Configuring and Administering Avaya Orchestrator™

Release 1.5
Issue 5
July 2023

© 2018-2023, Avaya LLC.

All Rights Reserved.

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

“Documentation” means information published in varying mediums which may include product information, operating instructions and performance specifications that are generally made available to users of products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of Documentation unless such modifications, additions, or deletions were performed by or on the express behalf of Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or Documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 under the link “Warranty & Product Lifecycle” or such successor site as designated by Avaya. Please note that if You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

“Hosted Service” means an Avaya hosted service subscription that You acquire from either Avaya or an authorized Avaya Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Avaya or Avaya Channel Partner (as applicable) for more information.

Hosted Service

THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN AVAYA HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO UNDER THE LINK “Avaya Terms of Use for Hosted Services” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF

YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO, UNDER THE LINK “AVAYA SOFTWARE LICENSE TERMS (Avaya Products)” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA LLC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA CHANNEL PARTNER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA LLC. OR THE APPLICABLE AVAYA AFFILIATE (“AVAYA”).

Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License as set forth below in the

Designated System(s) License (DS) section as applicable. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. “Designated Processor” means a single stand-alone computing device. “Server” means a set of Designated Processors that hosts (physically or virtually) a software application to be accessed by multiple users. “Instance” means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine (“VM”) or similar deployment.

License types

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only: 1) on a number of Designated Processors up to the number indicated in the order; or 2) up to the number of Instances of the Software as indicated in the order, Documentation, or as authorized by Avaya in writing. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Heritage Nortel Software

“Heritage Nortel Software” means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software is the software contained within the list of Heritage Nortel Products located at https://support.avaya.com/LicenseInfo under the link “Heritage Nortel Products” or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, and the product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Virtualization

The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Note, unless otherwise stated, that each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third Party Components

“Third Party Components” mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements (“Third Party Components”), which contain terms regarding the rights to use certain portions of the Software (“Third Party Terms”). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya’s website at: https://support.avaya.com/Copyright or such successor site as designated by Avaya. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

The following applies only if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD (“AVC VIDEO”) AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Service Provider

THE FOLLOWING APPLIES TO AVAYA CHANNEL PARTNER’S HOSTING OF AVAYA PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN AVAYA CHANNEL PARTNER’S HOSTING OF AVAYA PRODUCTS MUST BE AUTHORIZED IN WRITING BY AVAYA AND IF THOSE HOSTED PRODUCTS USE OR

EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE AVAYA CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE AVAYA CHANNEL PARTNER'S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE G.729 CODEC, H.264 CODEC, OR H.265 CODEC, THE

AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE WWW.SIPRO.COM/CONTACT.HTML. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (I) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (II) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP:// WWW.MPEGLA.COM.

Compliance with Laws

You acknowledge and agree that it is Your responsibility for complying with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Avaya product is used.

Preventing Toll Fraud

"Toll Fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: https://support.avaya.com or such successor site as designated by Avaya.

Security Vulnerabilities

Information about Avaya's security support policies can be found in the Security Policies and Support section of https://support.avaya.com/security.

Suspected Avaya product security vulnerabilities are handled per the Avaya Product Security Support Flow (https://support.avaya.com/css/P8/documents/100161515).

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: https://support.avaya.com, or such successor site as designated by Avaya.

Contact Avaya Support

See the Avaya Support website: https://support.avaya.com for product or Hosted Service notices and articles, or to report a problem with your Avaya product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: https://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, its licensors, its suppliers, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya LLC.
All non-Avaya trademarks are the property of their respective owners. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries

Chapter 1: Introduction to AvayaOrchestrator™ 9
Overview 9
Avaya Orchestrator™ configuration andconsiderations 10
Software 10
Virtual network 10
Recommended practices 10
Connecting to Avaya Orchestrator™ 11
Chapter 2: Deploying AvayaOrchestrator™ 13
Overview 13
Deploying AO 13
Confirming deployment 22
Chapter 3: Hardware configuration 23
Overview 23
SNMP protocol assignments 23
Configuring SNMP on VSP Devices 25
Configuring SNMP v2c on VSP 7254/7400 network devices 25
Configuring SNMP v3 on VSP 7254/7400 Network Switches 26
Configuring SNMP v2c on G450 Media Gateways 28
Configure SNMP v3 on the G450 Media Gateways 30
Configuring SNMP on HPE servers 31
Configuring SNMP v2c on ESXi 31
Configuring SNMP v3 on ESXi 32
Configuring SNMP on iLO 34
Configuring SNMP v2c on HPE Gen8/Gen9 servers for iLO 4 34
Configuring SNMP v2c on HPE Gen10 servers for iLO 5 36
Configuring SNMP v3 on HPE Gen8/Gen9 servers for iLO 4 37
Configuring SNMP v3 on HPE Gen10 servers for iLO 5 38
Configuring SNMP v2c on Sentry 4 PDUs 40
Configuring SNMP v2c on a Nimble Core 42
Configuring SNMP on an EMC VNXe3200 43
Chapter 4: Solution configuration 47
Overview 47
ACP rack configuration highlights 47
Configuring the ACP solution 47
Create the foundations 48
Editing the name and description of a rack 50
Deleting an ACP solution or rack 50
Administering Rack Elements 51
Editing or deleting an ACP/ASP solution 71
Configuring DNS/FQDN information 72
Based on the FQDN information provided in the LifeCycle Workbook (LCW)[1], administer the IP address and FQDN information for each ASP 4200 device node into a DNS server that supports the production environment. This information will be aligned with Avaya Orchestrator™ trap reporting output for each device. 72
Protocol requirements for hardware components 73
Managing rack devices 74
Rediscovering a Single Device 74
Moving a device within the ACP solution 76
Chapter 5: License Configuration 77
Overview 78
Configuration of server URLs 78
License type 78
Installing AO License 78

Installing AO license in Standalone WebLM 80
Configuring Centralized licensing on WebLM server 80
Installing AO license on SMGR Integrated WebLM 81
Configuring license on Avaya Orchestrator™ 85
Chapter 6: Setting up HTTPS 88
Overview 88
Secure Sockets Layer (SSL) 88
Setting up HTTPS Certificate 89
Creating the Certificate 89
Getting certificate sign request signed by a trusted company 93
Getting Certificate Sign Request (CSR) signed by the SystemManger as the Certificate Authority 94
Adding the SMGR root certificate to a web browser 98
Using ASP 4.1 Management Server Console server asCertificate Authority 100
Signing Certificate Sign Request (CSR) with MSC as theCertificate Authority 115
Activating SSL certificate 118
Validating the certificate 120
Chapter 7: Avaya Orchestrator™Dashboard Deployment 122
Overview 122
Accessing the Avaya Orchestrator™ dashboard 122
Manage Dashboards 122
Add Dashlets 125
The Dashlets 128
Deploying dashboard 131
Chapter 8: Dashboard Overview 133
Avaya Converged Platform (ACP) Dashboard 133
Home Dashboard Dashlets 134
Rack dashboard 137
Device dashboard 142
Services Status Detail 144
Chapter 9: Host and Service Details 151
Overview 151
Service Status overview 151
All Service Problems 152
Service Status 158
Service Status Detail 158
Host Status 161
Host Status Detail 161
Chapter 10: Event handlers and Reports 167
About event handlers 167
Reports 167
Availability Report 168
Executive Summary 170
State History 173
Top Alert Producers 174
Alert Histogram 175
Notifications 176
Event Log 177
Chapter 11: User Administration 180
Overview 180
Users vs. contacts 180
Adding a user 180
User preferences 181
Username 182

Email ... 183
Actions ... 183
Chapter 12: Alarm Notifications ... 186
Overview ... 186
Users vs. Contacts ... 186
Configuring user notifications ... 186
User Notification Administration ... 187
Configuring Notification Escalations ... 190
Administering Contact Groups ... 190
Administering Host Groups ... 193
Administering Service Groups ... 195
Chapter 13: User rights ... 197
User rights ... 197
Managing permissions ... 197
Administrator privileges ... 198
User security settings ... 198
Avaya Orchestrator™ API ... 200
User privileges ... 200
Advanced user with change control ... 200
Basic read-only user ... 201
Chapter 14: User authentication and import ... 202
Authenticate and import users with Active Directory orLDAP ... 202
Using a DNS server ... 202
Configuring authentication servers ... 203
Importing users from Active Directory and LDAP ... 204
Linking existing Avaya Orchestrator™ users to ActiveDirectory users ... 205
Linking existing Avaya Orchestrator™ users to LDAPusers ... 206
LDAP account requirements ... 207
Chapter 15: Email configuration ... 208
Email configuration ... 208
Accessing the email settings ... 208
Web browser behavior ... 208
Configuring the email address from which email messagesare sent ... 208
Methods for sending emails ... 209
Configuring Sendmail / Postfix as the method for sending emailmessages ... 209
Configuring SMTP as the method for sending email messages ... 210
Chapter 16: Maintenance andTroubleshooting ... 212
Overview ... 212
Log files ... 212
System time configuration ... 213
Configuring the system time zone ... 214
Verifying the configuration ... 214
Change passwords ... 214
Default password considerations ... 214
Changing the Linux aoadmin (super user) password ... 215
Configuring downtime ... 215
Configuring recurring downtime ... 216
Scheduling downtime by using mass acknowledgement ... 217
Notification configuration ... 218
Opening the iLO web interface from Rack view or Deviceview ... 218
Access the SSH terminal: Opening a device in the SSHconsole from a Rack view or Device view ... 220
Opening a device in the SSH console from the Host StatusDetail page ... 222
Troubleshooting ... 223

Start with the bird's eye view 223
Drilling down for information 225
Chapter 17: Trap Forwarding 230
Overview 230
Menu Guidelines 230
Administration 232
Trap Receiver 232
Device Selection 232
Enabling Forwarding 232
Chapter 18:Backup and restore 233
Backup configuration 233
Creating a backup by using the web interface 233
Scheduling backups 234
Configuring backup retention 235
Storing backup files 235
Downloading the backup files 236
Troubleshooting backups 237
Avaya Orchestrator™ system restore 237
Restoring a backup file by using the Avaya Orchestrator™ CLI 237
Restoring a backup file by using the Avaya Orchestrator™ webGUI 238
Export and Import ACP Configuration Wizard-Administration 239
Exporting rack configuration 239
Importing rack configuration 240
Chapter 19: Upgrade and update AvayaOrchestrator™ 243
Overview 243
Verifying the installed version of Avaya Orchestrator™ 243
Upgrading Avaya Orchestrator™ 243
Chapter 20: Altering Trap Severity 261
Chapter 21: Events and Alert Messages 264
Chapter 22: Resources 313
Documentation 313
Finding documents on the Avaya Support website 314
Avaya Documentation Portal navigation 314
Training 315
Viewing Avaya Mentor videos 316
Support 316
Using the Avaya InSite Knowledge Base 316

Chapter 1: Introduction to Avaya Orchestrator™

Overview

This document provides administration guidelines for configuring and supporting Avaya Orchestrator™, for Avaya Solutions Platform (ASP) 4200, after initial site installation and deployment.

Avaya Orchestrator™ (AO) is a network management system (NMS) tool that replaces the previous orchestration suite known as Pod Orchestration Suite (POS). Pod Orchestration Suite is end-of-sale with Pod Fx 3.1. The process of migrating from POS to Avaya Orchestrator™ will be supported by Avaya Professional Services, Business Partners, solution integrators, or other professional technical staff representatives. Prior to the migration, existing POS systems can be backed up (Optional) and removed. For more information about backing up all POS data and removing the applications and their supporting infrastructure, see the *Installing and Maintaining the Avaya Solutions Platform 4200* guide at https://support.avaya.com.0

AO allows for the administration and monitoring of up to 300 nodes. A node is defined as a device or object with an IP address assigned. For example, an Avaya G450 media gateway requires one administered node/IP address to be administered in AO for alarm monitoring, and an HPE host server requires two nodes to be administered in AO, one for ESXi IP address and another one for HPE iLO IP address. Information about node assignments for each device is covered later in this document.

Avaya Orchestrator™ (AO) is a visualization and management application used to monitor your ASP 4200 infrastructure.

The following are the functionalities of Avaya Orchestrator™:

- ✓ Works in conjunction with the SAL Gateway to monitor alarms and notifications across all Legacy/New ACP/ASP 4200 infrastructure hardware.
- ✓ Provides a single dashboard view for monitoring state of health of all ACP/ASP 4200 racks, components, and services.
- ✓ Presents robust data access in a simple, uncluttered manner.
- ✓ Allows SMS and email notifications for product hardware alarm escalations.
- ✓ Brings a means of customizing point-specific alarm escalation groups and schedules.
- ✓ Provides consistent proactive monitoring, as well as passive trap reception for all administered hardware components.
- ✓ Configures monitored environments via an intuitive gui wizard support SNMP v1, v2 and v3.
- ✓ Forward supported SNMP traps coming from 4200 racks to an alternate SNMP trap receiver.
- ✓ Supports NFS, FTP, and SFTP file backup.
- ✓ Provides drill-down capability for a rich variety of system reports.

For Avaya Orchestrator™ Release 1.5, Software applications continue to support alarms

through the SAL gateway. Software alarm support will be available in a later release.

Each new release of AO will target improvements and innovations to meet the requirements and needs of Avaya's user communities.

Avaya Orchestrator™ configuration and considerations

The following sections describe the Avaya Orchestrator™ configuration and provide some technical guidelines and considerations for maintaining optimal application performance and behaviors.

Software

Avaya Orchestrator™ is a Red Hat Linux 7.7 (Maipo) virtual appliance intended for use by customers and Avaya support services teams.

Avaya Orchestrator™ has a standardized virtual footprint.

Storage (disk)	**120 GB**
CPU	**16 vCPUs**
RAM	**24 GB**
Network	**1 VNIC**

It is meant to support a one-size-fits-all approach, allowing several simultaneous user requests and monitoring activities, without inhibiting product responsiveness to proactive maintenance investigations and alerting.

Virtual network

In VMware infrastructures, for applications, such as AO, that depend on communication with their server host's iLO port, ensure that you keep the network VLAN of the VM on a different network VLAN than that of the iLO port. The Avaya services deployment teams adheres to this rule during the initial application installation. AO is deployed on the Management VLAN and the iLO IP is deployed on the Application VLAN. It is important for the user community to continue abiding by this rule so that AO continues to perform optimally.

Recommended practices

Historical reports

The Avaya Orchestrator™ reporting engine is a multi-faceted tool that reviews vast amounts of information prior to consolidating the requested information into an historical report. Therefore, Avaya recommends that users consider this fact when requesting data and not consistently click on the report request buttons if more detailed reports are not displayed immediately. Consistent clicks or requests cause the report generation process to restart and can slow the report requests of other users.

If your report request is scheduled, it is recommended you wait a few minutes for AO to process the output. You may now request an email when your report is available to be viewed.

Configuration administration

The ACP Configuration Wizard consumes most AO threads and cycles as each rack is taken through the *Finish* sequence. During this timeframe, an extensive discovery process is underway and blocks all other AO application requests until the process is finished. All alarm monitoring and processing continues in the background and is not impacted, but no UI responses are provided until the *Finish* (discovery) process is concluded. Therefore, Avaya recommends that you perform all Wizard Configuration activities during maintenance windows or low use timeframes.

Connecting to Avaya Orchestrator™

About this task

You can access Avaya Orchestrator™ when the virtual appliance server is deployed and running.
You may use the following browsers Chrome, Firefox, IE or Safari when connecting to Avaya Orchestrator™.

Note:
Chrome and Safari do not come standard with the Management Server Console VM.

Procedure

1. On a web browser, go to: https://*<AO IP Address>/orchestrator.*
2. Type the appropriate credentials to log in.

Note:
All deployed IP addresses and credentials are documented in the *Customer Lifecycle Workbook*.
The following are the default credentials for Avaya Orchestrator™ UI access.

Login: **aoadmin**
Password: **Avaya123$**

Avaya highly recommends changing all solution default passwords immediately after the application/device deployment. When doing so ensure the *Customer Lifecycle Workbook* gets updated accordingly.

Chapter 2: Deploying Avaya Orchestrator™

Overview

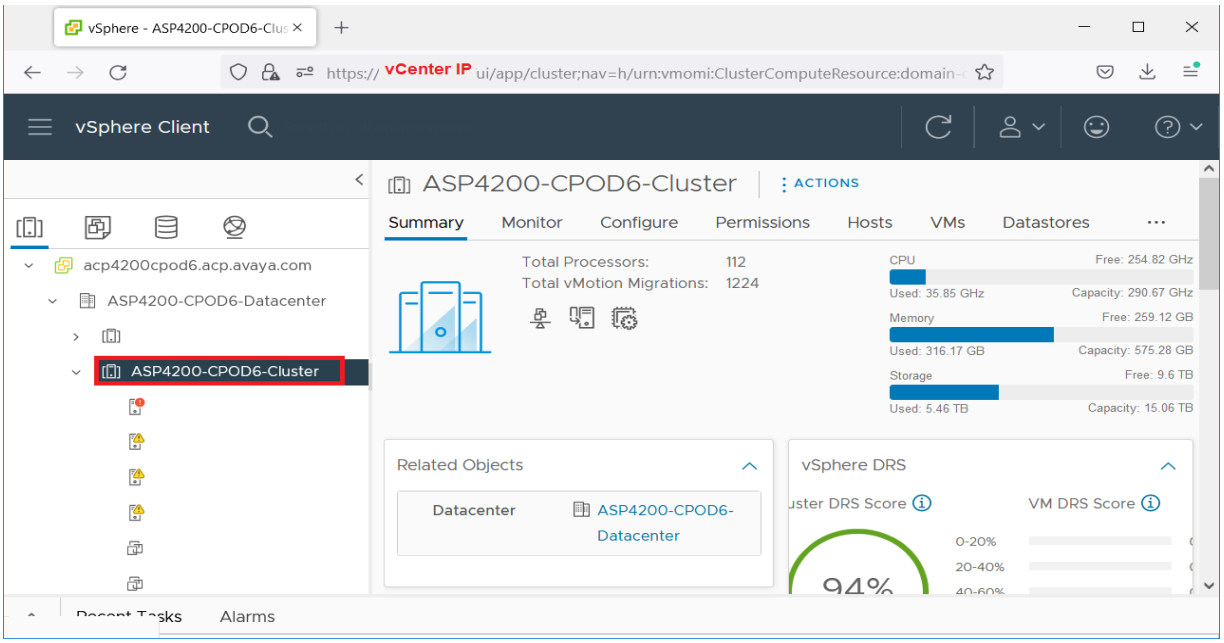
This chapter provides information about how to deploy an Avaya Orchestrator™ OVA.

Deploying AO

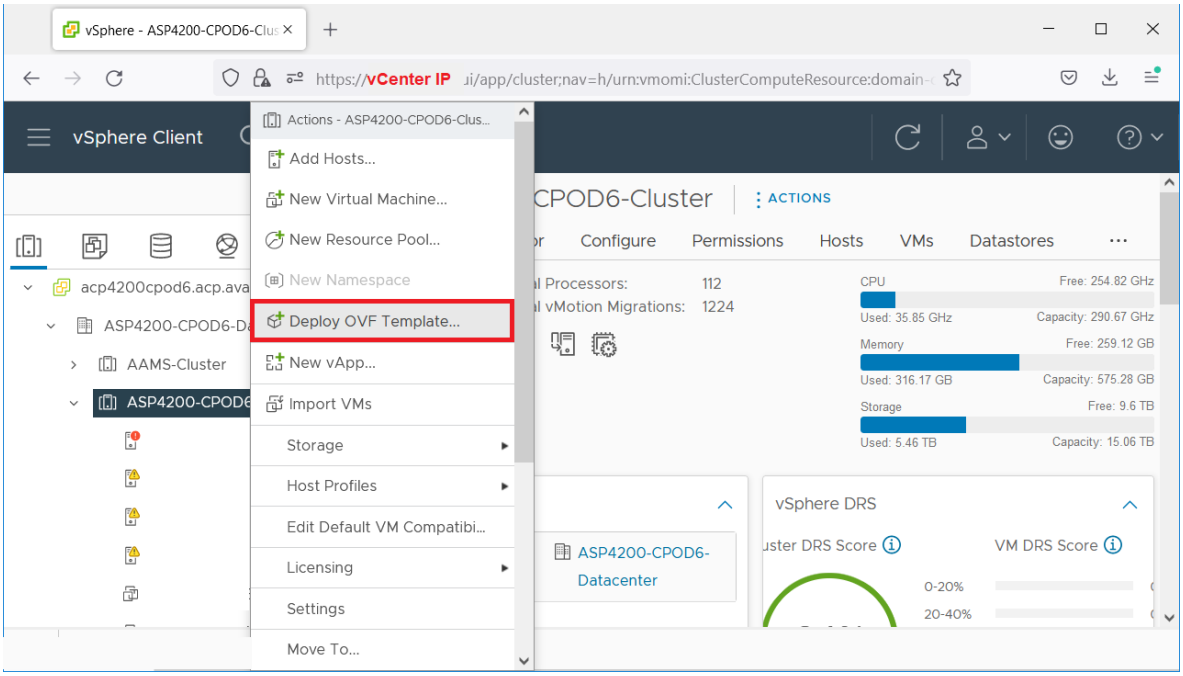
Procedure

1. From Avaya PLDS site, download the OVA (.vmx file) to the Management Server Console (MSC). Relocate the file to the E: drive and into the folder created for storing SW files.

2. AO now can also be deployed from vCenter 7.0. From the vCenter web client, select the **Host and Clusters** tab.



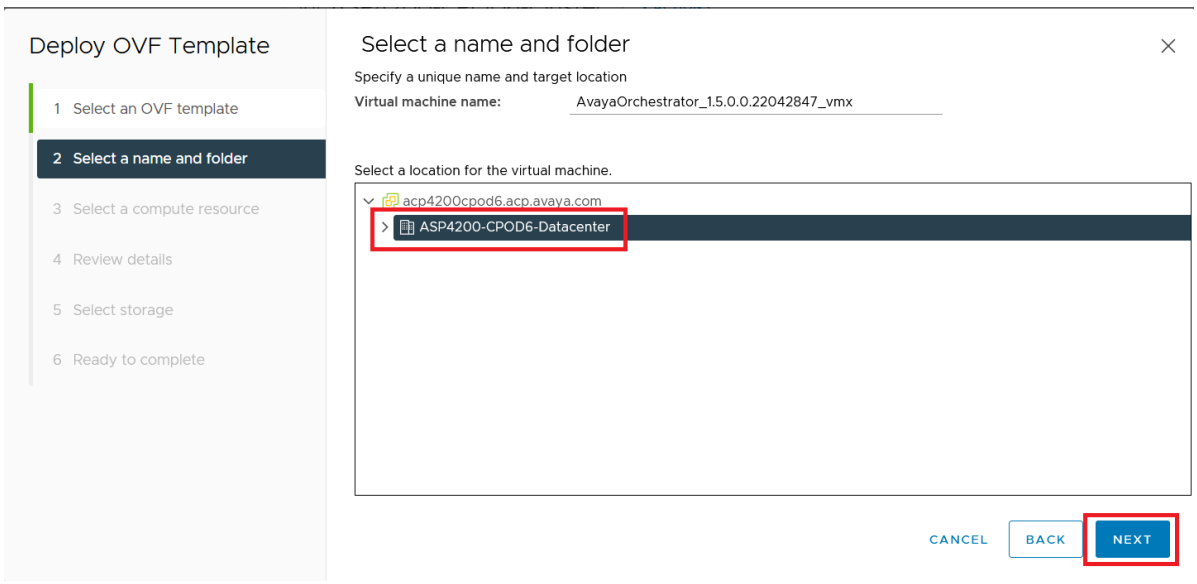
3. Right click the Cluster where the application will be deployed and select **Deploy OVF Template**.



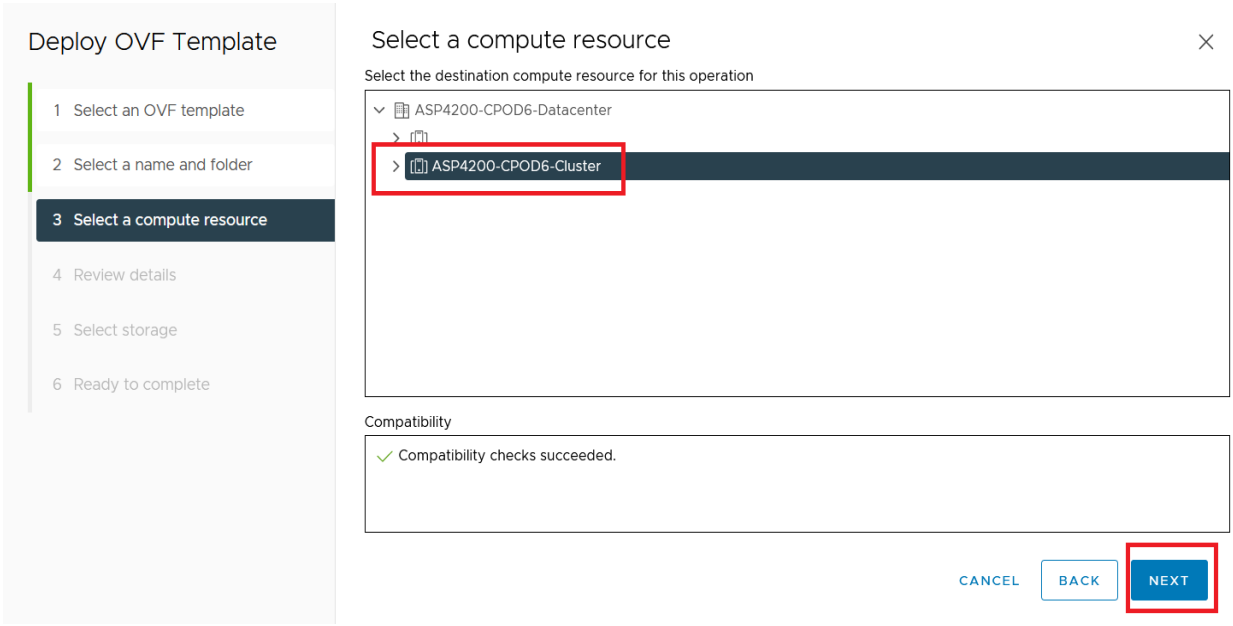
4. Click **Browse** to locate and select the OVA file, then click **Next**:



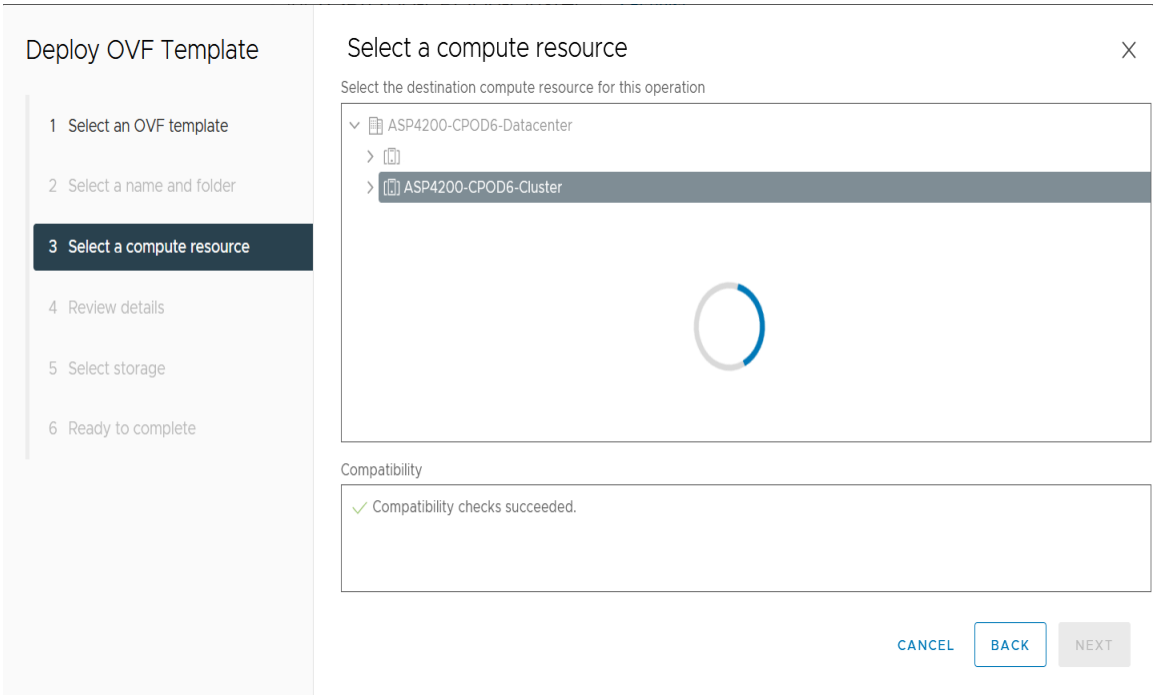
5. Administer the AO name from the IP template, or some easily identifiable name, then select the cluster level deployment location. If specific folders have been allocated for VM groupings, this is an acceptable option. Then click **Next**.



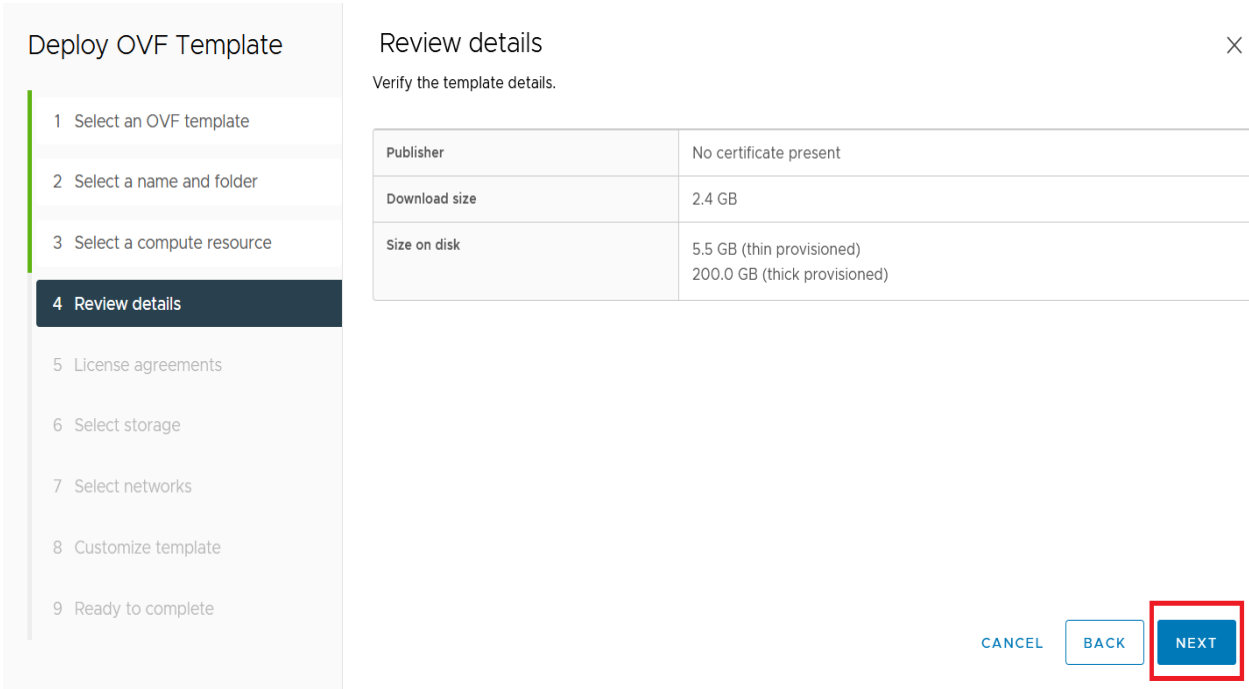
6. Select a specific host resource for a targeted deployment, if preferred, or select the cluster name to allow VMware to select the appropriate host based on load balancing algorithms. When complete, click **Next**:



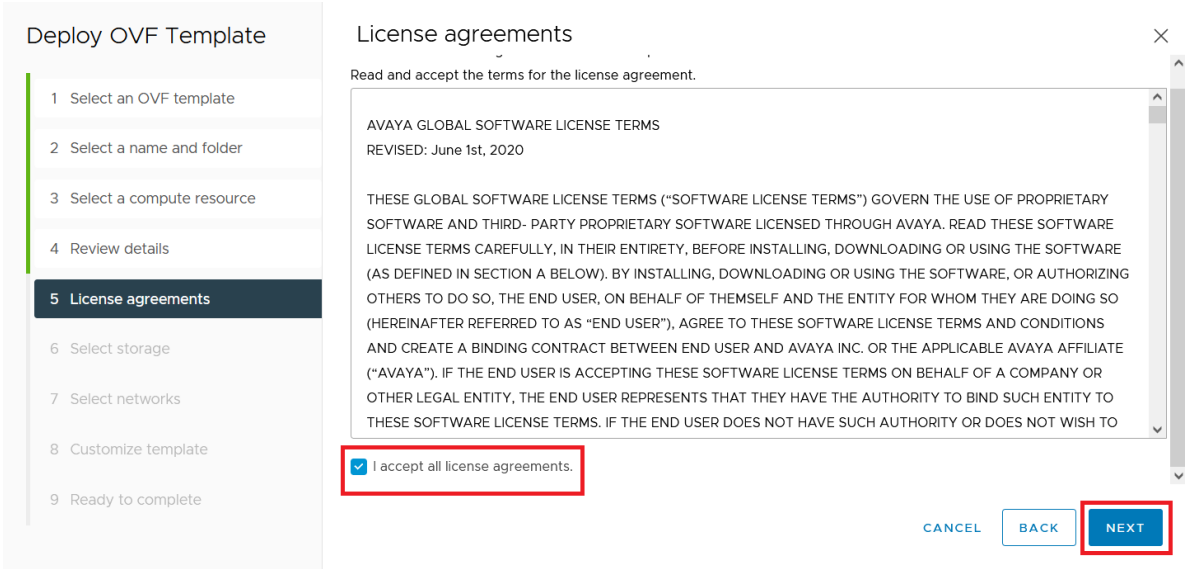
7. VMware will calculate the capacity available in a specific host selection, as well as identify where best to deploy the OVA, if the Cluster level option was previously selected. Wait for the process to complete before clicking other options.



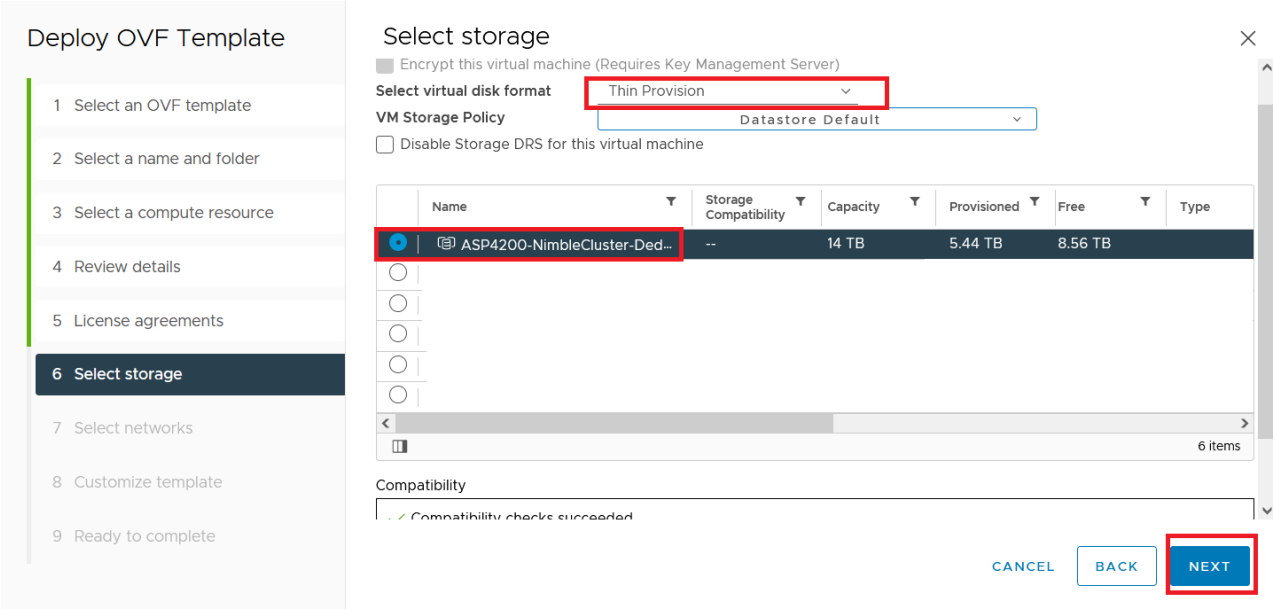
8. Review the OVA details and click **Next**.



