8.1.101.15: Stats collection service [cpass-statsd-server] is running

Stats Aggregation service stop SNMP trap

snmpTrapOID: .1.3.6.1.2.1.88.2.0.2
.1.3.6.1.2.1.88.2.1.1.0: extTable
.1.3.6.1.2.1.88.2.1.2.0
.1.3.6.1.2.1.88.2.1.3.0
.1.3.6.1.2.1.88.2.1.4.0: .1.3.6.1.4.1.2021.8.1.100.14
.1.3.6.1.2.1.88.2.1.5.0: 1
.1.3.6.1.4.1.2021.8.1.2.14: cpass-carbon-server
.1.3.6.1.4.1.2021.8.1.101.14: Stats aggregation service [cpass-carbon-server] is stopped

stats Aggregation service start SNMP trap

snmpTrapOID: .1.3.6.1.2.1.88.2.0.3
.1.3.6.1.2.1.88.2.1.1.0: extTable
.1.3.6.1.2.1.88.2.1.2.0

.1.3.6.1.2.1.88.2.1.3.0
 .1.3.6.1.2.1.88.2.1.4.0: .1.3.6.1.4.1.2021.8.1.100.14
 .1.3.6.1.2.1.88.2.1.5.0: 0
 .1.3.6.1.4.1.2021.8.1.2.14: cpass-carbon-server
 .1.3.6.1.4.1.2021.8.1.101.14: Stats aggregation service [cpass-carbon-server] is running.

CPU Load Average Exceed Events for 1, 5, and 15 Minute Thresholds

OIDs

.1.3.6.1.4.1.2021.9.1.100.1 ==> Error flag for disk partition
 .1.3.6.1.4.1.2021.9.1.2.1 ==> Name of the partition

CPU Load Average Traps

OIDs

.1.3.6.1.4.1.2021.10.1.100.1 ==> Error flag on the CPU load-1 average. Value of 1 indicates the load-1 has crossed its threshold and 0 indicates otherwise.
 .1.3.6.1.4.1.2021.10.1.2.1 ==> Name of CPU load-1 average

Figure 740: CPU load-1 average example

```

25-Mar-13 01:57 PM 10.162.111.30 public
1.3.6.1.2.1.3.0 = 44
1.3.6.1.6.3.1.1.4.1.0 = 1.3.6.1.2.1.88.2.0.3
1.3.6.1.2.1.88.2.1.1.0 = laTable
1.3.6.1.2.1.88.2.1.2.0 =
1.3.6.1.2.1.88.2.1.3.0 =
1.3.6.1.2.1.88.2.1.4.0 = 1.3.6.1.4.1.2021.10.1.100.1
1.3.6.1.2.1.88.2.1.5.0 = 0
1.3.6.1.4.1.2021.10.1.2.1 = Load-1
1.3.6.1.4.1.2021.10.1.101.1 =
  
```

.1.3.6.1.4.1.2021.10.1.100.2 ==> Error flag on the CPU load-5 average. Value of 1 indicates the load-5 has crossed its threshold and 0 indicates otherwise.

.1.3.6.1.4.1.2021.10.1.2.2 ==> Name of CPU load-5 average

Figure 741: CPU load-5 average example

```

25-Mar-13 01:57 PM 10.162.111.30 public
1.3.6.1.2.1.3.0 = 44
1.3.6.1.6.3.1.1.4.1.0 = 1.3.6.1.2.1.88.2.0.3
1.3.6.1.2.1.88.2.1.1.0 = laTable
1.3.6.1.2.1.88.2.1.2.0 =
1.3.6.1.2.1.88.2.1.3.0 =
1.3.6.1.2.1.88.2.1.4.0 = 1.3.6.1.4.1.2021.10.1.100.2
1.3.6.1.2.1.88.2.1.5.0 = 0
1.3.6.1.4.1.2021.10.1.2.2 = Load-5
1.3.6.1.4.1.2021.10.1.101.2 =
  
```

.1.3.6.1.4.1.2021.10.1.100.3 ==> Error flag on the CPU load-15 average. Value of 1 indicates the load-15 has crossed its threshold and 0 indicates otherwise.

.1.3.6.1.4.1.2021.10.1.2.3 ==> Name of CPU load-15 average.

Figure 742: CPU load-15 average example

```

25-Mar-13 01:57 PM 10.162.111.30 public
1.3.6.1.2.1.3.0 = 44
1.3.6.1.6.3.1.1.4.1.0 = 1.3.6.1.2.1.88.2.0.3
1.3.6.1.2.1.88.2.1.1.0 = laTable
1.3.6.1.2.1.88.2.1.2.0 =
1.3.6.1.2.1.88.2.1.3.0 =
1.3.6.1.2.1.88.2.1.4.0 = 1.3.6.1.4.1.2021.10.1.100.3
1.3.6.1.2.1.88.2.1.5.0 = 0
1.3.6.1.4.1.2021.10.1.2.3 = Load-15
1.3.6.1.4.1.2021.10.1.101.3 =
  
```


Important System Events

This section provides the following information:

- Admin User Interface Events
- Admin Server Events
- Async Service Events
- W-ClearPass/Domain Controller Events
- W-ClearPass System Configuration Events
- W-ClearPass Update Events
- Cluster Events
- Command Line Events
- Database Replication Services Events
- Licensing Events
- Policy Server Events
- RADIUS/TACACS+ Server Events
- Service Names
- SNMP Events
- Support Shell Events
- System Auxiliary Service Events
- System Monitor Events

This topic describes the important System Events logged by W-ClearPass. These messages are available for consumption on the administrative interface, and in the form of a syslog stream. The events below are in the following format

<Source>, <Level>, <Category>, <Message>

Elements listed below within angle brackets (for example, *<content>*) are variable, and are substituted by W-ClearPass as applicable (such as an IP address).

For the list of available service names, refer to [Service Names on page 800](#).

Admin User Interface Events

Critical Events

"Admin UI", "ERROR" "Email Failed", "Sending email failed"

"Admin UI", "ERROR" "SMS Failed", "Sending SMS failed"

"Admin UI", "WARN", "Login Failed", "User:<X>"

"Admin UI", "WARN", "Login Failed", description

Info Events

"Admin UI", "INFO", "Logged out"

"Admin UI", "INFO", "Session destroyed"

"Admin UI", "INFO", "Logged in", description

"Admin UI", "INFO", "Clear Authentication Cache", "Cache is cleared for authentication source <X>"

"Admin UI", "INFO", "Clear Blacklist User Cache", "Blacklist Users cache is cleared for authentication source <X>"

"Admin UI", "INFO", "Server Certificate", "Subject:<X>", "Updated"
"Install Update", "INFO", "Installing Update", "File: <X>", "Success"
"Admin UI", "INFO", "Email Successful", "Sending email succeeded"
"Admin UI", "INFO", "SMS Successful", "Sending SMS succeeded"

Admin Server Events

Info Events

"Admin server", "INFO", "Performed action start on Admin server"

Async Service Events

Info Events

"Async DB write service", "INFO", "Performed action start on Async DB write service"
"Multi-master cache", "INFO", "Performed action start on Multi-master cache"
"Async netd service", "INFO", "Performed action start on Async netd service"

W-ClearPass/Domain Controller Events

Critical Events

"netleave", "ERROR", "Failed to remove <HOSTNAME> from the domain <DOMAIN_NAME>"
"netjoin", "WARN", "configuration", "<HOSTNAME> failed to join the domain <DOMAIN NAME> with domain controller as <DOMAIN CONTROLLER>"

Info Events

"Netjoin", "INFO", "<HOSTNAME> joined the domain <REALM>"
"Netjoin", "INFO", "<HOSTNAME> removed from the domain <DOMAIN_NAME>"

W-ClearPass System Configuration Events

Critical Events

"DNS", "ERROR", "Failed configure DNS servers = <X>"
"datetime", "ERROR", "Failed to change system datetime."
"hostname", "ERROR", "Setting hostname to <X> failed"
"ipaddress", "ERROR", "Testing cluster node connectivity failed"
"System TimeCheck ", "WARN", "Restarting CPPM services as the system detected time drift , Current system time= 2016-07-13 17:00:01, System time 5 mins back = 2016-06-20 16:55:01"

Info Events

"Cluster", "INFO", "Setup", "Database initialized"
"hostname", "INFO", "configuration", "Hostname set to <X>"
"ipaddress", "INFO", "configuration", "Management port information updated to - IpAddress = <X>, Netmask = <X>, Gateway = <X>"
"IpAddress", "INFO", "Data port information updated to - IpAddress = <X>, Netmask = <Y>, Gateway = <Z>"

"DNS", "INFO", "configuration", "Successfully configured DNS servers - <X>"

"Time Config", "INFO", "Remote Time Server", "Old List: <X>\nNew List: <Y>"

"timezone", "INFO", "configuration", ""

"datetime", "INFO", "configuration", "Successfully changed system datetime.\nOld time was <X>"

W-ClearPass Update Events

Critical Events

"Install Update", "ERROR", "Installing Update", "File: <X>", "Failed with exit status - <Y>"

"ClearPass Firmware Update Checker", "ERROR", "Firmware Update Checker", "No subscription ID was supplied. To find new plugins, you must provide your subscription ID in the application configuration"

Info Events

"ClearPass Updater", "INFO", "Hotfixes Updates", "Updated Hotfixes from File"

"ClearPass Updater", "INFO", "Fingerprints Updates", "Updated fingerprints from File"

"ClearPass Updater", "INFO", "Updated AV/AS from ClearPass Portal (Online)"

"ClearPass Updater", "INFO", "Updated Hotfixes from ClearPass Portal (Online)"

Cluster Events

Critical Events

"Cluster", "ERROR", "SetupSubscriber", "Failed to add subscriber node with management IP=<IP>"

Info Events

"AddNode", "INFO", "Added subscriber node with management IP=<IP>"

"DropNode", "INFO", "Dropping node with management IP=<IP>, hostname=<Hostname>"

Command Line Events

Info Events

"Command Line", "INFO", "User:appadmin"

Database Replication Services Events

Info Events

"DB replication service", "INFO", "Performed action start on DB replication service"

"DB replication service", "INFO", "Performed action stop on DB replication service"

"DB change notification server", "INFO", "Performed action start on DB change notification server"

"DB replication service", "INFO", "Performed action start on DB replication service"

Licensing Events

Critical Events

"Admin UI", "WARN", "Activation Failed", "Action Status: This Activation Request Token is already in use by another instance\nProduct Name: Policy Manager\nLicense Type: <X>\nUser Count: <Y>"

Info Events

"Admin UI", "INFO", "Add License", "Product Name: Policy Manager\nLicense Type: <X>\nUser Count: <Y>"

Policy Server Events

Info Events

"Policy Server", "INFO", "Performed action start on Policy server"

"Policy Server", "INFO", "Performed action stop on Policy server"

RADIUS/TACACS+ Server Events

Critical Events

"TACACSServer", "ERROR", "Request", "Nad Ip=<X> not configured"

"RADIUS", "WARN", "Authentication", "Ignoring request from unknown client <IP>:<PORT>"

"RADIUS", "ERROR", "Authentication", "Received packet from <IP> with invalid Message-Authenticator! (Shared secret is incorrect.)"

"RADIUS", "ERROR", "Received Accounting-Response packet from client <IP Address> port 1813 with invalid signature (err=2)! (Shared secret is incorrect.)"

"RADIUS", "ERROR", "Received Access-Accept packet from client <IP Address> port 1812 with invalid signature (err=2)! (Shared secret is incorrect.)"

Info Events

"RADIUS", "INFO", "Performed action start on Radius server"

"RADIUS", "INFO", "Performed action restart on Radius server"

"TACACS server", "INFO", "Performed action start on TACACS server"

"TACACS server", "INFO", "Performed action stop on TACACS server"

Service Names

- AirGroup notification service
- Async DB write service
- Async network services
- DB change notification server
- DB replication service
- Micros Fidelio FIAS
- Multi-master cache
- Policy server
- RADIUS server
- System auxiliary services
- System monitor service
- TACACS server
- Virtual IP service
- [YourServerName] Domain service

SNMP Events

Critical Events

"SNMPService", "ERROR", "ReadDeviceInfo", "SNMP GET failed for device <X> with error=No response received\nReading sysObjectId failed for device=<X>\nReading switch initialization info failed for <X>"

"SNMPService", "ERROR", "Error fetching table snmpTargetAddr. Request timed out. Error reading SNMP target table for NAD=10.1.1.1 Maybe SNMP target address table is not supported by device? Allow NAD update. SNMP GET failed for device 10.1.1.1 with error=No response received Reading sysObjectId failed for device=10.1.1.1 Reading switch initialization info failed for 10.1.1.1"

Info Events

"SNMPService", "INFO", "Device information not read for <Ip Address> since no traps are configured to this node"

Support Shell Events

Info Events

"Support Shell", "INFO", "User:customersupport"

System Auxiliary Service Events

Info Events

"System auxiliary service", "INFO", "Performed action start on System auxiliary service"

System Monitor Events

Critical Events

"Sysmon", "ERROR", "System", "System is running with low memory. Available memory = <X>%"

"Sysmon", "ERROR", "System", "System is running with low disk space. Available disk space = <X>%"

"System TimeCheck", "WARN", "Restart Services", "Restarting CPPM services as the system detected time drift. Current system time= <X>, System time 5 mins back = <Y>"

Info Events

"<Service Name>", "INFO", "restart", "Performed action restart on <Service Name>"

"SYSTEM", "INFO", "<X> restarted", "System monitor restarted <X>, as it seemed to have stopped abruptly"

"SYSTEM", "ERROR", "Updating CRLs failed", "Could not retrieve CRL from <URL>."