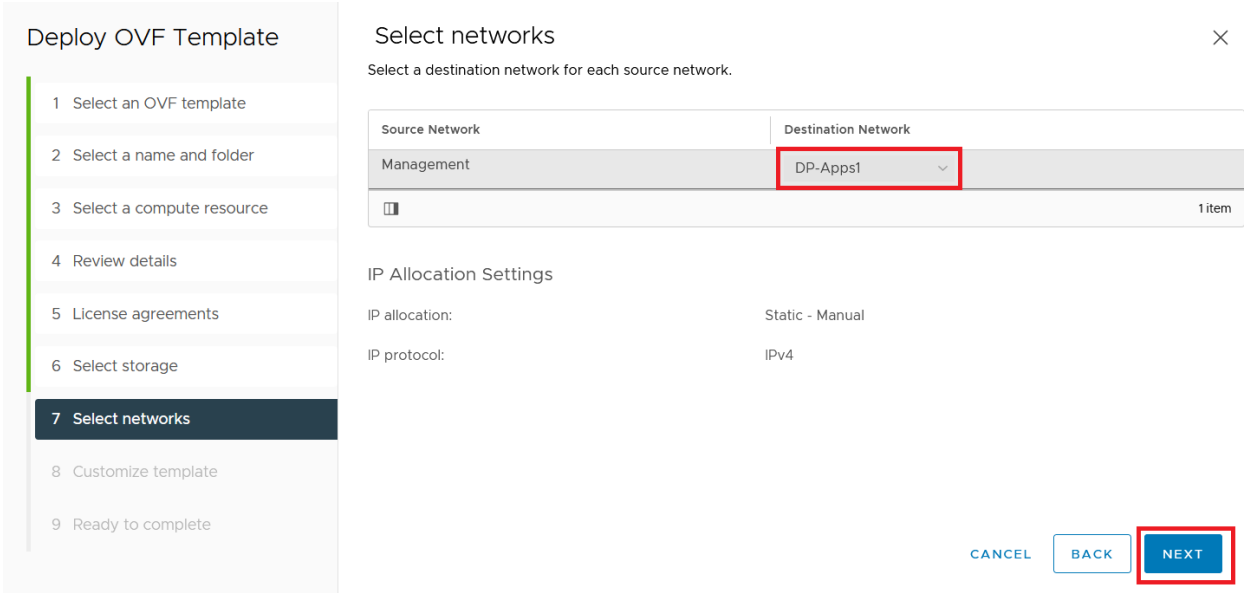
9. This is the Avaya EULA that must be accepted before being allowed to proceed. Click **Accept** and then **Next**.



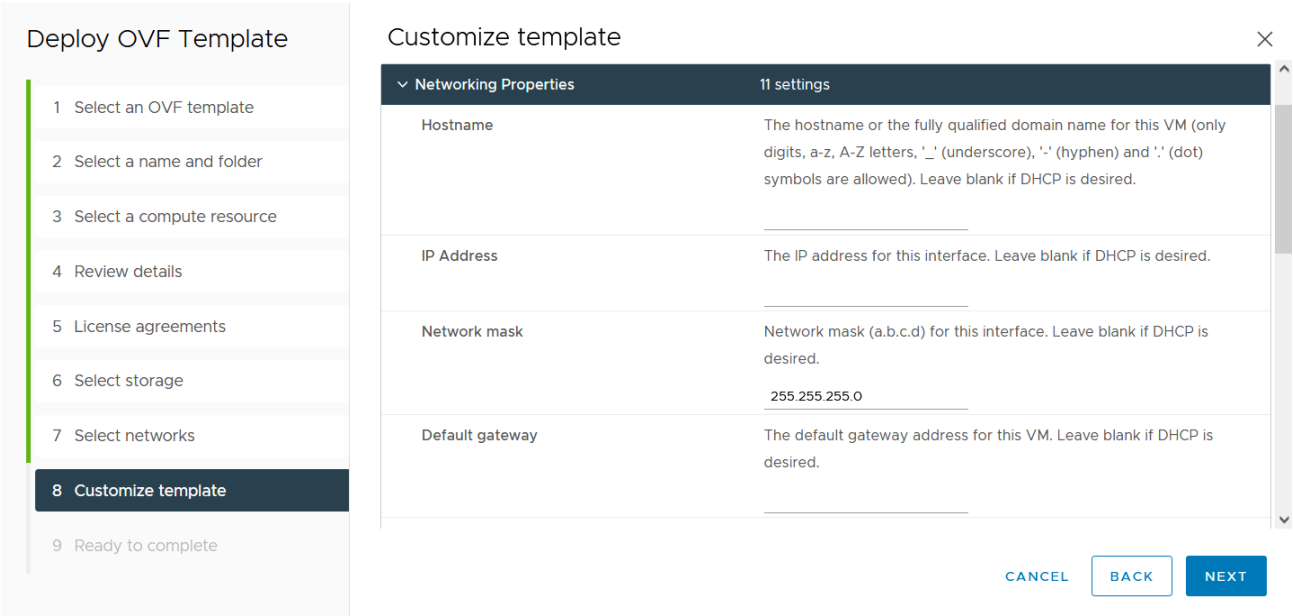
10. Click **Select virtual disk format** drop down list and select **Thin provision**, select the desired Nimble or EMC datastore, then click **Next**.

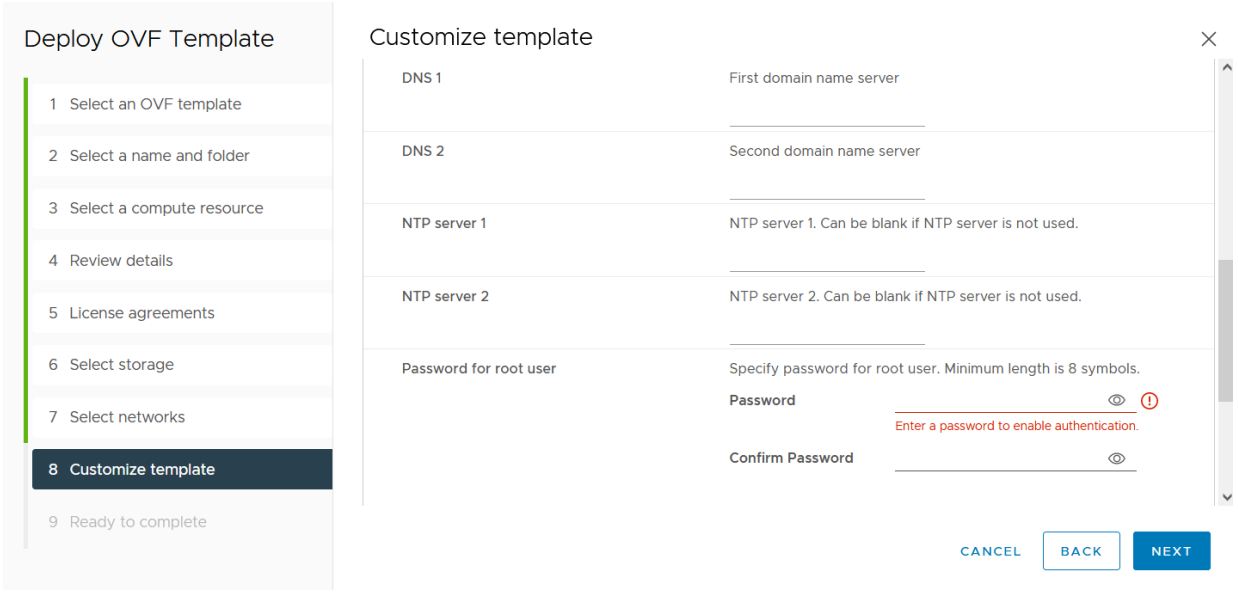


11. Click the **Standard Network** drop down list to select the **Management** network assignment and then click **Next**.



12. Now administer the AO VM network elements. In AO 1.5, customers are encouraged to create their own aodmin and root credential passwords. You can use entrie in the IP Template. If none are present, enter a password of Avaya123$ for both *aoadmin* and *root* logins, and confirm the customer knows the default credentials are administered. When finished, click **Next**.



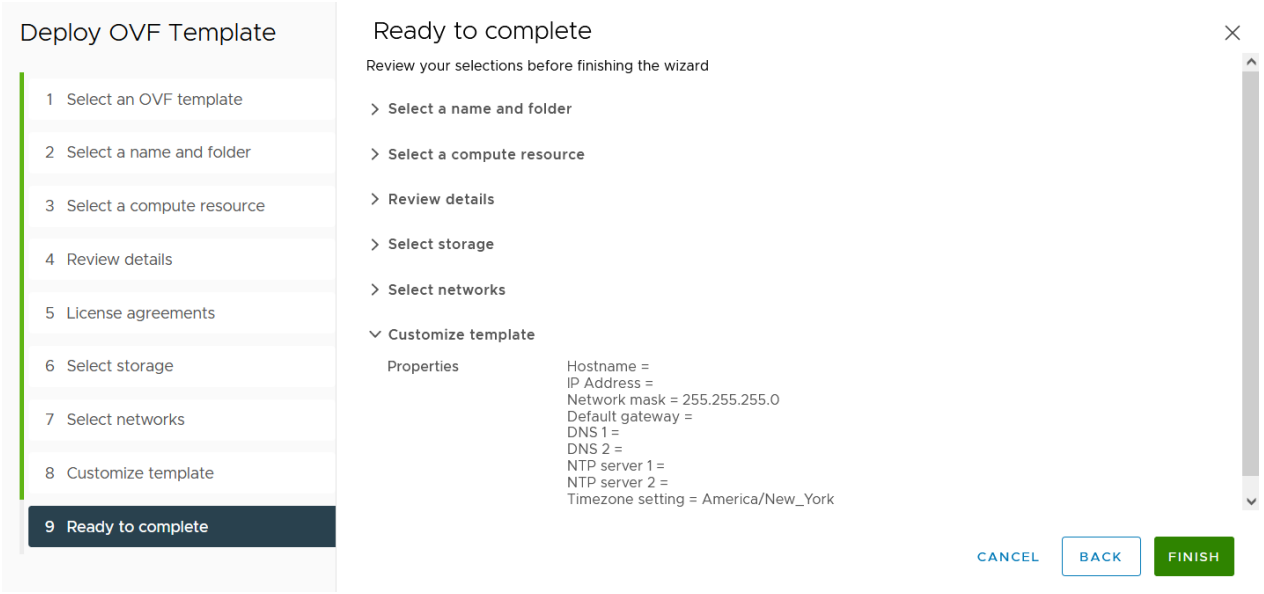


Note: <u>After VM deployment</u>, change the passwords using the following process.

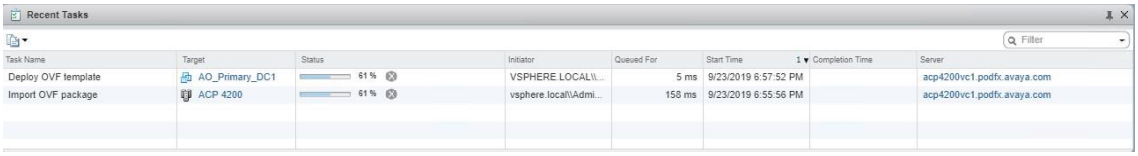
- Login to the AO CLI using credentials *root* and *Avaya123$.*
- Type
  # passwd aoadmin
- At the next prompt, **New password:** type the new preferred password for aoadmin.
- You will be prompted to confirm it: **Retype new password**.
- The password will then be changed.
- Repeat the same steps to change the root password.

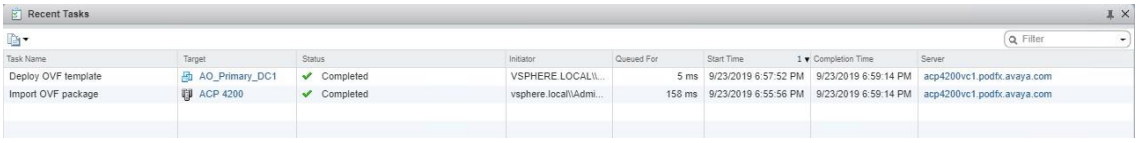
```
[root@aoprimdcl ~]# passwd aoadmin
Changing password for user aoadmin.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
[root@aoprimdcl ~]#
```

13. Review and confirm the administration. To fix incorrect entries, click **Back**. When confirmed to be accurate, click **Finish**.

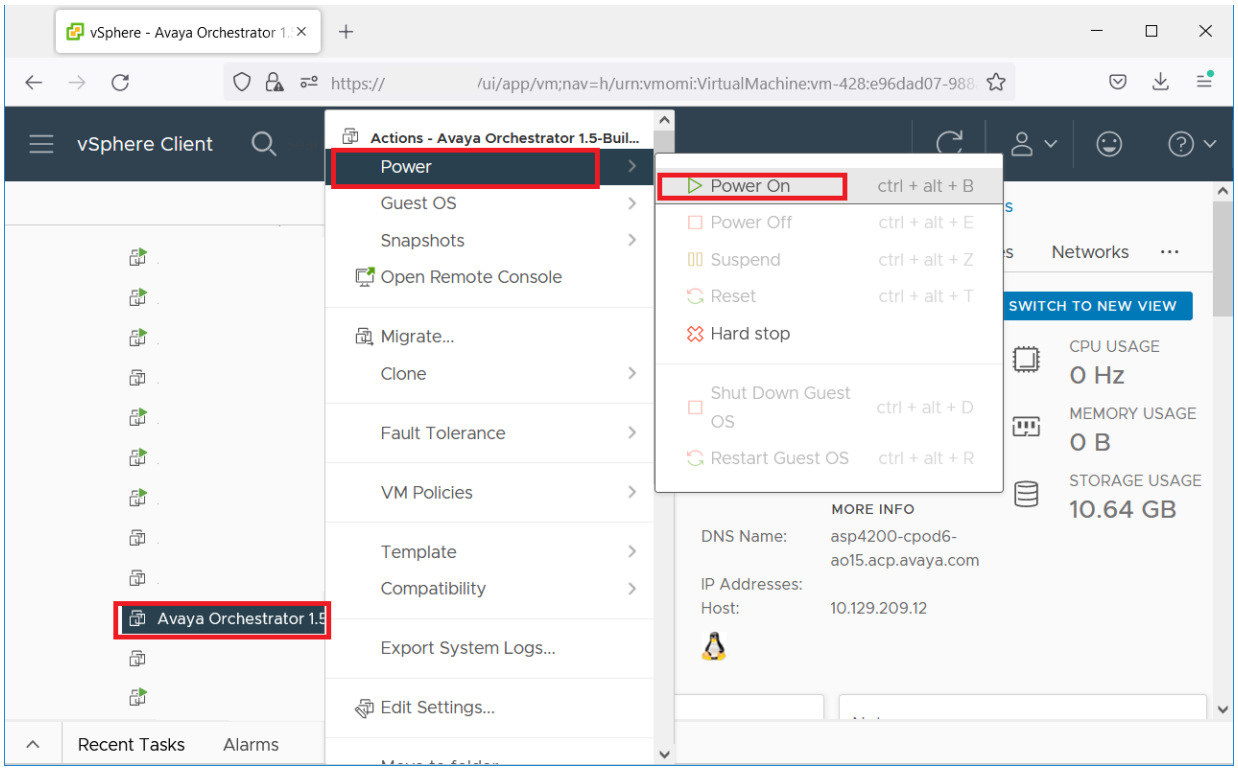


14. The OVA import could take several minutes to upload the OVA files and complete the deployment. If the OVA is imported across a WAN connection, the process could take much longer than a local network deployment, depending on network bandwidth and reliability.

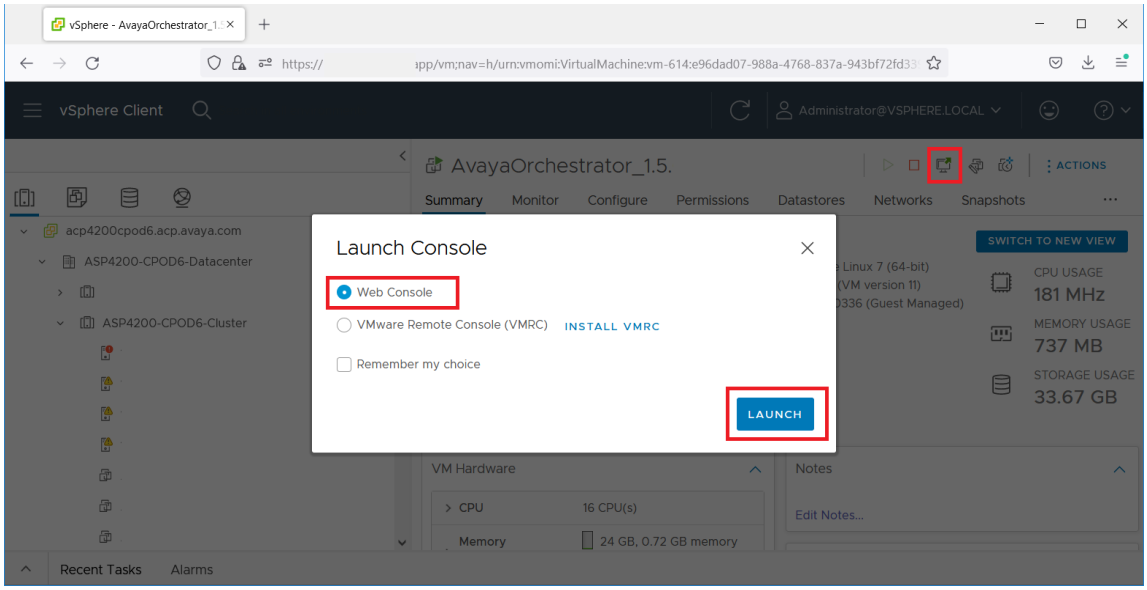




15. Once the OVA deployment is successfully completed, you may power up the VM. Find and highlight the new VM within the selected cluster, then click the green **Power-On** arrow in the tool bar to the right.

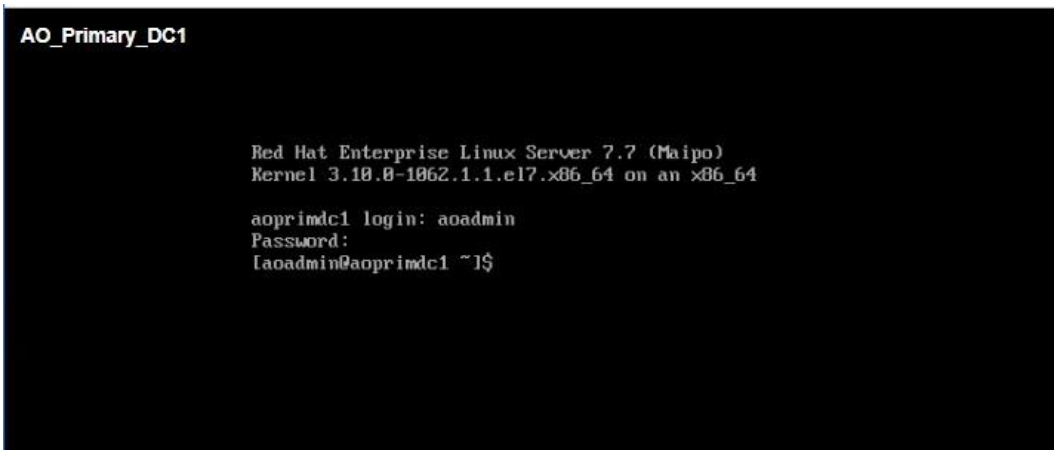


16. Once the VM has powered up, open the VM console by selecting the monitor icon on the tool bar to the right.

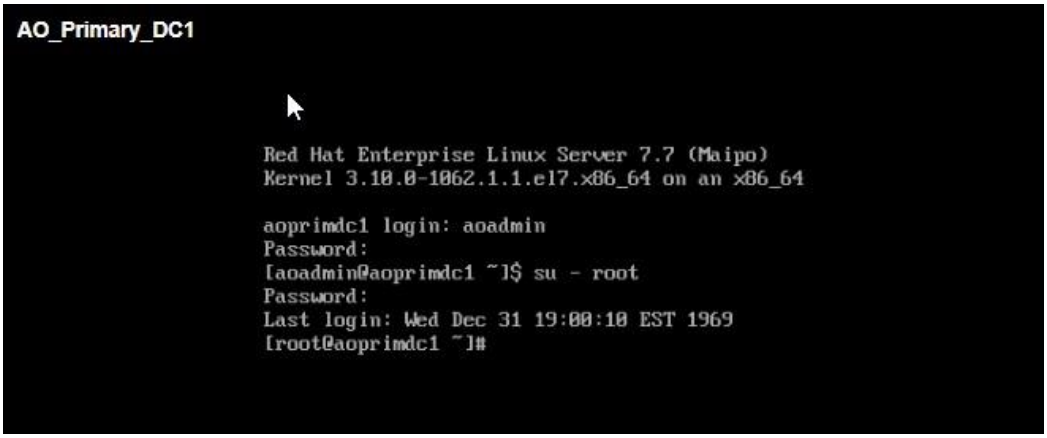


Confirming deployment

1. Log in as user *aoadmin*. There is no longer a default password. You will use the password administered previously during OVA deployment. This will confirm the aoadmin credential is functional.



2. From the Linux prompt, type *su – root.* Enter the password types during the OVA deployment. This will confirm the functionality of the root password.



If either the aoadmin or root password credentials fail, the OVA will need to be redeployed.

Chapter 3: Hardware configuration

This chapter contains information about how to administer each hardware device with the appropriate SNMP, REST API, and CLI API settings.

Overview

Prior to administering new devices in the ACP Configuration Wizard, each hardware device must be administered for SNMP. When the SNMP administration is finished, the device detection activity in Avaya Orchestrator™ succeeds during the subsequent rack administration of the deployment process. This section explains how to configure each hardware element with the appropriate level of SNMP.

Where supported by the device, SNMPv3 is administered in new deployments and upgrades as the default SNMP variety in the ASP 4200 4.1 solution. For users who may still wish to continue using SNMPv2, the administration for that variable is also documented.

SNMP protocol assignments

For more information about SNMP assignment for all hardware components supported in an ASP 4200 solutions, see

Configuring DNS/FQDN information.

For all AO releases:
Without the administration of FQDN host information, by default, all reports display only the source IP address for each trap that is received or proactively collected. Therefore, to produce an easily distinguishable reference name for each trap/alarm, you must configure an FQDN or host name and DNS authentication for each element that is monitored.

> Important:
> *For AO 1.5*:
> For certificates and licensing to work correctly, FQDN resolution via DNS is required.

If you want device names to appear, instead of IP address information, in all AO reporting output, you must create all DNS or /etc/hosts file entries before administering devices in the ACP Configuration Wizard.

If devices have already been administered into the Configuration Wizard, the subsequent administration of FQDN information in a DNS server or /etc/hosts file in AO will not provide the required device naming presentation. To display the FQDN information instead of the IP addresses, remove the devices from the Wizard and re-administer them, so that next time AO populates all related device tags, that is, an FQDN instead of an IP address.

Procedure

Option 1: Administer the FQDN information in a DNS server.

Based on the FQDN information provided in the Life Cycle Workbook (LCW), administer the IP address and FQDN information for each ACP/ASP 4200 device node into a DNS server that supports the production environment. This information will be aligned with Avaya Orchestrator™ trap reporting output for each device.

Option 2: Build an FQDN or host table inside Avaya Orchestrator™.

Warning

This option is only for AO configurations that will not be using certificates.

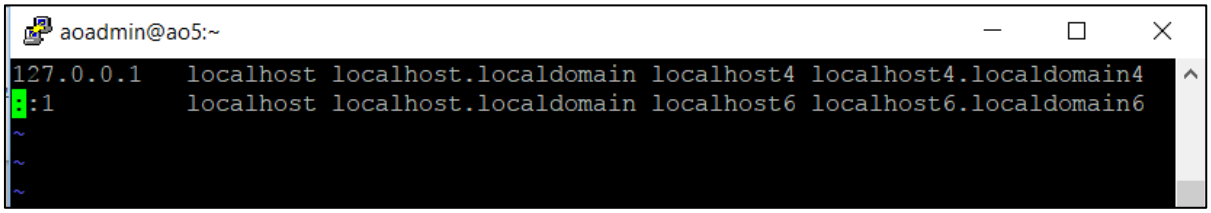
If a DNS server is not available for the environment, you can administer a table within the Avaya Orchestrator™ application to provide the same FQDN naming outcome. You can get the FQDN naming information for each node from the Life Cycle Workbook. Do the following:

1. SSH into Avaya Orchestrator™ by using the *aoadmin* login credentials from the Customer IP Template Workbook.

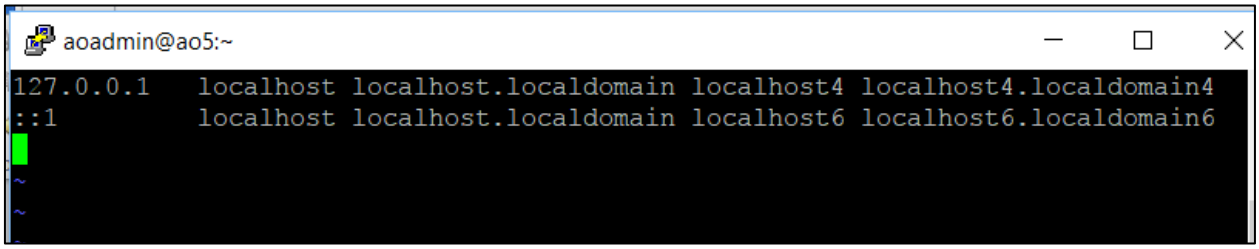
2. At the Linux prompt, type: *sudo vi /etc/hosts*

The hosts file is opened for editing.

3. Use the arrow keys on your keyboard to move the cursor down to the bottom row of entries. Press the **Esc** key and then *o*.



The cursor repositions on a new line for you to insert the entries.



4. Use the following Linux vi procedure to update the hosts table:
    a. Type the IP address for the first device, and then press the **Tab** key.
    b. Type the host name and press the **Tab** key.

- **Note**: This host name is presented with each trap from the device.

c. Type the associated FQDN/host entry. For example: *net1dc1.avaya.com*.

d. Press **Return** and type the information of the next host.

e. After you type the final IP address, press **Esc** to stop the vi editing process.

f. To write and save the file information, type :*wq!*

g. To close the window, type **Exit**.

Configuring SNMP on VSP Devices

Configuring SNMP v2c on VSP 7254/7400 network devices

Procedure

1. SSH into VSP 7254/7400 device.

2. At the command prompt, run the following commands in succession:
   enable
   configure terminal

3. Run the following commands to configure VSP:

   no snmp-server community public
   no snmp-server community private
   snmp-server community <community string> group readgrp index < WORD<1-32> secname readview

4. If SAL Gateway is also being deployed in the solution, run the following command to configure SAL Gateway:

   snmp-server host < AO IP or NMS Tool IP > v2c readview

5. Run the following commands to save the changes and exit the configuration:
   exit
   save config

6. At the command prompt, run the following command to verify SNMP administration.
   show running-config

   Press the space bar to scroll through the configuration to find the SNMP settings and values.

Configuring SNMP v3 on VSP 7254/7400 Network Switches

Procedure

1. SSH into VSP 7254/7400 device.

2. At the command prompt, run the following commands in succession:
   enable
   configure terminal

3. Add the SNMP v3 username, authentication and privacy admin and access to read or write data. The information inside the brackets represents the default credentials values to be deployed.
   no snmp-server community public
   no snmp-server community private
   snmp-server user <avaya> group <initial> md5 < avaya123> aes <avaya123>

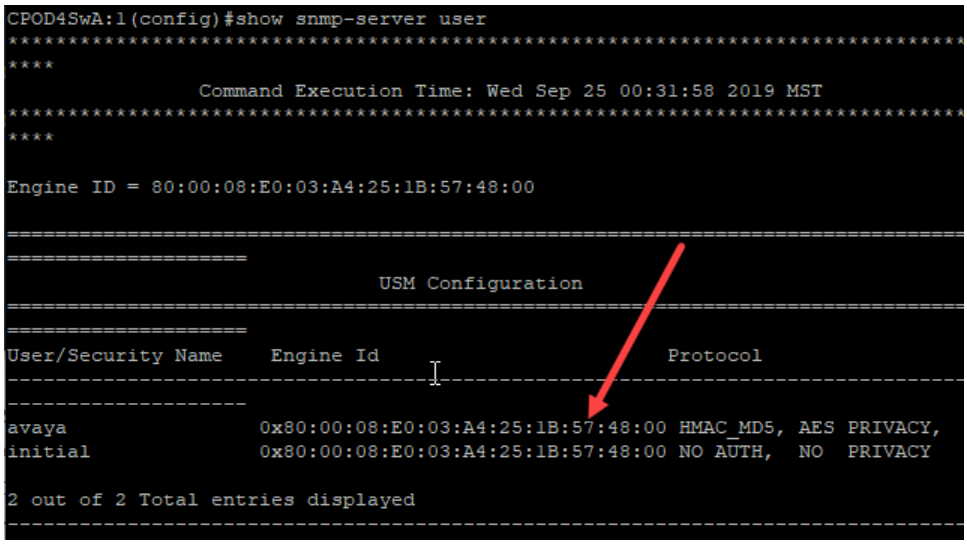
4. Enter the trap receiver information.
   snmp-server host <AO IP or NMS Tool IP> v3 authPriv <avaya>

5. Run the following commands to save the changes and exit the configuration.
   exit
   save config

6. At the command prompt, run the following command to verify SNMP administration.
   show running config

7. Collect the Engine ID information that will be used to administer the AO SNMPv3 handshakewith the device.
   show snmp-server user

   In the screen capture below, collect the numerical sequence after the 0x and remove the : (colon) in between each group of digits, such that you would have 800008E003A4251B574800 as the Engine ID to enter into AO. For more information, see Chapter 4: Solution configuration.



Optional Configuration Settings

Information provides insights for administrators and services personnel. The following settings are optional for the VSP network devices. The do not come as part of the standard configuration, but may be configured per desire/need.

- Login-success traps
  By default, the VSP devices will notify trap receivers, like AO, if there is a failed login attempt to any device. Some users may wish to also know about successful login attempts, to have any network access captured in an SNMP log.
  snmp-sever login-success-trap enable
- Location
  Create a specific location to be displayed in AO for the device(s). There are 255 characters allowed and they must be contiguous, i.e., joined together by an underscore character (_).
  snmp-server location <enter location>

- Contact
  Add in contact information that may help with identifying a group responsible for the device to help during escalation issue work. Like the location, 255 contiguous characters are available for entry.
  snmp-server contact <enter contact info>

Here's an example, from the cabinet drill down, into the VSP drill down page, where this information can be easily referenced.

Device information

Entity name	Entity value
Device host name/FQDN	cpod4vsp7254sw2.cpod.com
Device IP	10.129.94.61
Serial No	15JP402CF00L
entPhysicalModelName	7254XSQ
sysDescr	VSP-7254XSQ (8.0.6.0)
sysObjectID	iso.3.6.1.4.1.2272.209
sysName	CPOD4SwB
sysUpTime	73 days 2h:41m:31s
sysContact	Engineering
sysLocation	12121GrantStreet
sysServices	6

Device information

Entity name	Entity value
Device IP	[redacted]
Serial No	2217Q-40322
entPhysicalModelName	7400-48Y-8C
sysDescr	VSP-7400-48Y-8C (8.9.0.0)
sysObjectID	iso.3.6.1.4.1.1916.2.325
sysName	asp-vsp74K1
sysUpTime	154 days 17h:32m:37s
sysContact	Ricardo Arriagada
sysLocation	3rd Floor Lab, Thornton, CO
sysServices	6

Configuring SNMP v2c on G450 Media Gateways

Procedure

1. SSH into the G450 media gateway by using root credentials.

2. At the command prompt, run the following commands in succession:
   set port trap enable
   snmp-server enable notifications
   snmp-server host <AO_IP_Address> traps v2c avaya123

3. If SAL Gateway is also being deployed, run the following command:
   snmp-server host <AO_IP_Address>,<SAL_GW_IP> traps v2c avaya123

4. Run the following commands to write and save changes and add the configuration to the boot parameters:
   copy running-config startup-config
   reset
5. At the command prompt, type the following command to verify SNMP administration:
   show snmp

Configure SNMP v3 on the G450 Media Gateways.

- Note: SNMP configuration settings have been added to the Gateway template config for ASP 4.1 at the factory. Following procedure should be use a reference or in case snmpv3 requires to be configured on existing environment.

Configuration reference:

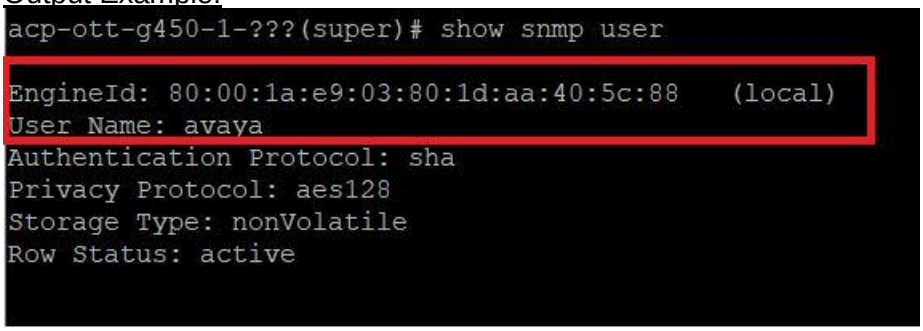
1. Using SSH, access the G450 host IP address.
2. Login using the root credentials.
3. Configure the SNMPv3 user+ privacy and authentication credentials and view by executing the following command:

   snmp-server user avaya v3AdminViewG v3 auth SHA avaya123 priv aes128 avaya123

4. Collect the Engine ID information to be used during AO administration of each G450 device (supporting SNMP v3).

   show snmp user

   Output Example:



5. Configure the Engine ID to be associated with the user (avaya) previously created.

   snmp-server remote-user avaya <EngineID> (hexadecimal numbers separated by colons (5-32 numbers) **v3AdminViewG auth SHA avaya123 priv aes128 avaya123**

   Example:

   snmp-server remote-user avaya 80:00:1a:e9:03:80:1d:aa:40:5c:88 v3AdminViewG auth SHA avaya123 priv aes128 avaya123

6. Configure the trap receivers' IP addresses to receive traps from the G450.

   snmp-server host <AO_IP> traps v3 priv avaya all
   snmp-server host <SAL_GW_IP> traps v3 priv avaya all

7. Set the alarm informs function.

snmp-server host <AO_IP> informs v3 priv avaya all

8. Enable SNMP on the G450.

   set snmp trap enable

9. Enable traps from the primary NIC interface.

   set port trap 10/5 enable

10. Enable traps from the secondary NIC interface.

    set port trap 10/6 enable

11. Save your changes.

    copy running-config startup-config

Configuring SNMP on HPE servers

Note: Servers require two elements to be administered: ESXi and iLO.

Configuring SNMP v2c on ESXi

Procedure

1. Using SSH, access the ESXi host IP address.

2. Run the following command to enable SNMP on the ESXi host:
   esxcli system snmp set --enable true

3. Run the following command to set the community string to be exchanged between the ESXi host and the trap receivers:
   esxcli system snmp set --communities <community string>

4. Run the following command to configure the trap receiver target for the ESXi SNMP output:
   ***esxcli system snmp set -t <target IP* Address>@162/CommunityString, SAL_GW_IP@162/CommunityString**

   Port 162 is the standard and default SNMP port for receiving, but any port number can be assigned.

Up to three trap destinations can be administered and must be separated by commas with no subsequent space.

5. Run the following command to enable the traps to be send to the target receivers:
   esxcli system snmp set -e yes

6. Run the following command to review and confirm the SNMP settings:
   esxcli system snmp get

7. Run the following command to send a test trap and confirm that the administered destination receives notifications:
   esxcli system snmp test

Configuring SNMP v3 on ESXi

Procedure

1. Using SSH, access the ESXi host IP address.

2. Run the following command to enable SNMP on the ESXi host:
   esxcli system snmp set --enable true

3. Set the *authorization* and *privacy* types in ESXi.

   esxcli system snmp set -a SHA1 -x AES128

4. To help create a unique Engine ID, which is preferable to using the locally generated option, find a Mac address used on the ESXi host. Any Mac address from the list presented will serve the purpose.

   vim-cmd hostsvc/net/info | grep “mac =”

5. If there are several MAC addresses present, select one. Using the Mac Address info, set the engine ID. The digits after the --engineid option below are part of an example Mac Address. The colons present in the MAC address format have obviously been removed for the engineid entry.

   esxcli system snmp se --engineid 98f2b324c0a1

Note: Ensure you make a note of the engine ID. You need to administer this ID in Avaya Orchestrator™.

6. Generate hash values for the privacy and authentication settings based on the SNMP engine ID.

esxcli system snmp hash -r -A avaya123 -X avaya123

The following output will be presented.

```
[root@acp4200G9-lesxi:~] esxcli system snmp hash -r -A avaya123 -X avaya123
   Authhash: c25a9983f6e4e6ec0988186047f7f615
   Privhash: c25a9983f6e4e6ec0988186047f7f615
[root@acp4200G9-lesxi:~]
```

7. Using the hash output values, as seen in the screen capture above, create a user that will query the SNMP service. The following command will be typed as a 1 line (continuous) command.

   esxcli system snmp set –u avaya/c25a9983f6e4e6ec0988186047f7f615/ c25a9983f6e4e6ec0988186047f7f615/priv

   Note: The user name (avaya) will be administered in Avaya Orchestrator™. Ensure you make note of it.