"System monitor service", "INFO", "Performed action start on System monitor service"

"Shutdown" "INFO" system "System is shutting down" Success

Error Codes

Table 434 describes the W-ClearPass Policy Manager error codes:

Table 434: *W-ClearPass Policy Manager Error Codes*

Code	Description	Type
0	Success	Success
101	Failed to perform service classification	Internal Error
102	Failed to perform policy evaluation	Internal Error
103	Failed to perform posture notification	Internal Error
104	Failed to query authstatus	Internal Error
105	Internal error in performing authentication	Internal Error
106	Internal error in RADIUS server	Internal Error
201	User not found	Authentication failure
202	Password mismatch	Authentication failure
203	Failed to contact Authentication Source	Authentication failure
204	Failed to classify request to service	Authentication failure
205	Authentication Source not configured for service	Authentication failure
206	Access denied by policy	Authentication failure
207	Failed to get client MAC Address in order to perform Web authentication	Authentication failure
208	No response from home server	Authentication failure
209	No password in request	Authentication failure
210	Unknown CA in client certificate	Authentication failure
211	Client certificate not valid	Authentication failure
212	Client certificate has expired	Authentication failure
213	Certificate comparison failed	Authentication failure
214	No certificate in authentication source	Authentication failure
215	TLS session error	Authentication failure
216	User authentication failed	Authentication failure
217	Search failed due to insufficient permissions	Authentication failure

Table 434: *W-ClearPass Policy Manager Error Codes (Continued)*

Code	Description	Type
218	Authentication source timed out	Authentication failure
219	Bad search filter	Authentication failure
220	Search failed	Authentication failure
221	Authentication source error	Authentication failure
222	Password change error	Authentication failure
223	Username not available in request	Authentication failure
224	CallingStationID not available in request	Authentication failure
225	User account disabled	Authentication failure
226	User account expired or not active yet	Authentication failure
227	User account needs approval	Authentication failure
228	User account has exceeded bandwidth limit	Authentication failure
229	User account has exceeded session duration limit	Authentication failure
230	User account has exceeded session count limit	Authentication failure
5001	Internal Error	Command and Control
5002	Invalid MAC Address	Command and Control
5003	Invalid request received	Command and Control
5004	Insufficient parameters received	Command and Control
5005	Query - No MAC address record found	Command and Control
5006	Query - No supported actions	Command and Control
5007	Query - Cannot fetch MAC address details	Command and Control
5008	Request: MAC address not online	Command and Control
5009	Request: No MAC address record found	Command and Control
6001	Unsupported TACACS parameter in request	TACACS Protocol
6002	Invalid sequence number	TACACS Protocol
6003	Sequence number overflow	TACACS Protocol

Table 434: *W-ClearPass Policy Manager Error Codes (Continued)*

Code	Description	Type
6101	Not enough inputs to perform authentication	TACACS Authentication
6102	Authentication privilege level mismatch	TACACS Authentication
6103	No enforcement profiles matched to perform authentication	TACACS Authentication
6201	Authorization failed as session is not authenticated	TACACS Authorization
6202	Authorization privilege level mismatch	TACACS Authorization
6203	Command not allowed	TACACS Authorization
6204	No enforcement profiles matched to perform command authorization	TACACS Authorization
6301	New password entered does not match	TACACS Change Password
6302	Empty password	TACACS Change Password
6303	Change password allowed only for local users	TACACS Change Password
6304	Internal error in performing change password	TACACS Change Password
9001	Wrong shared secret	RADIUS Protocol
9002	Request timed out	RADIUS Protocol
9003	Phase 2 PAC failure	RADIUS Protocol
9004	Client rejected after PAC provisioning	RADIUS Protocol
9005	Client does not support posture request	RADIUS Protocol
9006	Received error TLV from client	RADIUS Protocol
9007	Received failure TLV from client	RADIUS Protocol
9008	Phase 2 PAC not found	RADIUS Protocol
9009	Unknown Phase 2 PAC	RADIUS Protocol
9010	Invalid Phase 2 PAC	RADIUS Protocol
9011	PAC verification failed	RADIUS Protocol
9012	PAC binding failed	RADIUS Protocol
9013	Session resumption failed	RADIUS Protocol
9014	Cached session data error	RADIUS Protocol

Table 434: *W-ClearPass Policy Manager Error Codes (Continued)*

Code	Description	Type
9015	Client does not support configured EAP methods	RADIUS Protocol
9016	Client did not send Cryptobinding TLV	RADIUS Protocol
9017	Failed to contact OCSP Server	RADIUS Protocol
9018	RADIUS protocol error	RADIUS Protocol
9019	Client sent conflicting identities	RADIUS Protocol

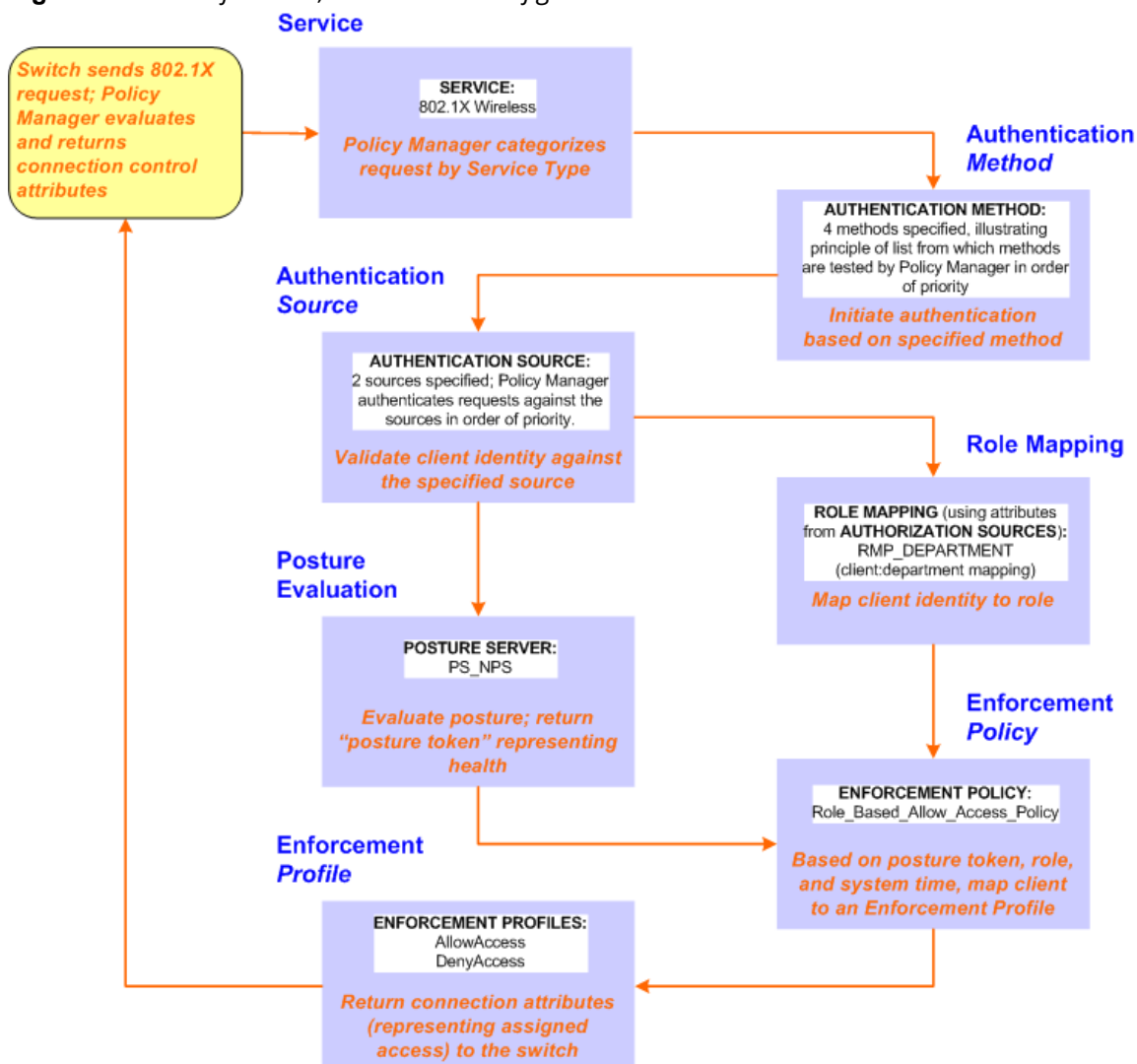
This appendix contains several specific W-ClearPass Policy Manager use cases. Each one explains what it is typically used for, and then describes how to configure W-Policy Manager for that use case.

- 802.1X Wireless Use Case on page 807
- Web Based Authentication Use Case on page 813
- MAC Authentication Use Case on page 820
- TACACS+ Use Case on page 823
- Single Port Use Case on page 824

802.1X Wireless Use Case

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

Figure 743: Flow of Control, Basic 802.1X Configuration Use Case



Policy Manager ships with fourteen preconfigured services. In this use case, you select a service that supports 802.1X wireless requests. Follow the steps below to configure this basic 802.1X service that uses **[EAP FAST]**, one of the pre-configured Policy Manager authentication methods, and **Active Directory Authentication Source (AD)**, an external authentication source within your existing enterprise.



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

Policy Manager tests client identity against role-mapping rules, appending any match (multiple roles acceptable) to the request for use by the enforcement policy. In the event of role-mapping failure, Policy Manager assigns a default role. This use case create the role mapping policy **RMP_DEPARTMENT** that distinguishes clients by department and the corresponding roles **ROLE_ENGINEERING** and **ROLE_FINANCE**, to which it maps.

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



For purposes of posture evaluation, you can configure a posture policy (internal to Policy Manager), a posture server (external), or an audit server (internal or external). Each of the first three use cases demonstrates one of these options; here, the posture server.

Configuring a Service

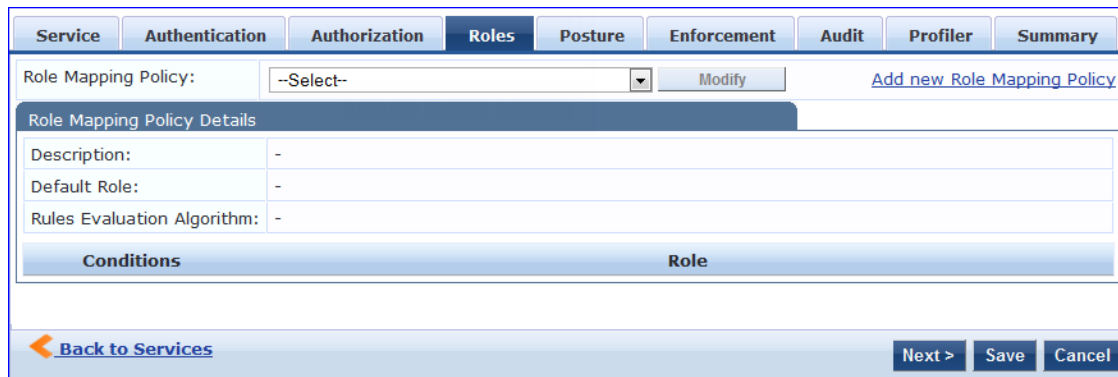
1. Navigate to **Configuration > Services**.
2. Click the **Add** icon to add a service. The **Configuration > Services > Add** window opens.
3. If it is not already selected, click the **Service** tab and define basic service information.
 - a. Enter a name for the service in the **Name** field.
 -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

Creating a New Role Mapping Policy

To create a new Role Mapping policy:

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

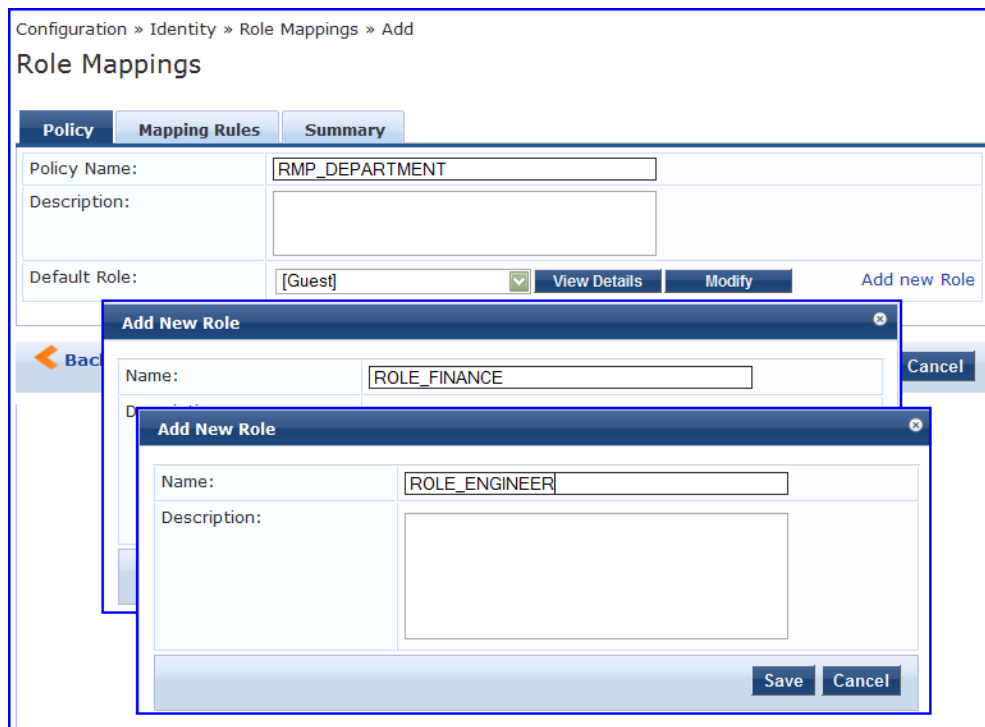
Figure 744: Role Mapping Navigation and Settings



The screenshot shows the 'Roles' tab in the Policy Manager interface. At the top, there are tabs for Service, Authentication, Authorization, Roles (selected), Posture, Enforcement, Audit, Profiler, and Summary. Below the tabs, there is a 'Role Mapping Policy:' section with a dropdown menu set to '--Select--' and a 'Modify' button. To the right is a link 'Add new Role Mapping Policy'. Below this is a 'Role Mapping Policy Details' section with fields for Description, Default Role, and Rules Evaluation Algorithm, all currently set to '-'. At the bottom, there are two tabs: 'Conditions' and 'Role'. At the very bottom, there is a 'Back to Services' link and buttons for 'Next >', 'Save', and 'Cancel'.

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

Figure 745: Policy Tab



The screenshot shows the 'Policy' tab in the Policy Manager interface. The breadcrumb trail at the top reads 'Configuration » Identity » Role Mappings » Add'. The main heading is 'Role Mappings'. Below this are three tabs: Policy (selected), Mapping Rules, and Summary. The 'Policy' tab contains fields for Policy Name (RMP_DEPARTMENT), Description, and Default Role ([Guest]). There are buttons for 'View Details', 'Modify', and 'Add new Role'. Overlaid on this are two 'Add New Role' dialog boxes. The first dialog box has 'Name:' set to 'ROLE_FINANCE' and a 'Cancel' button. The second dialog box has 'Name:' set to 'ROLE_ENGINEER' and 'Description:' fields, with 'Save' and 'Cancel' buttons at the bottom.

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

Figure 746: Mapping Rules Tab

Configuration » Identity » Role Mappings » Add

Role Mappings

Policy Mapping Rules Summary

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

Role Mapping Rules:

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

Add Rule Move Up Move Down Edit Rule Remove Rule

Rules Editor

Conditions

Matches ☒ ANY or ☐ ALL of the following conditions:

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

Actions

Role Name: [Contractor] [Contractor] [Employee] [Guest] [Other] [TACACS API Admin] [TACACS Help Desk] [TACACS Network Admin] [TACACS Read-only Admin] [TACACS Receptionist] [TACACS Super Admin]

Save Cancel

Back to Role Mappings Next > Save Cancel

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

Figure 747: Roles Tab

Service Authentication Authorization Roles Posture Audit Enforcement Summary

Role Mapping Policy: RMP_DEPARTMENT Modify Add new Role Mapping Policy

Role Mapping Policy Details

Description: -

Default Role: [Guest]

Rules Evaluation Algorithm: evaluate-all

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

Back to Services Next > Save Cancel

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

Figure 748: Posture Tab

The screenshot shows the **Posture** tab of the configuration interface. At the top, there are tabs for **Service**, **Authentication**, **Authorization**, **Roles**, **Posture** (selected), **Enforcement**, **Audit**, **Profiler**, and **Summary**. The main content area is divided into two sections: **Posture Policies:** and **Posture Servers:**. Each section contains a list box with a "--Select to Add--" dropdown and three buttons: **Remove**, **View Details**, and **Modify**. Below the **Posture Policies** section, there are fields for **Default Posture Token:** (set to UNKNOWN (100)), **Remediate End-Hosts:** (with a checkbox for "Enable auto-remediation of non-compliant end-hosts"), and **Remediation URL:**. At the bottom, there is a **Back to Services** link and buttons for **Next >**, **Save**, and **Cancel**.

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

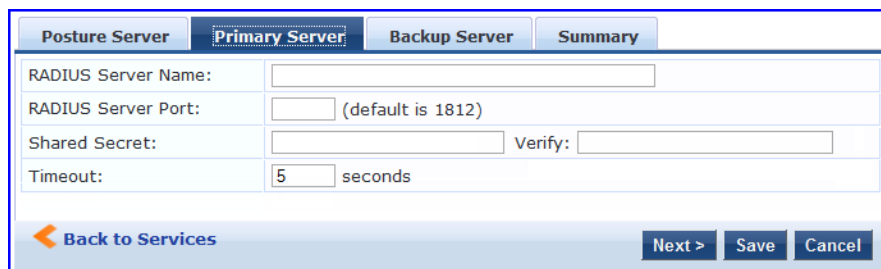
The following figure displays the **Posture Server** tab:

Figure 749: Posture Server Tab

The screenshot shows the **Posture Server** tab of the configuration interface. At the top, there are tabs for **Posture Server** (selected), **Primary Server**, **Backup Server**, and **Summary**. The main content area contains fields for **Name:**, **Description:**, **Server Type:** (with a radio button selected for **Microsoft NPS**), and **Default Posture Token:** (set to UNKNOWN (100)). At the bottom, there is a **Back to Services** link and buttons for **Next >**, **Save**, and **Cancel**.

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

Figure 750: Primary Server Tab



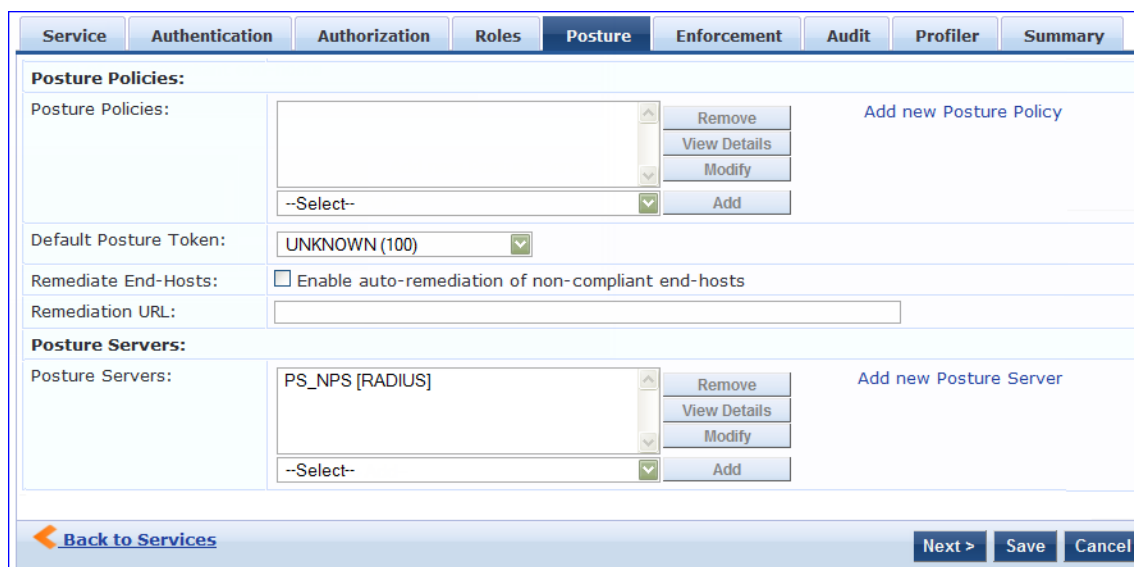
The Primary Server Tab configuration interface includes the following fields and controls:

- Posture Server** (selected tab)
- Primary Server** (selected sub-tab)
- Backup Server** (sub-tab)
- Summary** (sub-tab)
- RADIUS Server Name:** Text input field
- RADIUS Server Port:** Text input field (default is 1812)
- Shared Secret:** Text input field
- Verify:** Text input field
- Timeout:** Text input field (5) followed by "seconds"
- Back to Services** (button with left arrow)
- Next >** (button)
- Save** (button)
- Cancel** (button)

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

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

Figure 751: Posture Tab



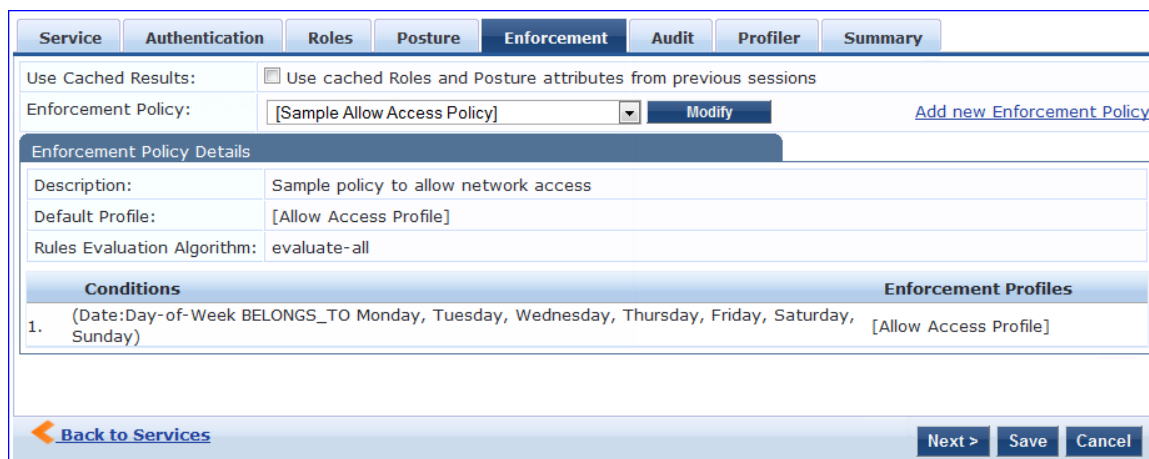
The Posture Tab configuration interface includes the following fields and controls:

- Service** (selected tab)
- Authentication** (tab)
- Authorization** (tab)
- Roles** (tab)
- Posture** (selected tab)
- Enforcement** (tab)
- Audit** (tab)
- Profiler** (tab)
- Summary** (tab)
- Posture Policies:**
 - Posture Policies:** List box with up/down arrows, buttons: Remove, View Details, Modify, Add
 - Default Posture Token:** Dropdown menu (UNKNOWN (100))
 - Remediate End-Hosts:** Check box (Enable auto-remediation of non-compliant end-hosts)
 - Remediation URL:** Text input field
- Posture Servers:**
 - Posture Servers:** List box with up/down arrows, buttons: Remove, View Details, Modify, Add
- Back to Services** (button with left arrow)
- Next >** (button)
- Save** (button)
- Cancel** (button)

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

19. Enforcement policies contain dictionary-based rules for evaluation of Role, Posture Tokens, and System Time to evaluation profiles. Policy Manager applies all matching enforcement profiles to the request. In the case of no match, Policy Manager assigns a default enforcement profile. The following figure displays the **Enforcement** tab:

Table 435: Enforcement Policy Navigation and Settings



The Enforcement Policy Navigation and Settings interface includes the following fields and controls:

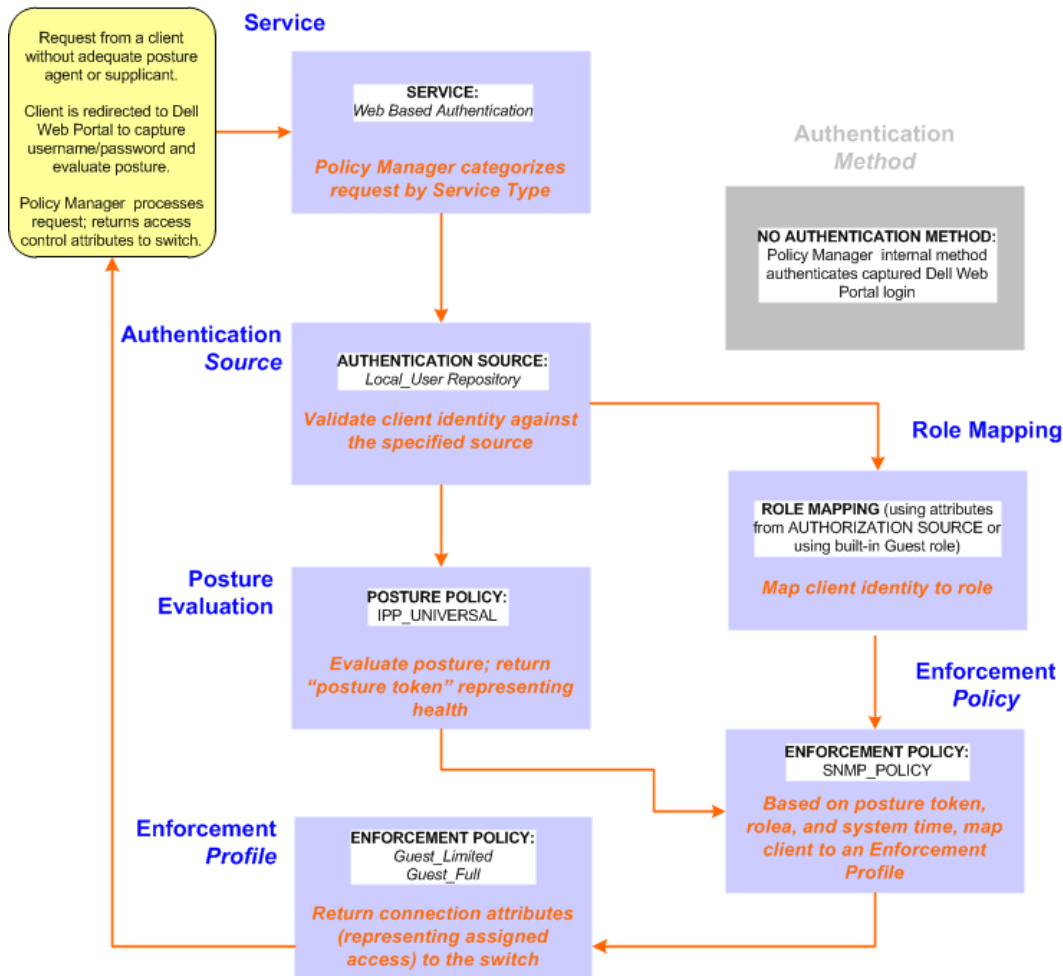
- Service** (selected tab)
- Authentication** (tab)
- Roles** (tab)
- Posture** (tab)
- Enforcement** (selected tab)
- Audit** (tab)
- Profiler** (tab)
- Summary** (tab)
- Use Cached Results:** Check box (Use cached Roles and Posture attributes from previous sessions)
- Enforcement Policy:** Dropdown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

20. From the **Enforcement** tab, select the **Enforcement Policy**. For instructions about how to build an enforcement policy, refer to [Configuring Enforcement Policies on page 343](#).
21. Save the service.

Web Based Authentication Use Case

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

Figure 752: Flow-of-Control of Web-Based Authentication for Guests



Configuring a Service

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

1. Prepare the switch to pre-process WebAuth requests for the Policy Manager *Dell WebAuth* service.
Refer to your Network Access Device documentation to configure the switch such that it redirects HTTP requests to the *Dell Guest Portal*, which captures username and password and optionally launches an agent that returns posture data.
2. Create a WebAuth-based Service.

Table 436: Service Navigation and Settings

Navigation	Settings															
Create a new Service: • Services > • Add Service >	Configuration » Services Services Add Import Export All															
Name the Service and select a pre-configured Service Type: • Service (tab) > • Type (selector): Dell Web-Based Authentication > • Name/Description (freeform) > • Upon completion, click Next.	Configuration » Services » Add Services Service Authentication Authorization Roles Posture Enforcement Summary Type: Web-based Authentication Name: Description: Web Based Authentication for Guests Monitor Mode: ☐ Enable to monitor network access without enforcement More Options: ☒ Authorization ☒ Posture Compliance Service Rule Matches ☐ ANY or ☒ ALL of the following conditions: <table><thead><tr><th>Type</th><th>Name</th><th>Operator</th><th>Value</th><th></th></tr></thead><tbody><tr><td>1. Host</td><td>CheckType</td><td>MATCHES_ANY</td><td>Authentication</td><td> </td></tr><tr><td>2. Click to add...</td><td></td><td></td><td></td><td></td></tr></tbody></table> Back to Services Next > Save Cancel	Type	Name	Operator	Value		1. Host	CheckType	MATCHES_ANY	Authentication		2. Click to add...				
Type	Name	Operator	Value													
1. Host	CheckType	MATCHES_ANY	Authentication													
2. Click to add...																

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



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

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

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

Table 437: Local Policy Manager Database Navigation and Settings

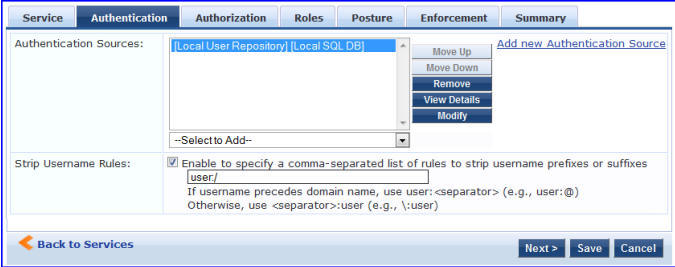
Navigation	Settings
Select the local Policy Manager database: ● Authentication (tab) > ● Sources (Select drop-down list): [Local User Repository] > ● Add > ● Strip Username Rules (check box) > ● Enter an example of preceding or following separators (if any), with the phrase “user” representing the username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

Table 438: *Posture Policy Navigation and Settings*

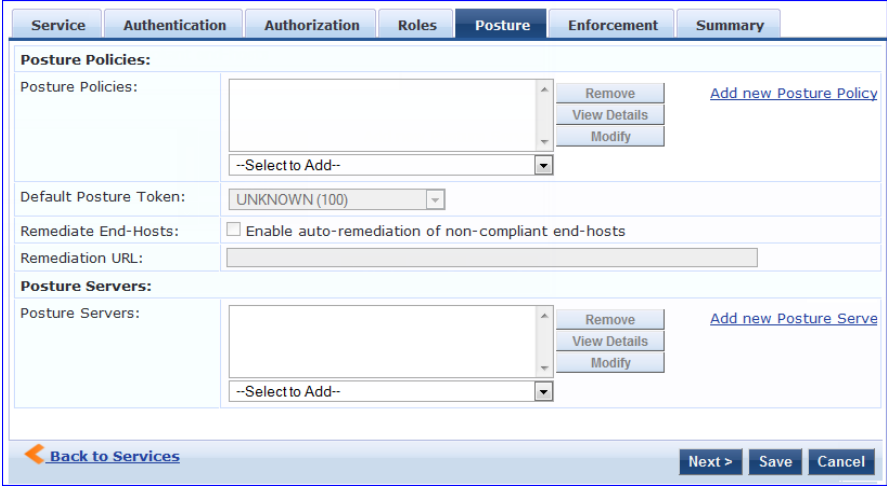
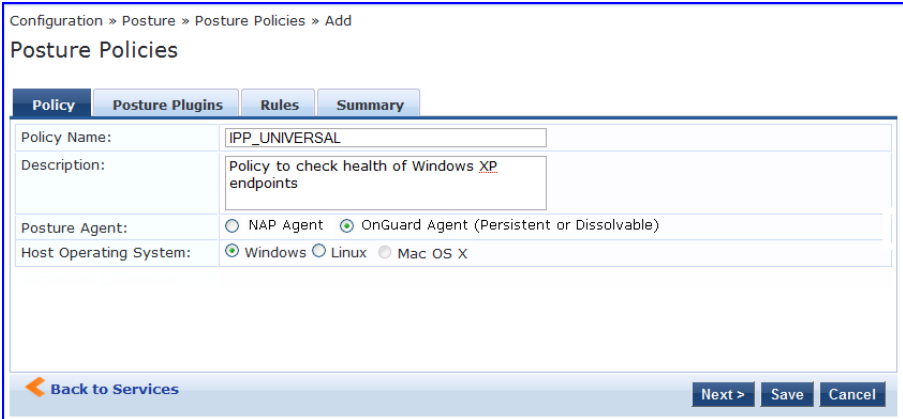
Navigation	Setting
Create a Posture Policy: ● Posture (tab) > ● Enable Validation Check (check box) > ● Add new Internal Policy (link) >	
Name the Posture Policy and specify a general class of operating system: ● Policy (tab) > ● Policy Name (freeform): <i>IPP_UNIVERSAL</i> > ● Host Operating System (radio buttons): Windows > ● When finished working in the Policy tab, click Next to open the Posture Plugins tab	

Table 438: Posture Policy Navigation and Settings (Continued)