8. Set the AO and SAL GW targets to receive traps.

   esxcli system snmp set --v3targets <AO IP Address>@162/avaya/priv/trap,<SAL GW IP Address>@162/avaya/priv/trap

9. Enable the SNMP service.

   esxcli system snmp set -e yes

10. Review the configuration you just administered for SNMP v3.

    esxci system snmp get

```
[root@asp4200-g9-svr3:~] esxcli system snmp get
   Authentication: SHA1
   Communities: avaya123
   Enable: true
   Engineid: e0071bf03c30
   Hwsrc: indications
   Largestorage: true
   Loglevel: warning
   Notraps:
   Port: 161
   Privacy: AES128
   Remoteusers:
   Syscontact:
   Syslocation:
   Targets:
   Users: avaya/8b29040ea9c56a303ef017b96761ab3ab78c209f/8b29040ea9c56a303ef017b
96761ab3ab78c209f/priv
   V3targets: 10.129.208.32@162 avaya priv trap
```

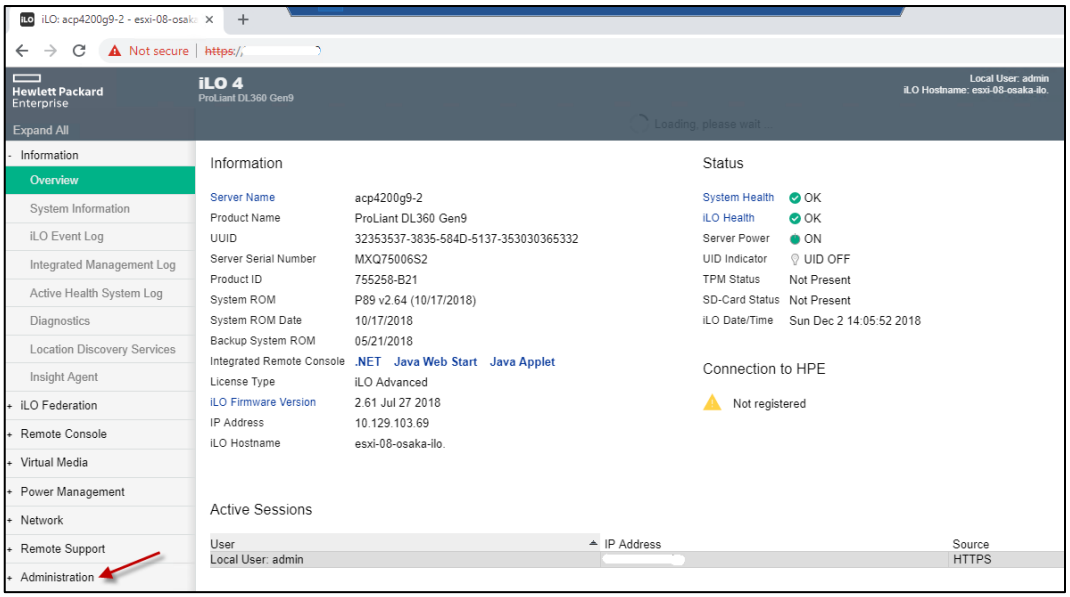
Configuring SNMP on iLO

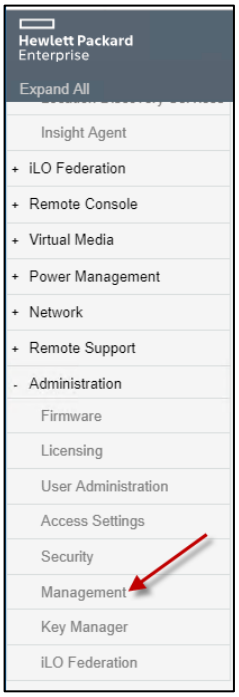
Configuring SNMP v2c on HPE Gen8/Gen9 servers for iLO 4

Procedure

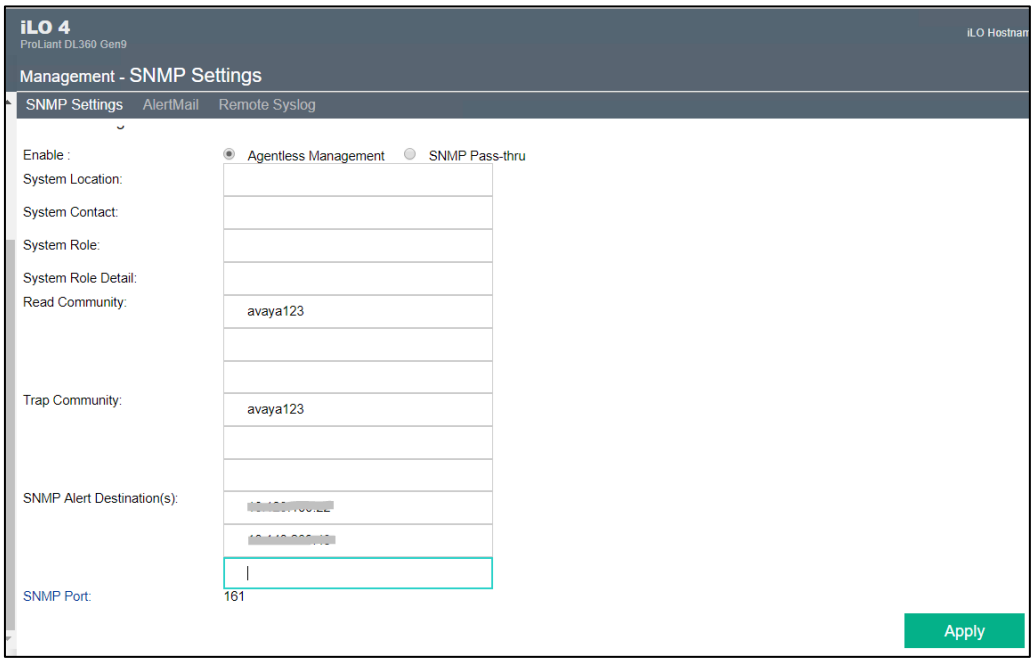
1. On the web UI, type the IP address of the iLO.

2. In the left navigation pane, click **Administration** > **Management**.





3. In the SNMP Settings area, do the following:
   a. Click **Agentless Management.**
   b. In the **Read Community** and **Trap community** fields, type the community string *avaya123.*
   c. In the **SNMP Alert Destination(s)** field, type the IP addresses of Avaya Orchestrator™ and SAL Gateway.
   d. Click **Apply**.



Configuring SNMP v2c on HPE Gen10 servers for iLO 5

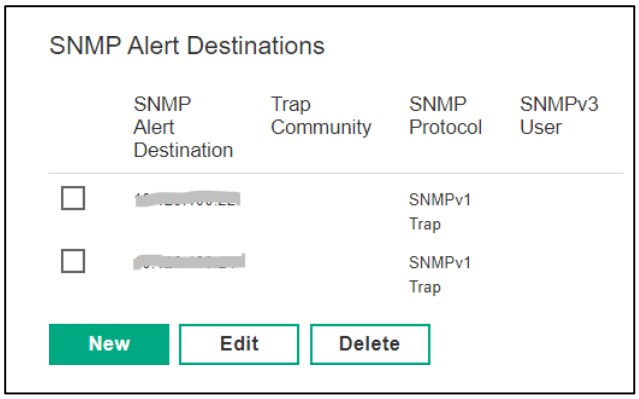
Procedure

1. On the web UI, type the IP address of the iLO from the LCW.
2. In the left navigation pane, click **Management**.

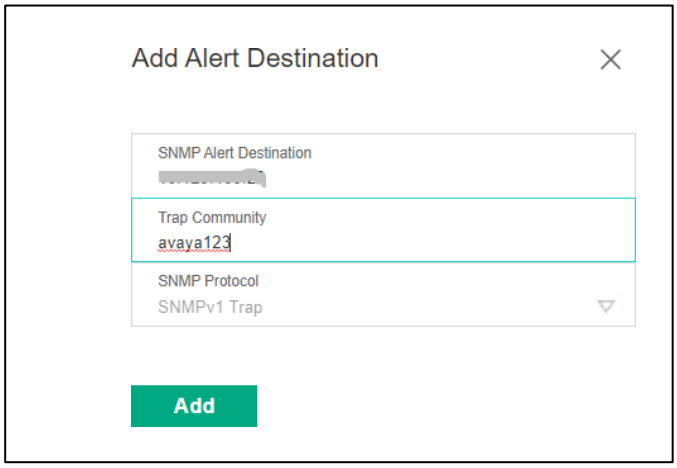


3. On the top portion of the administrative screen, in **Read Community**, type *avaya123,* and then click **Apply**.

4. At the bottom portion of the administrative screen, in the **SNMP Alert Destinations** area, click **New** to add a new SNMP trap receiver.



5. In the **SNMP Alert Destination** field, type the IP address of AO.
6. In the **Trap Community** field, type *avaya123*.
7. Click **Add**.
8. Repeat the new entry process and include the SAL Gateway IP address as a trap receiver.



Configuring SNMP v3 on HPE Gen8/Gen9 servers for iLO 4

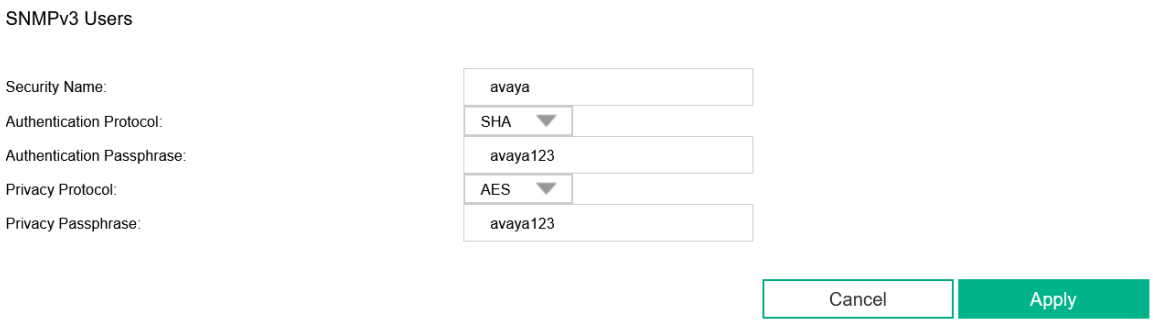
Procedure

1. From the left side menu, select **Administration - Management**.

2. Under SNMP settings, select a radio button for SNMPv3 Users and click **Edit**.



3. Under the SNMPv3 user details:
   - create a user name of avaya
   - select SHA authentication protocol with a password of *avaya123*
   - select AES privacy protocol with a password of *avaya123*
   - *Click **Apply** to save changes.*



4. To set the SNMPv3 engine ID, from the left side menu, select **Network -> Shared Network Port**.

5. Copy the MAC address from the summary page.

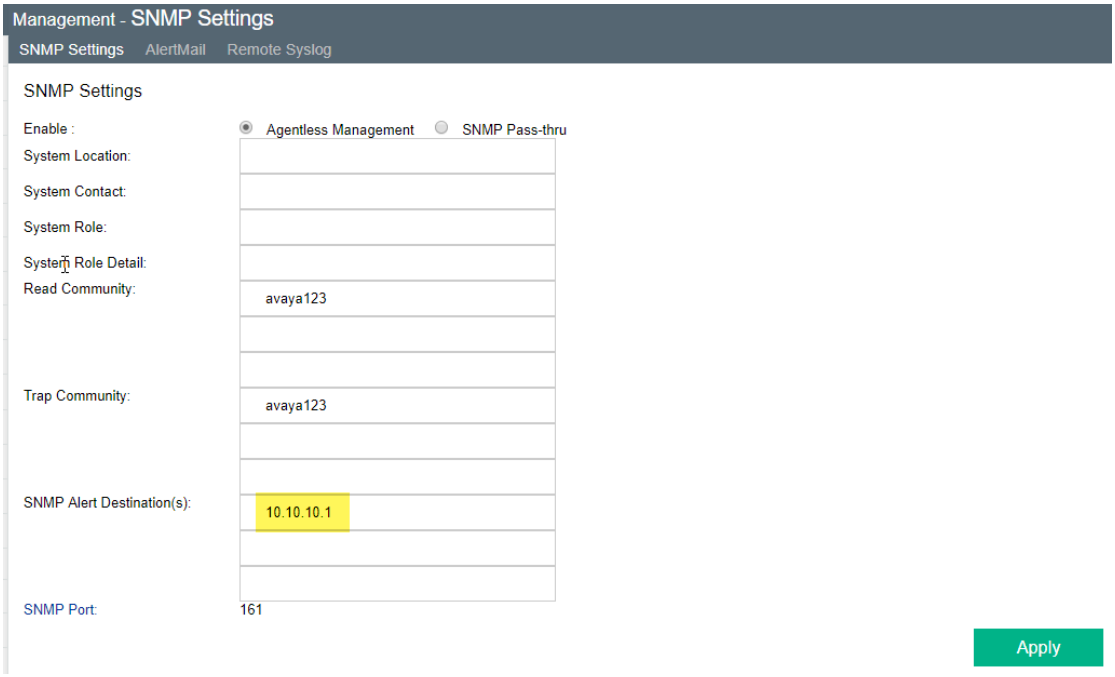
6. From the left side menu, select **Administration -> Management** -> **SNMP Settings.**

7. In the text box next to **SNMPv3 engine ID**, type in 0x followed by the MAC address of the shared network port.

8. Click **Apply** to save changes.

9. Under **SNMP Settings**, enter the Alert Destination of AO and the Sal GW.

10. Click **Apply** to save changes.



Configuring SNMP v3 on HPE Gen10 servers for iLO 5

Procedure

1. Log into the G10 server iLO using its iLO IP address and iLO login credentials.

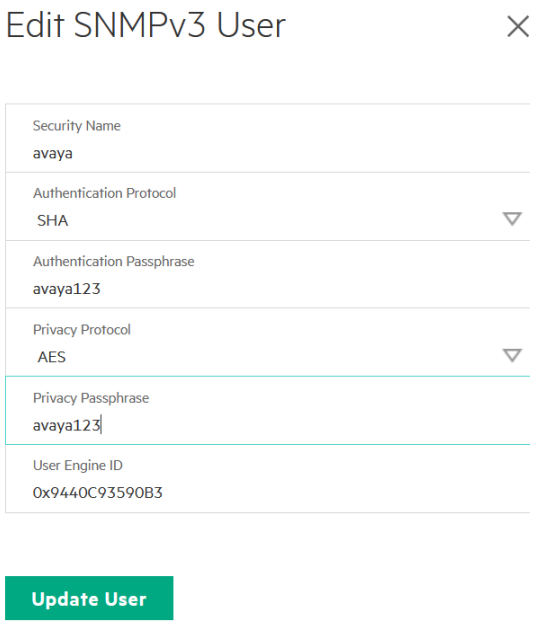
2. From the left side menu, select **iLO Shared Management Port** and copy the MAC address if the Shared Network Port from the summary page.

3. From the left side menu, select **Management**.

4. Scroll down on the **SNMP settings** page and select **New** under **SNMPv3 users**.

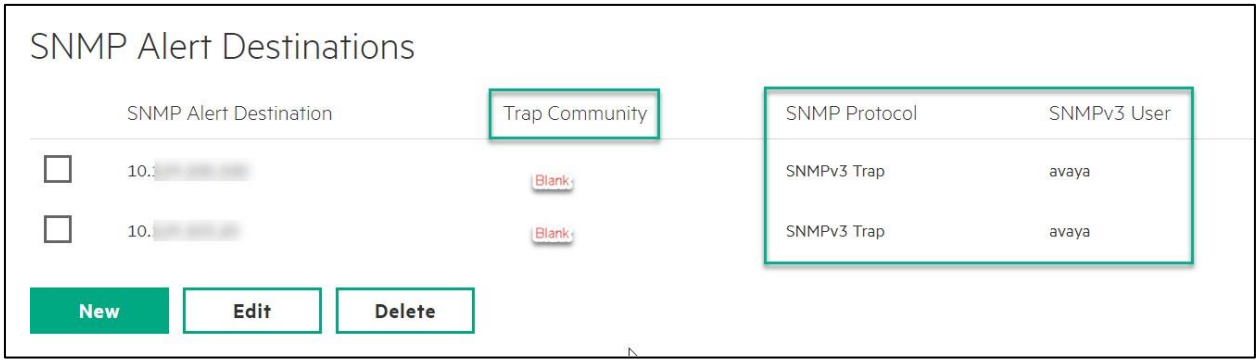
5. Fill in the details to add a new SNMPv3 user.

    - Create a security name of **avaya**
    - Select **SHA** authentication protocol and set a Passphrase of **avaya123**
    - Select **AES** privacy protocol and set a Passphrase of **avaya123**
    - In the text box below User engine ID, type in 0x followed by the MAC address of the shared network port copied on previous step. Please ensure that there are no colons in the MAC address when setting up the engine ID.
6. Click **Add User** to save changes.



7. Under SNMP Alert Destinations, click **New**.
8. Under the **Add Alert Destinations** details:
    - Enter the AO IP address under **SNMP Alert Destination.**
    - Leave the **Trap community** field blank.
    - Select **SNMPv3 Trap** from **SNMP Protocol** drop-down menu.
    - Select user **avaya** created from a previous step from **SNMPv3 User** drop down menu.
    - Click **Add** to save new changes.

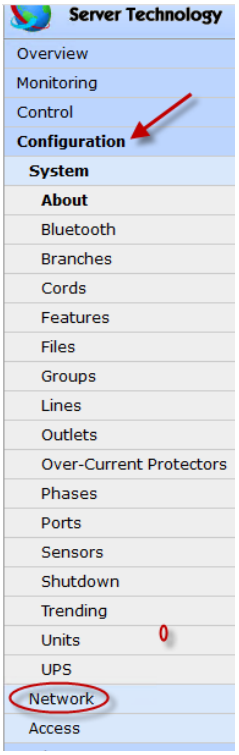
Repeat the steps to add the SAL GWas an SNMP alert destination. .



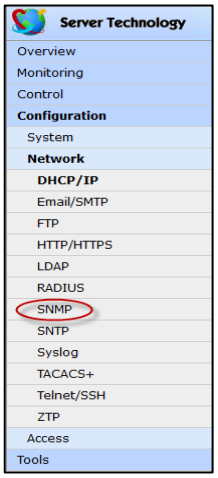
Configuring SNMP v2c on Sentry 4 PDUs

Procedure

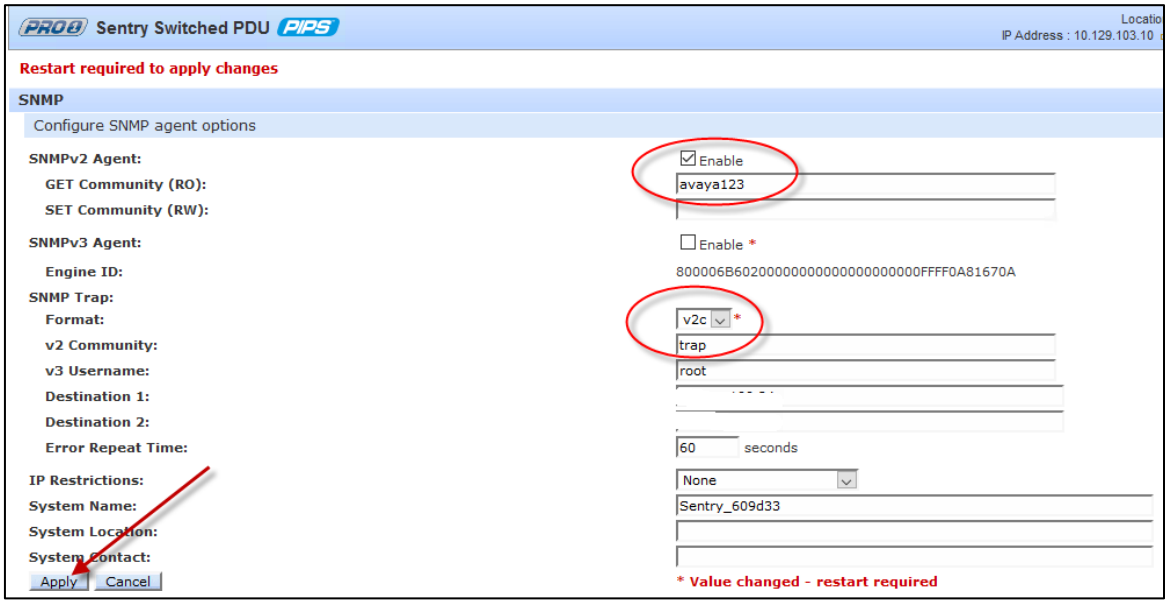
1. Open a web browser tab and access the PDU IP address by using the credentials provided in the IP template.
2. In the left navigation pane, click **Configuration** > **Network**.



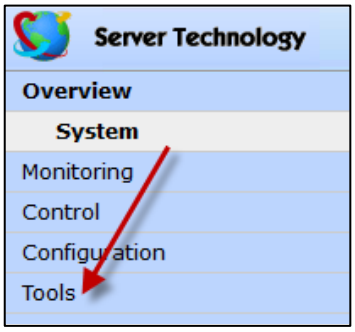
3. Click **SNMP**.

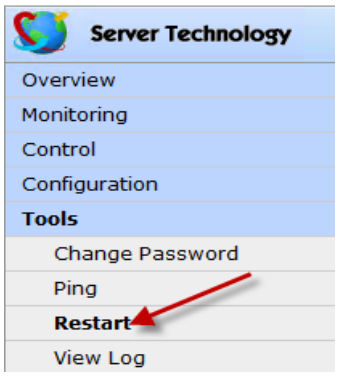


4. Select the **Enable** check box corresponding to the **SNMPv2c Agent** field.
5. In **Get Community (RO)** field, type the community string: avaya123
6. In **SNMP Trap**, in the **Format** field, click **v2c**.
7. Leave remaining default values and click **Apply**.



8. In the left navigation pane, click **Tools** > **Restart**.





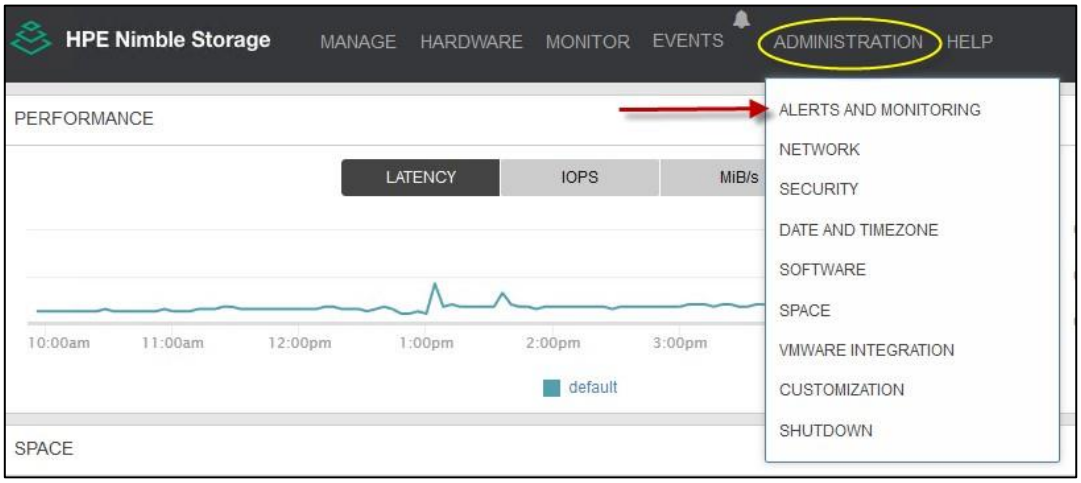
9. In the **Action** field, click **Restart**, and then click **Apply**.



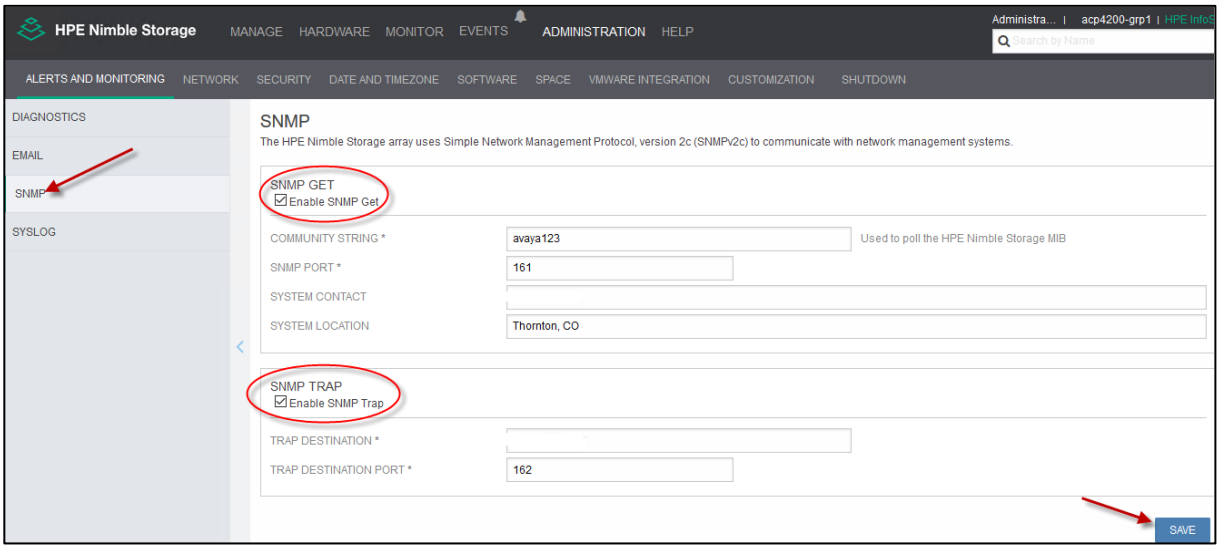
Configuring SNMP v2c on a Nimble Core

Procedure

1. Using the credentials in the IP template, access the Nimble Core IP address through a web UI and https.
2. Click **Administration** > **Alerts and Monitoring**.



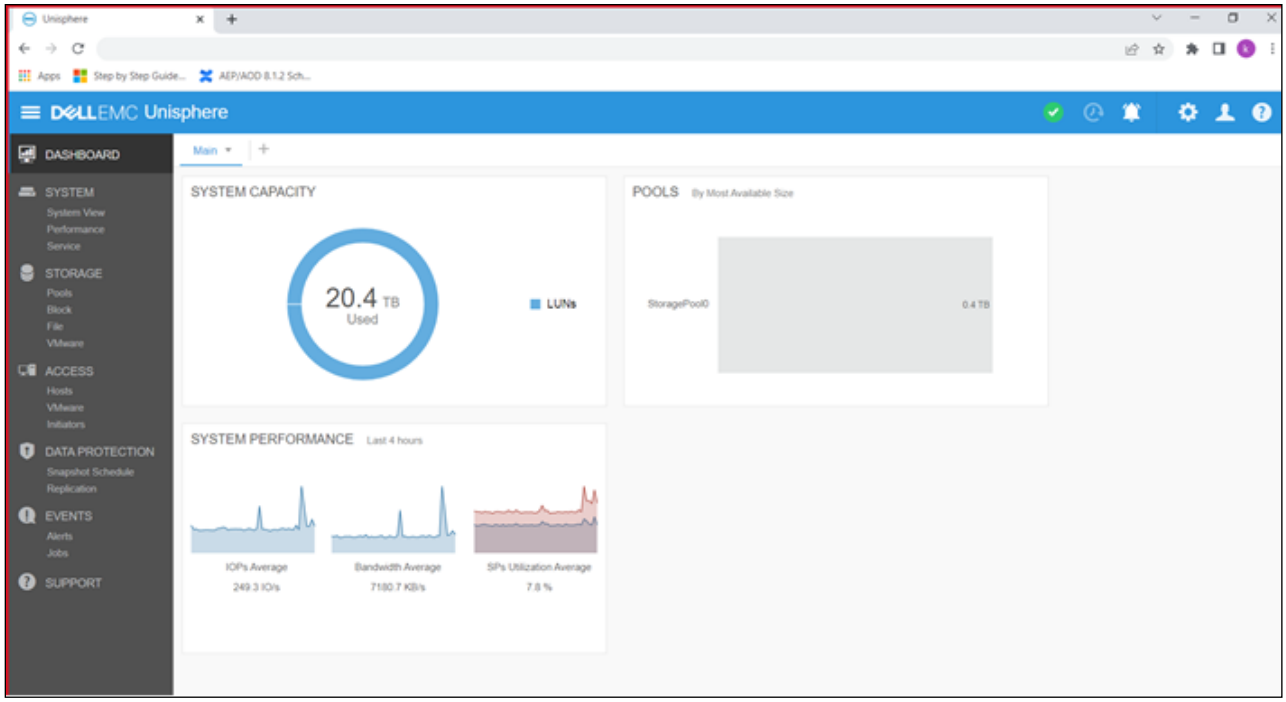
3. On the **Alerts and Monitoring** menu, click **SNMP**.
4. On the SNMP page, do the following:
   a. Select the **Enable SNMP Get** and **Enable SNMP Trap** check boxes**.**
   b. In the **Community String** field, type *avaya123*.
   c. In the **Trap Destination** field**,** type the IP address of the SAL Gateway that is provided in the IP template, and then click **Save***.*



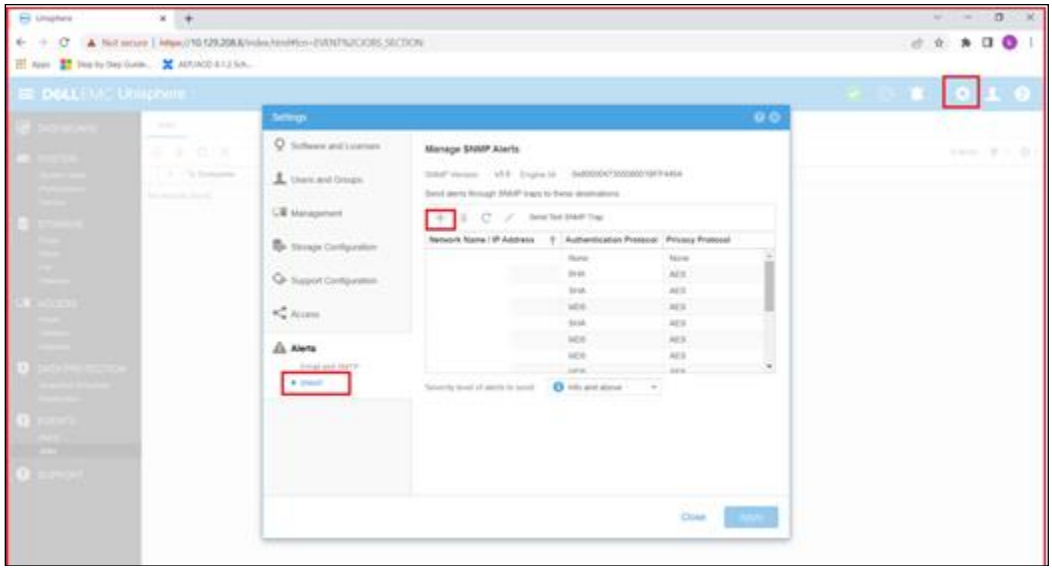
Configuring SNMP on an EMC VNXe3200

Procedure

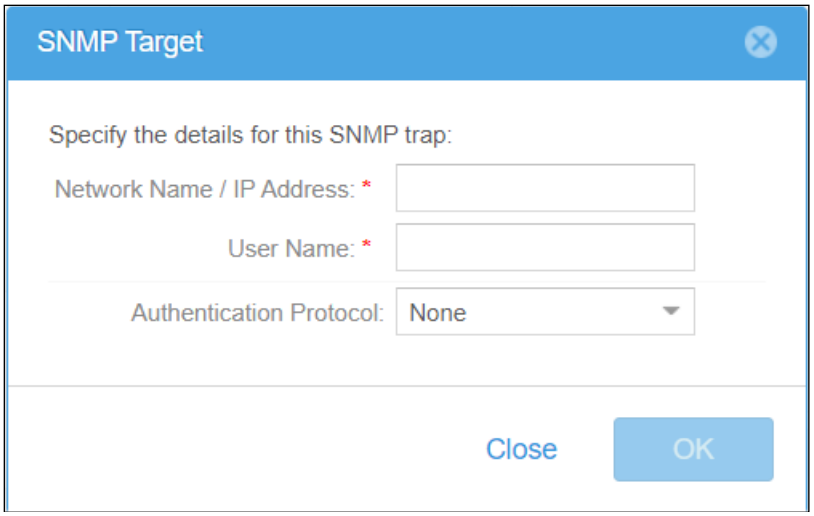
1. Open a web browser and access the 3200 device by using the IP and administrator login credentials provided in the IP template.
2. Click **Dashboard**.
3. Select **Settings** icon on the right corner of the task pane. Select Alerts and choose SNMP.



4. Click **Add** to administer Avaya Orchestrator™ as an SNMP trap destination.

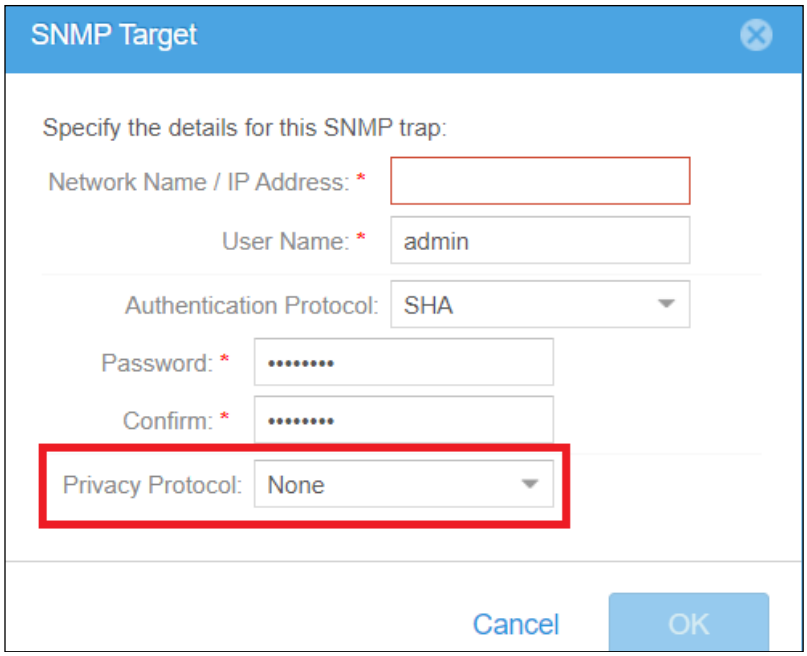


The **SNMP Target** dialog box appears.

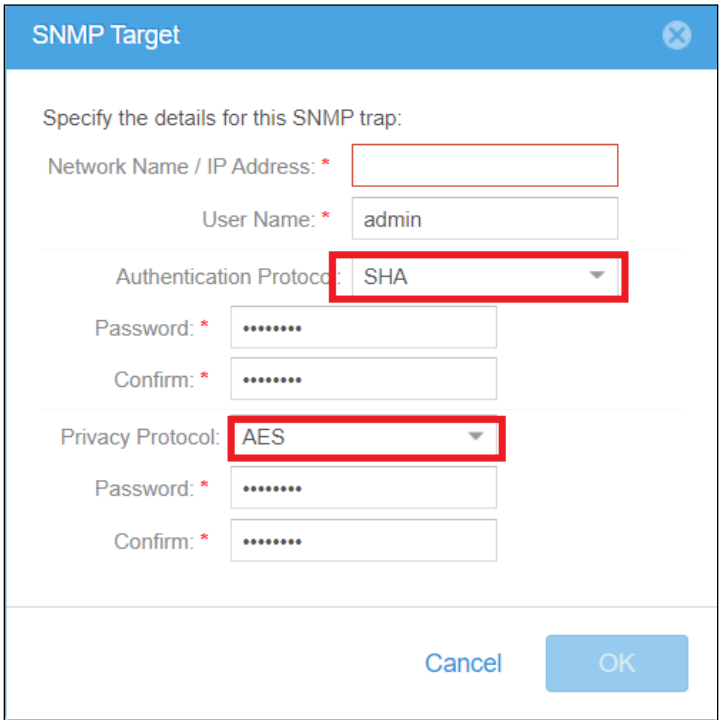


5. In the **Network Name / IP Address** field, type the IP address of Avaya Orchestrator™.
6. In the **User Name** field, type *avaya*.
7. In the **Authentication Protocol** field, click **SHA**.
8. In the **Password** field, type *avaya123*.
9. In the **Confirm** field, retype the password.
10. In the **Privacy Protocol** field, click **AES**.

    The **Privacy Protocol** field appears after you select the authentication protocol in the **Authentication Protocol** field.



11. In the **Privacy password** field, type *avaya123*.
12. In the **Confirm** field, retype the privacy password.



13. Click **OK**.

Chapter 4: Solution configuration

Overview

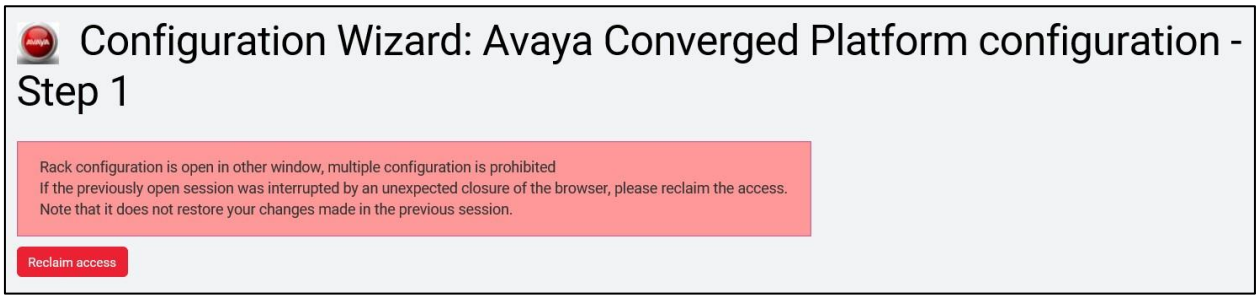
This chapter provides information about using the Configuration Wizard to administer ASP 4200 racks for alarm monitoring. After the ASP 4200 racks are administered, all devices are supported in Avaya Orchestrator™ for incoming traps and proactive state-of-health monitoring.