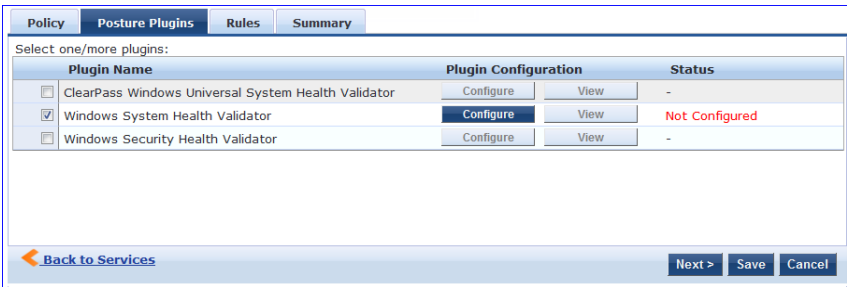
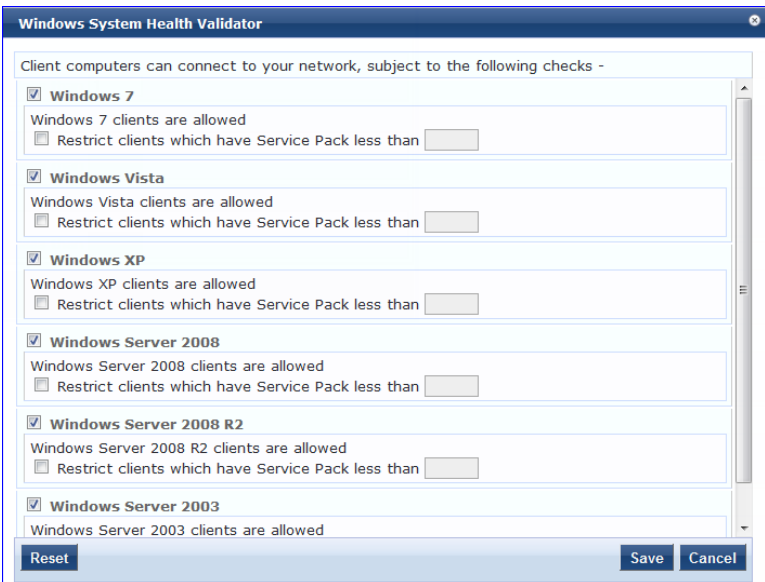
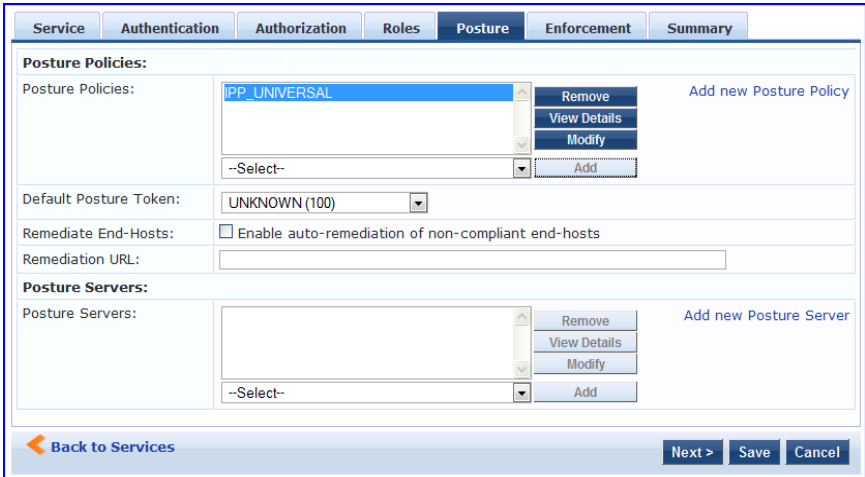
Navigation	Setting
Select a Validator: • Posture Plugins (tab) > • Enable Windows Health System Validator > • Configure (button) >	
Configure the Validator: • Windows System Health Validator (popup) > • Enable all Windows operating systems (check box) > • Enable Service Pack levels for Windows 7, Windows Vista®, Windows XP, Windows Server®, 2008, Windows Server 2008 R2, and Windows Server 2003 (check boxes) > • Save (button) >	

Table 438: *Posture Policy Navigation and Settings (Continued)*

Navigation	Setting
When finished working in the Posture Plugin tab click Next to move to the Rules tab)	
Set rules to correlate validation results with posture tokens: Rules (tab) > Add Rule (button opens popup) > Rules Editor (popup) > Conditions/ Actions: match Conditions (Select Plugin/ Select Plugin checks) to Actions (Posture Token)> - In the Rules Editor, upon completion of each rule, click the Save button > - When finished working in the Rules tab, click the Next button.	

Table 438: Posture Policy Navigation and Settings (Continued)

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

The following fields deserve special mention:

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

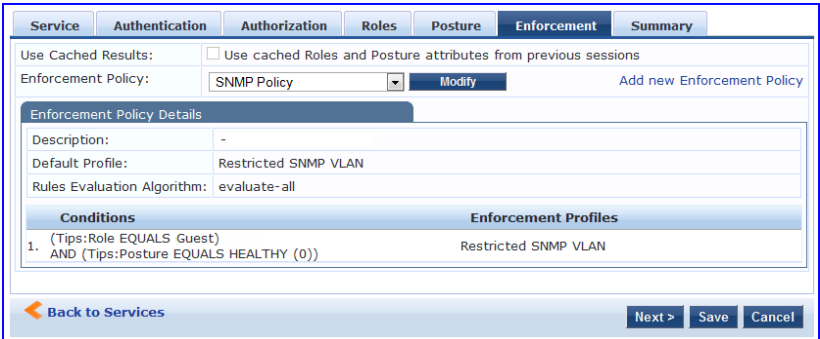
5. Create an Enforcement Policy.

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



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

Table 439: Enforcement Policy Navigation and Settings

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

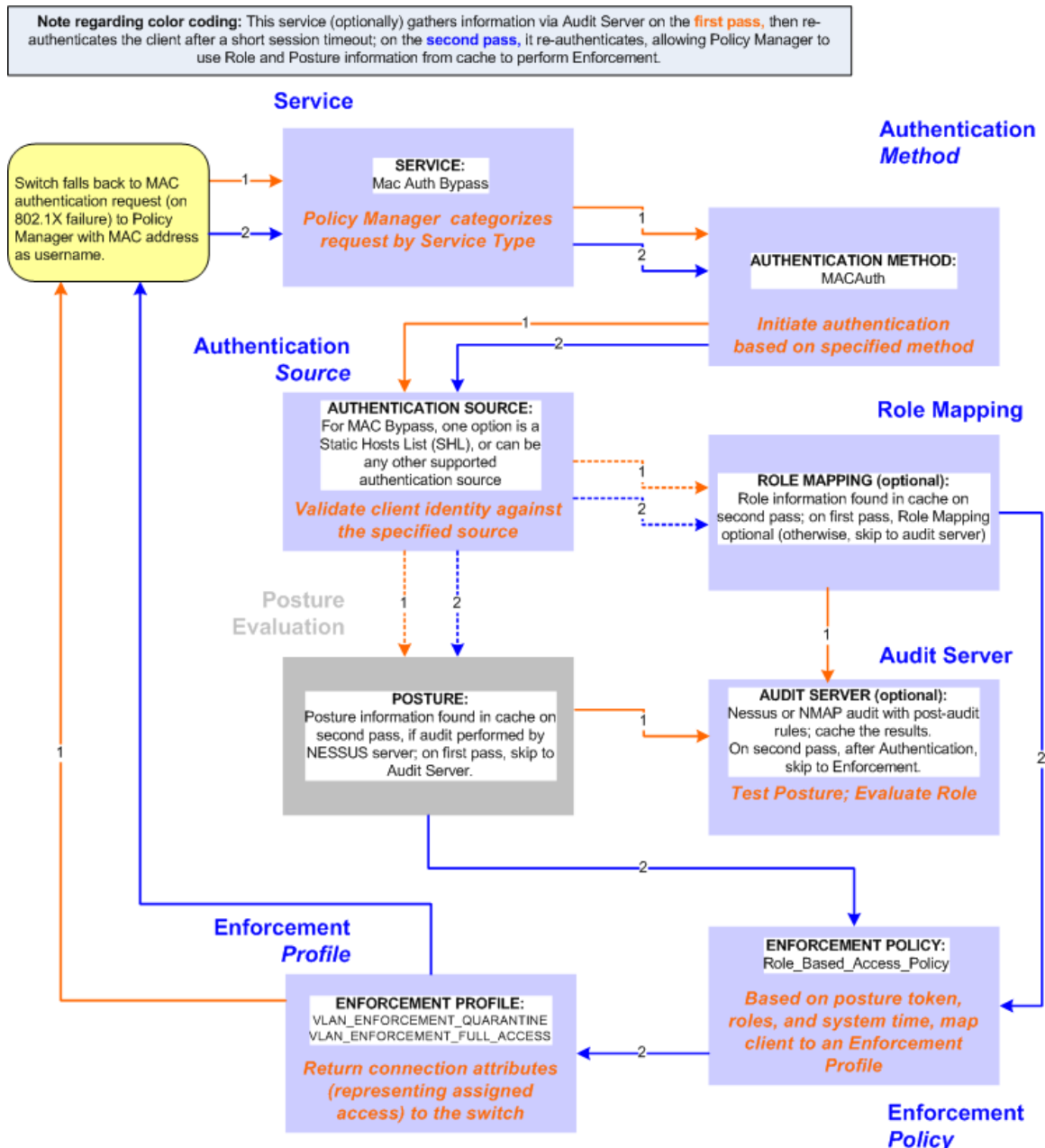
6. Save the Service.

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

MAC Authentication Use Case

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

Figure 753: Flow-of-Control of MAC Authentication for Network Devices



Configuring the Service

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

1. Create a MAC Authentication Service.

Table 440: MAC Authentication Service Navigation and Settings

Navigation	Settings																									
Create a new Service: • Services > • Add Service (link) >	Configuration » Services Services Add Import Export All																									
Name the Service and select a pre-configured Service Type: • Service (tab) > • Type (selector): MAC Authentication > • Name/Description (freeform) > • Upon completion, click Next to configure Authentication	Configuration » Services » Add Services Service Authentication Authorization Roles Enforcement Audit Profiler Summary Type: MAC Authentication Name: Description: MAC-based Authentication service Monitor Mode: ☐ Enable to monitor network access without enforcement More Options: ☒ Authorization ☒ Audit End-hosts ☒ Profile Endpoints Service Rule Matches ☐ ANY or ☒ ALL of the following conditions: <table><thead><tr><th>Type</th><th>Name</th><th>Operator</th><th>Value</th><th></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><td></td></tr><tr><td>2. Radius:IETF</td><td>Service-Type</td><td>EQUALS</td><td>Call-Check (10)</td><td></td></tr><tr><td>3. Connection</td><td>Client-Mac-Address</td><td>EQUALS</td><td>%{Radius:IETF:User-Name}</td><td></td></tr><tr><td>4. Click to add...</td><td></td><td></td><td></td><td></td></tr></tbody></table> Back to Services Next > Save Cancel	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...																										

2. Set up Authentication.

You can select any type of authentication/authorization source for a MAC Authentication service. Only a Static Host list of type MAC Address List or MAC Address Regular Expression shows up in the list of authentication sources (of type Static Host List). For more information on static host list, see ["Adding and Modifying Static Host Lists"](#) on page 1. You can also select any other supported type of authentication source.

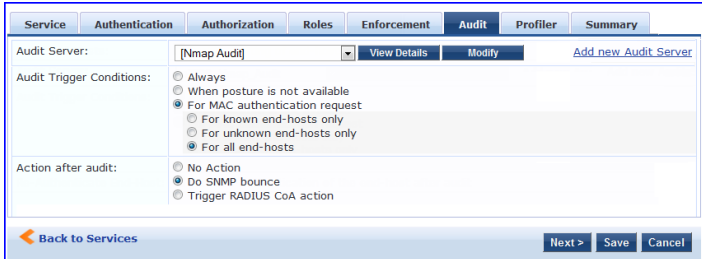
Table 441: Authentication Method Navigation and Settings

Navigation	Settings
Select an Authentication Method and two authentication sources - one of type Static Host List and the other of type Generic LDAP server (that you have already configured in Policy Manager): • Authentication (tab) > • Methods (This method is automatically selected for this type of service): [MAC AUTH] > • Add > • Sources (Select drop-down list): Handhelds [Static Host List] and Policy Manager Clients White List [Generic LDAP] > • Add > • Upon completion, Next (to Audit)	Service Authentication Authorization Roles Enforcement Audit Profiler Summary Authentication Methods: [MAC-AUTH] Move Up Move Down Remove View Details Modify Add new Authentication Method Authentication Sources: Handhelds [Static Host List] Move Up Move Down Remove View Details Modify Add new Authentication Source Strip Username Rules: ☐ Enable to specify a comma-separated list of rules to strip username prefixes or suffixes Back to Services Next > Save Cancel

3. Configure an Audit Server.

This step is optional if no Role Mapping Policy is provided, or if you want to establish health or roles using an audit. An audit server determines health by performing a detailed system and health vulnerability analysis (NESSUS). You can also configure the audit server (NMAP or NESSUS) with post-audit rules that enable Policy Manager to determine client identity.

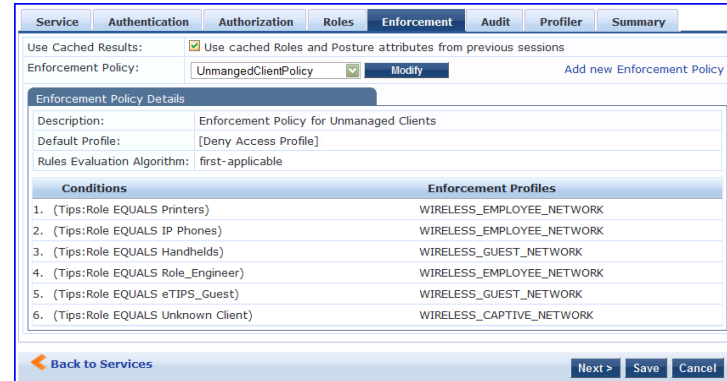
Table 442: *Audit Server Navigation and Settings*

Navigation	Settings
Configure the Audit Server: ● Audit (tab) > ● Audit End Hosts (enable) > ● Audit Server (selector): NMAP ● Trigger Conditions (radio button): For MAC authentication requests ● Reauthenticate client (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. Select an Enforcement Policy.

4. Select the Enforcement Policy *Sample_Allow_Access_Policy*:

Table 443: *Enforcement Policy Navigation and Settings*

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

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

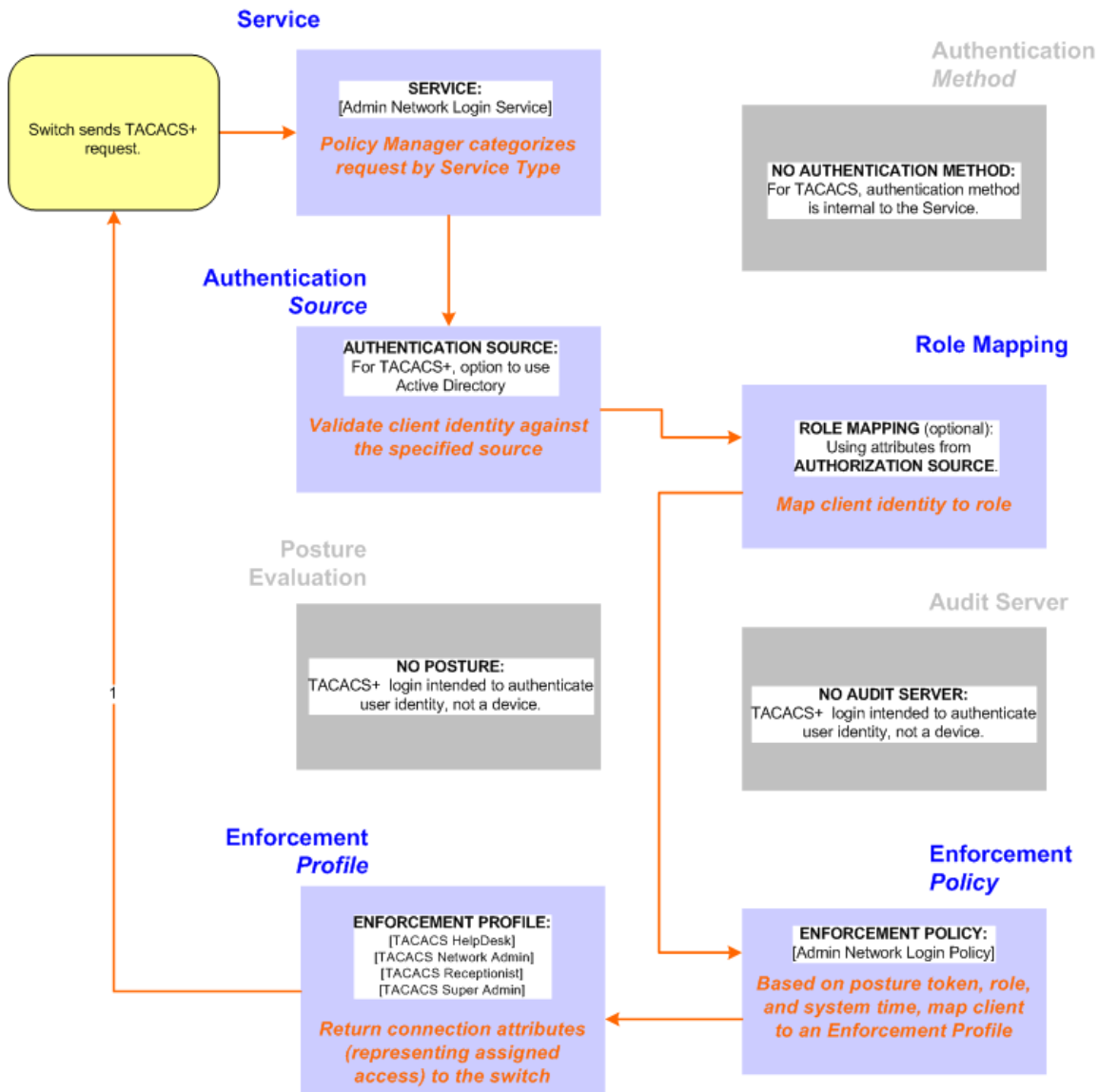
5. Save the Service.

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

TACACS+ Use Case

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

Figure 754: Administrator connections to Network Access Devices via TACACS+



Configuring the Service

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

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

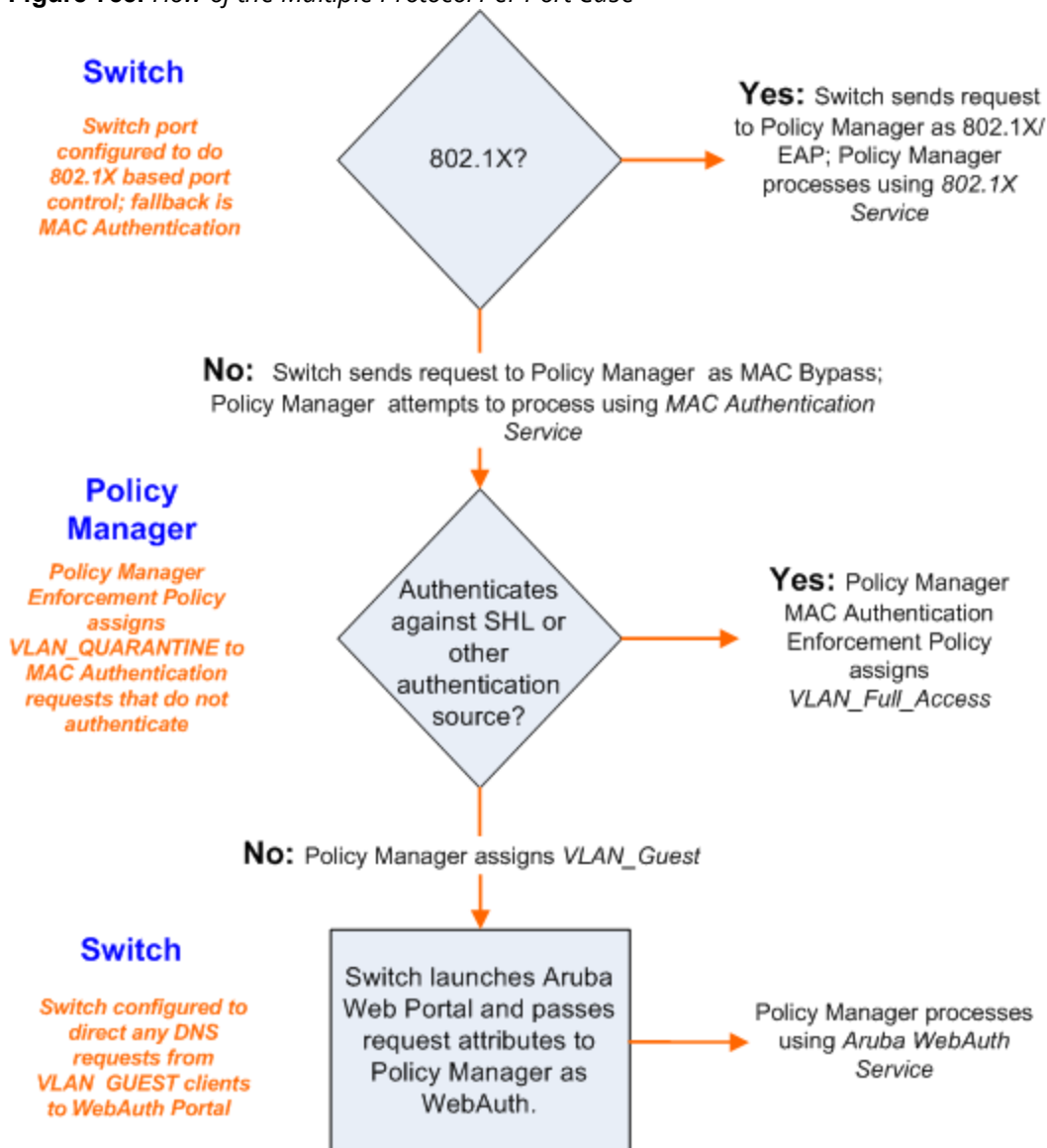
4. Define the Authentication settings for the service. Authentication methods can be left to their default values, as the Policy Manager TACACS+ service authenticates TACACS+ requests internally.
 - a. In the **Authentication Sources** section, click the **Select to Add** drop-down list.
 - b. Select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

Single Port Use Case

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

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

Figure 755: Flow of the Multiple Protocol Per Port Case



This appendix includes the following information:

- [Introduction](#)
- [Native Agents Only Mode](#)
- [Native Agents with Java Fallback Mode](#)
- [Configuring Web Agent Flow - Java Only Mode](#)
- [Native Dissolvable Agent Supported Operating Systems and Browsers](#)
- [OnGuard Dissolvable Agent Supported Browsers and Java Versions](#)

Introduction

W-ClearPass OnGuard controls compromised devices by detecting and blocking access to unsecure or unhealthy devices. The client is denied access to network resources across wired, wireless, and remote networks when it is determined as unsecure, which is accomplished by running an extensive posture assessment.

The OnGuard Agent is supported by Windows, Linux, and Mac OSX devices.

You can configure the OnGuard Dissolvable Agent flow in different modes to perform health scan on endpoints. This section provides information on configuring OnGuard Dissolvable Agent in the following modes and the end-to-end flow:

- **Native agents only:** Native Dissolvable Agent communicates with W-ClearPass Guest to send information about endpoints such as status, health status, remediation messages and so on. This communication is independent of the operating systems and browsers.
- **Native agents with Java fallback:** The configuration for the **Native agents with Java fallback** mode is similar to the **Native agents only** mode. The posture assessment is performed based on the user's preference.
- **Java Only:** The communication is dependent on the browsers and the Java Runtime Environment (JRE) versions installed. For the supported Java versions and browsers, see [OnGuard Dissolvable Agent Supported Browsers and Java Versions on page 839](#).

Native Agents Only Mode

The Native Dissolvable Agent communicates with W-ClearPass Guest portal to send information about endpoints, such as status, health status, remediation messages, and so on. This communication is independent of the operating systems and browsers.

Native Dissolvable Agent supports the following browsers and operating systems:

Table 444: *Supported Operating Systems and Browsers*

OS	Browsers
Windows	- Internet Explorer - FireFox - Google Chrome
Mac OS X	- Safari - FireFox - Google Chrome
Linux	FireFox

W-ClearPass Policy Manager hosts the Native Dissolvable Agent binary files with OnGuard Persistent Agent installers.

You can use the links to download the binaries in the **OnGuard Settings** page for Windows (.exe) and Mac OS X (.DMG).

Navigate to: **Administration > Agents and Software Updates > OnGuard Settings**.

Configuring Workflow in Native Agents Only Mode

In W-ClearPass Guest, the web login page is enhanced to avoid an additional web authentication service and simplifies the configuration on dissolvable agent flow with the policy-initiated login method.

To configure the OnGuard Dissolvable Agent in Native agents only mode:

1. In the **Login Method** field, select the **Policy-initiated - An enforcement policy will control a change of authorization** option .

The following figure displays the policy-initiated login method in the **Web Login Editor** page:

Figure 756: *Policy-Initiated Log-in Method*

Web Login (webagent)

Use this form to make changes to the Web Login **webagent**.

Web Login Editor	
* Name:	webagent Enter a name for this web login page.
Page Name:	webagent Enter a page name for this web login. The web login will be accessible from "/guest/page_name.php".
Description:	 Comments or descriptive text about the web login.
* Vendor Settings:	Aruba Networks Select a predefined group of settings suitable for standard network configurations.
Login Method:	Policy-initiated — An enforcement policy will control a change of authorization Select how the user's network login will be handled. Server-initiated logins require the user's MAC address to be available, usually from the captive portal redirection process.
Security Hash:	Do not check - login will always be permitted Select the level of checking to apply to URL parameters passed to the web login page. Use this option to detect when URL parameters have been modified by the user, for example their MAC address.

2. Select the **Require a successful OnGuard health check** option in the **Health Check** field. If you select this field, the guest needs to pass a health check before accessing the network. Select the **Native agents only** mode in the **Client Agents** field:

Figure 757: Native Agents Only Mode

Post-Authentication	
Actions to perform after a successful pre-authentication.	
Health Check:	☒ Require a successful OnGuard health check If selected, the guest will be required to pass a health check prior to accessing the network.
Client Agents:	Native agents only Select the agent options for client scanning. Native agents are available for Microsoft Windows and Apple OS X. All other OS will fall back to Java.

End-to-End Flow in Native Agents Only Mode

The following steps describe the end-to-end flow of the OnGuard Dissolvable Agent running on Native agents only mode:

1. You are redirected to the W-ClearPass Guest Portal where you can download the native agent installer.
2. After accepting the terms and conditions for collecting end point posture assessment scan checks and performing remediation actions, run the Native Agent Installer.

The following figure shows an example of the Native Dissolvable Agent **Login** page:

Figure 758: Native Dissolvable Agent - Login Page



The **Terms** specified in the **Login** page are optional. You can configure this optionally by selecting the **Require a Terms and Conditions confirmation** check box in the **Terms** field in the W-ClearPass Guest Login Form.

3. The figure similar to the following OnGuard Agent download prompt appears when you log in for the first time to the Native Dissolvable Agent:

Figure 759: Native Dissolvable Agent Installer Prompt

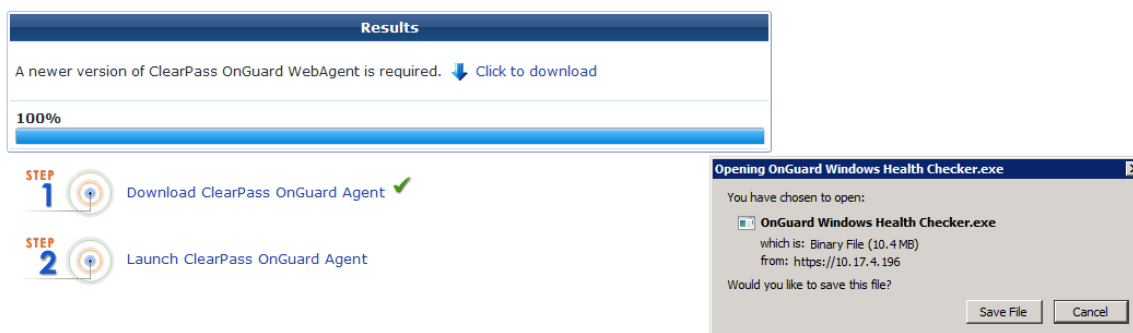


The download options are available only when you log in for the first time. Alternatively, you can download the OnGuard agent by clicking the **Download W-ClearPass OnGuard Agent** link.

4. To download the OnGuard Agent, click **OK**.

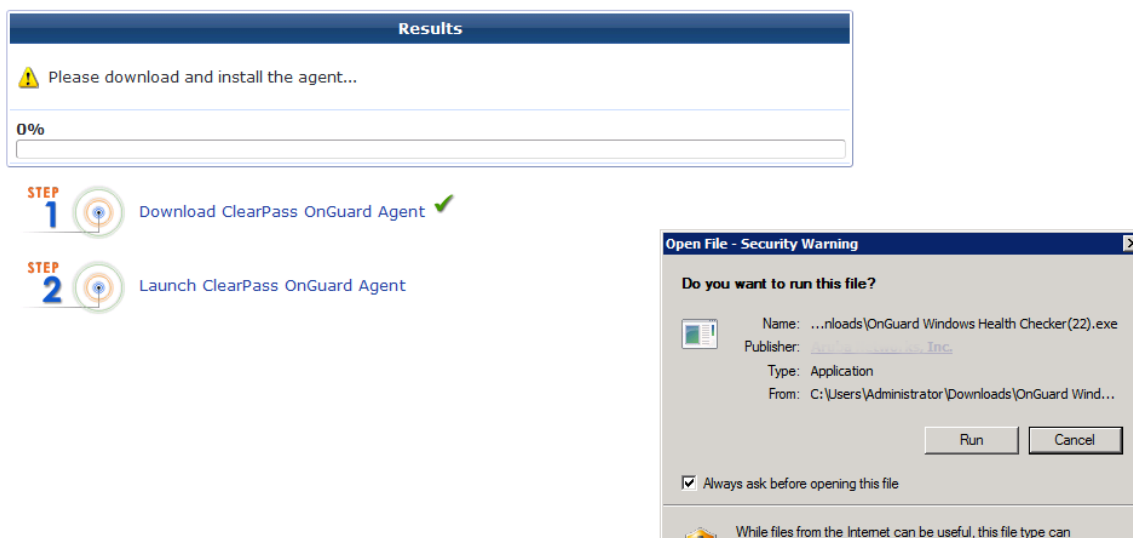
The figure shows an example of the **OnGuard Windows Health Checker** binary download window:

Figure 760: *Native Dissolvable Agent Binary Downloader*



5. To download the OnGuard agent, click **Save File**.
6. To install the OnGuard agent, click **Run**.

Figure 761: *Native Dissolvable Agent Installation*



If you are running Windows OS, Internet Explorer provides options to **Run** or **Save**. FireFox and Chrome browsers provide option to save the .exe files.