ACP rack configuration highlights

Important:

The ACP rack creation and configuration procedures are completed after you click **Finish**. If you leave the page either by pressing a back space or a web UI time-out occurs, all new un-submitted administration changes are lost. You must re-enter and re-submit the administration information.

Only one administrator at a time can administer the ACP Configuration Wizard. When another administrator attempts to access the Wizard while the original administrator is still active in the program, the following error is displayed:



It you leave the Wizard menu item open and unattended, other users cannot access the Wizard and make the necessary changes.

Configuring the ACP solution

Before you begin
You must have administrative user rights or have the **Can configure hosts and services** permission to access the **ACP Configuration Wizard**.

For more information, see
Managing permissions.

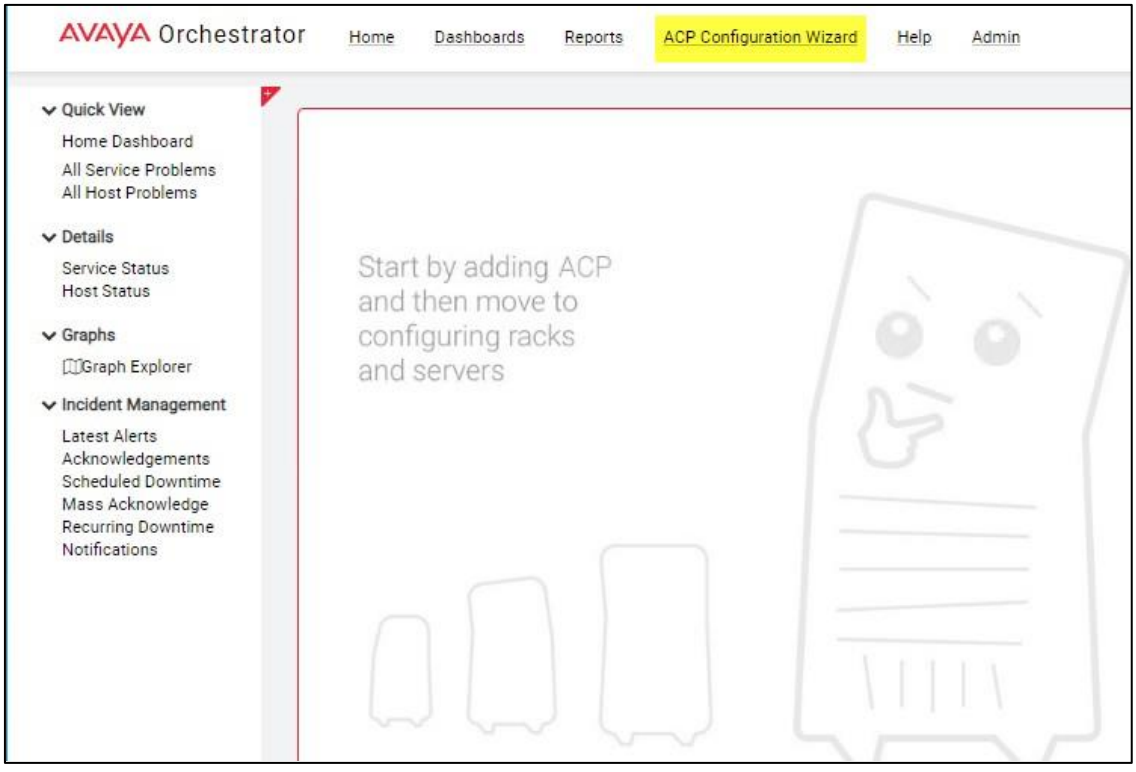
In the **ACP Configuration Wizard**, you must specify the IP addresses of the devices that you configure in the ACP solution; for example, PDUs and VSP devices.

When you enter the IP address of a device in the **ACP Configuration Wizard**, Avaya Orchestrator™ automatically tries to ping the IP address even before you click **Save & Detect hardware**. If the IP address is incorrect or does not respond, Avaya Orchestrator™ displays the following message:

Host <IP address> does not reply to ping.

Create the foundations

1. Log on to Avaya Orchestrator™ by using administrative credentials.
2. On the menu bar, click **ACP Configuration Wizard** to start the wizard.



Step 1 of the Configuration Wizard appears.

3. Do the following to add a new ACP:
   a. In the **ACP name** field, type the name intended for the new ACP/ASP solution as mentioned in the IP template.

Note: Only digits, a-z, A-Z letters, underscore (_), hyphen (-), and dot (.) symbols are allowed for the ACP name. Limit for symbols in the ACP name is 25. Spaces between characters are not permitted.

b. In the **ACP description** field, type a description for the new ACP/ASP solution. ACP description is optional.

c. Click **Add new ACP** to add the new ACP/ASP solution.

This will be the name applied to the view represented on the Home Dashboard. All devices administered in the Wizard will be represented on this dashboard. Therefore, if you intend to add racks from multiple data centers, choose the name that will best reflect the composite view.

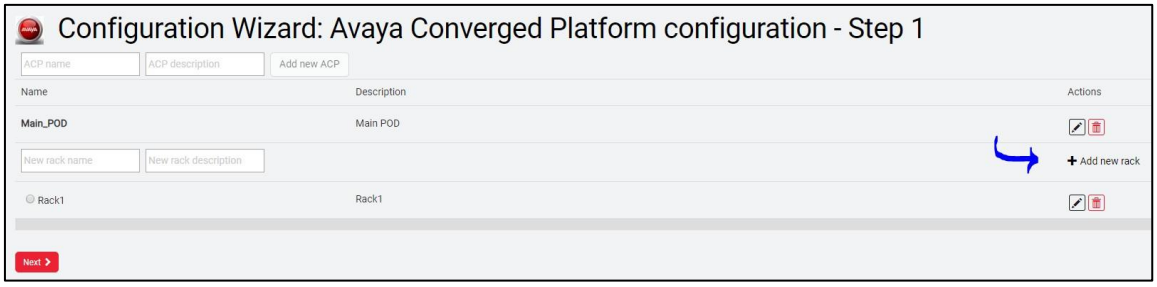
4. Do the following to add a new rack:

a. In the **New rack name** field, type a name for the first rack.

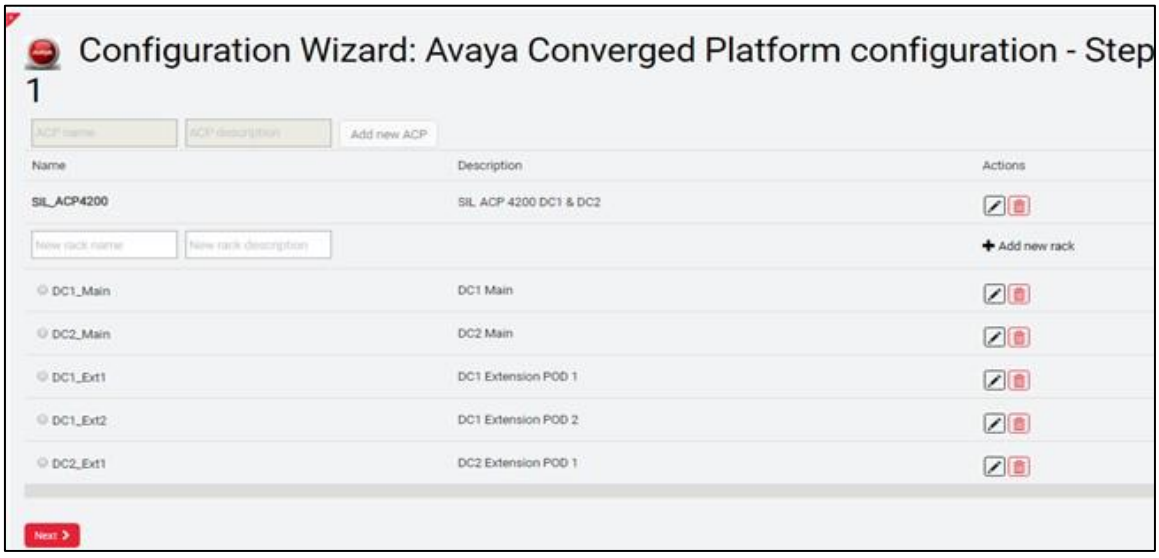
Note: Only digits, a-z, A-Z letters, underscore (_), hyphen (-), and dot (.) symbols are allowed for rack name. Limit for symbols in rack name is 25.

b. In the **New rack description** field, type a description for the new rack. The rack description is optional.

c. Click **Add new rack** to add the new rack.



5. Repeat Step 4 to add all racks in the solution.



Editing the name and description of a rack

Note:
Only digits, a-z, A-Z letters, underscore (_), hyphen (-), and dot (.) symbols are allowed for a rack name. Limit of symbols for rack name is 25.

Procedure

1. Log on to the Avaya Orchestrator™ web interface by using administrative credentials.
2. On the menu bar, click **ACP Configuration Wizard** to start the wizard.
3. On the Configuration Wizard: Avaya Converged Platform configuration - Step 1 page, click **Edit rack name/description** corresponding to rack that you want to edit.
4. Modify the rack name and description in the fields.
5. Click **Apply new rack name/description** .

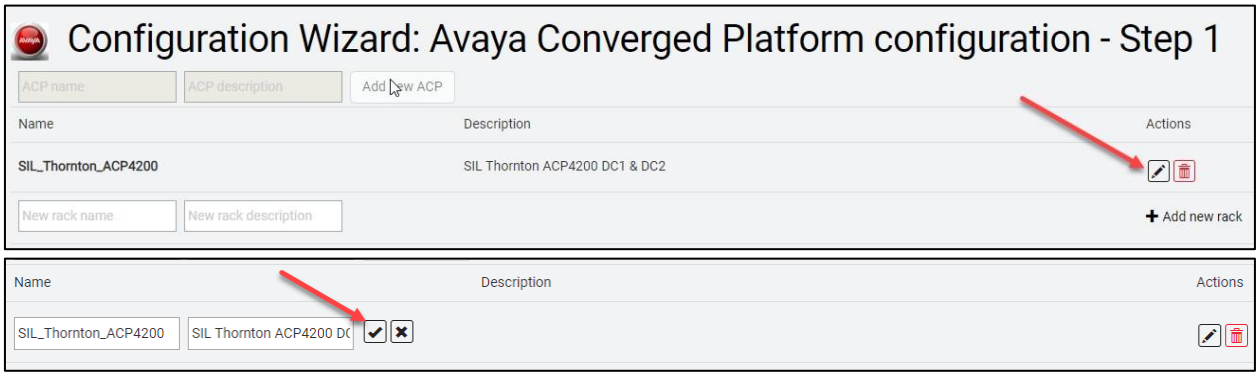
Deleting an ACP solution or rack

About this task

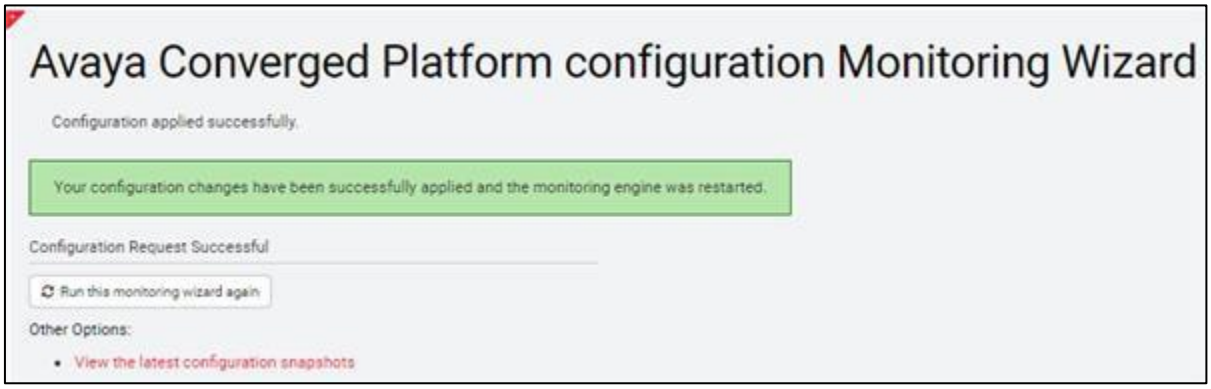
Administrators can delete 4200 racks any time after adding and administering the ACP/ASP solution.

Procedure

1. Log on to the Avaya Orchestrator™ web interface by using administrative credentials.
2. On the menu bar, click **ACP Configuration Wizard**.
3. On the Configuration Wizard: Avaya Converged Platform configuration - Step 1 page, click **Delete** corresponding to the ACP solution or rack that you want to delete.

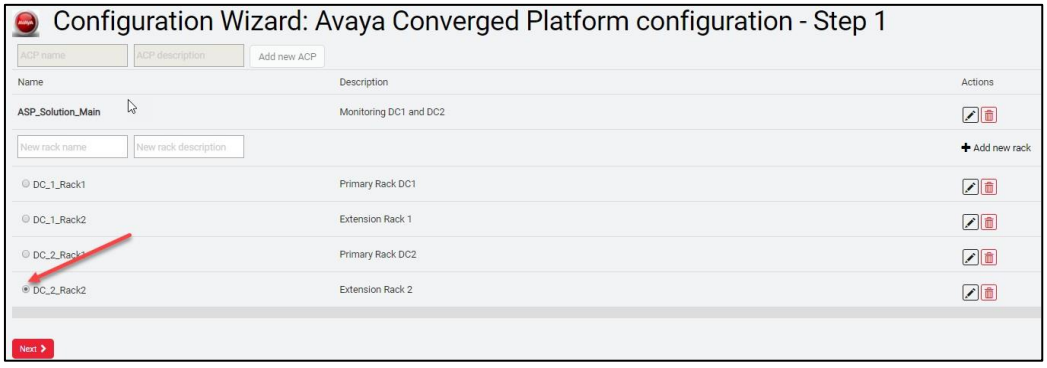


Note:
At this point, administers can continue to build the AO solution by clicking **Next** to proceed to the next section, or can opt to save the solution and rack information by clicking **Next**, and then **Finish** on the subsequent page. The current administered information is saved when you click **Finish**.

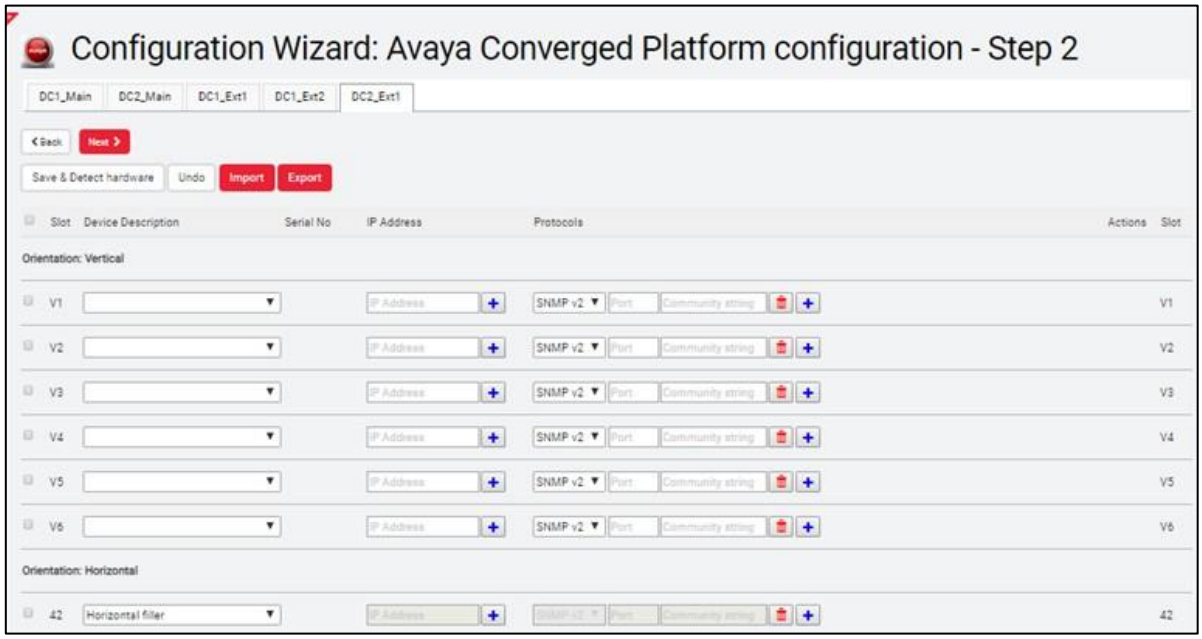


Administering Rack Elements

You may click **Run this monitoring wizard again,** as shown in the screen shot above, which will revert to the entry page of the ACP Wizard, or you may start directly from the entry page, where you will select the button corresponding to the rack that you want to deploy. Then click **Next**.
Step 2 of configuration wizard appears.



The administration wizard for the selected rack is presented.



Total 48 slots are displayed.

The first six slots (V1-V6) represent vertical equipment placement on the rear side of the rack, that is, PDU devices. The following charts indicate the placement of the devices based on the rack size being deployed.

48" Rack View of Vertical PDU Assignments					
V1	V2	V3	V4	V5	V6
Primary 3	Secondary 1	Primary 1	Primary 2	Secondary 2	Secondary 3

42" Rack View of Vertical PDU Assignments					
V1	V2	V3	V4	V5	V6
Secondary 1	Primary 1	Unused	Unused	Primary 2	Secondary 2

Slots 1-42 represent the horizontal MTUs that can be viewed from the front side of the rack and can support the following devices: servers, network switches and routers, storage arrays, media servers, and some horizontal PDUs.

There is no limit to the number of devices that you can add at any one time. However, the greater the quantity of devices and elements being simultaneously entered, the longer the Finish process takes to complete.

Note:
There are filler components that you can select for each slot. You can hover over the **Slot** and **Device Description** fields to view these filler components. One example of such a filler is the *Horizontal filler* that is used to represent empty slots, whether empty

for air flow considerations or for representing the availability of a slot for future hardware deployments.



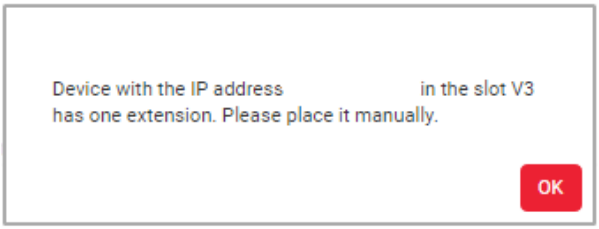


Adding a PDU

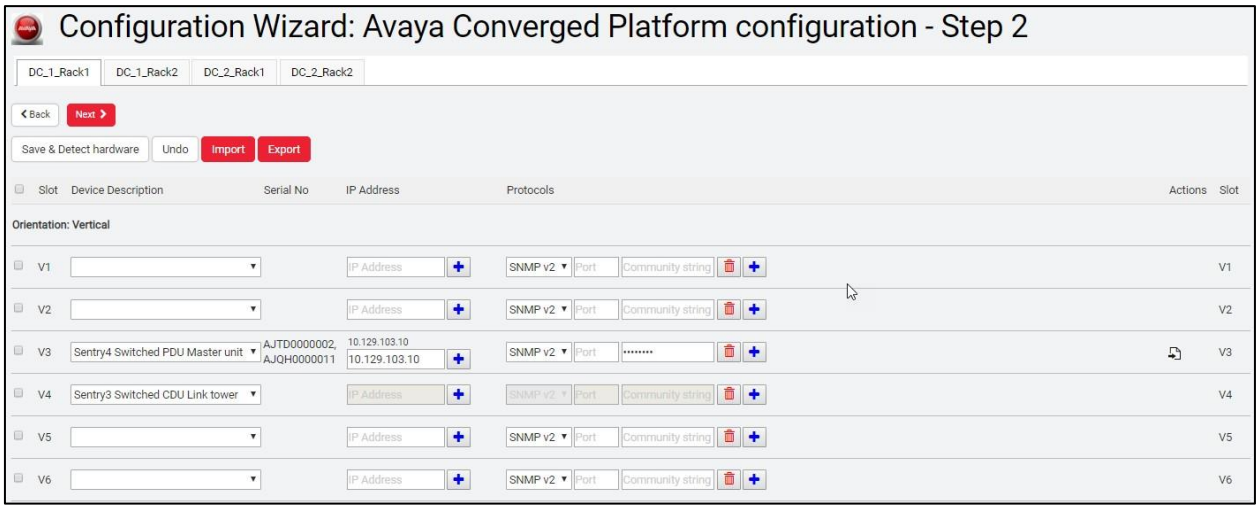
The Sentry 4 PDU supports only SNMP v2.

1. In the **IP address** field corresponding to slot V3, type the IP address of the first master PDU.
2. In the corresponding SNMP **Community string** field, type *avaya123*.
3. Add any additional PDUs in slots V2 and V1.
4. Click **Save & Detect hardware**.

   The expansion units associated with each master PDU do not have an IP address to administer. The AO tool reminds administrators to place a filler field where the partner expansion unit is to be located after the administrators click **Save & Detect hardware**.



5. Based on the PDU administration in slots V1-V3, click **Sentry Smart PDU Link unit** as filler information in the lists corresponding to slots V4-V6.



Note:

At this point, administrators can do one of the following:

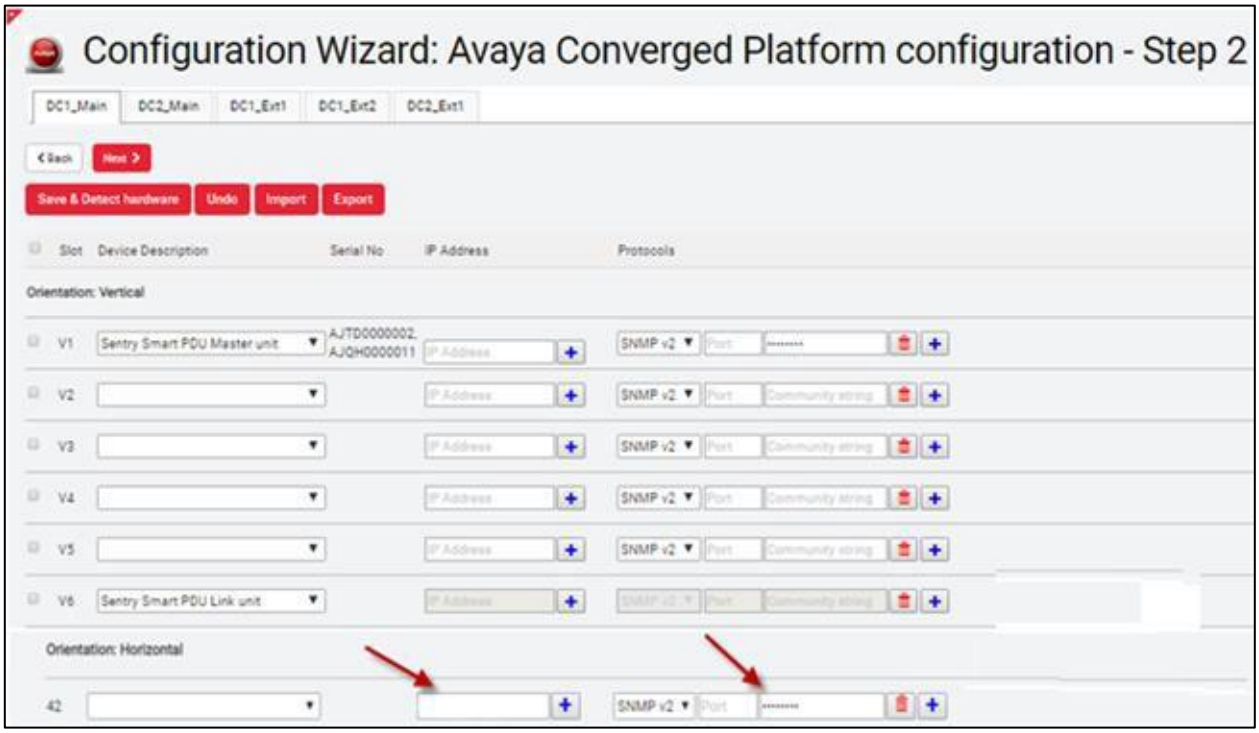
- Continue to the next device to be administered.
- Click **Save & Detect hardware**, click **Next**, and then click **Finish** to save the current administered values.

Administering VSP Network Devices

The VSP devices supported in the ACP/ASP 4200 solution include the 7024, 4850, 7254 and 7400. Each network device in the solution can support SNMP v2c or SNMP v3. The following sectionsdescribe the administration for SNMP v2c and SNMP v3.

SNMP v2c Administration

1. At the slot location for the first VSP device, type the IP address that is provided in the IP template.
2. In the **Community string** field corresponding to SNMP v2c, type *avaya123*.



Note:

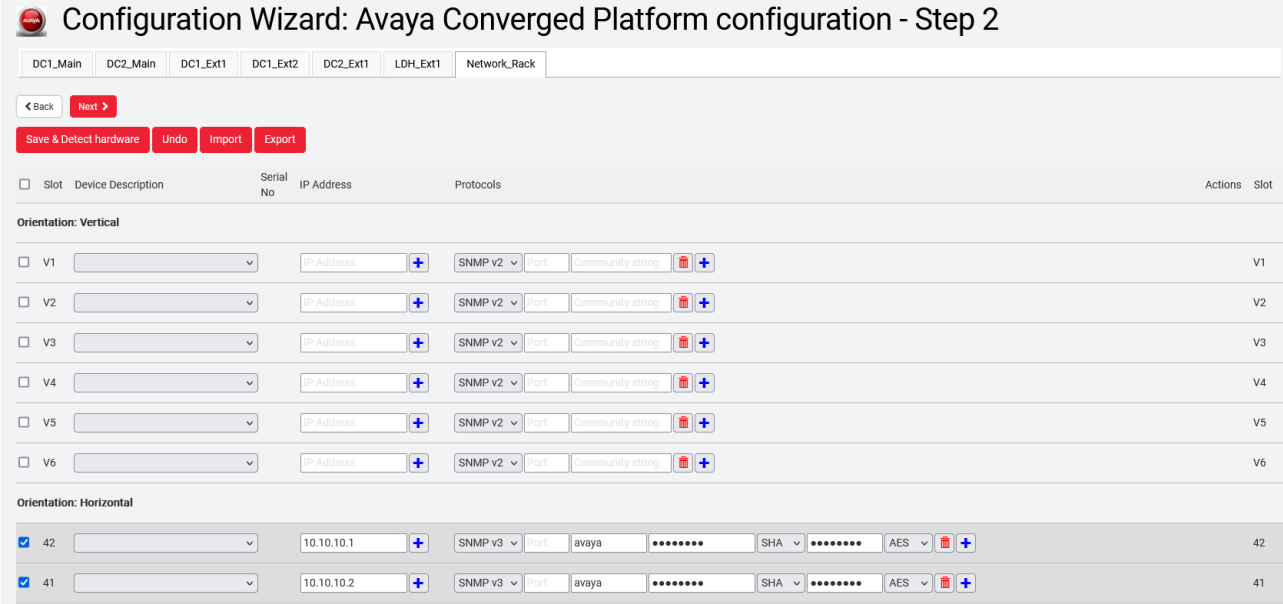
At this point, administrators can do one of the following:

- Continue to the next device to be administered.
- Click **Save & Detect hardware**, click **Next**, and then click **Finish** to save the current administered values.

SNMP v3 Administration

Configure the Wizard

a. At the RMU slot location for the first VSP device, enter the IP address from the IP Template.
b. Click the dropdown menu for SNMP type and select SNMPv3 and enter the user name *avaya.*
c. Enter the Authentication password (default = avaya123) and click the dropdown menu and select SHA.
d. Enter the Privacy password (default = avaya123) and click the dropdown menu and select *AES*.



Note:

At this point, administrators may continue to the next device to be administered, or select *Detect Hardware* again, then the *Next* button, followed by the *Finish* button to save the current administered values.

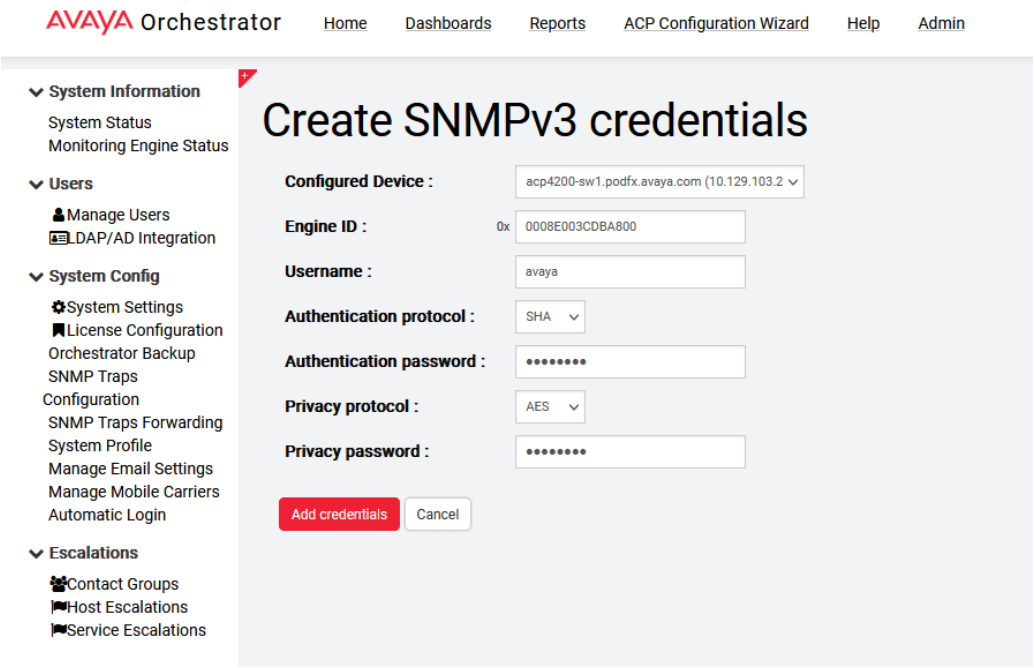
Configure SNMPv3 Encryption

- Redirect to *Admin > SNMP Traps Configuration*.
- Click on the Configured Device dropdown menu and locate the IP address and/or FQDN of the first VSP device and select it.
- For the Engine ID, locate the information collected during the SNMP administration of the device. If not available, SSH into the network device. From the CLI command, type *enable.* Then type *show snmp-server user* to display the Engine ID. Find the long alpha numeric sequence, like the one presented below. The Engine ID will be the letters and numbers located after the 0x, and without the : (colon: interjected between letters and integers). In this example, the Engine ID is 800008E0031B574800. This is the number to be entered into the Engine ID field.

avaya	**0x80:00:08:E0:03:A4:25:1B:57:48:00 HMAC_SHA, AES PRIVACY,**
initial	**0x80:00:08:E0:03:A4:25:1B:57:48:00 NO AUTH, NO PRIVACY**

- Enter the user name *avaya.*

- For Authentication protocol, select SHA.
- The Authentication protocol password default value is avaya123.
- For Privacy protocol, select AES.
- The Privacy protocol password default is avaya123.
- Select *Add credentials.*
- Repeat the process for additional VSP devices.



Configure VRRP Gateway Mapping

Note:

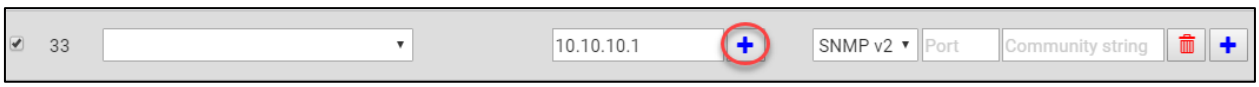
Mapping for 7400 switches is not a requirement

Administering Servers

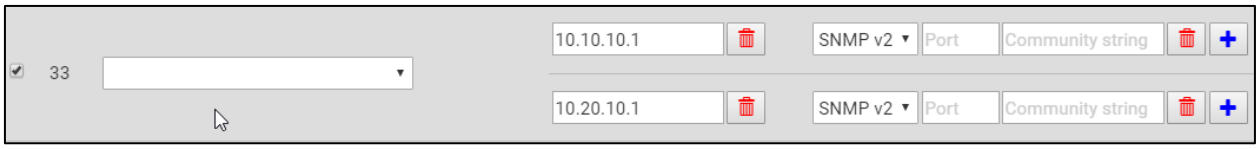
Both ESXi and iLO IP ports will be administered for each server. Since both the ESXi and iLO elements support SNMP v2c and SNMP v3, administration options for both will be covered here.

SNMP v2 Administration

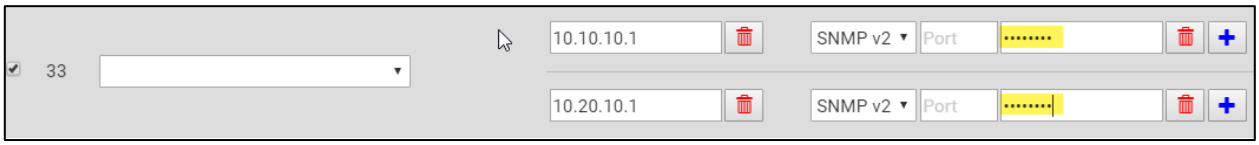
1. Locate the slot for the first server and type the IP address for the ESXi element.



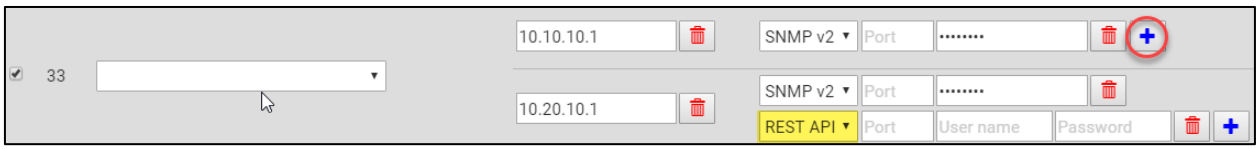
2. After you enter the ESXi IP address, click the + icon to add a second IP address field for the iLO IP address.

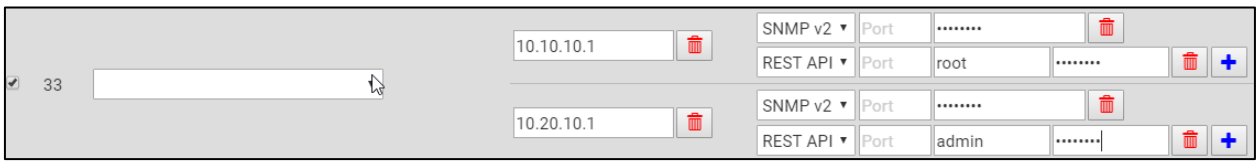


3. After you enter the ESXi and iLO IP addresses, administer the SNMP protocols for each element. The ESXi and iLO elements each require two APIs: SNMP v2 and REST. Configure the SNMP v2 settings for both first.



4. After SNMP administration is finished, click the + icon located at the right of each SNMP row to add a REST API entry for each element. AO knows the element types and will automatically select REST API as the administrable option.



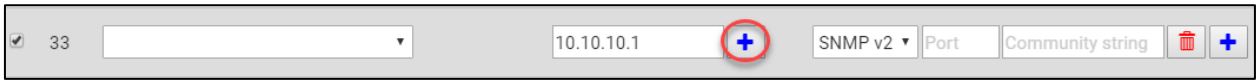


5. Type the *user name* and *password* for each REST API entry. These entries are the login credentials for the ESXi and iLO elements for each server, *root* crdential being associated to the ESXi host and *admin* being associated to the iLO port.

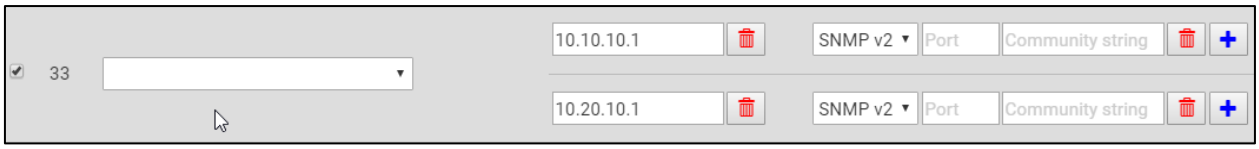
Note: Use the delete icon to remove unwanted protocols and IP credential entries.

SNMP v3 Administration

1. Locate the slot for the first server and type the IP address for the ESXi element.

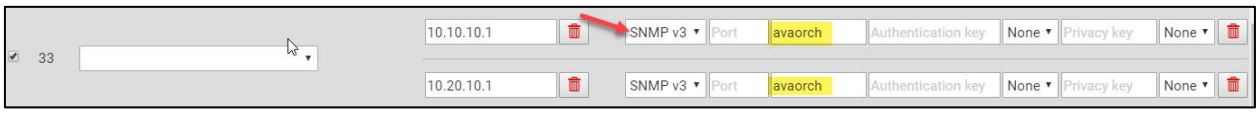


2. After you enter the ESXi IP address, click the + icon to add a second IP address field for the iLO IP address.



3. From the SNMP protocol drop down menu, select SNMP v3 for both ESXi and iLO elements. For the user name, enter the value that was administered during the ESXi and iLO element configurations previously.