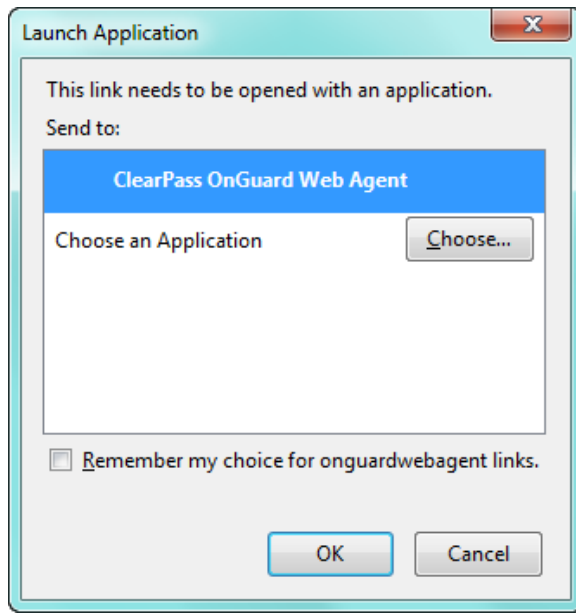


If you are running Mac OS X, FireFox provides options to open the binary with **DiskImageMounter** or save the .DMG files.

Safari and Google Chrome browsers provide the option to **Save** only.

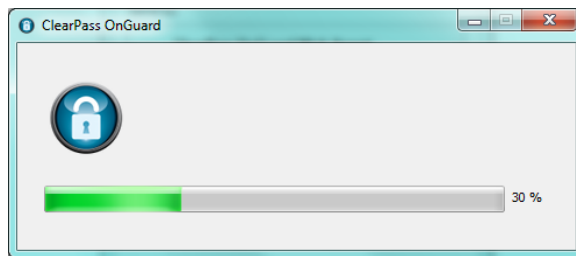
7. From the **Launch Application** page, select the **W-ClearPass OnGuard Web Agent** application.
8. To register and perform auto-launch of native OnGuard agent on successive log-ins, select **Remember my choice for onguardwebagent links**, then click **OK**.

Figure 762: *Native Dissolvable Agent Application Launcher*



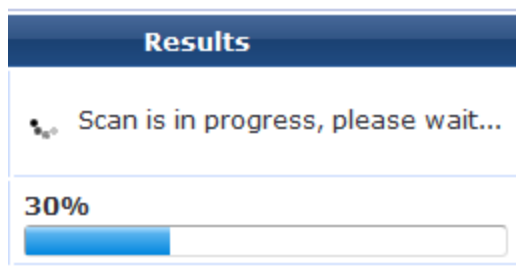
9. The following progress screen appears and shows the progress:

Figure 763: *Native Dissolvable Agent Installation Progress*



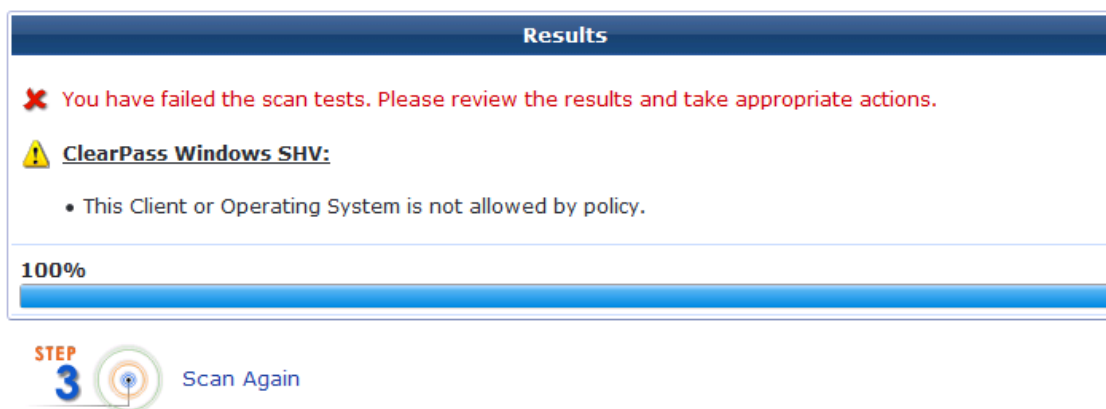
10. After the successful installation, the health check scanning is initiated. The following figure shows an example of the progress indicator:

Figure 764: *Health Check Progress*



11. After the health check scanning is completed, the figure similar to the following example appears with the health check results if the client is unhealthy:

Figure 765: Health Check Results



12. Take the appropriate actions to fix the issues listed in remediation and agent enforcement messages, then click **Scan Again**.

Repeat this step until the client becomes healthy. Once the client is healthy, you can access the destination URL.

13. You can track the events with the end-to-end flow in the **Access Tracker** page.

The following figure shows an example of the **Access Tracker** page with the Native Dissolvable Agent flow:

Figure 766: Access Tracker Page

10.1.1.97	RADIUS	suribabu	1X-Wireless	ACCEPT	2014/07/10 16:07:12
10.1.1.97	WEBAUTH	7cd1c373c4e4	Health-only	ACCEPT	2014/07/10 16:07:03
10.1.1.97	RADIUS	suribabu	1X-Wireless	ACCEPT	2014/07/10 16:06:30

The Auto-launch feature works in the **Native agents only** and **Java Only** modes without user intervention to click pop-ups and options that are described in the complete end-to-end flow above, except configuring **Terms** in the W-ClearPass Guest **Login** page.

Auto-Login

The Native Dissolvable Agent supports the **Auto-Login** method, which eliminates the **Require a Terms and Conditions confirmation** check box in the **Guest Web Login** page by avoiding the web page and submitting automatically.

Troubleshooting

In Windows, Native Dissolvable Agent flow logs are available at:

%appdata%\Aruba Networks\ ClearPassOnGuard Temp\Logs

In MAC OS X, the Native dissolvable agent flow logs are available at:

~/Library/Logs/ClearPassOnGuardTemp/logs.

Native Agents with Java Fallback Mode

The configuration steps for **Native agents with or Java fallback** work flow is similar to the **Native agents only** mode. The posture assessment is performed based on your selection.

Configuring Native Agents with Java Fallback Mode

Use the following steps to configure the OnGuard Dissolvable Agent in **Native agents with Java fallback** mode:

1. Select the **Policy-initiated - An enforcement policy will control a change of authorization** option from the drop-down list in the **Login Method** field. The following figure shows an example configuration of the Policy-initiated **Login** method:

Figure 767: Policy-initiated Login Method

Web Login (webagent)

Use this form to make changes to the Web Login **webagent**.

Web Login Editor	
* Name:	webagent Enter a name for this web login page.
Page Name:	webagent Enter a page name for this web login. The web login will be accessible from "/guest/page_name.php".
Description:	 Comments or descriptive text about the web login.
* Vendor Settings:	Aruba Networks Select a predefined group of settings suitable for standard network configurations.
Login Method:	Policy-initiated — An enforcement policy will control a change of authorization Select how the user's network login will be handled. Server-initiated logins require the user's MAC address to be available, usually from the captive portal redirection process.
Security Hash:	Do not check - login will always be permitted Select the level of checking to apply to URL parameters passed to the web login page. Use this option to detect when URL parameters have been modified by the user, for example their MAC address.

2. Select the **Require a successful OnGuard health check** option in the **Health Check** field. If you select this field, the guest needs to pass a health check before accessing the network. Select the **Native agents with Java fallback** mode in the **Client Agents** field:

Figure 768: Native Agents with Java Fallback Mode

Post-Authentication	
Actions to perform after a successful pre-authentication.	
Health Check:	☒ Require a successful OnGuard health check If selected, the guest will be required to pass a health check prior to accessing the network.
Client Agents:	Native agents with Java fallback Select the agent options for client scanning. Native agents are available for Microsoft Windows and Apple OS X. All other OS will fall back to Java.

End-to-end flow in Native Agents with Java Fallback Mode

The posture assessment is performed based on your selection. If you select Java, the Java applet is downloaded and posture assessment is performed. The native agent link is provided in **Java launcher** to avoid the JRE files loaded into the system. The following figure shows an example of the **Native agents with Java fallback** options:

Figure 769: *Native Dissolvable Agents with Java Fallback*

Results	
Status	Detecting agent...
Progress	0%

➔ Launch ClearPass OnGuard Agent

➔ Launch Java Agent

⬇ Download ClearPass OnGuard Agent

Configuring Web Agent Flow - Java Only Mode

You can configure a new web agent flow in two different locations (W-ClearPass Policy Manager and W-ClearPass Guest) to perform health scan on endpoints.

Configuring Web Agent Flow in W-ClearPass Policy Manager

Use the following steps to configure a new web agent flow in W-ClearPass Policy Manager:

1. Create a 802.1X service to perform RADIUS authentication and enforce restricted or full access based on end point posture assessments. The following figure shows an example of the **Web Agent Flow - 802.1X Service** page:

Figure 770: *Web Agent Flow - 802.1X Service*

Configuration » Services » Edit - 1X-Wireless

Services - 1X-Wireless

Summary	Service	Authentication	Roles	Enforcement
Use Cached Results:	☒ Use cached Roles and Posture attributes from previous sessions			
Enforcement Policy:	Radius-enforcement			Modify
Enforcement Policy Details				
Description:				
Default Profile:	suri-cp-role			
Rules Evaluation Algorithm:	first-applicable			
Conditions		Enforcement Profiles		
1.	(Tips:Posture EQUALS HEALTHY (0))	suri-auth-role		

2. Create a service named **Web-based Health Check Only** on the W-ClearPass Policy Manager server. The following figure shows an example of the **Web Agent Flow - Health Only** page:

Figure 771: Web Agent Flow - Health Only

Configuration » Services » Edit - Health-Only

Services - Health-Only

Summary	Service	Roles	Posture	Enforcement
Use Cached Results: ☐ Use cached Roles and Posture attributes from previous sessions				
Enforcement Policy:		Web-CoA-enforcement		Add new Enforcement Policy
Enforcement Policy Details				
Description:				
Default Profile:		Web-CoA-init		
Rules Evaluation Algorithm:		first-applicable		
Conditions		Enforcement Profiles		
1.	(Tips:Posture EQUALS HEALTHY (0))	[Aruba Terminate Session], Entity-updatelasthealthstate		
2.	(Tips:Posture NOT_EQUALS HEALTHY (0))	Entity-updatelasthealthstate		

3. Create a simple Web Auth service to authenticate users against W-ClearPass Guest user database to accept or perform App authentication request after completing a sandwich flow. The following figure shows an example of the **Web Agent Flow - Services Web Auth** page:

Figure 772: Web Agent Flow - Services Web Auth

Configuration » Services » Edit - Web-auth					
Services - Web-auth					
Summary	Service	Authentication	Roles	Posture	Enforcement
Authentication Sources:		[Guest User Repository] [Local SQL DB] AD-Pegasus [Active Directory] [Local User Repository] [Local SQL DB] --Select to Add-- Add Move Up Move Down Remove View Details Modify			
Strip Username Rules:		☐ Enable to specify a comma-separated list of rules to strip username prefixes or suffixes			

Configuring Web Agent Flow in W-ClearPass Guest

Use the following steps to create a web agent flow in W-ClearPass Guest:

1. Click **Create a new web login page** on the right corner of the W-ClearPass Guest UI. The following figure shows an example of the **Web Login Editor** page:

Figure 773: Web Login Editor

Web Login (new)

Use this form to create a new Web Login.

Web Login Editor	
* Name:	Webagent Enter a name for this web login page.
Page Name:	Webagent Enter a page name for this web login. The web login will be accessible from "/guest/page_name.php".
Description:	 Comments or descriptive text about the web login.
* Vendor Settings:	Aruba Networks Select a predefined group of settings suitable for standard network configurations.
Login Method:	Server-initiated — Change of authorization (RFC 3576) sent to controller Select how the user's network login will be handled. Server-initiated logins require the user's MAC address to be available, usually from the captive portal redirection process.
Security Hash:	Do not check – login will always be permitted Select the level of checking to apply to URL parameters passed to the web login page. Use this option to detect when URL parameters have been modified by the user, for example their MAC address.

2. Select the **Anonymous - Do not require a username or password** option from the drop-down.
3. Check the **Enable bypassing the Apple Captive Network Assistant** option in the **Prevent CNA** field.
4. Select the **Local - match a local account** option in the **Pre-Auth Check** field.
5. Check the **Require Terms and Conditions confirmation** option in the **Terms** field.
6. Specify the destination URL to which the client must be redirected after health checks in the **Default destination** field.

Figure 774: Web Login - Login Form

Login Form	
Options for specifying the behaviour and content of the login form.	
Authentication:	Anonymous - Do not require a username or password Select the authentication requirement. Access Code requires a single code (username) to be entered. Anonymous allows a blank form requiring just the terms or a Log In button. A pre-existing account is required. Access Code and Anonymous require the account to have the Username Authentication field set.
Auto-Generate:	☒ Auto-generate the anonymous account The account will be created without a session limit or expiration time, and with the Guest role (ID 2).
* Anonymous User:	 The account to use for anonymous authentication. The password will be visible within the HTML. It is recommended to increase the account Session Limit to the number of guests you wish to support.
Prevent CNA:	☒ Enable bypassing the Apple Captive Network Assistant The Apple Captive Network Assistant (CNA) is the pop-up browser shown when joining a network that has a captive portal. Note that this option may not work with all vendors, depending on how the captive portal is implemented.
Custom Form:	☐ Provide a custom login form If selected, you must supply your own HTML login form in the Header or Footer HTML areas.
Custom Labels:	☐ Override the default labels and error messages If selected, you will be able to alter labels and error messages for the current login form.
* Pre-Auth Check:	Local — match a local account Select how the username and password should be checked before proceeding to the NAS authentication.
Terms:	☒ Require a Terms and Conditions confirmation If checked, the user will be forced to accept a Terms and Conditions checkbox.
Default Destination	
Options for controlling the destination clients will redirect to after login.	
* Default URL:	http://example.com Enter the default URL to redirect clients. Please ensure you prepend "http://" for any external domain.
Override Destination:	☐ Force default destination for all clients If selected, the client's default destination will be overridden regardless of its value.

- Select the **Local - match a local account** option in the **Post Authentication** field. The following figure shows an example of the **Web Login - Post-Authentication** page:

Figure 775: Web Login - Post-Authentication

Post-Authentication	
Actions to perform after a successful pre-authentication.	
Health Check:	☒ Require a successful OnGuard health check If selected, the guest will be required to pass a health check prior to accessing the network.

The following figure shows an example of the final web agent flow:

10.17.4.197	RADIUS	Suribabu	1X-Wireless	ACCEPT	2014/03/07 16:36:07
10.17.4.197	WEBAUTH	21886813	Web-auth	ACCEPT	2014/03/07 16:35:59
10.17.4.197	WEBAUTH	f0b47912ab19	Health-Only	ACCEPT	2014/03/07 16:35:58
10.17.4.197	RADIUS	suribabu	1X-Wireless	ACCEPT	2014/03/07 16:33:46

For more information, refer to W-ClearPass Guest Online Help.