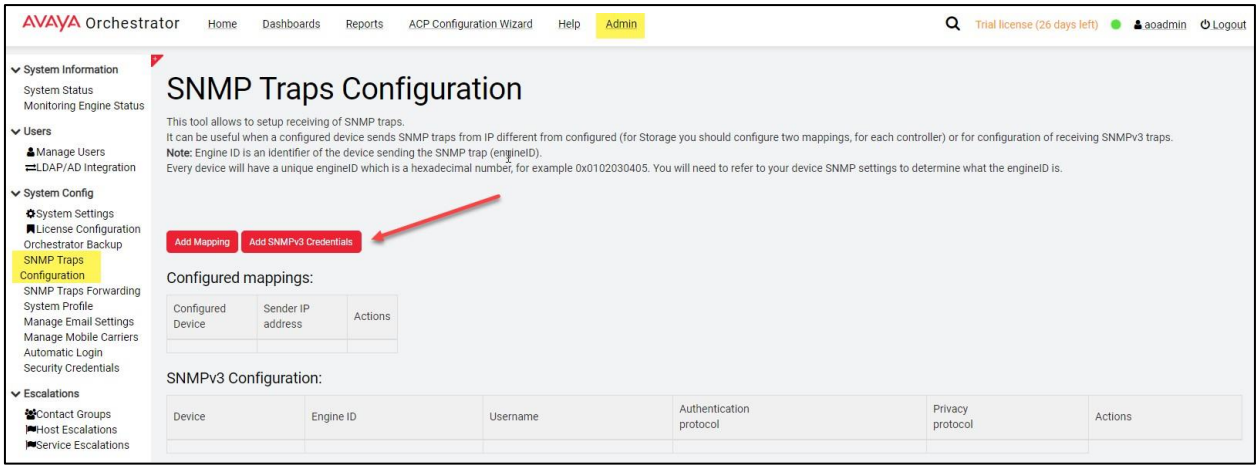
   Avaya recommends using *avaorch*, however, you can administer any user name for both the element and the AO as long as they match.



4. From the Authentication and Privacy type drop down menus, select SHA and AES respectively. In the Authentication and Privacy key fields, highlighted below, enter *avaya123.* A different secure key phrase may be used, as long as it is administered the same in ESXi, iLO and AO.

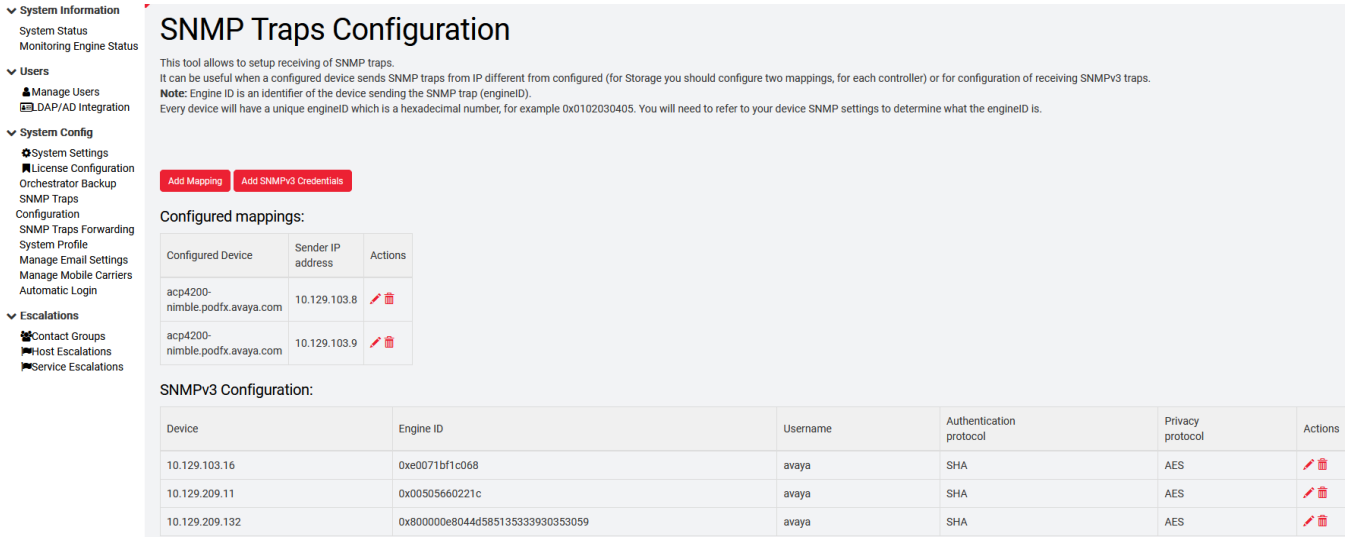


5. Go to the menu path Admin > SNMP Traps Configuration and click *Add SNMPv3 Credentials*.

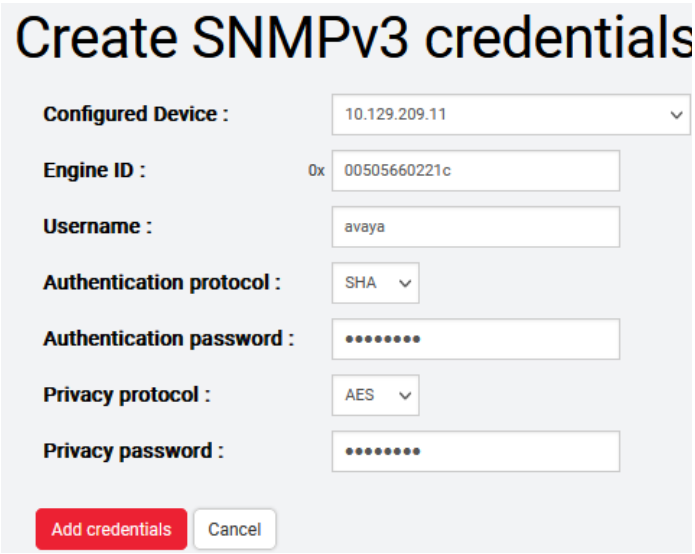


Note: Use the trashcan  button to remove unwanted protocols and IP address entries.

6. Go to *Admin > SNMP Traps Configuration* and click *Add SNMPv3 Credentials*.



7. Enter the ESXi element IP address. Enter the Engine ID previously administered in this ESXi host earlier in the deployment process (can be found via ESXi cli, with the command: *show snmp-server user).* Add the user name of *avaya.* Administer the Authentication and Privacy protocols SHA and AES respectively, giving both protocols a password of *avaya123*.
8. Repeat the same administration process for the iLO element IP.
9. Click *Add Credentials* to save changes.

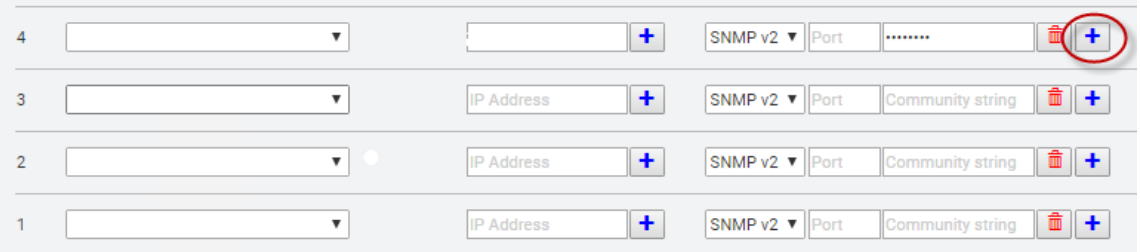


Administering the Nimble Storage Array

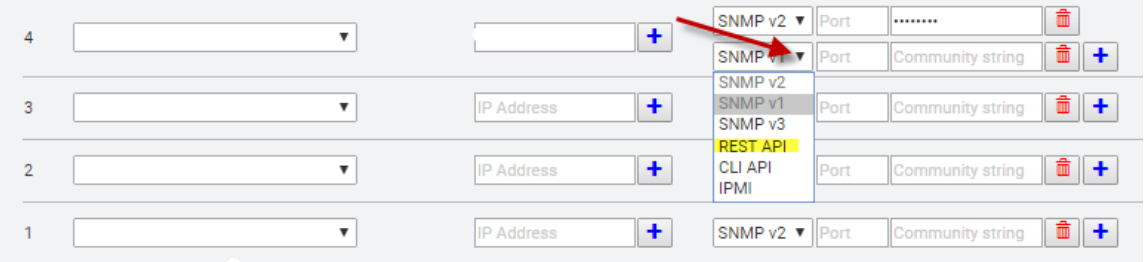
1. Locate the upper most slot location for the Nimble core (RMU 4). This is where the IP address will be administered.
2. The Nimble device will require 2 API interfaces: SNMP and REST API.
    i. Administer the SNMP v2c interface first. For “Community string” use

avaya123.

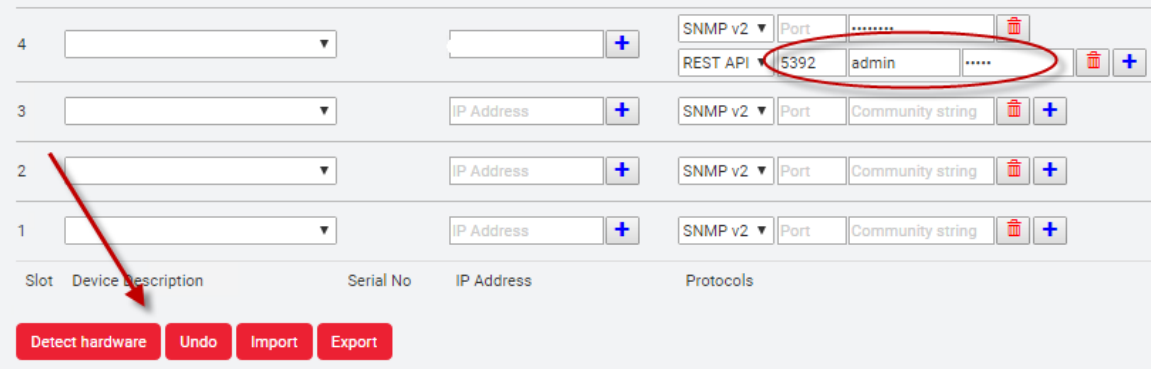
ii. Click the + next to the SNMP v2c entry to create a second entry interface.



- Click on the new API drop down menu and select REST API.



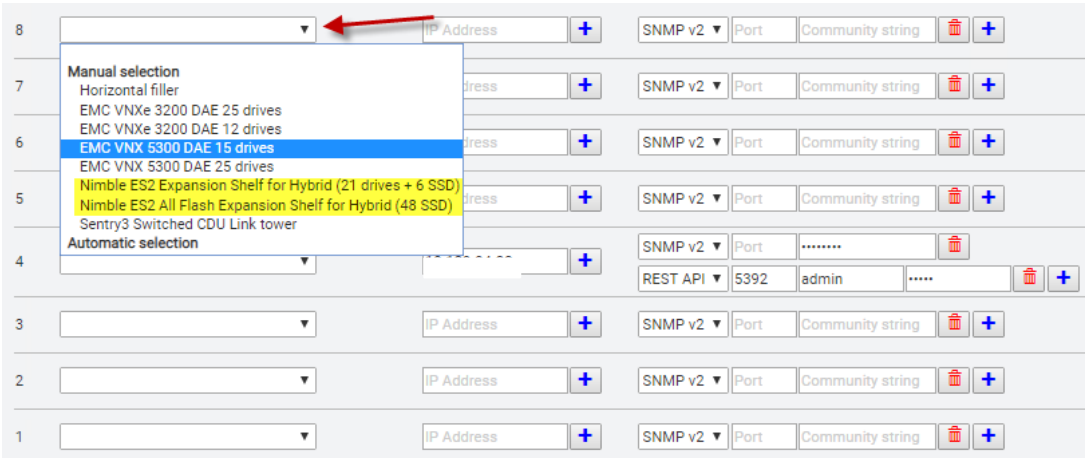
- Enter port **5392** and the login credentials for the Nimble array noted in the IP Template. Then click on *Detect Hardware* to confirm acceptance and communication between AO and Nimble.



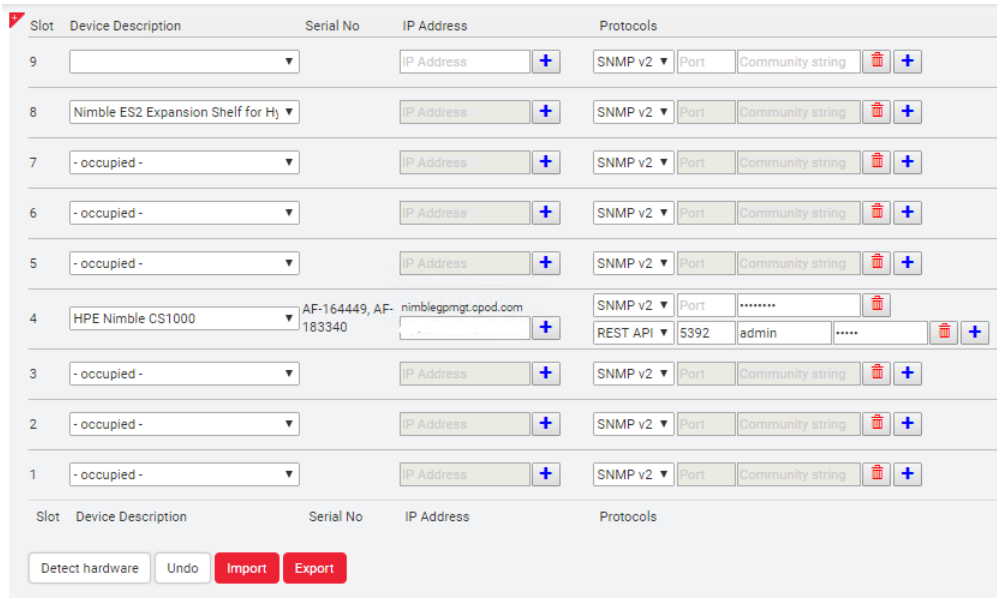
3. An info message will be presented if there is an extension module present on the Nimble array.



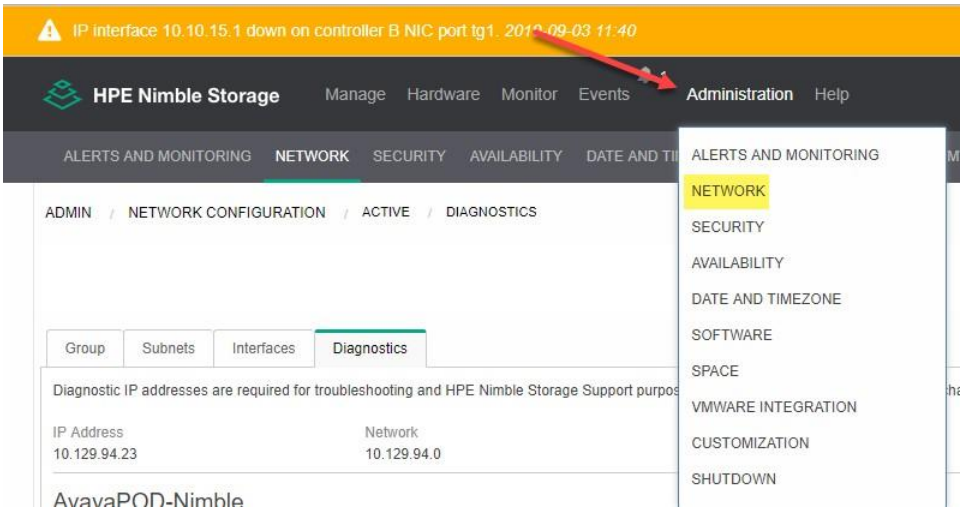
4. If an expansion unit is also being deployed in the same rack, locate the RMU of the upper most row supporting the expansion location and click on the drop down menu. Select the appropriate EMC 3200 expansion device.



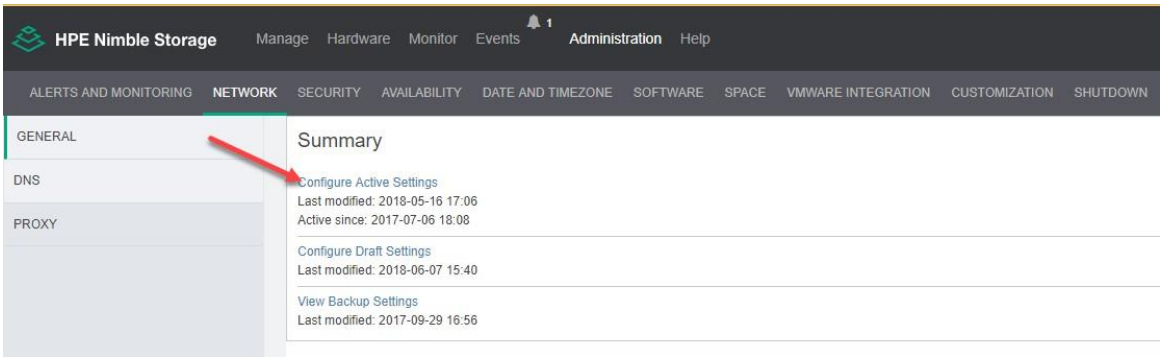
5. Continue with admin, or press *Next* and then *Finish* to save admin.



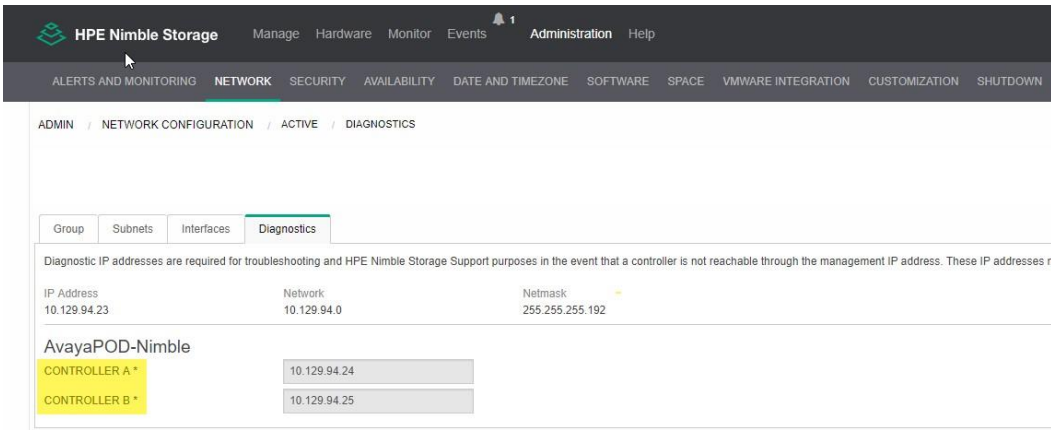
6. Log in to the Nimble array management IP port.
7. Click on *Administration* form the top menu bar and select *Network* from the submenu.



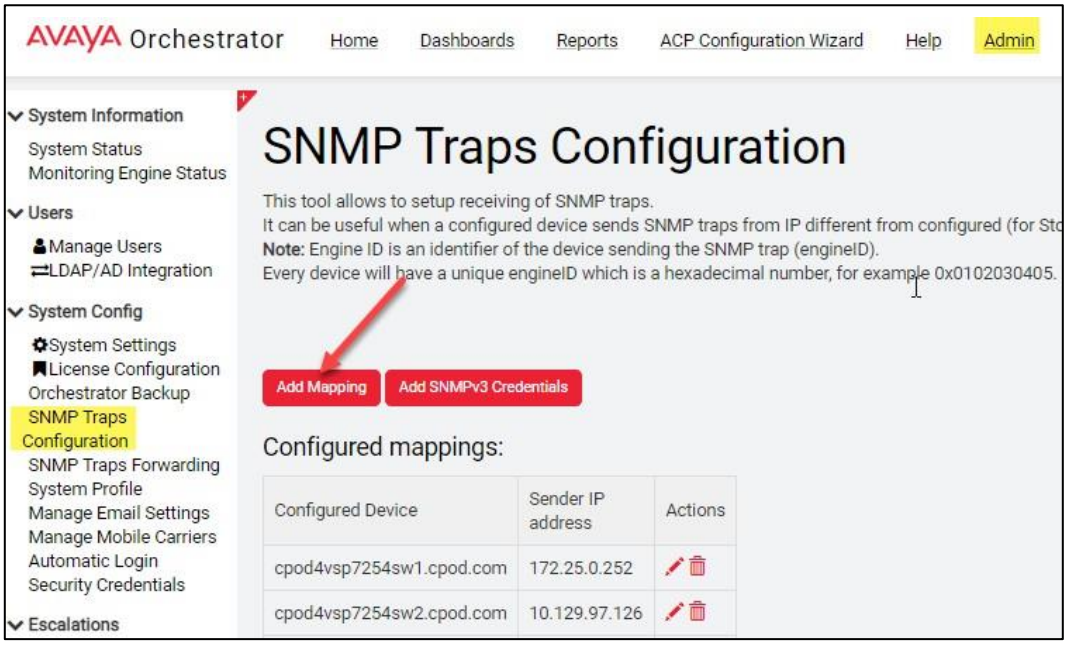
8. From the Network page, select *Configure Active Settings.*



9. From the Active Settings menu, select the *Diagnostics* tab. Note the Controller A and B IP addresses.



10. From AO, go to *Admin* > *SNMP Traps Configuration* and select *Add Mapping.*



11. From the drop down for the *Configured Device*, select the Nimble array. For the *Sender IP address*, enter the Controller A IP address and click *Add Mapping* to commit the admin. Repeat this step, and add the mapping to the Nimble array for the Controller B IP address.



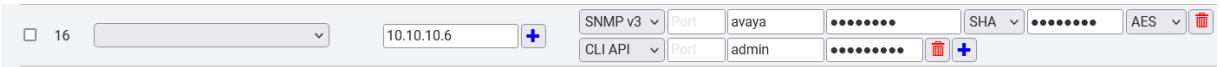
Administering EMC VNXe3200

Note:
Proactive monitoring is not working in AO due to the OS change from flash to HTML5, this might be fixed in the next release. Alarming works through SAL Gateway.

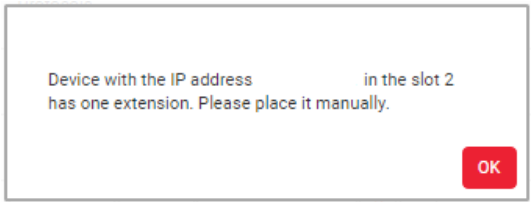
1. Locate the upper-most slot location for the EMC 3200 core. This is where the IP address is administered.
   The EMC device requires two API interfaces: SNMP and CLI.
2. Administer the SNMP v3 interface first:

a. In the **User name** field, type *avaya.*
b. In the **Authentication key** and **Privacy key** fields, type *avaya123*.
c. In the **Authentication type** field, click **SHA**.
d. Click on the Privacy type, and then click AES.

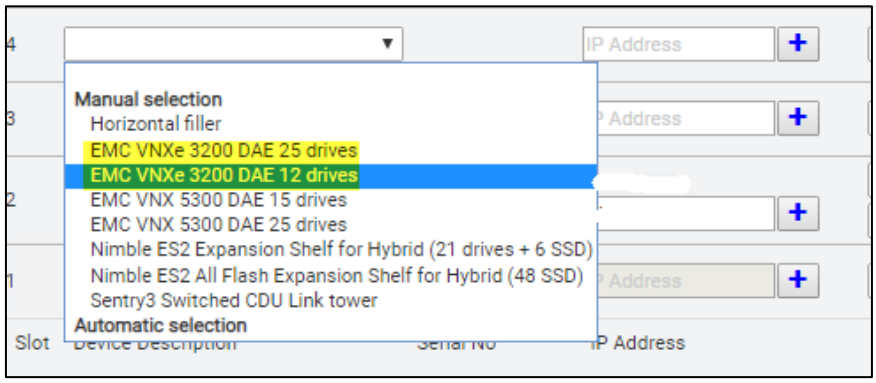
Click the + icon at the far-right end of the row to create a second entry interface.



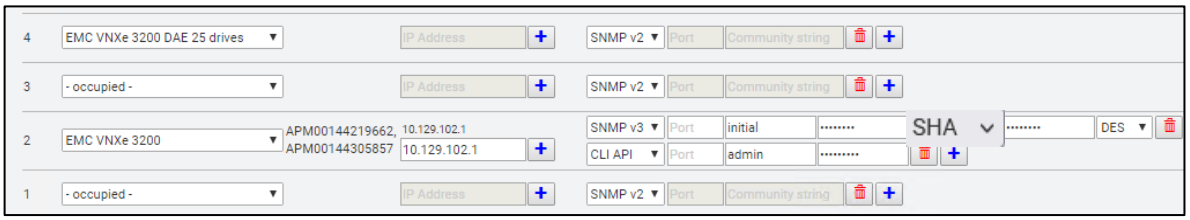
3. In the second API drop-down list, click **CLI API**.
4. In the **User name** and **Password** fields, type the login credentials for EMC 3200.
5. Click **Discover hardware** to confirm device acceptance and communication between AO and the EMC 3200 device.
6. If an expansion unit is present in the rack, an information message appears to alert the administrator to add it manually. There is no IP address associated with an expansion storage device.



7. Locate the upper-most slot location where the expansion unit is located, and then in slot filler drop-down list, click the EMC expansion device to be deployed.

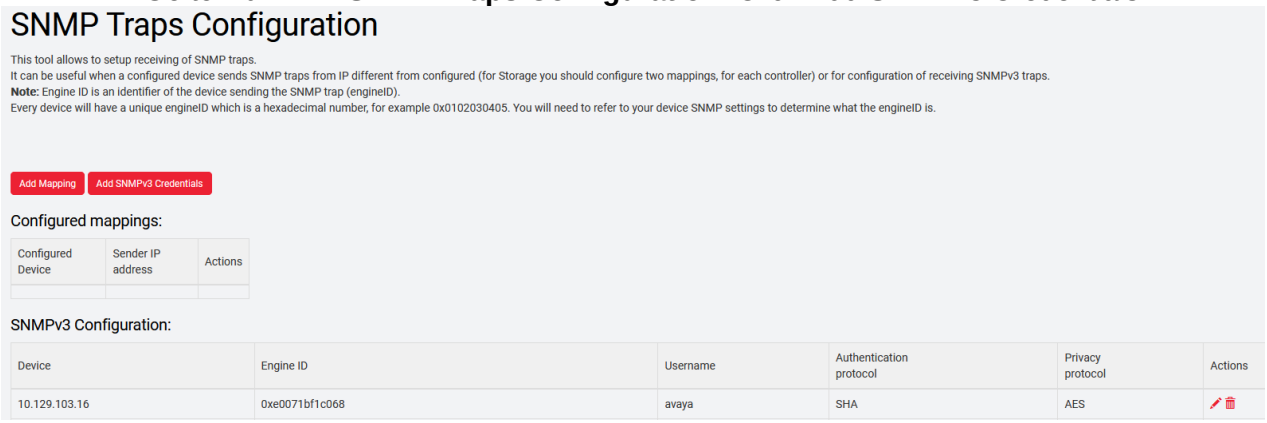


8. After you select the EMC expansion device, click **Next**, and then click **Finish** to complete and save the current administration.
AO populates the subseuqent slots to represent the physical location of the device.

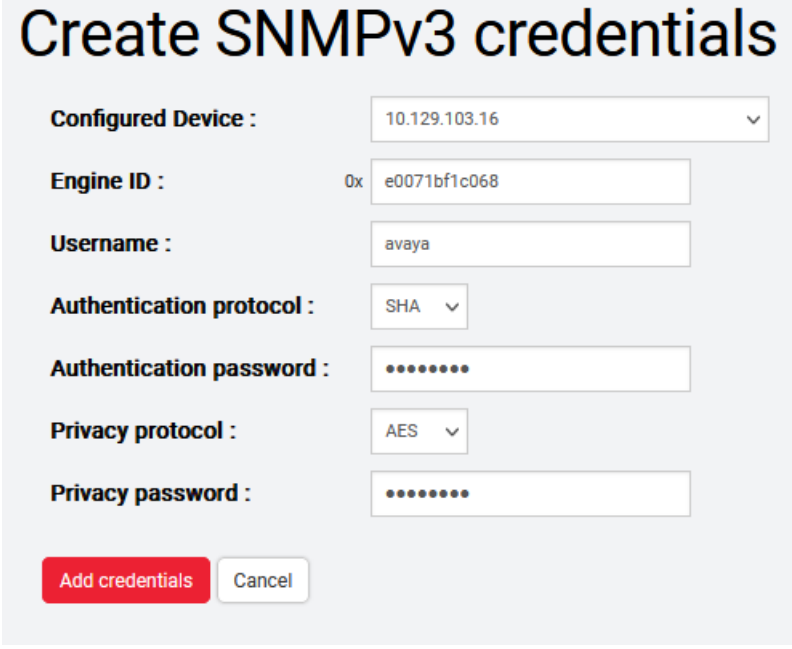


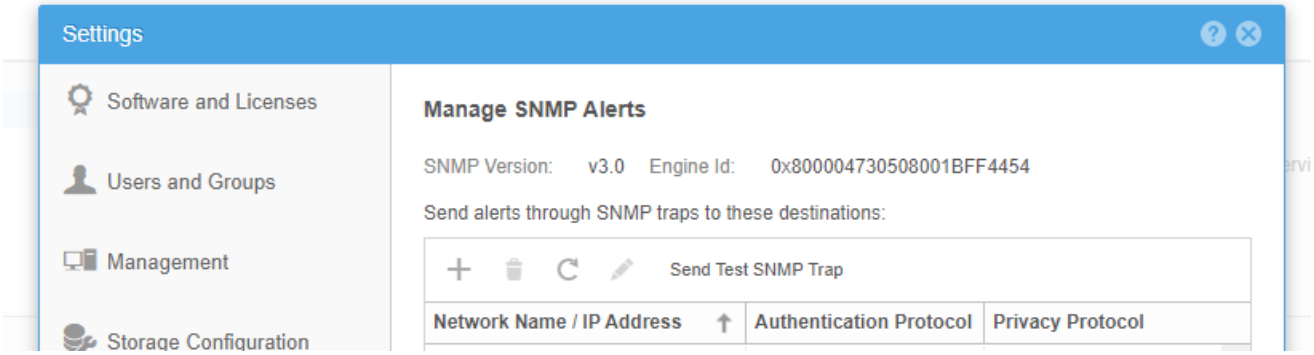
Add EMC 3200 SNMP Credentials and Mapping

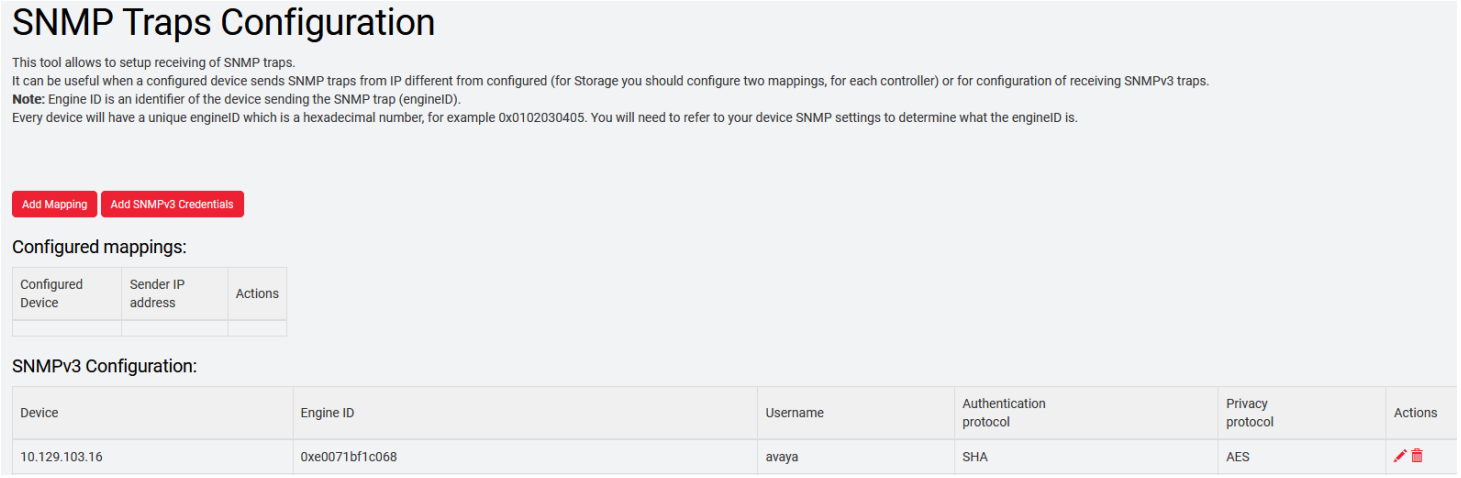
1. Go to **Admin > SNMP Traps Configuration.** Click Add SNMPv3 Credentials.



2. From the **Configured Device** drop down menu, locate the EMC 3200 IP address or FQDN. Then enter the Engine ID that may be identified via the EMC Unisphere login (see screen capture below). Continue entering the same user name and authentication protocols and passwords entered previously into the Configuration Wizard. Press **Add Credentials.**







Administering G450 Media Gateways

SNMP v2c Configuration

1. Locate the rack and slot where you want to place the G450s.
2. Type the IP address for each device in the appropriate slot.
3. In the **Community string** field, type *avaya123*.
4. After all the G450 components are administered, click **Save & Detect hardware** to confirm communication between AO and G450 devices.

Note:
After the devices are administered or if you want to temporarily stop the administration process, do not leave the AO administration process without saving the administered information. Do the following to enter and save the administered information in Avaya Orchestrator™: Click **Save & Detect hardware**.

The hardware types and serial numbers are automatically detected and displayed

in their corresponding slots.



If there is undetectable administration entered, an error message appears.

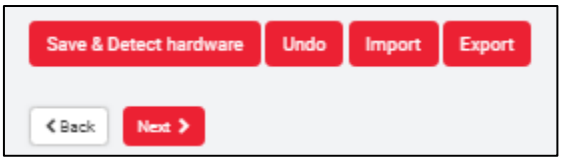
Do the following to identify failed entry fields:

The fields that fail do not successfully detect the hardware type and serial number. The failed entries can be identified by the empty *Slot Device Description* fields alongside previously entered IP and SNMP information. If the administration error is known and can be rectified, do the necessary changes and click **Save & Detect hardware** after each change until all devices are accepted.

Do the following to remove unwanted entries:

After you click **Save & Detect hardware**, any entry that is incorrect must be removed. For example, a wrong slot administered. Press the space bar in the **IP address** field to remove the IP address, and then click **Save & Detect hardware**. AO removes all associated entry data from the form.

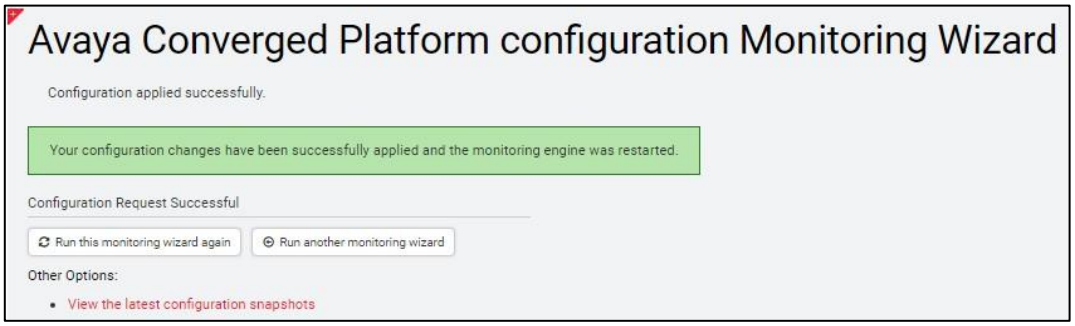
5. After the hardware administration is complete and all hardware is successfully detected and/or removed as needed, click **Next**.



Step 3 of the configuration wizard appears.



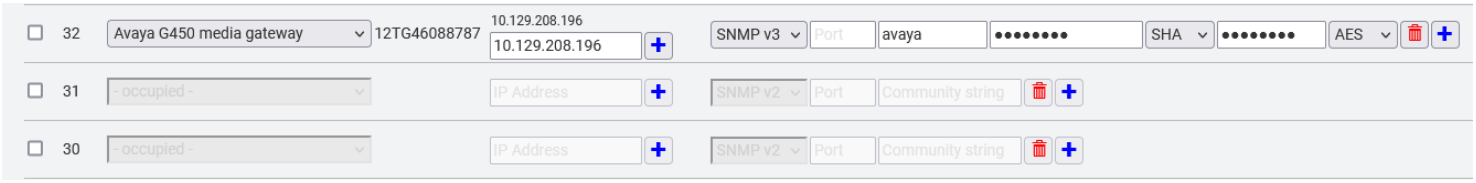
6. Click **Finish** to save the administered information. Depending on the number of devices and racks administered, this process may take 30 seconds or up to 10 minutes. The following message appears on successful completion.