Native Dissolvable Agent Supported Operating Systems and Browsers

This section provides information on the supported operating systems and browsers for the Native Dissolvable Agent. The versions given in the following table are tested and are up-to-date at the time of this release:

Table 445: Native Dissolvable Agent Supported Browsers and Java Versions

Operating System	Browser	Test Results	Known Issues	Tested Versions
Windows Operating System Support				
Windows 10 64-bit	Chrome	Passed		W-ClearPass Policy Manager 6.6.0.79875 , Chrome 48.X
	Firefox	Passed		W-ClearPass Policy Manager 6.6.0.79875 , Firefox 44.X
	Internet Explorer	Passed		W-ClearPass Policy Manager 6.6.0.79875 , IE-11.X
Windows 10 32-bit	Chrome	Passed	Health data collection does not work in a 64-bit JRE/ browser	W-ClearPass Policy Manager 6.6.0.79875 , Chrome 48.X
	Firefox	Passed		W-ClearPass Policy Manager 6.6.0.79875 , Firefox 44.X
	Internet Explore	Passed		W-ClearPass Policy Manager 6.6.0.79875 , IE-8.X
Windows 8.1 64-bit	Chrome	Passed		W-ClearPass Policy Manager 6.6.0.79875 , Chrome 49.X

Table 445: *Native Dissolvable Agent Supported Browsers and Java Versions (Continued)*

Operating System	Browser	Test Results	Known Issues	Tested Versions
	Firefox	Passed		W-ClearPass Policy Manager 6.6.0.79875 , Firefox 44.X
	Internet Explorer	Passed		W-ClearPass Policy Manager 6.6.0.79875 , IE-11.x
Windows 7 64-bit	Chrome	Passed		W-ClearPass Policy Manager 6.6.0.79875, Chrome 48.X
	Firefox	Passed	None	W-ClearPass Policy Manager 6.6.0.79875, Firefox 44.X
	IE	Passed	None	W-ClearPass Policy Manager 6.6.0.79875, IE-11.x
Windows 8 64-bit	Chrome	Passed		W-ClearPass Policy Manager 6.6.0.79875 , Chrome 48.X
	Firefox	Passed		W-ClearPass Policy Manager 6.6.0.79875 , Firefox 44.X
	Internet Explorer	Passed		W-ClearPass Policy Manager 6.6.0.79875 , IE-10.X
Windows 8 32-bit	Chrome	Passed		W-ClearPass Policy Manager 6.6.0.79875 , Chrome 48.X
	Firefox	Passed		W-ClearPass Policy Manager 6.6.0.79875 , Firefox 44.X
	Internet Explorer	Passed		W-ClearPass Policy Manager 6.6.0.79875 , IE-10.X
Windows 2008 64-bit	Chrome	Passed		W-ClearPass Policy Manager 6.6.0.79875, Chrome 41.X
	Firefox	Passed	None	W-ClearPass Policy Manager 6.6.0.79875, Firefox 44.X
	IE 8.X 32-bit	Passed		W-ClearPass Policy Manager 6.6.0.79875 , IE-8.x
Windows XP SP3	Chrome	Not supported	None	W-ClearPass Policy Manager 6.6.0.79875, Chrome 34.X
	Firefox	Not supported	None	W-ClearPass Policy Manager 6.6.0.79875, Firefox 30.X
	IE 8.X 32-bit	Not supported		W-ClearPass Policy Manager 6.6.0.79875, IE-8.x

Table 445: *Native Dissolvable Agent Supported Browsers and Java Versions (Continued)*

Operating System	Browser	Test Results	Known Issues	Tested Versions
Windows 2003 32-bit	Chrome	Not supported		W-ClearPass Policy Manager 6.6.0.79875, Chrome 35.X
	Firefox	Not supported		W-ClearPass Policy Manager 6.6.0.79875, Firefox 30.X
	IE	Not supported		W-ClearPass Policy Manager 6.6.0.79875, IE-8.x
Windows Vista	Chrome	Passed		W-ClearPass Policy Manager 6.6.0.79875, Chrome 48.X
	Firefox	Passed	None	W-ClearPass Policy Manager 6.6.0.79875, Firefox 44.X
	IE 7.X 32-bit	Passed	None	W-ClearPass Policy Manager 6.6.0.79875, IE-7.X
Mac OS X Support				
Mac OS X 10.11	Safari 9.x	Passed		W-ClearPass Policy Manager 6.6.0.79875, Safari 9.X
	Firefox 44.x	Passed		W-ClearPass Policy Manager 6.6.0.79875, Firefox 44.X
	Chrome 48.x	Passed		W-ClearPass Policy Manager 6.6.0.79875, Chrome-48.x
Mac OS X 10.10	Safari 9.x	Passed		W-ClearPass Policy Manager 6.6.0.79875, Safari 9.X
	Firefox 44.x	Passed		W-ClearPass Policy Manager 6.6.0.79875, Firefox 44.X
	Chrome 48.x	Passed		W-ClearPass Policy Manager 6.6.0.79875, Chrome-48.x
Mac OS X 10.9	Safari	Passed		W-ClearPass Policy Manager 6.6.0.79875, Safari 7
	Firefox	Passed		W-ClearPass Policy Manager 6.6.0.79875, Firefox 44
	Chrome	Passed		W-ClearPass Policy Manager 6.6.0.79875, Chrome-48.
Mac OS X 10.8	Safari	Passed		W-ClearPass Policy Manager 6.6.0.79875, Safari-6.x

Table 445: *Native Dissolvable Agent Supported Browsers and Java Versions (Continued)*

Operating System	Browser	Test Results	Known Issues	Tested Versions
	Firefox	Passed		W-ClearPass Policy Manager 6.6.0.79875, Firefox-43.x
	Chrome	Passed		W-ClearPass Policy Manager 6.6.0.79875, Chrome-47.x
Mac OS X 10.7.5	Safari	Passed		W-ClearPass Policy Manager 6.6.0.79875, Safari-6.x
	Firefox	Passed		W-ClearPass Policy Manager 6.6.0.79875, Firefox-44.x
	Chrome	Passed		W-ClearPass Policy Manager 6.6.0.79875, Chrome-48.x
Mac OS X 10.11	Safari	Passed		W-ClearPass Policy Manager 6.6.0.79875, Safari 9.X
	Firefox	Passed		W-ClearPass Policy Manager 6.6.0.79875, Firefox 44.X
	Chrome	Passed		W-ClearPass Policy Manager 6.6.0.79875, Chrome-48.X
Ubuntu Operating System Support				
Ubuntu 12.04 32-bit LTS	Firefox	Passed		W-ClearPass Policy Manager 6.6.0.79875, Firefox-38.x
	Chrome	No support		W-ClearPass Policy Manager 6.6.0.79875, Chrome 39.X
Ubuntu 12.04 64-bit LTS	Firefox	Passed	None	W-ClearPass Policy Manager 6.6.0.79875, Firefox-34.x
	Chrome	No support		W-ClearPass Policy Manager 6.6.0.79875, Chrome 39.X
Ubuntu 14.04 32-bit LTS	Firefox	Passed	None	W-ClearPass Policy Manager 6.6.0.79875, Firefox-38.x
	Chromium	Failed		W-ClearPass Policy Manager 6.6.0.79875, Chrome 39.X
Ubuntu 14.04 64-bit LTS	Firefox	Passed	None	W-ClearPass Policy Manager 6.6.0.79875, Firefox-44.X
	Chromium	Failed		W-ClearPass Policy Manager 6.6.0.79875, Chrome 39.X1 and Chromium 39.X

For more information on known issues, refer to the *W-ClearPass Policy Manager 6.6 Release Notes*.

OnGuard Dissolvable Agent Supported Browsers and Java Versions

This section provides information on supported browsers and Java versions for the OnGuard Dissolvable Agent. The versions given in the following table are tested and are up-to-date at the time of this release:

Table 446: *OnGuard Dissolvable Agent Supported Browsers and Java Versions*

Operating System	Browser	Java Version	Test Results	Known Issues	Tested Versions
Windows 10 64-bit	Chrome	8u73	Failed	Health data collection does not work in a 64-bit JRE/ browser	W-ClearPass Policy Manager 6.6.0.79875, Chrome 41.X
	Firefox 44.x	8u73	Passed		W-ClearPass Policy Manager 6.6.0.79875, Firefox 44.X
	Internet Explorer 11.x	8u73	Passed		W-ClearPass Policy Manager 6.6.0.79875, IE-11.x
Windows 10 32-bit	Chrome	8u73	Failed	Health data collection does not work in a 64-bit JRE/ browser	W-ClearPass Policy Manager 6.6.0.79875, Chrome 414
	Firefox 44.x	8u73	Passed		W-ClearPass Policy Manager 6.6.0.79875, Firefox 44.X
	Internet Explorer 11.x	8u73	Passed		W-ClearPass Policy Manager 6.6.0.79875, IE11.x
Windows 7 64-bit	Chrome	8u73	Failed	Health data collection does not work in a 64-bit JRE/ browser	W-ClearPass Policy Manager 6.6.0.79875, Chrome 48.X
	Firefox	8u73	Passed		W-ClearPass Policy Manager 6.6.0.79875, Firefox 44.X
	IE	8u73	Passed		W-ClearPass Policy Manager 6.6.0.79875, IE-11.X

Table 446: OnGuard Dissolvable Agent Supported Browsers and Java Versions (Continued)

Operating System	Browser	Java Version	Test Results	Known Issues	Tested Versions
Windows 7 32-bit	Chrome	8u73	Failed		W-ClearPass Policy Manager 6.6.0.79875, Chrome 44.X
	Firefox	8u73	Passed		W-ClearPass Policy Manager 6.6.0.79875, Firefox 44.X
	IE	8u73	Passed		W-ClearPass Policy Manager 6.6.0.79875, IE-11.X
Windows 8 64-bit	Chrome	8u73	Failed	Health data collection does not work in a 64-bit JRE/ browser	W-ClearPass Policy Manager 6.6.0.79875, Chrome 48.X
	Firefox	8u73	Passed		W-ClearPass Policy Manager 6.6.0.79875, Firefox 44.X
	IE 32-bit	8u73	Passed		W-ClearPass Policy Manager 6.6.0.79875, IE-10.X
Windows 8 32-bit	Chrome	8u73	Failed		W-ClearPass Policy Manager 6.6.0.79875, Chrome 48.X
	Firefox	8u73	Passed		W-ClearPass Policy Manager 6.6.0.79875, Firefox 44.X
	IE	8u73	Passed		W-ClearPass Policy Manager 6.6.0.79875, IE-10.X
Windows 8.1 64-bit	Chrome	8u73	Failed		W-ClearPass Policy Manager 6.6.0.79875, Chrome 44.X
	Firefox	8u73	Passed		W-ClearPass Policy Manager 6.6.0.79875, Firefox 40.X
	IE	8u73	Passed		W-ClearPass Policy Manager 6.6.0.79875, IE-11.X

Table 446: OnGuard Dissolvable Agent Supported Browsers and Java Versions (Continued)

Operating System	Browser	Java Version	Test Results	Known Issues	Tested Versions
Windows 8.1 32-bit	Chrome	8u73	Failed		W-ClearPass Policy Manager 6.6.0.80940, Chrome 49.X
	Firefox	8u73	Passed		W-ClearPass Policy Manager 6.6.0.80940, Firefox 45.X
	IE	8u73	Passed		W-ClearPass Policy Manager 6.6.0.80940, IE-11.x
Windows 2008 64-bit	Chrome	8u73	Failed	Health data collection does not work in a 64-bit JRE/ browser	W-ClearPass Policy Manager 6.6.0.79875, Chrome 41.X
	Firefox	8u73	Passed		W-ClearPass Policy Manager 6.6.0.79875, Firefox 44.X
	IE	8u73	Passed		W-ClearPass Policy Manager 6.6.0.79875, IE-7.x
Windows Vista	Chrome	8u73	Failed	Health data collection does not work in a 64-bit JRE/ browser	W-ClearPass Policy Manager 6.6.0.79875, Chrome 48.X
	Firefox	8u73	Passed		W-ClearPass Policy Manager 6.6.0.79875, Firefox 44.X
	IE	8u73			W-ClearPass Policy Manager 6.6.0.79875, IE-9.X
Windows 2003 32-bit	Chrome	8u73	Not supported		W-ClearPass Policy Manager 6.6.0.79875, Chrome 35.X
	Firefox	8u73	Not supported		W-ClearPass Policy Manager 6.6.0.79875, Firefox 30.X
	IE	8u73	Not supported		W-ClearPass Policy Manager 6.6.0.79875, IE

Table 446: OnGuard Dissolvable Agent Supported Browsers and Java Versions (Continued)

Operating System	Browser	Java Version	Test Results	Known Issues	Tested Versions
					8.X
Windows XP 32-bit	Chrome	8u73	Not supported		W-ClearPass Policy Manager 6.6.0.79875, Chrome 35.X
	Firefox	8u73	Not supported		W-ClearPass Policy Manager 6.6.0.79875, Firefox 30.X
	IE	8u73	Not supported		W-ClearPass Policy Manager 6.6.0.79875, IE-8.x
Mac 10.11	Safari	8u73	Passed	Java plug-in must be enabled to "Run in Unsafe Mode"	W-ClearPass Policy Manager 6.6.0.79875, Safari 9.X
	Firefox	8u73	Passed		W-ClearPass Policy Manager 6.6.0.79875, Firefox 44.X
	Chrome	8u73	Failed		W-ClearPass Policy Manager 6.6.0.79875, Chrome-44.x
Mac 10.10	Safari	8u73	Passed	Java plug-in must be enabled to "Run in Unsafe Mode"	W-ClearPass Policy Manager 6.6.0.79875, Safari 9.X
	Firefox	8u73	Passed		W-ClearPass Policy Manager 6.6.0.79875, Firefox 44.X
	Chrome	8u73	Failed		W-ClearPass Policy Manager 6.6.0.79875, Chrome-44.x
Mac 10.9.5	Safari	8u73	Passed	Java plug-in must be enabled to "Run in Unsafe Mode"	W-ClearPass Policy Manager 6.6.0.79875, Safari 7.X

Table 446: *OnGuard Dissolvable Agent Supported Browsers and Java Versions (Continued)*

Operating System	Browser	Java Version	Test Results	Known Issues	Tested Versions
	Firefox	8u73	Passed		W-ClearPass Policy Manager 6.6.0.79875, Firefox 44.X
	Chrome	8u73	Failed		W-ClearPass Policy Manager 6.6.0.79875, Chrome-44.x
Mac 10.8	Safari	8u73	Passed	Java plug-in must be enabled to "Run in Unsafe Mode"	W-ClearPass Policy Manager 6.6.0.79875, Safari 6.X
	Firefox	8u73	Passed		W-ClearPass Policy Manager 6.6.0.79875, Firefox 44.X
	Chrome	8u73	Failed		W-ClearPass Policy Manager 6.6.0.79875, Chrome-44.x
Unbuntu	Firefox	8u73	Passed		W-ClearPass Policy Manager 6.6.0.79875, Firefox 44.X
Fedora	Firefox	8u73	Failed		W-ClearPass Policy Manager 6.6.0.79875, Firefox 44.X
CentOS	Firefox	8u73	Passed		W-ClearPass Policy Manager 6.6.0.79875, Firefox 44.X
RedHat	Firefox	8u73	Passed		W-ClearPass Policy Manager 6.6.0.7987, Firefox 44.X
Suse	Firefox	8u73	Passed		W-ClearPass Policy Manager 6.6.0.7987, Firefox 44.X

For more information on Known Issues, refer to *W-ClearPass Policy Manager 6.6 Release Notes*.

The W-Policy Manager administration User Interface allows you to create different types of objects:

- Service rules
- Role mapping policies
- Internal user 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 list 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 list 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, variables, and operators:

- [Namespaces on page 845](#)
- [Variables on page 855](#)
- [Operators on page 856](#)

Namespaces

Multiple namespaces are displayed in the rules editing interfaces, depending upon what you are editing. For example, multiple namespaces are displayed 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.

For detailed information about the available namespaces, see the following topics:

- [Application Namespace on page 846](#)
- [Audit Namespaces on page 847](#)

- [Authentication Namespaces on page 847](#)
- [Authorization Namespaces on page 849](#)
- [Certificate Namespaces on page 850](#)
- [Connection Namespaces on page 851](#)
- [Date Namespaces on page 852](#)
- [Device Namespaces on page 852](#)
- [Endpoint Namespaces on page 853](#)
- [Guest User Namespaces on page 853](#)
- [Host Namespaces on page 853](#)
- [Local User Namespaces on page 853](#)
- [Posture Namespaces on page 854](#)
- [RADIUS Namespaces on page 854](#)
- [TACACS Namespaces on page 855](#)
- [Tips Namespaces on page 855](#)

Application Namespace

The Application namespace has one name attribute. This attribute is an enumerated type currently containing the following string values:

- Guest
- Insight
- PolicyManager
- Onboard
- W-ClearPass

The Application:ClearPass namespace has the following string values available for the **Name** field:

- AssertionConsumerUrl
- Configuration-Profile-ID
- Device-Compromised
- Device-ICCID
- Device-IMEI
- Device-MAC
- Device-MDM-Managed
- Device-NAME
- Device-OS
- Device-PRODUCT
- Device-SERIAL
- Device-UDID
- Device-VERSION
- IDDP-COOKIE-TIMEOUT-MINS
- IDPURL
- MDM-Data-Roaming
- MDM-Voice-Roaming
- Onboard-Max-Devices

- Page-Name
- Provisioning-Settings-ID
- SAMLRequest
- SAMLResponse
- Session-Timeout
- User-Email-Address

Audit Namespaces

The dictionaries in the audit namespace come pre-packaged with the product. The Audit namespace has the notation *Vendor:Audit*, where *Vendor* is the name of the company that has defined attributes in the dictionary.