SNMP v3 Configuration

1. Locate the rack and slot where you want to place the G450s.
2. Type the IP address for each device in the appropriate slot.
3. From the protocol drop down menu, select SNMPv3.
4. For the user name, enter *avaya.*
5. From the associated authentication key drop down menu, select SHA and enter and Authentication key of *avaya123.*
6. From the associated privacy key drop down menu, select AES and enter and Authentication key of *avaya123.*
7. After all the G450 components are administered, click **Save & Detect hardware** to confirm communication between AO and G450 devices.

   The hardware types and serial numbers are automatically detected and displayed in their corresponding slots.



   If there is undetectable administration entered, an error message appears.

Do the following to identify failed entry fields:

The fields that fail do not successfully detect the hardware type and serial number. The failed entries can be identified by the empty *Slot Device Description* fields alongside previously entered IP and SNMP information. If the administration error is known and can be rectified, do the necessary changes and click **Save & Detect hardware** after each change until all devices are accepted.

Do the following to remove unwanted entries:

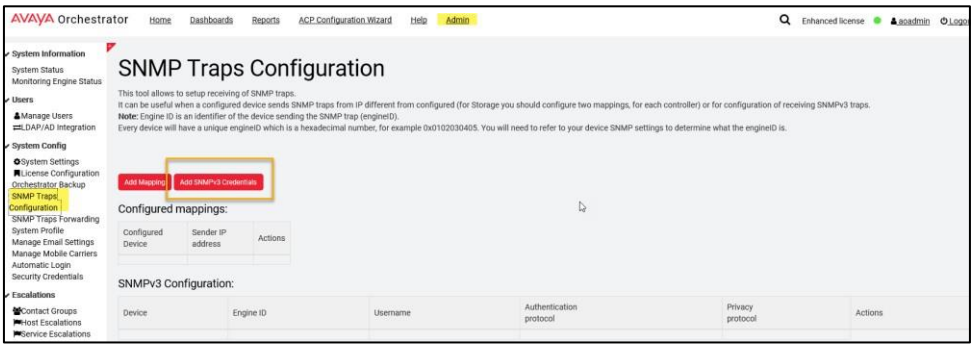
After you click **Save & Detect hardware**, any entry that is incorrect must be removed. For example, a wrong slot administered. Press the space bar in the **IP address** field to

remove the IP address, and then click **Save & Detect hardware**. AO removes all associated entry data from the form.

8. After the hardware administration is complete and all hardware is successfully detected and/or removed as needed, click **Next**.

9. Click **Finish** to save the administered information. Depending on the number of devices and racks administered, this process may take 30 seconds or up to 10 minutes. The following message appears on successful completion.

10. Go to Admin > SNMP Traps Configuration.



11. Click *Add SNMPv3 Credentials.*

12. From the Configured Device drop down menu, locate the IP address or FQDN of the gateway being administered.

13. Enter the Engine ID previously collected when administering SNMPv3 on the gateway.

14. Enter the user name *avaya.*

15. Select SHA as the Authentication Protocol from the drop down menu and enter the Authentication password *avaya123.*

16. Select AES as the Privacy Protocol from the drop down menu and enter the Authentication password *avaya123.*

17. Click *Add credentials*.

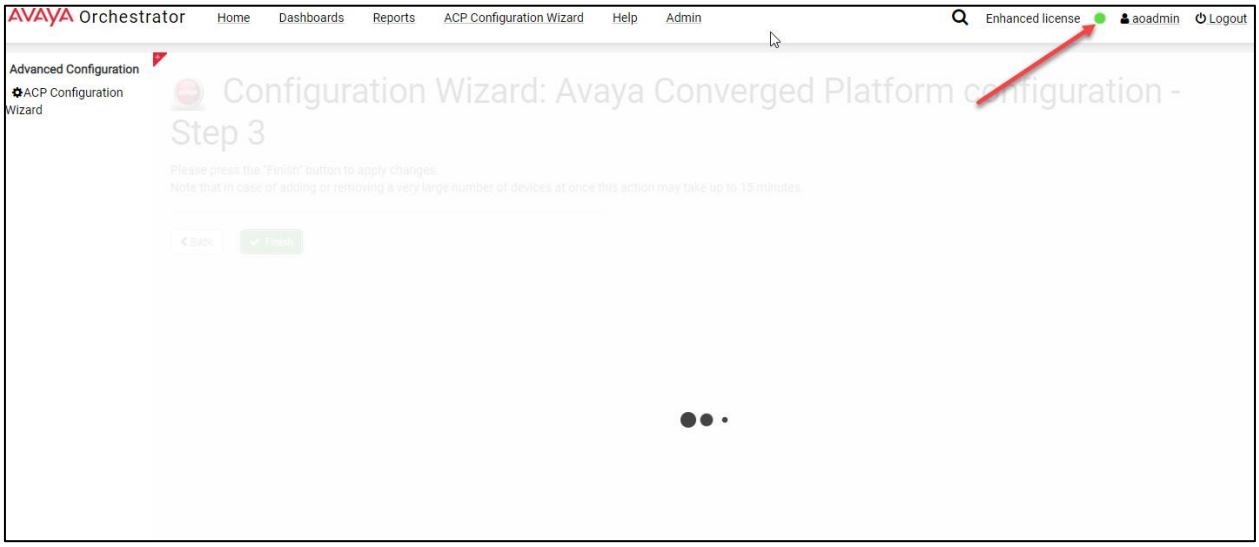
SNMPv3 Configuration:

Device	Engine ID	Username	Authentication protocol	Privacy protocol	Actions
10.129.208.196	0x8e003cdba800	avaya	SHA	AES	

Note:

While AO is in discovery mode, during the finishing process, the system will not be able to be accessed by other users.

While monitoring the session where the finishing process is in progress, the database connectivity button, in the upper right hand corner of the form, will go amber, and provide an idication of blocked connectivity. When the device discovery process is completed, DB connectivity is freed and access is again available and reflected in the radio dial button as a green status lamp.



Editing or deleting an ACP/ASP solution

About this task

Administrators can edit or delete an ACP solution or a rack any time after adding and administering the ACP solution and rack.

Procedure

1. Log on to Avaya Orchestrator™ by using administrative credentials.
2. On the menu bar, click **ACP Configuration Wizard**.
3. On the Step 1 page of the configuration wizard, click **Edit** or **Delete** corresponding to

the ACP solution or rack that you want to edit or delete.



Configuring DNS/FQDN information

For all AO releases:
Without the administration of FQDN host information, by default, all reports display only the source IP adnodress for each trap that is received or proactively collected. Therefore, to produce an easily distinguishable reference name for each trap/alarm, you must configure an FQDN or host name and DNS authentication for each element that is monitored.

For AO 1.5:
For certificates and licensing to work correctly, FQDN resolution is required. Therefore, implement one of the following procedures to support these functions.

Important:

If you want device names to appear, instead of IP address information, in all AO reporting output, you must create all DNS or /etc/hosts file entries **before** administering devices in the ACP Configuration Wizard.

If devices have already been administered into the Configuration Wizard, the subsequent administration of FQDN information in a DNS server or /etc/hosts file in AO will not provide the required device naming presentation. To display the FQDN information instead of the IP addresses, remove the devices from the Wizard and re-administer them, so that next time AO populates all related device tags, that is, an FQDN instead of an IP address.

Procedure

Option 1: Administer the FQDN information in a DNS server.

Based on the FQDN information provided in the Life Cycle Workbook (LCW)[1], administer the IP address

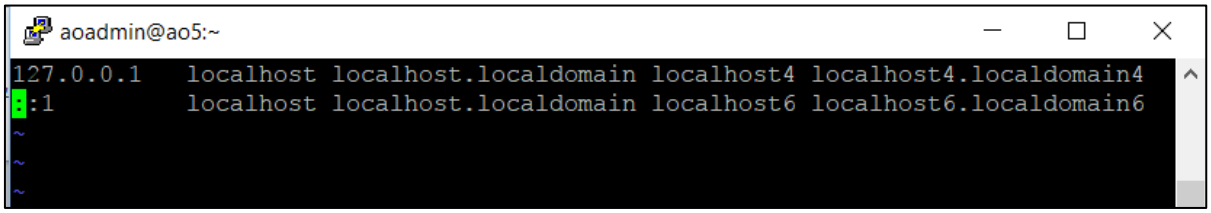
[1] The FQDN information in the LCW was used when deploying ASP 4200 devices.

and FQDN information for each ASP 4200 device node into a DNS server that supports the production environment. This information will be aligned with Avaya Orchestrator™ trap reporting output for each device.

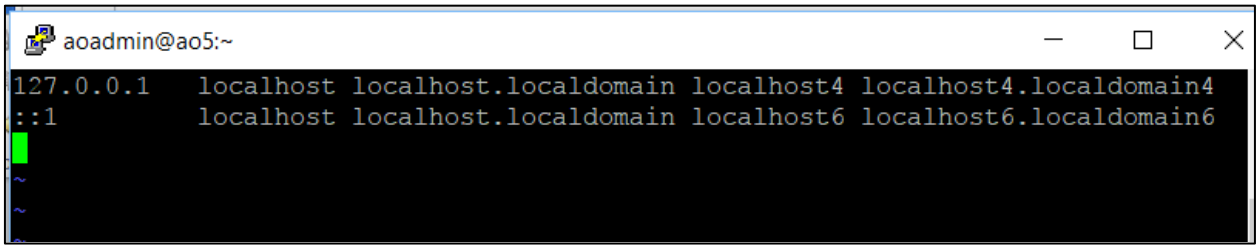
Option 2: Build an FQDN or host table inside Avaya Orchestrator™.

If a DNS server is not available for the environment, you can administer a table within the Avaya Orchestrator™ application to provide the same FQDN naming outcome. You can get the FQDN naming information for each node from the Life Cycle Workbook. Do the following:

1. SSH into Avaya Orchestrator™ by using the *aoadmin* login credentials from the Customer IP Template Workbook.
2. At the Linux prompt, type: *sudo vi /etc/hosts*
   The *hosts* file is opened for editing.
3. Use the arrow keys on your keyboard to move the cursor down to the bottom row of entries. Press the *Esc* key and then *o.*



The cursor repositions on a new line for you to insert the entries.



4. Use the following Linux vi procedure to update the *hosts* table:
   a. Type the IP address for the first device, and then press the *Tab* key.
   b. Type the host name and press the *Tab* key.
      Note: This host name is presented with each trap from the device.
   c. Type the associated FQDN/host entry. For example: net1dc1.avaya.com
   d. Press **Return** and type the information of the next host.
   e. After you type the final IP address, press **Esc** to stop the vi editing process.
   f. To write and save the file information, type *:wq!*
   g. To close the window, type *exit.*

Protocol requirements for hardware components

The following table contains protocol requirements for hardware components.

HW Type	HW Model	SNMP v1	SNMP v2c	SNMP v3	REST API	CLI API
Media	G450		Yes			
PDU	Sentry 3 smart		Yes			
PDU	Sentry 4 PIPS		Yes			
Ethernet Switch	VSP 7254XSQ		Yes	Yes		
Ethernet Switch	VSP 7400-48Y-8C		Yes	Yes		
Ethernet Switch	VSP 4850GTS		Yes	Yes		
Ethernet Switch	VSP 7024XLS		Yes	Yes		
Server	HPE Gen 8, Gen 9 and Gen 10 *ESXi element*		Yes	Yes	Yes	
Server	HPE Gen 8, Gen 9 and Gen 10 *iLO element*		Yes	Yes	Yes	
Server	Lenovo RD540 (IMM)	Yes				Yes
Server	Lenovo RD540 (ESXi)	Yes			Yes	
Server	Lenovo RD340 (IMM)	Yes				Yes
Server	Lenovo RD340 (ESXi)	Yes			Yes	
Server	Lenovo RD530 (IMM)	Yes				Yes
Server	Lenovo RD530 (ESXi)	Yes			Yes	
Storage	HPE Nimble CS1000		Yes		Yes	
Storage	EMC VNX3200e			Yes		Yes
Storage	EMC VNX5300	Yes				Yes

Managing rack devices

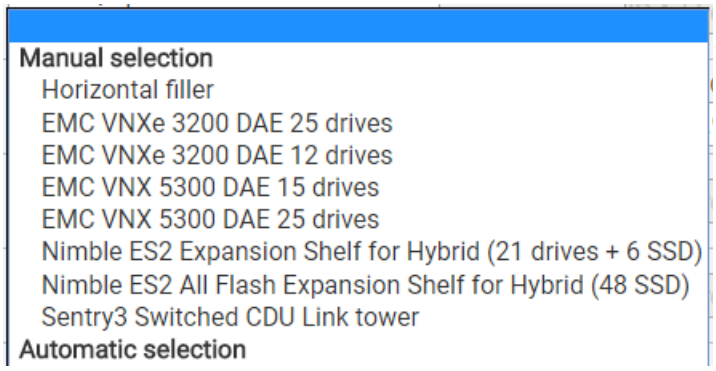
About this task

Along with adding new hardware elements, you might want to remove devices or edit the configuration. This topic contains information about additional editing options within the AO Configuration Wizard.

Procedure

1. Do the following to add a filler slot to the solution:
    i. Click **ACP Configuration Wizard**.
    ii. Click the slot in the diagram that corresponds to a slot targeted for a filler label.
    iii. To produce a filler panel, click the **Device Description** drop-down list to view the options.

    For reserving an empty slot for rack ventilation purposes or for future growth, click **Horizontal filler**.
    The other items noted are storage and PDU expansion elements that occupy slot space, but do not have their own IP addresses for event monitoring. After the primary/master devices are administered, AO shows a message that these partner devices must be administered manually.



    iv. Click **Detect hardware**.
    v. Click **Next**, and then **Finish**.

    The hardware type and serial number of the element are automatically displayed based on the information that you provide.

Note:

The *Failed to get device type* message appears if an error occurs during hardware discovery. Go to the Wizard entry form to confirm the IP address and protocol information/credentials and make the necessary rectifications, and then click **Detect hardware**.

2. Do the following to delete an element from the solution:
    i. Locate the element in the list.
    ii. Delete the associated IP address.
    iii. Click **Detect hardware**.

    The system clears the **Device description** and **Serial No** fields.

3. Click **Next**, and then click **Finish**.

Rediscovering a Single Device

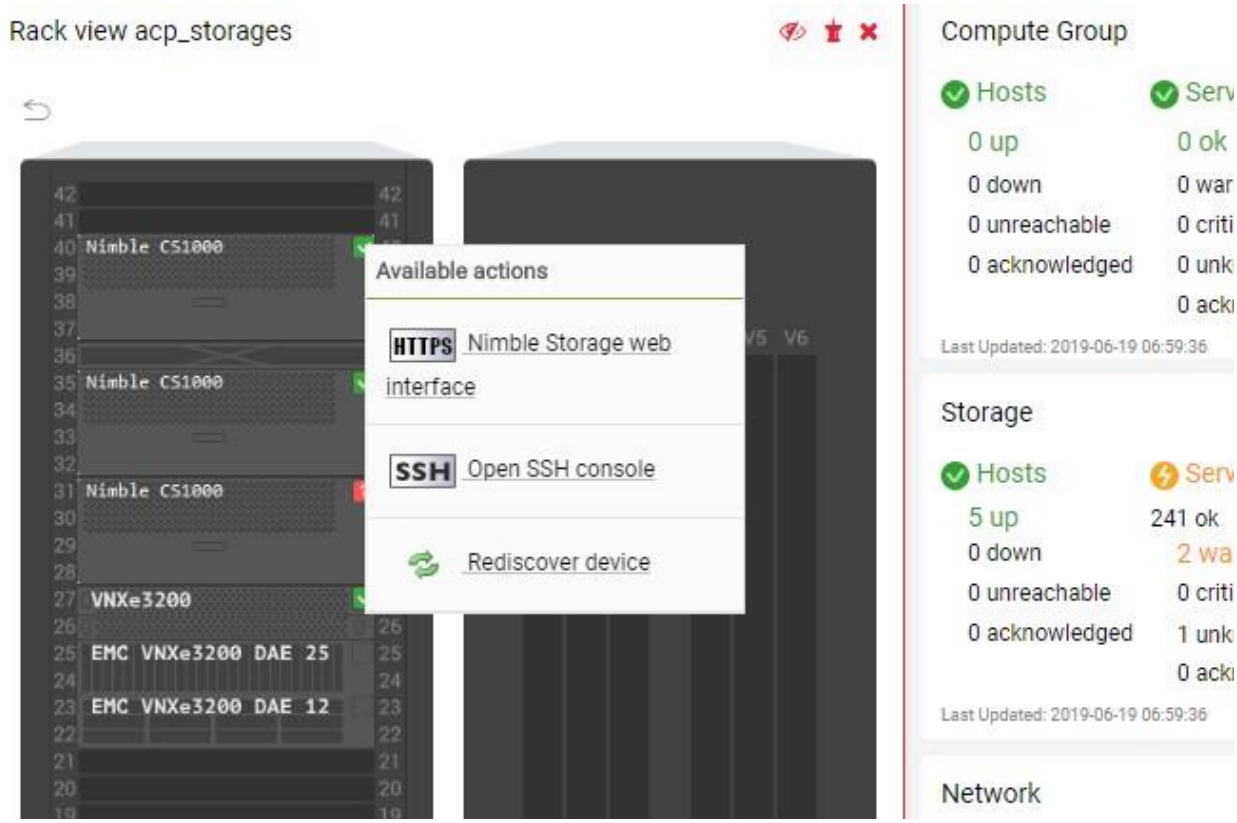
About this task

You can rediscover a single device from a Rack or a Device view. The Rediscovery process tries to recreate all device services without losing the previously collected data.

Procedure

1. Log on to the Avaya Orchestrator™ web interface by using administrative credentials.
2. Click **Home**.
3. Click the rack dashboard that contains the device that you want to rediscover.
4. Do any of the following:
   a. In the Rack dashboard view, right-click the device status icon corresponding to the device that you want to rediscover, and then click **Rediscover device**.
   b. In the Rack dashboard, click the rack that contains the device that you want to rediscover. In the Device dashboard view, right-click the device status icon in the device that you want to rediscover, and then click **Rediscover device**.

   The rediscovery process takes some time to complete.



Moving a device within the ACP solution

About this task

You can move devices within the ACP solution without losing previously collected data.

Note: If you click **Finish** in the **ACP Configuration Wizard** without moving a cut device in a slot, the device is removed from the ACP.

Procedure

1. Log on to the Avaya Orchestrator™ web interface by using administrative credentials.
2. Click **ACP Configuration Wizard.**
3. Select the rack that contains the device that you want to move, and then click **Next**.
4. Click **Cut device**  corresponding to the device that you want to move.
5. If you want to move the device to another rack, navigate to the rack and open the rack.
6. Click **Paste device**  corresponding to the empty slot where you want to move the device.

You can cut multiple devices from a rack at one time. Avaya Orchestrator™ displays the list of cut devices in the **Buffer** field in the **ACP Configuration Wizard**. You can select the device in the **Buffer** field, and then click **Paste device** corresponding to the slot where you want to move the device.

Chapter 5: License Configuration

Overview

This chapter provides information about configuring primary and secondary WebLM server addresses and checking the licenses availability.

Avaya professionals must complete the initial customer configuration and licensing for the application. All required licensing is applied during product installation. For more information about licensing, contact your Avaya sales representative.

Configuration of server URLs

Important:

The modification of WebLM server URLs is completed after pressing the **Update settings** button. Leaving the page by back spacing, or via a web UI time-out, results in the loss of all new configuration.

License type

The **License configuration** page contains information about the current types of the licenses available to Avaya Orchestrator™. The following types of licenses are available:

- Trial license
- Basic license
- Basic license, grace period
- Enhanced license
- Enhanced license, grace period

The Avaya Orchestrator™ license life cycle starts from the trial license. This license is automatically activated during the first boot of the operating system after the VM deployment or an upgrade from 1.4 version.

The Trial license is active for 30 days and allows all Avaya Orchestrator functionalities available under the Basic license. This consists of adding devices via the **ACP Configuration Wizard** and monitoring their states.

When a Trial license expires, the access to the **ACP Configuration Wizard** and all other pages except the **License configuration** page is blocked. You cannot monitor any configured devices in this case.

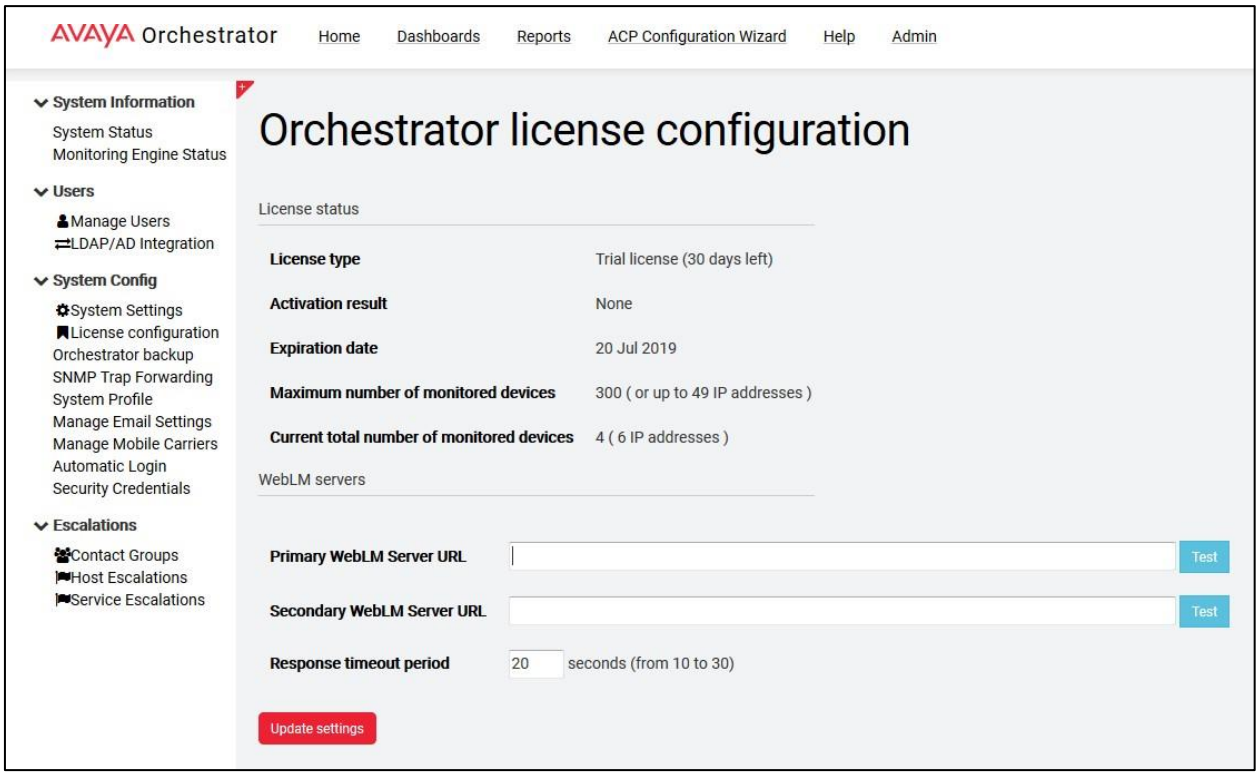
A Trial, Basic, or Enhanced license allows monitoring up to 300 devices or 300 IP addresses.

ACP Configuration Wizard will reference the maximum number of devices and IP addresses allowed by the configured license; when a capacity is reached, the Wizard will block all additional device deployments by not offering the “Finish” administration option.

An Enhanced license has the following additional functionalities over a Trial or Basic license:

- SNMP traps forwarding (**Admin > System Config > SNMP Trap Forwarding**)
- Custom dashboards (**Dashboards > Manage Dashboards** and **Dashboards > Deploy Dashboards**)
- Notification escalation (**Admin > Escalations**)

When Avaya Orchestrator™ obtains a Basic or an Enhanced license from the WebLM server, but the server is temporarily unavailable or your license has expired, AO provides a grace period of 30 days. The period starts immediately upon encountering a license-detect-failure issue. During this period, all normal functionalities allowed by the license type are still available. If the license is not renewed, or the connection to the WebLM server is not restored after this period ends, the license will be set to Expired Basic license or Expired Enhanced license based on your license type. The functionalities available for the active license are still allowed; however, the access to the ACP Configuration Wizard is blocked and device rediscovery is not possible. During the grace period, the Expiration date field in the License Configuration page displays the end date of the grace period.



Installing AO License

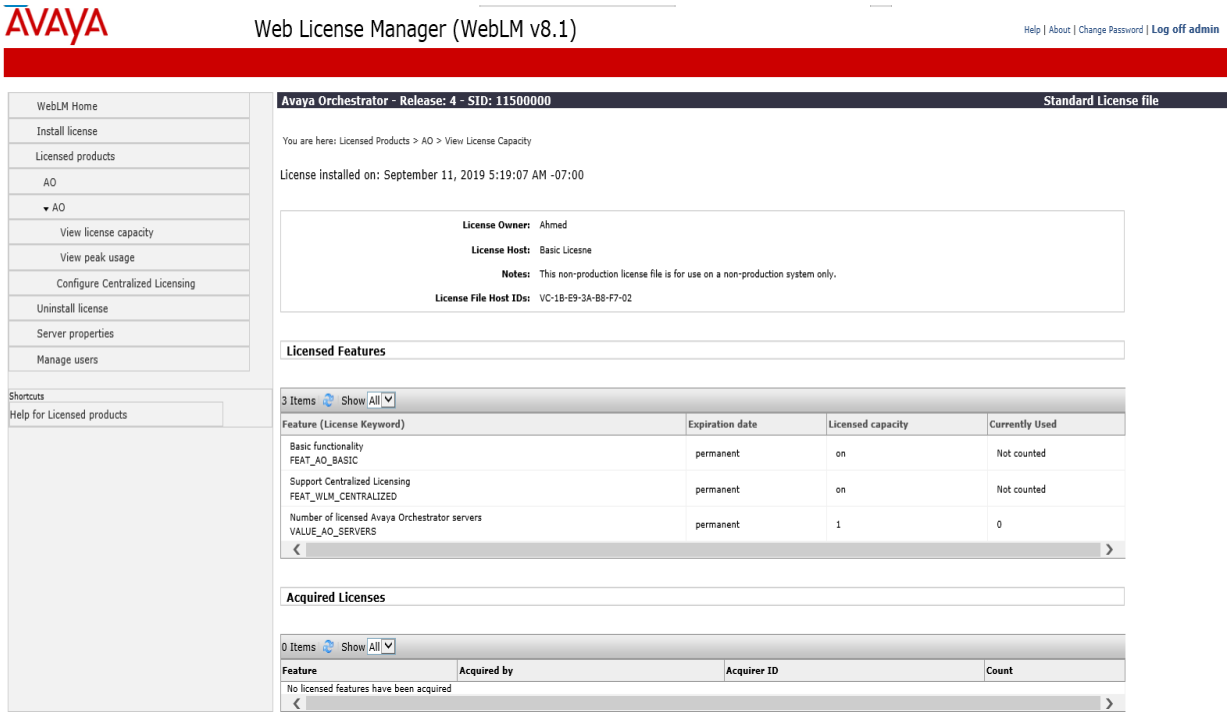
The following procedures explain how to install Avaya Orchestrator™ in Standalone WebLM and on SMGR Integrated WebLM.

Installing AO license in Standalone WebLM

Procedure

1. Open a web browser and launch WebLM server: <FQDN/IP address:52233/WebLM>
2. Login using administrative credentials.
3. Click **Install license**.
4. Click the browse option and select the desired license file.
5. Accept the **License Terms and conditions**.
6. Click **Install**.
7. In the left navigation pane on the WebLM page, click **AO** to verify if the license has installed successfully.

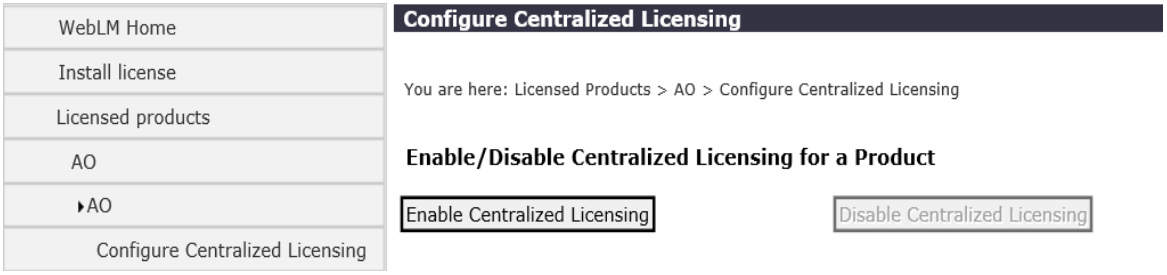
Note: Ensure that you download the license file to your PC prior to proceeding with the license application.



Configuring Centralized licensing on WebLM server

Procedure

1. Open a web browser and launch: https to SMGR <FQDN/IP address > / Standalone WebLM <FQDN/IP address:52233/WebLM>
2. Login using administrative credentials.
3. For SMGR integrated WebLM, navigate to **Services** > **Licenses**.
4. Click **Configure Centralized Licensing**.
5. Click **Enable Centralized Licensing**.

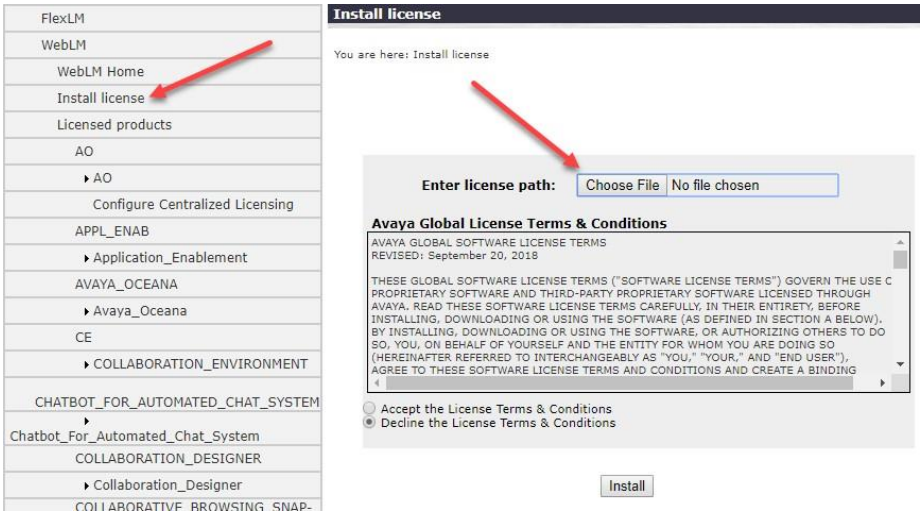


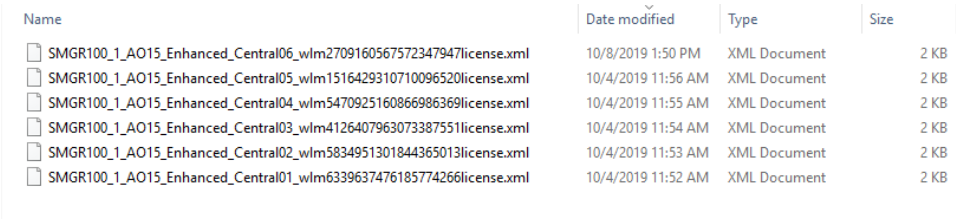
Installing AO license on SMGR Integrated WebLM

Procedure

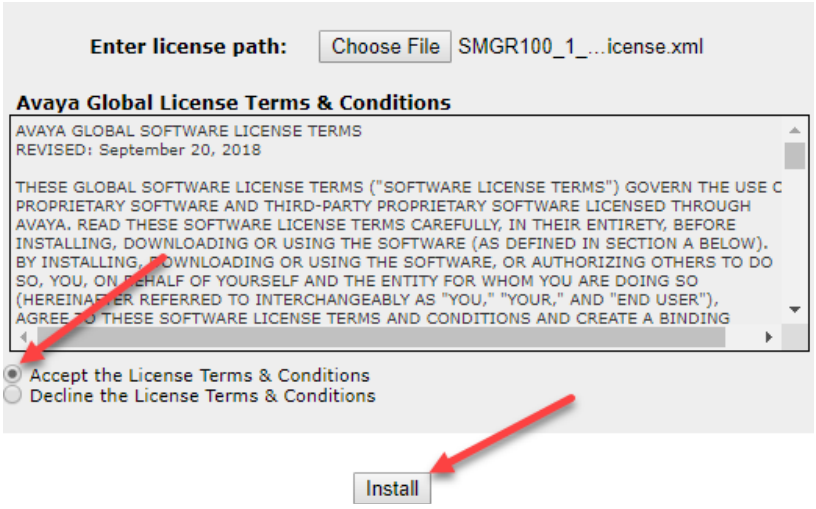
Your PC must be on the customer network and have access to the customer SMGR to be able to install the license.

1. Download the appropriate AO license from the PLDS website.
2. Open a web browser and launch SMGR Page: https to SMGR <FQDN/IP address >
3. Login using administrative credentials.
4. Navigate to **Services** > **Licenses**.
5. From the left pane menu list, click **Install license**.
6. Click the **Choose File** browser and select the desired license file.

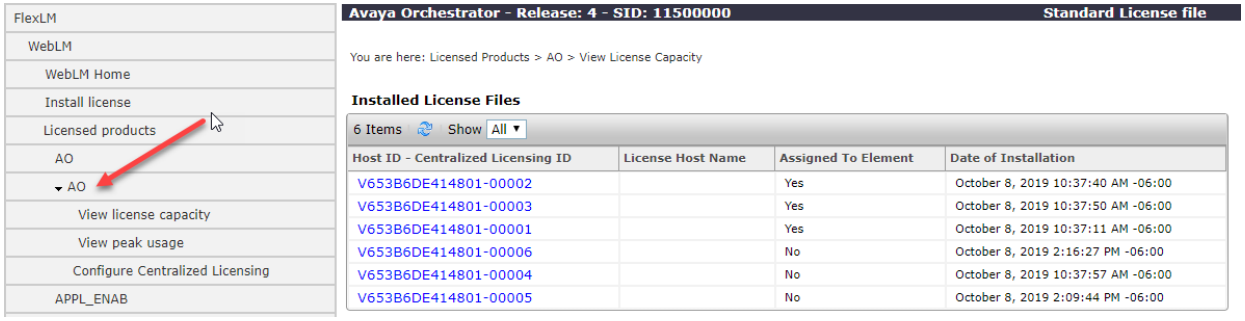




7. Accept the License Terms and conditions.
8. Click **Install**.

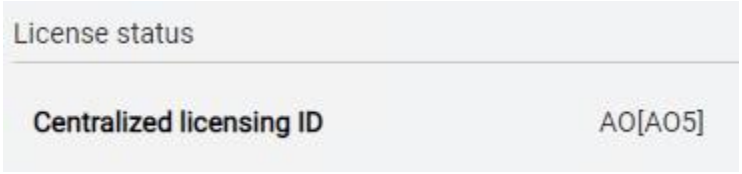


9. Resulting output should display “License file installed successfully”.
10. In the left navigation pane, click **AO** to verify if the license has installed successfully.



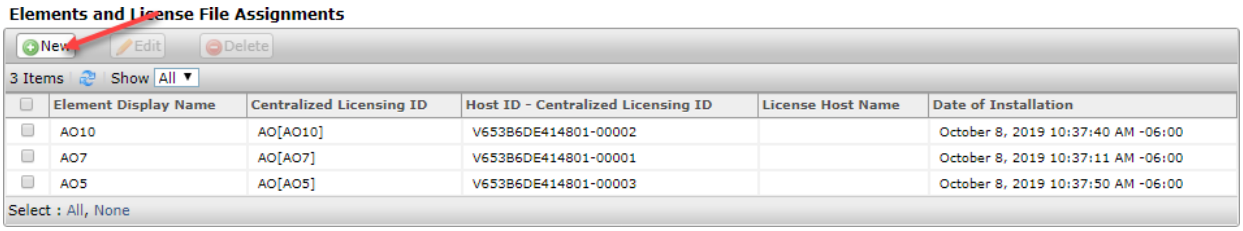
11. Get the AO Centralized Licensing ID to make association between the element instance and the license file.
    a. Login to AO Application: https://<IP address/FQDN>
    b. Login *with aoadmin* user and password.
    c. Navigate to **Admin** > **License Configuration**.
    d. Copy the **AO Centralized License ID**.

Example: The ID consists of **AO** + **[AO** + (host name)

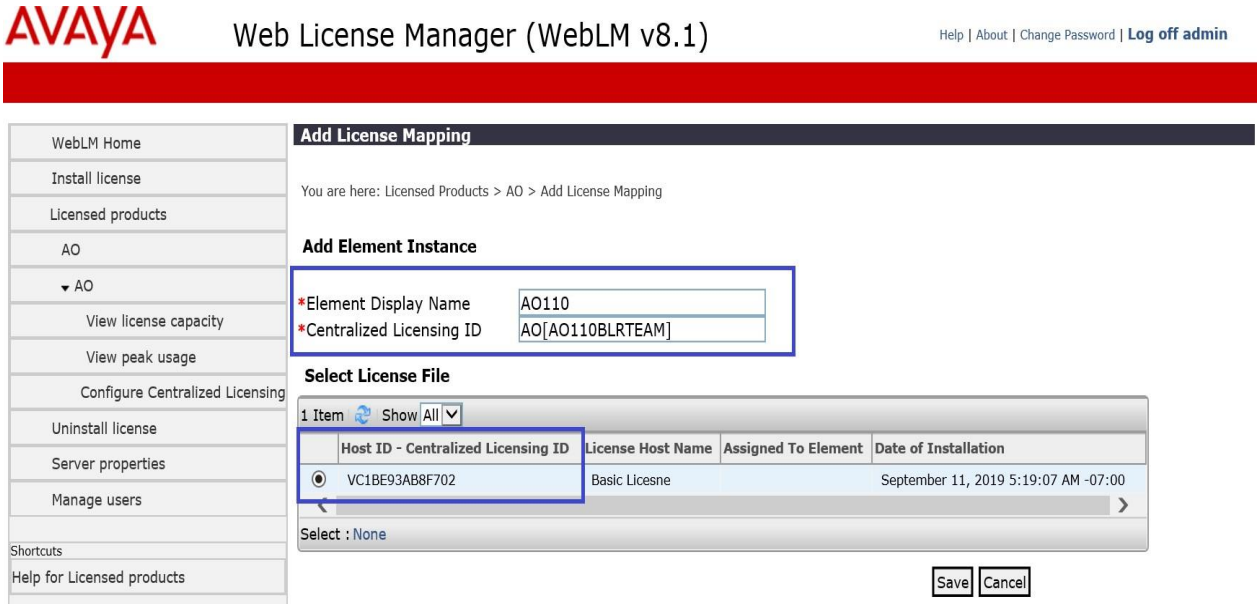


Avaya Orchestrator™ License Configuration Page

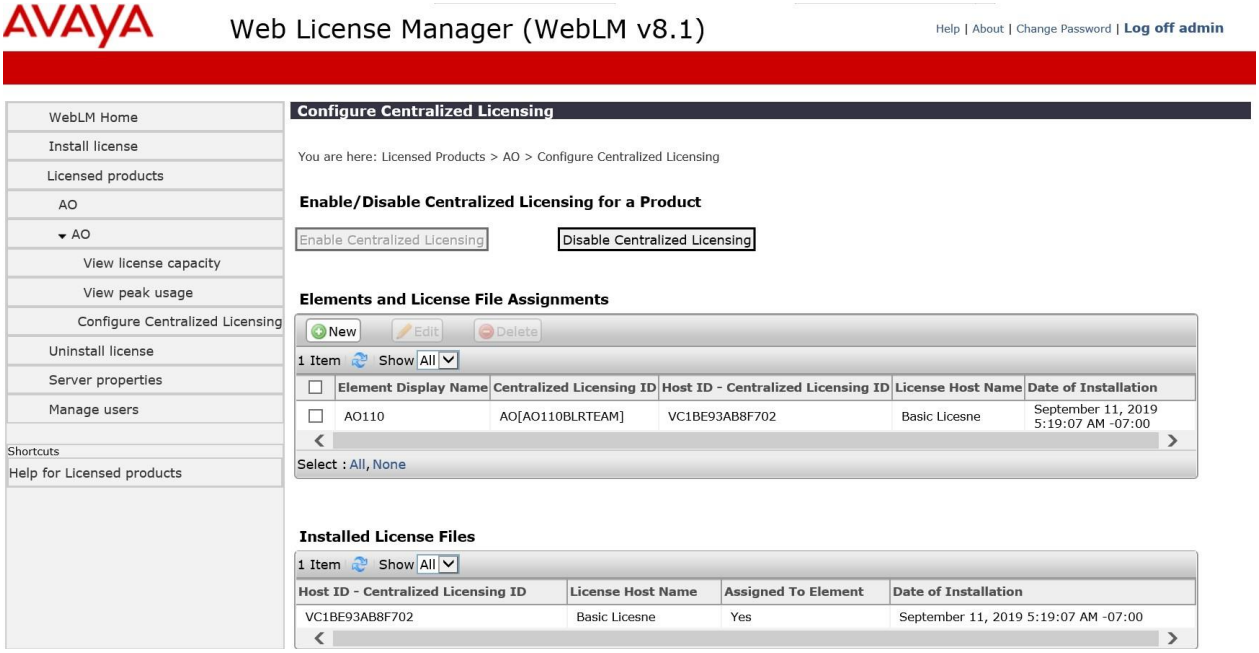
12. Return to SMGR WebLM. From the left navigation pane, click **Configure Centralized licensing**.
13. Click **New** under **Elements and License File Assignments**.



14. Enter **Element Display Name.**
15. Enter AO Centralized Licensing ID.
16. Select License file to associate with the configured element Instance.
17. Click **Save.**



You can see that the association has been made between the element instance and the license file.



Configuring license on Avaya Orchestrator™

Procedure

1. Log in to Avaya Orchestrator™ application:

   https://<IP address/FQDN>
2. Login using administrative credentials (*aoadmin*).
3. Navigate to **Admi**n > **License Configuration**.
4. In the **Primary WebLM Server URL** field**,** type the URL of WebLM server.

   Syntax: <IP address/FQDN:52233/ WebLM/LicenseServer>

   For example:

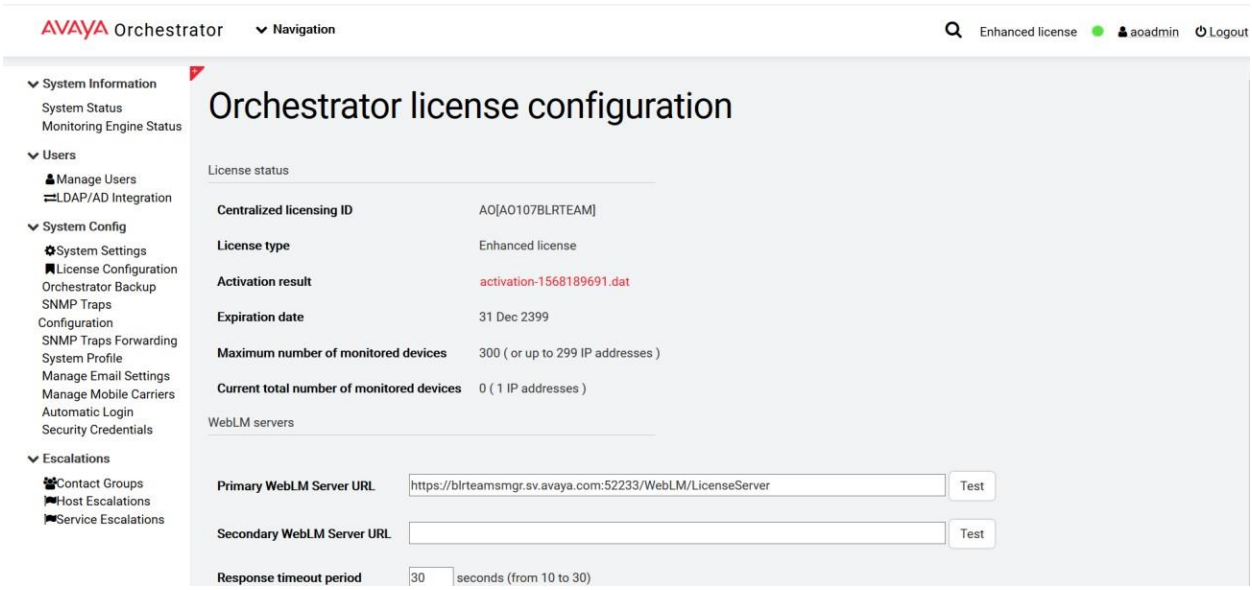
   https://10.129.100.97:52233/WebLM/LicenseServer

   or

   https://blrteamsmgr.sv.avaya.com:52233/WebLM/LicenseServer
5. Click **Test** to confirm if the WebLM server is reachable from Avaya Orchestrator™.



6. Click **Update settings** to apply the new settings.

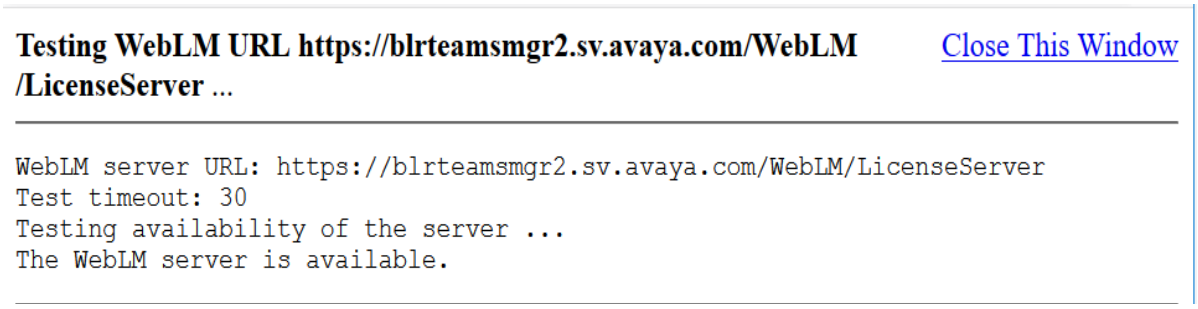


7. Secondary WebLM Server URL is optional. If the secondary WebLM URL is available, enter the URL in the Secondary WebLM Server URL field:

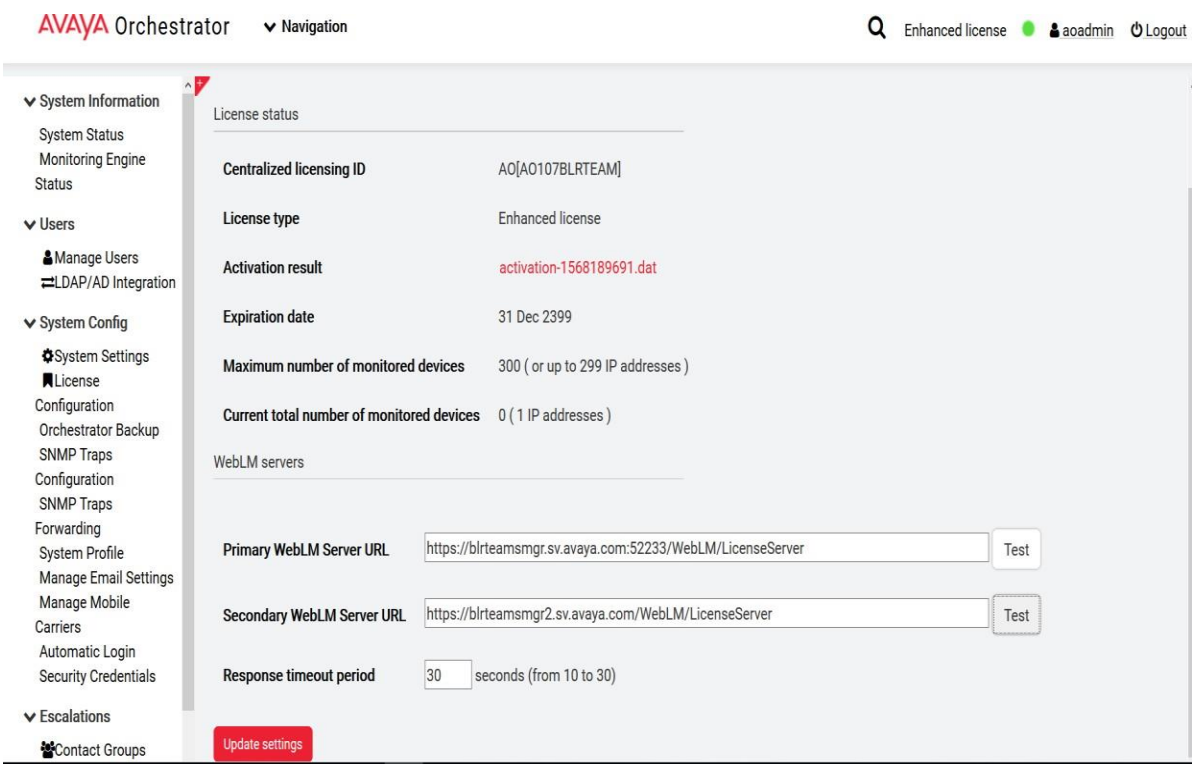
   <IP address/FQDN:52233/ WebLM/LicenseServer>

   For example:
   https://10.129.100.98:52233/WebLM/LicenseServer
   or
   https://blrteamsmgr2.sv.avaya.com:52233/WebLM/LicenseServer

8. Click **Test** to confirm if the WebLM server is reachable from Avaya Orchestrator™.



9. Click **Update settings** to apply the new settings.



Note: The green circle notifies a successful connection between WebLM server and AO, and the Amber color notifies that the connection is temporarily lost.
When backup is taken as part of the trial license, the license temporarily shows expired, however after a few seconds, it shows the correct information. Similarly, when processing the entered information during configuration of the rack using wizard, the connection between WebLM and AO can display amber for a temporary period, however, it shows successful connection afterwards.

Chapter 6: Setting up HTTPS

Overview

This chapter provides instructions for configuring a secure access to the web UI of Avaya Orchestrator™. For Secure access, it is necessary to generate a certificate that further needs to be signed by a Certificate Authority (CA).

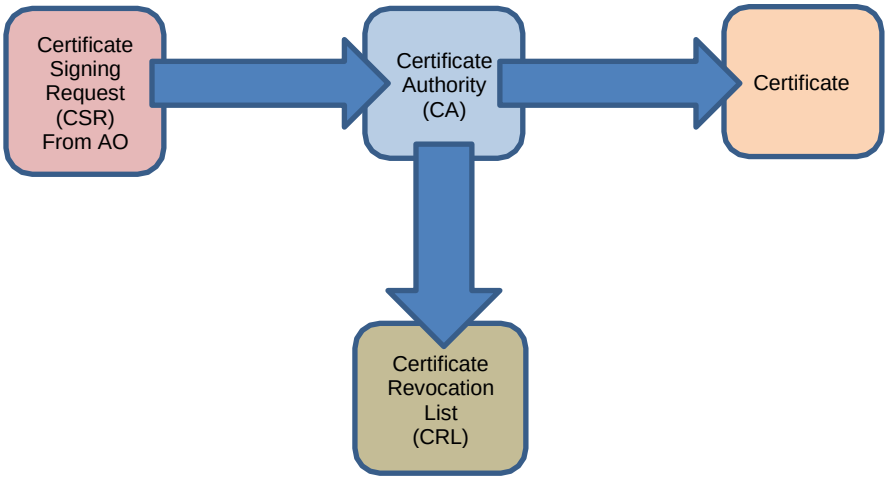
The CA can be any of the following authority:

- A trusted company like VeriSign
- An internal CA that is part of your IT infrastructure, like a Microsoft Windows CA, Avaya Aura System Manager, SMGR etc.
- The Avaya Orchestrator™ server itself. This method produces a self-signed certificate, which is not accepted as a secure protection by browsers. Therefore, this is the least preferred way.

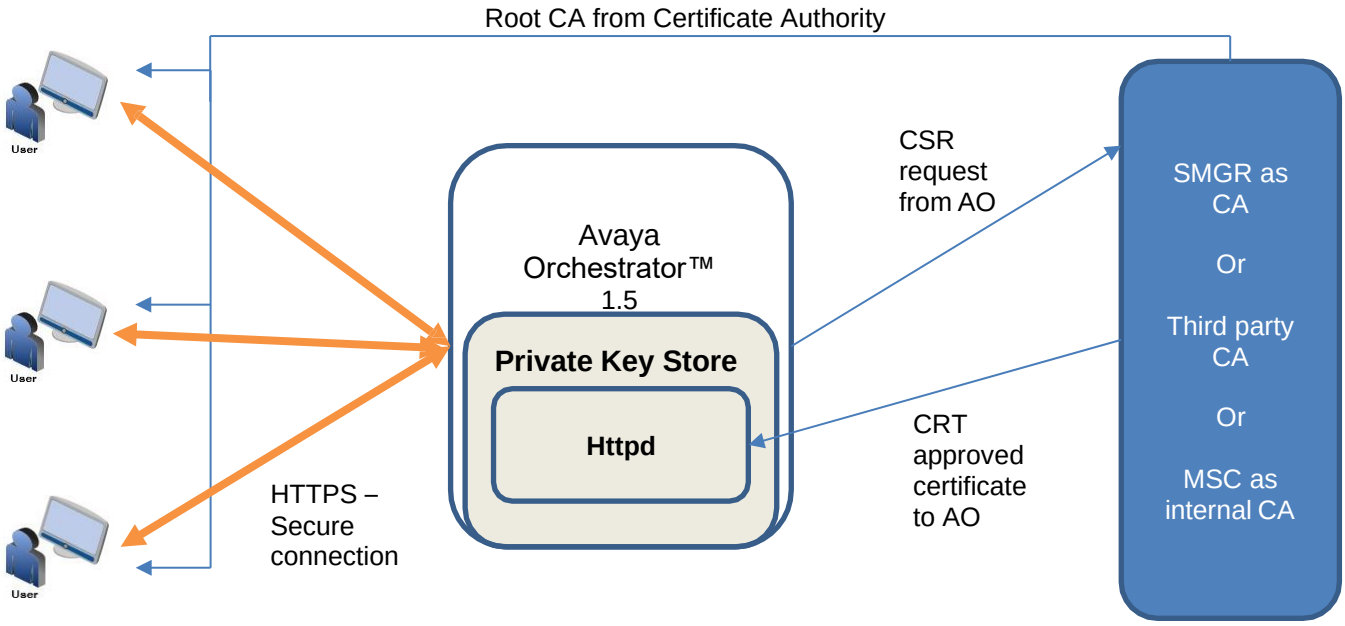
Secure Sockets Layer (SSL)

Secure Sockets Layer (Transport Layer Security (TLS) more accurately) is the technology that you can use for a secure connection. The root certificate, often called a trusted root, is at the center of the trust model that provides support for the Public Key Infrastructure issued by trusted Certificate Authority.

In the SSL ecosystem, you can generate a signing key and sign a new certificate with that signature. The certificate is considered valid only when it gets directly signed by a trusted Certificate Authority (CA). To validate the certificate, the device compares the certificate issuer with the list of trusted CAs. If there is no match, the client checks to see if the certificate of the issuing CA was issued by a trusted CA, and this continues until the end of the certificate chain where the root certificate issued by a trusted Certificate Authority is found. The following image shows the HTTPS communication from Root CA and AO:



The image shows Certificate Authority in Avaya Orchestrator™:



The certificate identifies and authenticates the AO servers used by the web users and the client web browsers using the protocols HTTPS and TLSv1.2.

Setting up HTTPS Certificate

The following procedures explain how to set up the HTTPS access for a secure connection with Avaya Orchestrator™.

Creating the Certificate

Procedure

1. Log in to Avaya Orchestrator™ by using SSH and **aoadmin** credentials.
2. Run the following command to change user to superuser `root`:
   Type `su -` and then type the `root` password.
3. Run the following command to change the current directory:
   `cd /usr/local/nagiosxi/var/certs/`
4. Run the following command to generate a private key:
   `openssl genrsa -out ao.key 2048`

5. Perform the following steps to create the configuration file for generating certificate sign request.

   Note: You can execute this process directly within AO by using the `vi`text editor.

   a. In a text editor (for example, Notepad or WordPad), copy the following content as is:

```
[ req ]
days                = 365
req_extensions      = req_ext
distinguished_name = req_distinguished_name
prompt              = no

[req_distinguished_name]
countryName             = <2 letter code>
stateOrProvinceName     = <full name>
localityName            = <city name>
organizationName        = <company name>
organizationalUnitName = <section name>
commonName              = <FQDN / IP address>
emailAddress            = <email address of the contact
person>

[req_ext]
subjectAltName    = @alt_names

[alt_names]
IP.1 = <IP address>
DNS.1   = <FQDN>
DNS.2   = <short host name>
```

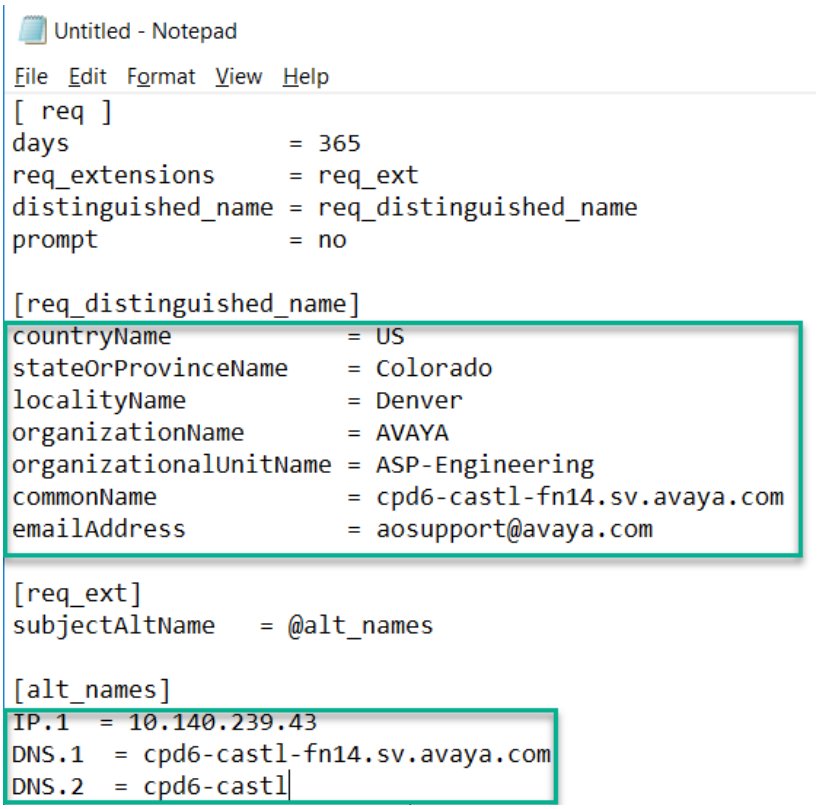
   b. Edit the content in the following fields as follows:

      Remove lines in the '[req_distinguished_name]' section with an empty value. Otherwise, an error 'string too short' appears during the CSR generation.

      `countryName:` Type the two-letter country code without the punctuation. For example, `US`.
      `stateOrProvinceName:` Type the name of the state or province. For example, `Colorado`.
      `localityName:` Type the name of the city. For example, `Denver`.

organizationName: Type the name of the organization.
For example, AVAYA.
OrganizationalUnitName(Optional): Type the name of the of the department or organization unit making the request.
For example, IT,Engineering
commonName: Type the Fully Qualified Domain Name or IP address of the Avaya Orchestrator™ server.
For example, ao.avaya.com
emailAddress(Optional): Type the email address of the contact person responsible for Avaya Orchestrator™ or customer IT department.
For example, aosupport@avaya.com
IP.1: Type the Avaya Orchestrator™ IP Address.
For example, 10.10.10.45
DNS.1: Type the Fully Qualified Domain Name of the Avaya Orchestrator™ server.
For example, ao.avaya.com
DNS.2: Type the short, hostname for the Avaya Orchestrator™ server.
For example, ao

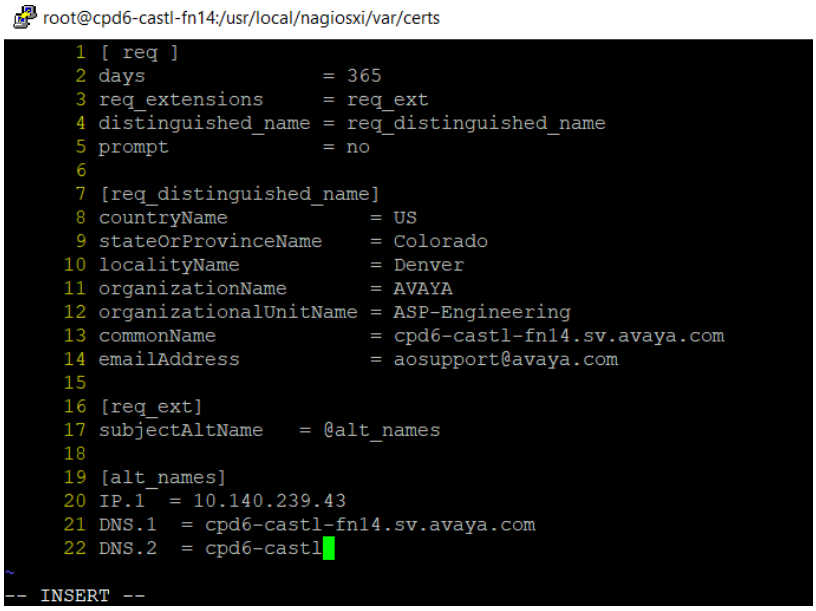
Following image is an example of an edited configuration file:



c. Return to the AO SSH session and run the following commands to create the configuration file needed to generate the certificate sign request:

- `vi v3csr.config`
- Type `i` to enable the insert function of the visual editor.
- Copy the edited content from notepad and paste it into the new file. Right-click to paste the data into the SSH session box if you are using Putty.

The following image shows an example of `v3csr.config` file from the Putty:



- Press `Esc` to exit from the insert mode.
- Type: `:wq!` to save new `v3csr.config` file.

6. Run the following command to generate the certificate sign request using the configuration file created in the previous step:

```
openssl req -new -key ao.key -out ao.csr -config v3csr.config
```

7. Perform the following steps to save certificate sign request locally in computer:
   a. Run the command: `cat ao.csr`
   b. Copy the entire content, including `-----BEGIN CERTIFICATE REQUEST-----` and `-----END CERTIFICATE REQUEST ------`and provide the Certificate Authority.
   c. Paste the content into a new notepad and save file as `ao.crt`

Getting certificate sign request signed by a trusted company

Procedure

1. If a trusted company (for example, VeriSign) is used to get the csr signed, provide the `ao.crt` file obtained in the previous step.
2. If the Certificate Authority has returned the certificate in a different extension other than `.crt`, convert certificate to `.crt` before installing within AO.

   Use the following procedure to convert a certificate with a different extension to `.crt`:

   a. Transfer the certificate received from CA to AO using any desired tool. Use **WinSCP** if you are using a windows computer or use **scp** if you are using linux/RHEL machine.

   Note: Certificate can be transferred to either `/tmp` or `/home/aoadmin` directory.

   b. Open an SSH session to AO with any desired tool such as Putty.

   c. Login using the `aoadmin` credentials.

   d. Run the following command to change user to superuser root:

      Type `su -` and then type the `root` password.

   e. Run the following command to change directory to the location of certificate
   cd /<certificate_path> example: `cd /home/aoadmin | cd /tmp`

   f. Run the following command to convert the respective certificate to `.crt`:

   Certificates with `.p12` extension

   ```
   openssl pkcs12 -in <filename>.p12 -clcerts -nokeys -out
   ao.crt
   ```

   Certificates with `.pfx` extension

   ```
   openssl pkcs12 -in <filename>.pfx -clcerts -nokeys -out
   ao.crt
   ```

   Certificates with .cer extension

   ```
   openssl x509 -inform der -in <filename>.cer -out ao.crt
   ```

   Certificates with .der extension

   ```
   openssl x509 -inform der -in <filename>.der -out ao.crt
   ```

   Certificates with .p7b extension

   ```
   openssl pkcs7 -print_certs -inform der -in <filename>.p7b -
   out ao.crt
   ```

Certificates with .pem extension

```
cp <filename>.pem ao.crt
```

3. Run following command to replace the existing `ao.crt` with the one recently converted:

   ```
   cp /<directory>/ao.crt /usr/local/nagiosxi/var/certs/
   ```

Note: Type `Y` for overwrite confirmation.

4. Proceed to next section to complete the certificate procedure.

Getting Certificate Sign Request (CSR) signed by the System Manger as the Certificate Authority

Pre-requisites

- Access System Manager server prior to conducting the activity.
- Transfer the `ao.crt` file saved in the previous step in a location accessible to the System Manager.

Procedure

1. Using a Web browser, access **Avaya Aura System Manager**.
2. Login with administrative credentials.
   For example, **admin**
3. Navigate to **Service**s > **Security** > **Certificates** > **Authority.**
4. Under RA Functions, select **Add End Entity .**
5. Enter the following information in the respective fields:

Username

a. **End Entity Profile**: `EXTERNAL_CSR_PROFILE`
b. **Username**: Enter any desire username.
   For Example, `aoadmin`
c. **Password** (or Enrollment code): Enter any desire password.
   For Example, `avaya123`
d. **Confirm Password**: `avaya123`
e. **E-mail address** (optional): Same value from `v3csr.config`

Subject DN Attributes

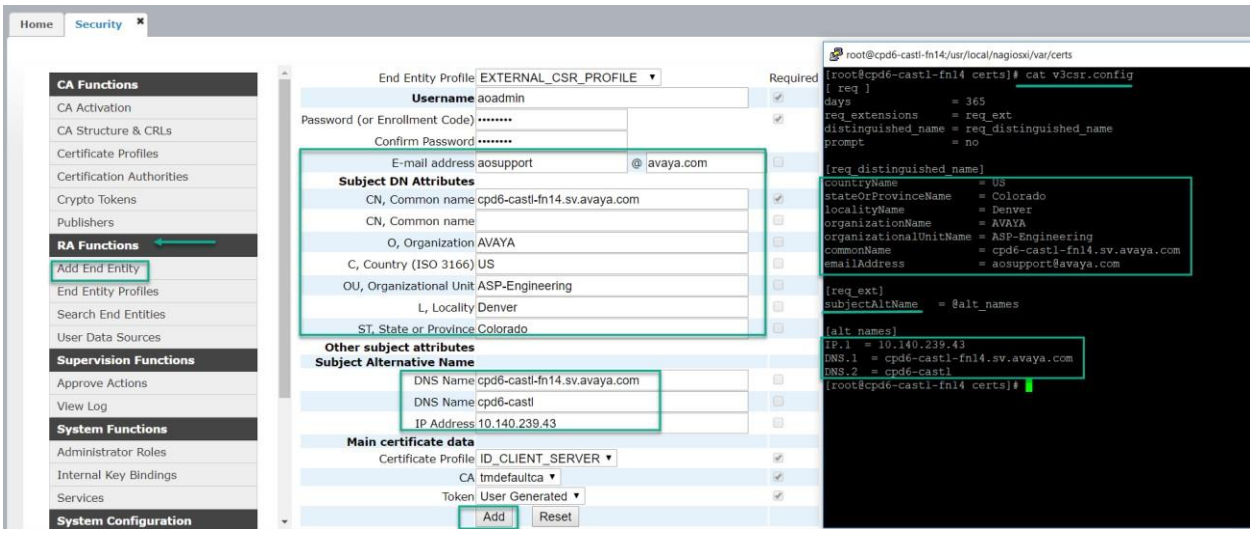
a. **CN, Common name**: Same value from `v3csr.config`
b. **O, Organization**: Same value from `v3csr.config`

c. **C, Country (ISO 3166)**: Same value from `v3csr.config`
d. **OU, Organizational Unit** (optional): Same value from `v3csr.config`
e. **L, Locality**: `v3csr.config`
f. **ST, State or Province:** Same value from `v3csr.config`

Subject Alternative Name

a. **DNS Name**: Enter DNS.1 value from `v3csr.config`
b. **DNS Name**: Enter DNS.2 value from `v3csr.config`
c. **IP Address**: Same value from `v3csr.config`

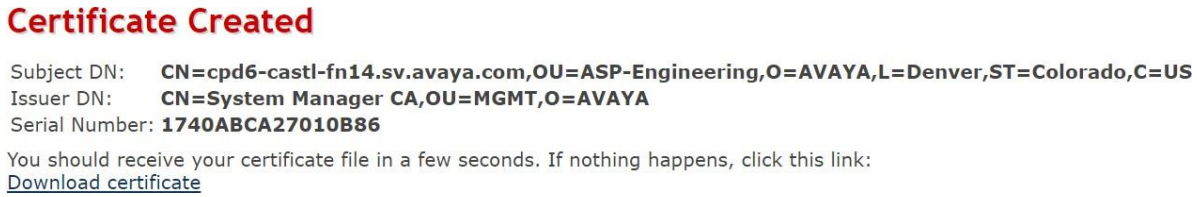
The following image shows the completed fields using the values from the `v3csr.config` created in the previous steps:



6. Click **Add** when ready to create the new Entity.
7. From the menu on the left pane, select **Public Web**. A new tab opens.
8. From the **EJBCA** webpage, select **Create Certificate from CSR** under **Enroll**.
9. Enter the following information:

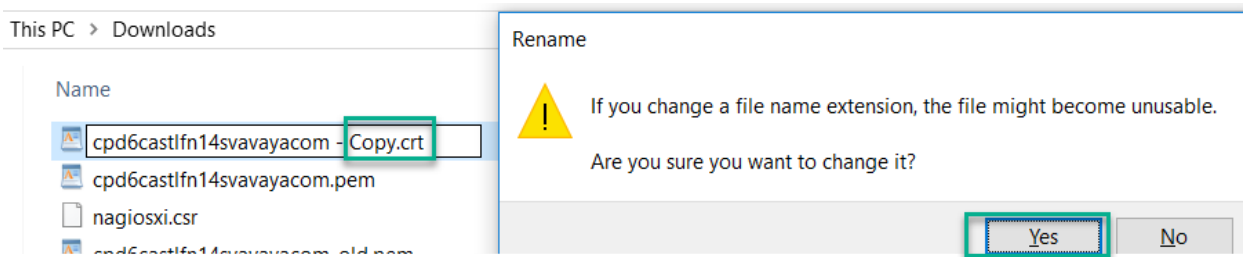
   a. **Username**: Use the name configured while creating the `EXTERNAL_CSR_PROFILE`.
   b. **Enrollment code**: Use the name configured while creating the `EXTERNAL_CSR_PROFILE`.
   c. **Request file**: Select `Choose File` to import the `ao.crt` file saved locally in the computer in the previous steps.
   d. **Result type**: From drop-down menu, select `PEM-certificate only`
   e. Select **OK** to generate the certificate.

A certificate is created and downloaded automatically to the computer from where the request is issued.

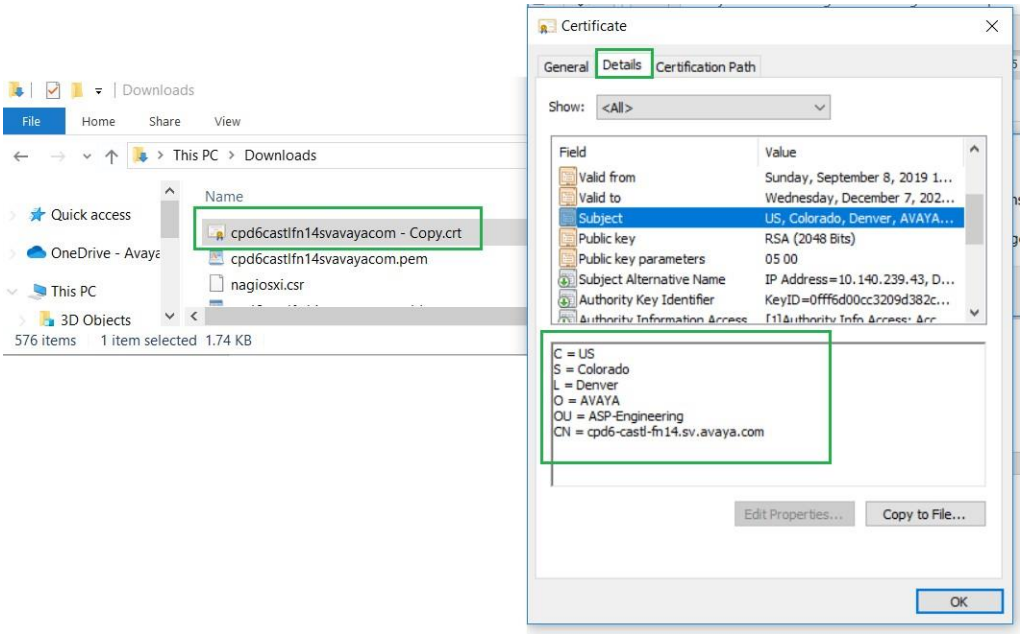


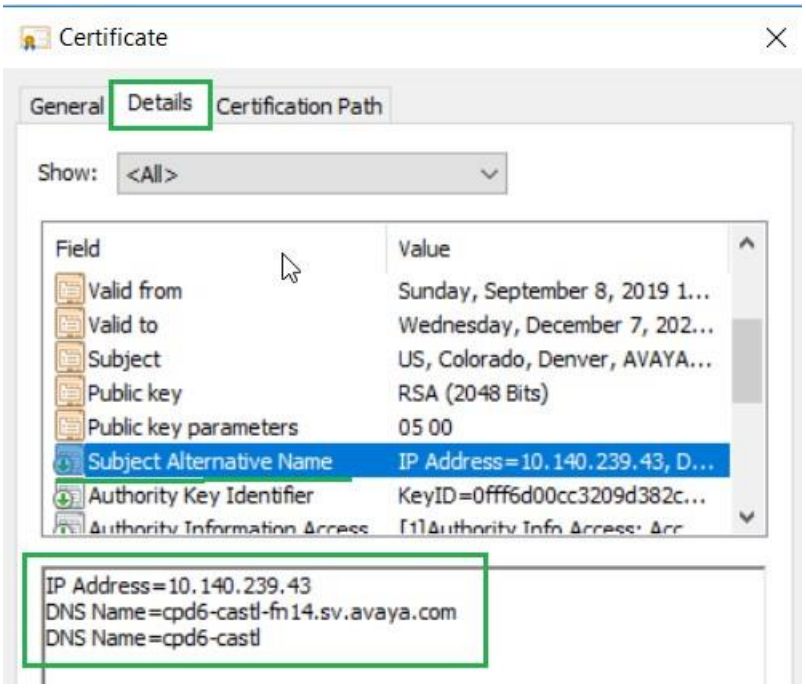
10. Navigate to the location where certificated is downloaded.
11. Create a copy of the `pem` file and change the extension to `.crt`.