Examples of dictionaries in the audit namespace are AvendaSystems:Audit or Qualys:Audit.

The Audit namespace appears when editing post-audit rules. See [Audit Servers](#) for more information.

The Avenda Systems:Audit namespace appears when editing post-audit rules for Nessus and NMAP audit servers.

The following figure displays the Audit Namespace attributes:

Table 447: *Audit Namespace Attributes*

Attribute Name	Values
Audit-Status	• AUDIT_ERROR • AUDIT_INPROGRESS • AUDIT_SUCCESS
Device-Type	Type of device returned by an NMAP port scan.
Output-Msgs	The output message returned by Nessus plugin after a vulnerability scan.
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.

Authentication Namespaces

The authentication namespace can be used in role mapping policies to define roles based on the type of authentication method used or the status of the authentication.

Authentication Namespace Editing Context

The following table describes the **Authentication Namespace Attributes** parameters:

Table 448: *Authentication Namespace Attributes*

Attribute Name	Values
InnerMethod	• CHAP • EAP-GTC • EAP-MD5 • EAP-MSCHAPv2 • EAP-TLS • MSCHAP • PAP NOTE: The EAP-MD5 authentication type is not supported if you use the W-ClearPass Policy Manager in the FIPS mode.
OuterMethod	• CHAP • EAP-FAST • EAP-MD5 • EAP-PEAP • EAP-TLS • EAP-TTLS • MSCHAP • PAP NOTE: The EAP-MD5 authentication type is not supported if you use the W-ClearPass Policy Manager in the FIPS mode.
Phase1PAC	• None - No PAC was used to establish the outer tunnel in the EAP-FAST authentication method • Tunnel - A tunnel PAC was used to establish the outer tunnel in the EAP-FAST authentication method • Machine - 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 in Adding and Modifying Authentication Methods on page 169).
Phase2PAC	• None - No PAC was used instead of an inner method handshake in the EAP-FAST authentication method • UserAuthPAC - A user authentication PAC was used instead of the user authentication inner method handshake in the EAP-FAST authentication method • PosturePAC - A posture PAC was used instead of the posture credential handshake in the EAP-FAST authentication method
Posture	• Capable - The client is capable of providing posture credentials • Collected - Posture credentials were collected from the client • Not-Capable - The client is not capable of providing posture credentials • Unknown - It is not known whether the client is capable of providing credentials
Status	• None - No authentication took place • User - The user was authenticated • Machine - The machine was authenticated • Failed - Authentication failed

Table 448: *Authentication Namespace Attributes (Continued)*

Attribute Name	Values
	• AuthSource-Unreachable - The authentication source was unreachable
MacAuth	• NotApplicable - Not a MAC Auth request • Known Client - Client MAC address was found in an authentication source • Unknown Client - Client MAC address was not found in an authentication source
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.

Authorization Namespaces

W-Policy Manager supports multiple 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).

Authorization editing context

Role mapping policies

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. For W-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 on page 193](#) for more information).

Authorization

The authorization namespace has one attribute: sources. The values are pre-populated with the authorization sources defined in W-Policy Manager. Use this to check for the authorization source(s) from which attributes were extracted for the authenticating entity.

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. For W-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 on page 193](#)).

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 defined when you created an instance of this authentication source. The attribute names are pre-populated for administrative convenience.

Sources

This is the list of the authorization sources from which attributes were fetched for role mapping. Authorization namespaces appear in Role mapping policies.

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 defined when you created an instance of this authentication source. The attribute names are pre-populated for administrative convenience. For W-Policy Manager to fetch the values of attributes from a SQL-compliant database, you need to define filters for that authentication source.

Certificate Namespaces

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).

Certificate Namespace Editing Context

Role mapping policies

Table 449: *Certificate Namespace Attributes*

Attribute Name	Values
Version	Certificate version
Serial-Number	Certificate serial number
• Subject-C • Subject-CN • Subject-DC • Subject-DN • Subject-emailAddress • Subject-GN • Subject-L • Subject-O • Subject-OU • Subject-SN • Subject-ST • Subject-UID	Attributes associated with the subject (user or machine, in this case). Not all of these fields are populated in a certificate.
• Issuer-C • Issuer-CN • Issuer-DC • Issuer-DN • Issuer-emailAddress • Issuer-GN • Issuer-L	Attributes associated with the issuer (Certificate Authorities or the enterprise CA). Not all of these fields are populated in a certificate.

Table 449: *Certificate Namespace Attributes (Continued)*

Attribute Name	Values
• Issuer-O • Issuer-OU • Issuer-SN • Issuer-ST • Issuer-UID	
• Subject-AltName-DirName • Subject-AltName-DNS • Subject-AltName-EmailAddress • Subject-AltName-IPAddress • Subject-AltName-msUPN • Subject-AltName-RegisterdID • Subject-AltName-URI	Attributes associated with the subject (user or machine, in this case) alternate name. Not all of these fields are populated in a certificate.

Connection Namespaces

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.

Connection Namespace Editing Contexts

- Role mapping policies
- Service rules

The following table describes the **Connection Namespace Pre-defined Attributes** parameters:

Table 450: *Connection Namespace 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.

Table 450: *Connection Namespace Pre-defined Attributes (Continued)*

Attribute	Description
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).

Date Namespaces

The date namespace has three pre-defined attributes:

- Day-of-Week
- Date-of-Year
- Time-of-Day

For Day-of-Week, the supported operators 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 icon in the value field.

The Date-of-Year attribute shows a date, month and year icon 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.

Date Namespace Editing Contexts

- Enforcement policies
- Filter rules for Access Tracker and Activity Reports
- Role mapping policies
- Service rules

Device Namespaces

The Device namespace has four pre-defined attributes:

- Location
- OS-Version
- Device-Type
- Device-Vendor

Custom attributes also appear in the attribute list if they are defined as custom tags for the device.



These attributes can be used only if you have pre-populated the values for these attributes when a network device is configured.

Endpoint Namespaces

Use these attributes to look for attributes of authenticating endpoints, which are present in the Policy Manager endpoints list. The Endpoint namespace has the following attributes:

- Disabled By
- Disabled Reason
- Enabled By
- Enabled Reason
- Info URL

Guest User Namespaces

The GuestUser namespace has the attributes associated with the guest user (resident in the Policy Manager guest user database) who authenticated in this session. This namespace is only applicable if a guest user is authenticated. The GuestUser namespace has six pre-defined attributes:

- Company-Name
- Designation
- Email
- Location
- Phone
- Sponsor

Custom attributes also appear in the attribute list if they are defined as custom tags for the guest user.



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.

Host Namespaces

The Host namespace has the following predefined attributes:

- Name*
- OType*
- FQDN*
- UserAgent**
- CheckType**
- UniqueID
- AgentType*
- InstalledSHAs*

* Only populated when request is originated by a Microsoft NAP-compatible agent.

** Only present if Policy Manager acts as a Web authentication portal.

Local User Namespaces

The LocalUser namespace has the attributes associated with the local user (resident in the Policy Manager local user database) who authenticated in this session. This namespace is only applicable if a local user is authenticated.

The LocalUser namespace has four pre-defined attributes:

- Designation

- Email
- Phone
- Sponsor

Custom attributes also appear in the attribute list if they are defined as custom tags for the local user.



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.

Posture Namespaces

The dictionaries in the posture namespace are pre-packaged with the product. The administration interface provides a way to add dictionaries into the system (see [Posture Dictionary](#).) 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:

- W-ClearPass:LinuxSHV
- Microsoft:SystemSHV
- Microsoft:WindowsSHV
- Trend:AV

Posture Namespace Editing Context

- Filter rules for Access Tracker and Activity Reports
- Internal posture policies actions - Attributes marked with the OUT qualifier
- Internal posture policies conditions - Attributes marked with the IN qualifier
- Policy simulation attributes

RADIUS Namespaces

Dictionaries in the RADIUS namespace come pre-packaged with the product. The administration interface does provide a way to add dictionaries into the system (See [RADIUS Dictionary on page 637](#) 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:Aruba
- RADIUS:IETF
- RADIUS:Juniper
- RADIUS:Microsoft

RADIUS Namespace Editing Contexts

- Filter rules for Access Tracker and Activity Reports
- Policy simulation attributes
- Post-proxy attribute pruning rules

- RADIUS Enforcement profiles: All RADIUS namespace attributes that can be sent back to a RADIUS client (the ones marked with the OUT or INOUT qualifier)
- Role mapping policies
- Service rules: All RADIUS namespace attributes that can appear in a request (the ones marked with the IN or INOUT qualifier)

TACACS Namespaces

The TACACS (Terminal Access Controller Access-Control System) namespace has the attributes associated with attributes available in a TACACS+ request. Available attributes are:

- AuthSource
- AvendaAVPair
- UserName

Tips Namespaces

The pre-defined attributes for the Tips namespace are *Role* and *Posture*. Values are assigned to these attributes at run-time after Policy Manager evaluates role mapping and posture related policies.

Role

The value for the Role attribute is a set of roles assigned by either the role mapping policy or the post-audit policy. The value of the Role attribute can also be a dynamically fetched “Enable as role” attribute from the authorization source. The posture value is computed after Policy Manager evaluates internal posture policies, and gets posture status from posture servers or audit servers.

Posture

The value for the Posture attribute is one of the following:

- CHECKUP
- HEALTHY
- INFECTED
- QUARANTINE
- TRANSITION
- UNKNOWN

Tips Namespace Editing Context

Enforcement policies

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.

W-Policy Manager does in-place substitution of the value of the variable during run-time rule evaluation.

The following built-in variables are supported in W-Policy Manager:

Table 451: *W-Policy Manager Variables*

Variable	Description
<code>%{attribute-name}</code>	<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 on page 193.
<code>%{RADIUS:IETF:MAC-Address-Colon}</code>	MAC address of client in aa:bb:cc:dd:ee:ff format
<code>%{RADIUS:IETF:MAC-Address-Hyphen}</code>	MAC address of client in aa-bb-cc-dd-ee-ff format
<code>%{RADIUS:IETF:MAC-Address-Dot}</code>	MAC address of client in aabb.ccdd.eeff format
<code>%{RADIUS:IETF:MAC-Address-NoDelim}</code>	MAC address of client in aabbccddeeff format



You can also use any other dictionary-based attributes (or namespace attributes) 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 W-Policy Manager supports a rich set of operators.

The type of operators presented are based on the data type of the attribute for which the operator is being used. Where the data type of the attribute is not known, the attribute is treated as a string type.

The following table lists the operators presented for common attribute data types:

Table 452: *Attribute Operators*

Attribute Type	Operators
String	• BELONGS_TO • NOT_BELONGS_TO • BEGINS_WITH • NOT_BEGINS_WITH • CONTAINS • NOT_CONTAINS • ENDS_WITH • NOT_ENDS_WITH • EQUALS • NOT_EQUALS • EQUALS_IGNORE_CASE • NOT_EQUALS_IGNORE_CASE • EXISTS • NOT_EXISTS • MATCHES_REGEX • NOT_MATCHES_REGEX
Integer	• BELONGS_TO • NOT_BELONGS_TO • EQUALS • NOT_EQUALS • EXISTS • NOT_EXISTS • GREATER_THAN • GREATER_THAN_OR_EQUALS • LESS_THAN • LESS_THAN_OR_EQUALS
Time or Date	• EQUALS • NOT_EQUALS • GREATER_THAN • GREATER_THAN_OR_EQUALS • LESS_THAN • LESS_THAN_OR_EQUALS • IN_RANGE

Table 452: Attribute Operators (Continued)

Attribute Type	Operators
Day	• BELONGS_TO • NOT_BELONGS_TO
List (Example: Role)	• EQUALS • NOT_EQUALS • MATCHES_ALL • NOT_MATCHES_ALL • MATCHES_ANY • NOT_MATCHES_ANY • 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 operator types:

Table 453: Operator Types

Operator	Description
BEGINS_WITH	For string data type, true if the run-time value of the attribute begins with the configured value. Example: <code>RADIUS:IETF:NAS-Identifier BEGINS_WITH "SJ-"</code>
BELONGS_TO	For string data type, true if the run-time value of the attribute matches a set of configured string values. Example: <code>RADIUS:IETF:Service-Type BELONGS_TO Login-User, Framed-User, Authenticate-Only</code> For integer data type, true if the run-time value of the attribute matches a set of configured integer values. Example: <code>RADIUS:IETF:NAS-Port BELONGS_TO 1,2,3</code> For day data type, true if run-time value of the attribute matches a set of configured days of the week. Example: <code>Date:Day-of-Week BELONGS_TO MONDAY, TUESDAY, WEDNESDAY</code> 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.
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). Example: <code>RADIUS:IETF:Calling-Station-Id BELONGS_TO_GROUP</code>

Operator	Description
	Printers.
CONTAINS	For string data type, true if the run-time value of the attribute is a substring of the configured value. Example: RADIUS:IETF:NAS-Identifier CONTAINS "VPN"
ENDS_WITH	For string data type, true if the run-time value of the attribute ends with the configured value. Example: RADIUS:IETF:NAS-Identifier ENDS_WITH "DEVICE"
EQUALS	True if the run-time value of the attribute matches the configured value. For string data type, this is a case-sensitive comparison. Example: RADIUS:IETF:NAS-Identifier EQUALS "SJ-VPN-DEVICE"
EQUALS_IGNORE_CASE	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. Example: RADIUS:IETF:NAS-Identifier EQUALS_IGNORE_CASE "sj-vpn-device"
EXISTS	For string data type, true if the run-time value of the attribute exists. This is a unary operator. Example: RADIUS:IETF:NAS-Identifier EXISTS
GREATER_THAN	For integer, time and date data types, true if the run-time value of the attribute is greater than the configured value. Example: RADIUS:IETF:NAS-Port GREATER_THAN 10
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. Example: RADIUS:IETF:NAS-Port GREATER_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. Example: Date:Date-of-Year IN_RANGE 2007-06-06,2007-06-12
LESS_THAN	For integer, time and date data types, true if the run-time value of the attribute is less than the configured value. Example: 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. Example: RADIUS:IETF:NAS-Port LESS_THAN_OR_EQUALS 10
MATCHES_ALL	For list data types, true if all of the run-time values in the list are found in the configured values. Example: Tips:Role MATCHES_ALL HR,ENG,FINANCE. In this example, if

Operator	Description
	the run-time values of Tips:Role are HR,ENG,FINANCE,MGR,ACCT the condition evaluates to true.
MATCHES_ANY	For list data types, true if any of the run-time values in the list match one of the configured values. Example: <code>Tips:Role MATCHES_ANY HR,ENG,FINANCE</code>
MATCHES_EXACT	For list data types, true if all of the run-time values of the attribute match all of the configured values. Example: <code>Tips:Role MATCHES_ALL HR,ENG,FINANCE</code> . 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.
MATCHES_REGEX	For string data type, true if the run-time value of the attribute matches the regular expression in the configured value. Example: <code>RADIUS:IETF:NAS-Identifier MATCHES_REGEX sj-device[1-9]-dev*</code>