Note: This step validates the input entered by the user when generating the CSR.



12. Double-click the `.crt` file and validate the information in the certificate to ensure that the information is correct before proceeding. Once the validation is complete, click **OK** to close the file.





13. Double-click to open the original `.pem` obtained in the previous step.
    For Example, cpd6-castl-fn14svavayacom.pem

Note: If the computer doesn't recognize the extension to open the `pem` file, select a text editor such as WordPad to open the file.

14. Copy the entire content including
    `-----BEGIN CERTIFICATE REQUEST-----` and `-----END CERTIFICATE REQUEST-----`

15. If you are not connected already, open an SSH session to AO with any desired tool such as Putty.

16. Log in in using the **aoadmin** credentials.

17. Run the following command to change user to superuser `root`:
    Type `su -` and then type the `root` password.

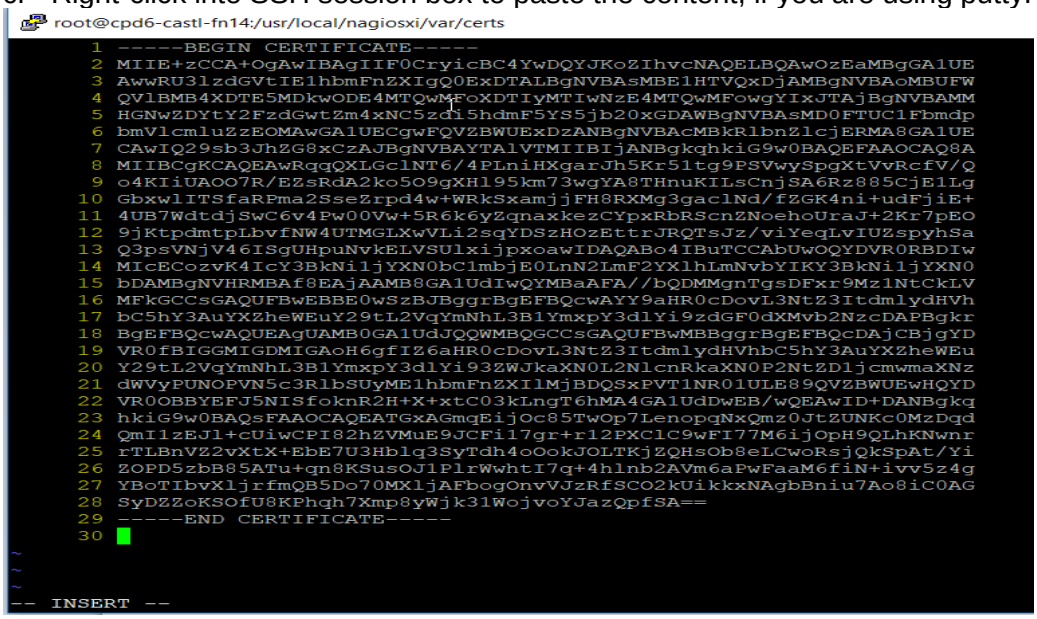
18. Run the following command to change the current directory:
    `cd /usr/local/nagiosxi/var/certs/`

19. Type the following command to empty the content of existing `ao.crt` file:
    `true > ao.crt`

20. Type the following commands to paste the content from the `pem` file to the `ao.crt` file:

    a. `vi ao.crt`
    b. Type `I` to insert the copied content from `pem` file.

c. Right-click into SSH session box to paste the content, if you are using putty.



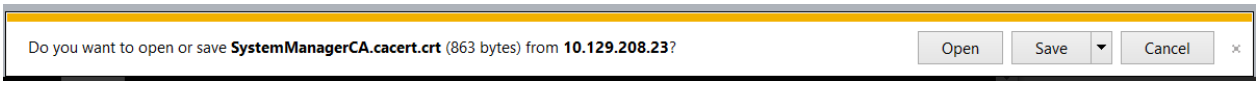
21. Press **Esc** to exit from the **INSERT** mode.
    d. Type `:wq!`

22. Proceed to Activating SSL certificate for enabling https connection.

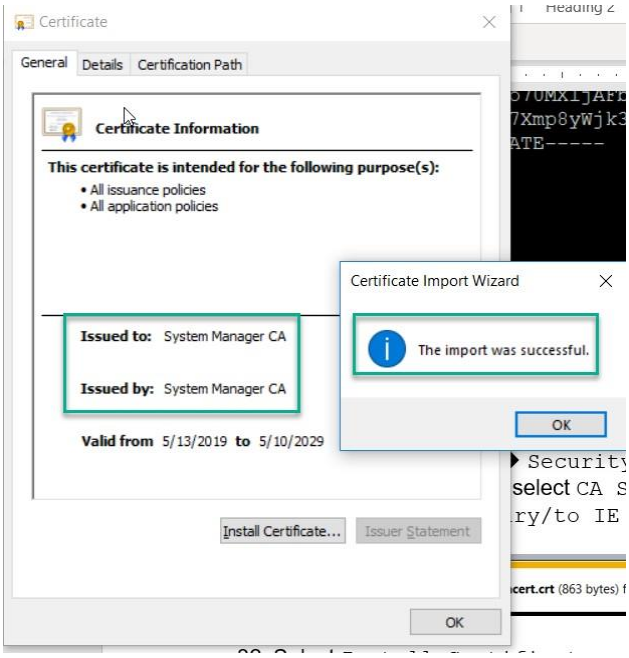
Adding the SMGR root certificate to a web browser

Internet Explorer/Chrome

1. Open **Internet Explorer** and access Avaya Aura System Manager.
2. Login with administrative credentials. For example, **admin**.
3. Navigate to **Services > Security > Certificates > Authority**.
4. Under **CA Functions**， select **CA Structure & CRLs**.
5. Select **Download binary/to IE**.



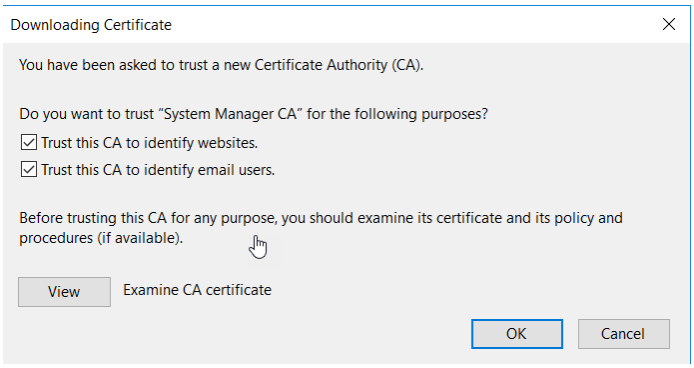
6. Select **Open**.
7. Select **Install Certificate**.
8. Select **Local Machine**.
9. Select **Next**.
10. Select **Place all certificates in the following store** and click **Browse**.
11. Select **Trusted Root Certification Authorities** and click **OK**.
12. Select **Next**.
13. Select **Finish**.



14. Proceed to next section to complete the certificate procedure.

FireFox

1. Open **Internet Explorer** and access Avaya Aura System Manager.
2. Login with administrative credentials: For example, **admin**.
3. Navigate to **Services > Security > Certificates > Authority**.
4. Under **CA Functions** select **CA Structure & CRLs**.
5. Select **Download to Firefox**.
6. Check both selections and click **OK**.



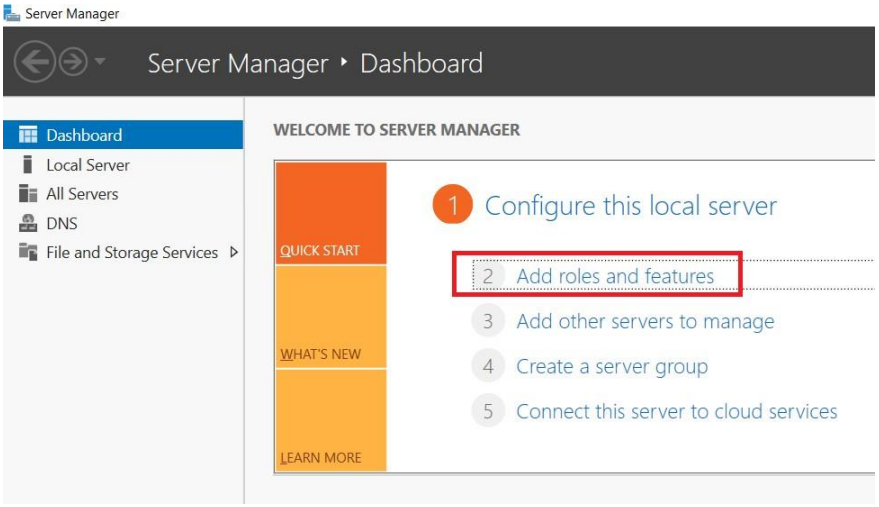
7. Proceed to the next section to complete the certificate procedure.

Using ASP 4.1 Management Server Console server as Certificate Authority

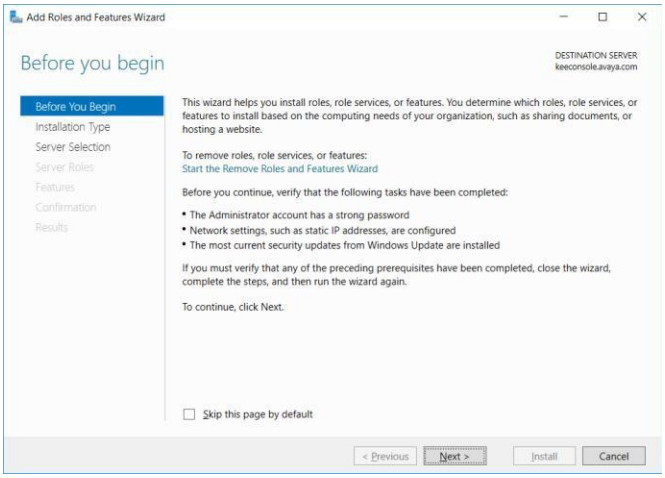
Management Server Console (MSC) can be used as the Microsoft Certificate Authority. The following procedure explains how to set up a simple Certificate Authority on Windows Server 2016 Server.

Procedure

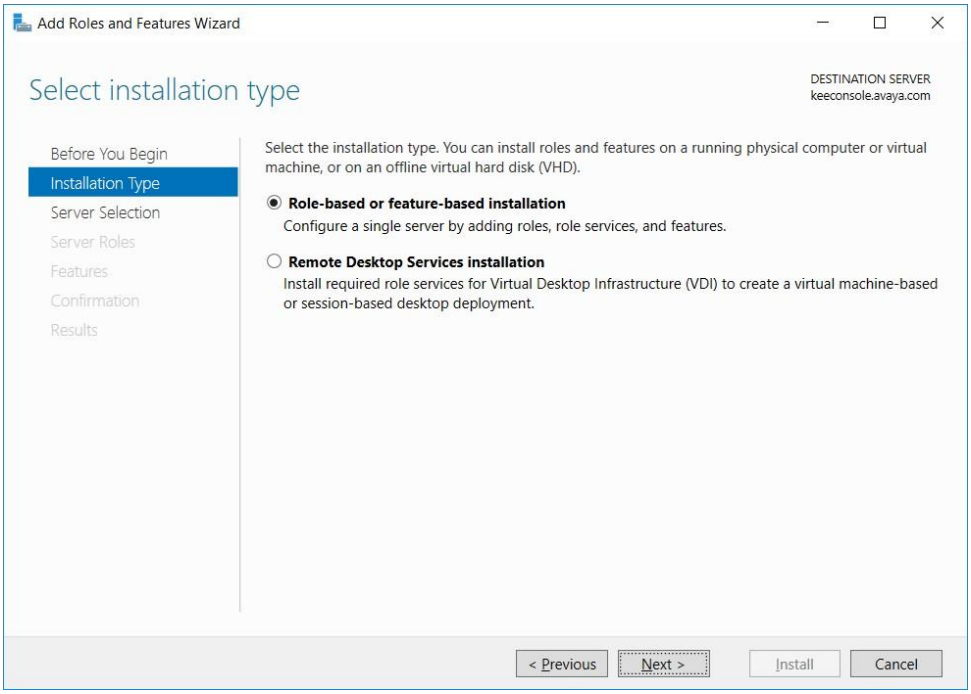
1. Add the Certificate Authority Role to the server. Open the Server Manager and then select **Add roles and features**.



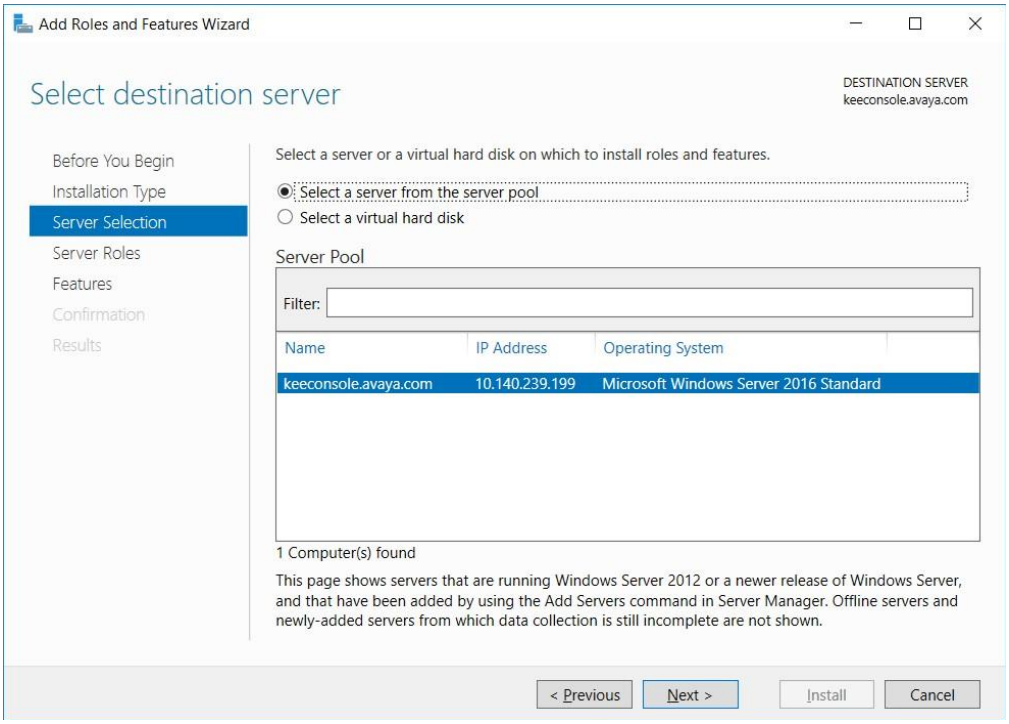
2. In **Before You Begin** section, click **Next**.



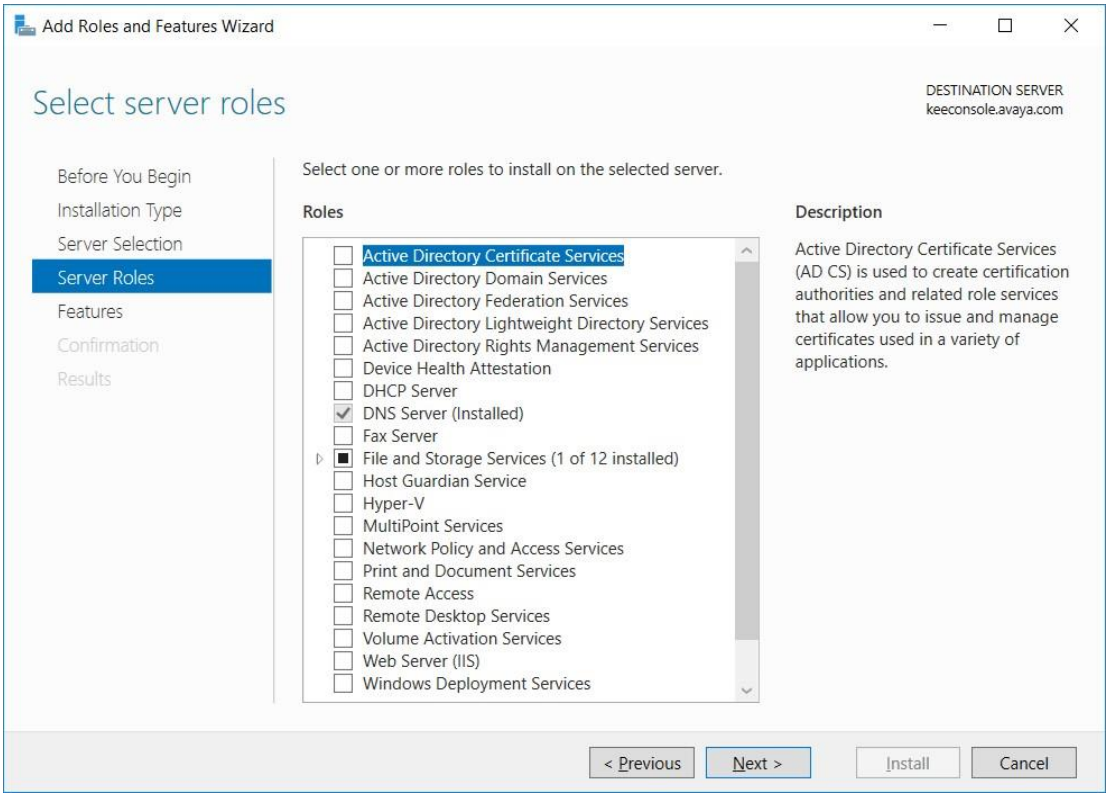
3. In **Installation Type** selection, select **role-based or feature-based installation** and click **Next**.



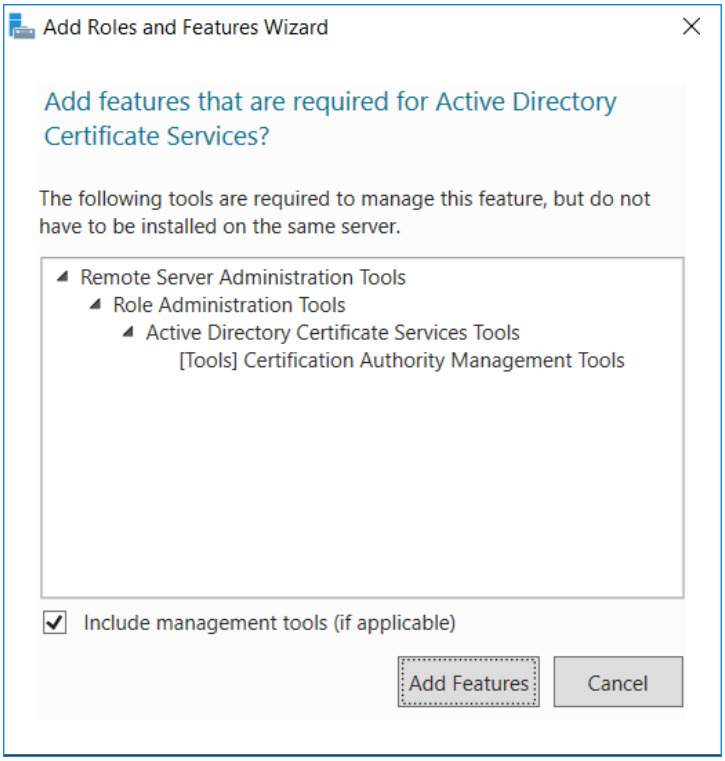
4. In **Server Selection** page, Select the Destination Server. The list shows the destination server you are working on and this must be the only one destination server in the list. Click **Next**.



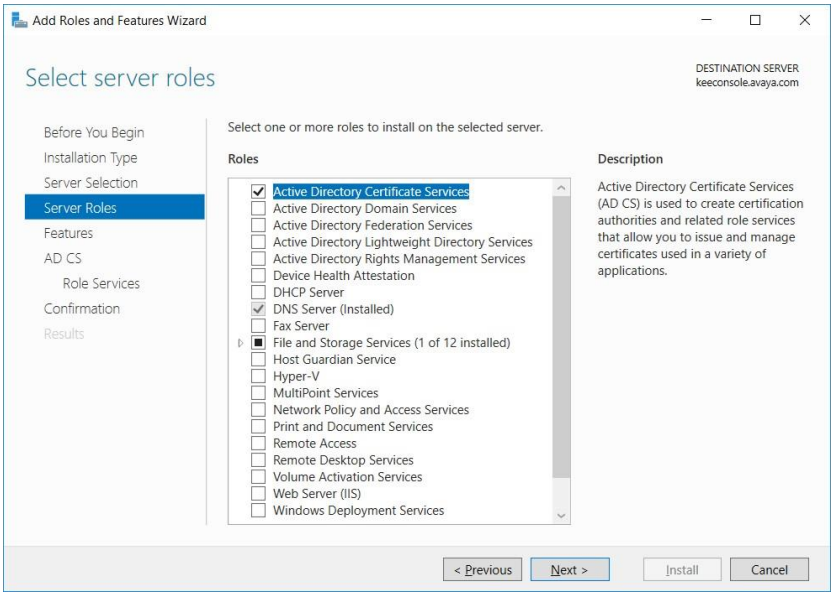
5. In **Server Roles** selection, select the **Active Directory Certificate Services**. A popup appears for the additional features.



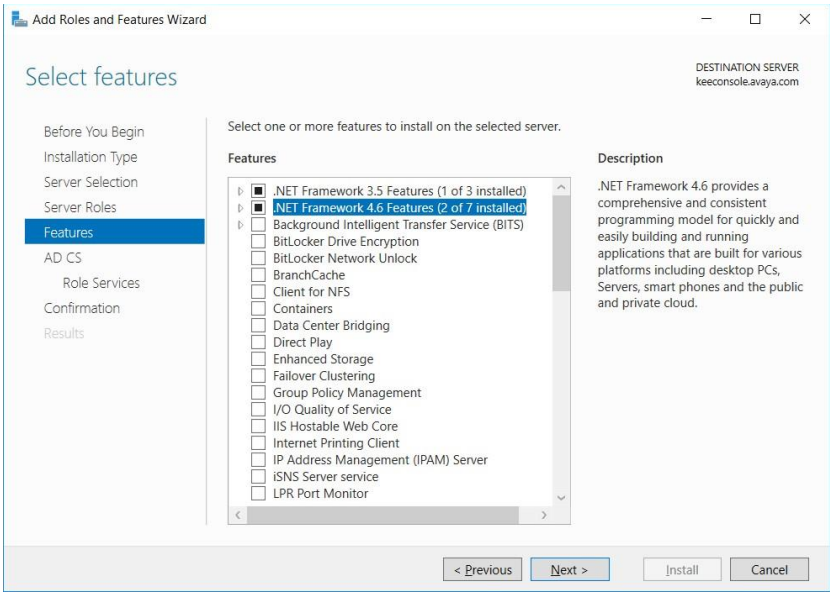
Once the pop up appears, click **Add Features**.



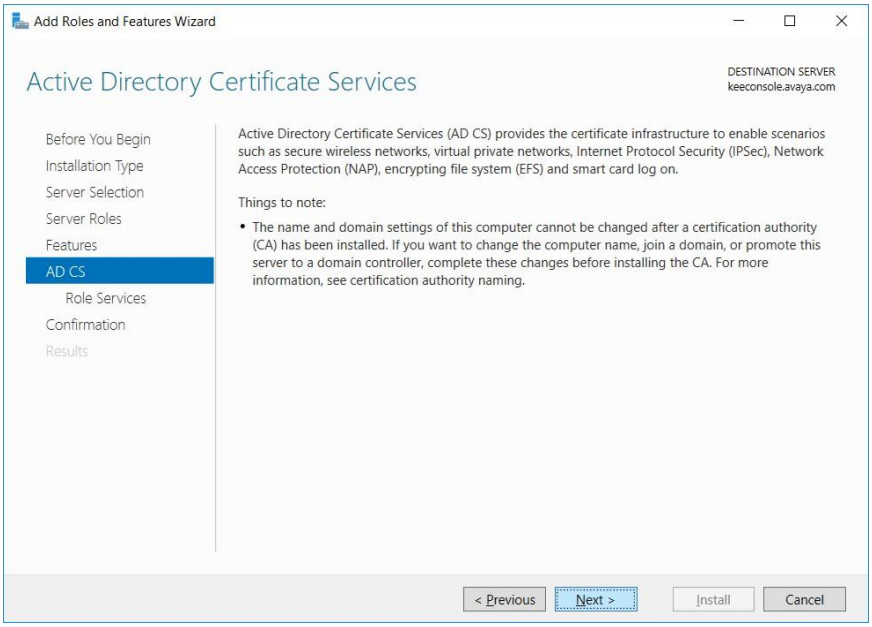
6. The **Active Directory Certificate Services** is now selected. Click **Next**.



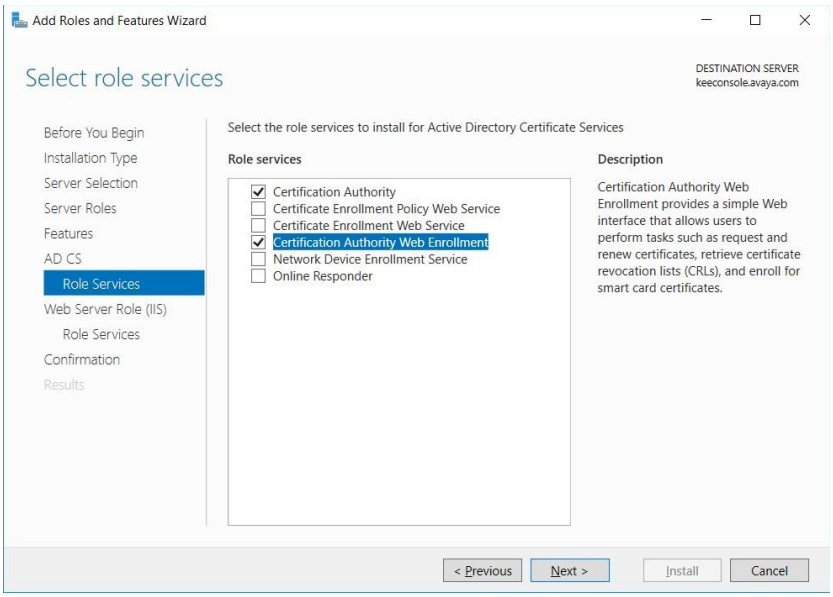
7. In the **Features** page, do not make any changes. Proceed to **Next**.

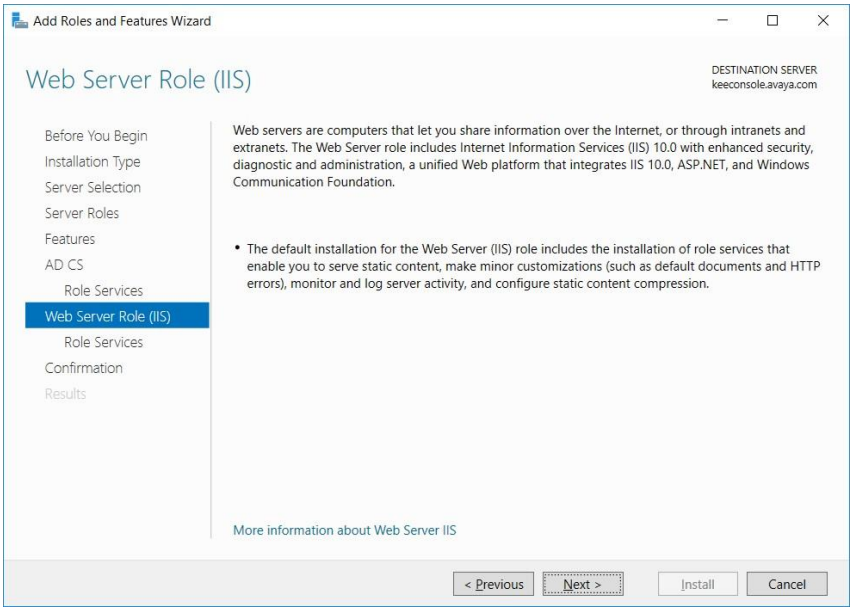


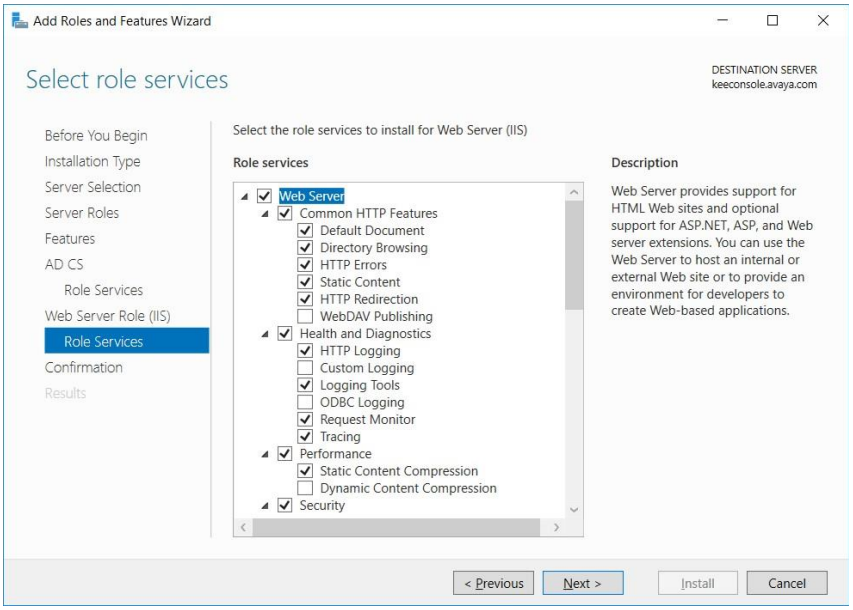
8. In the **Active Directory Certificate Services** (ADCS) page, click **Next**.



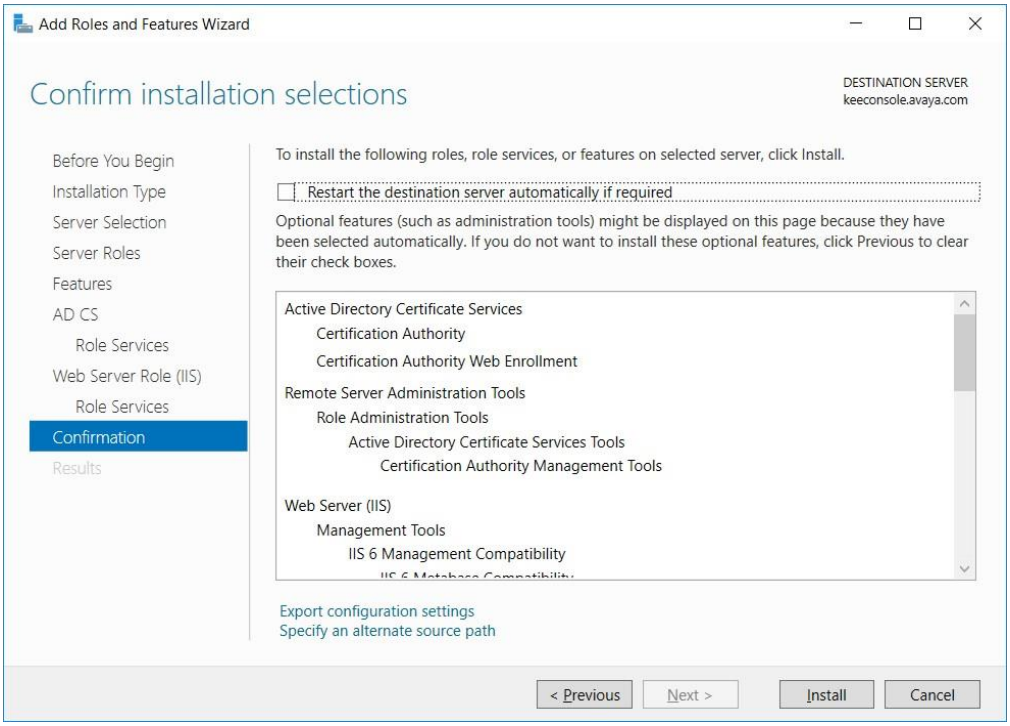
9. In the **Role Services** page, select **Certification Services** and click **Next**.



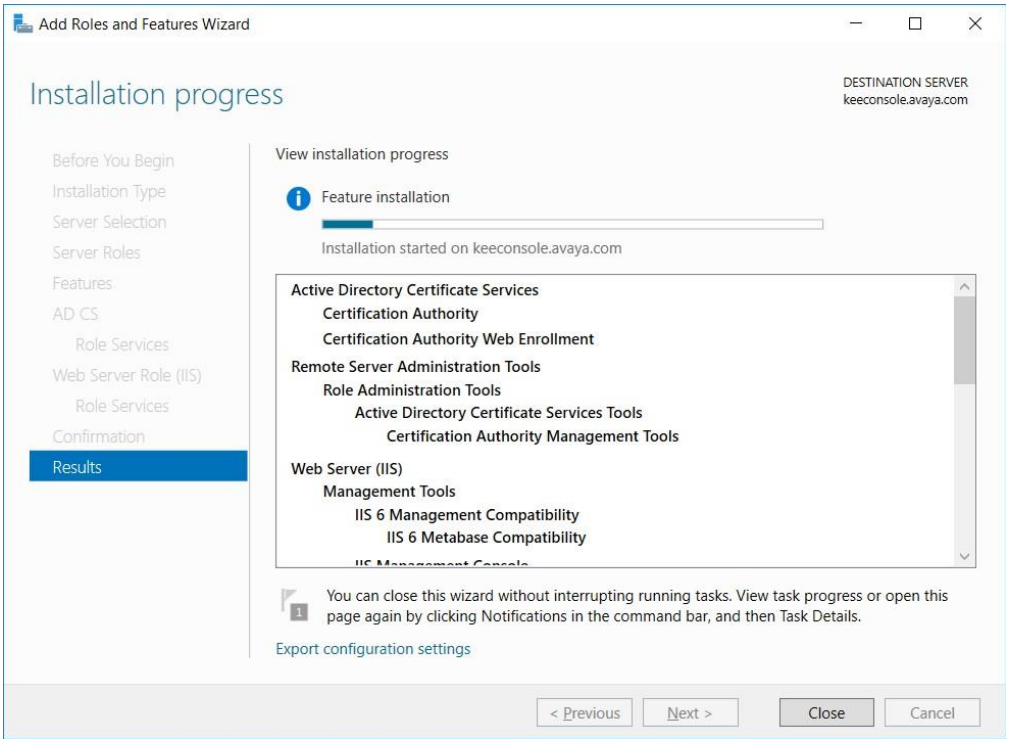




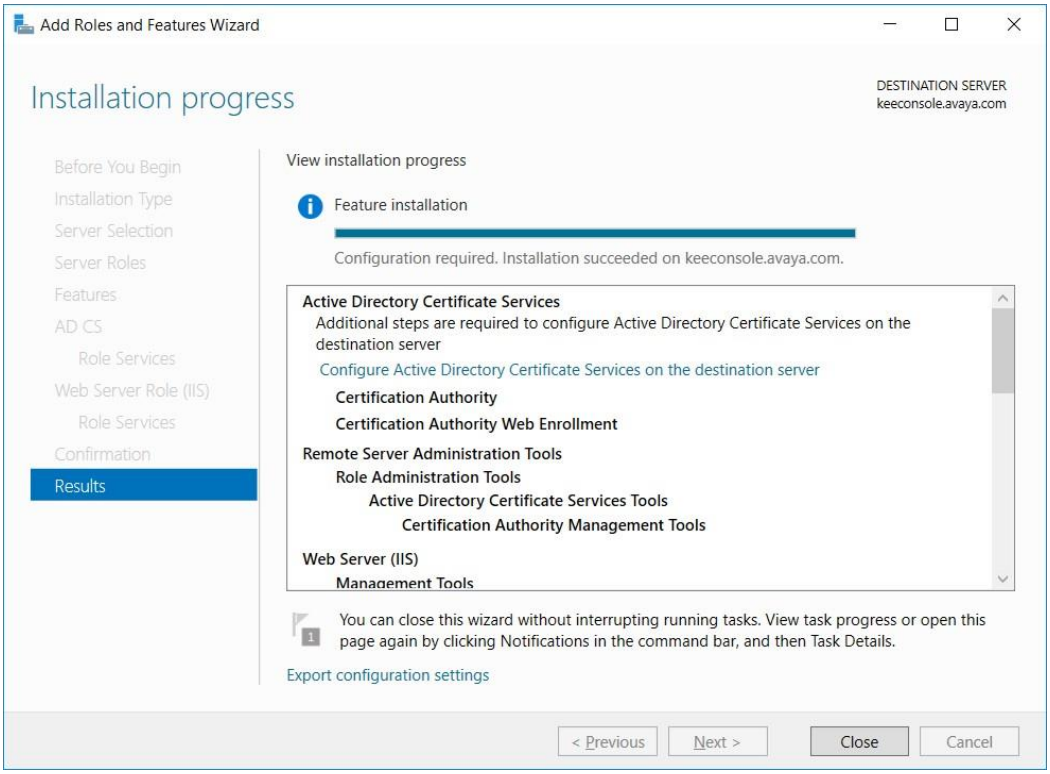
10. In **Confirmation** page, select **Restart the destination server automatically if required** and click **Yes** in the popup. Click **Install**.



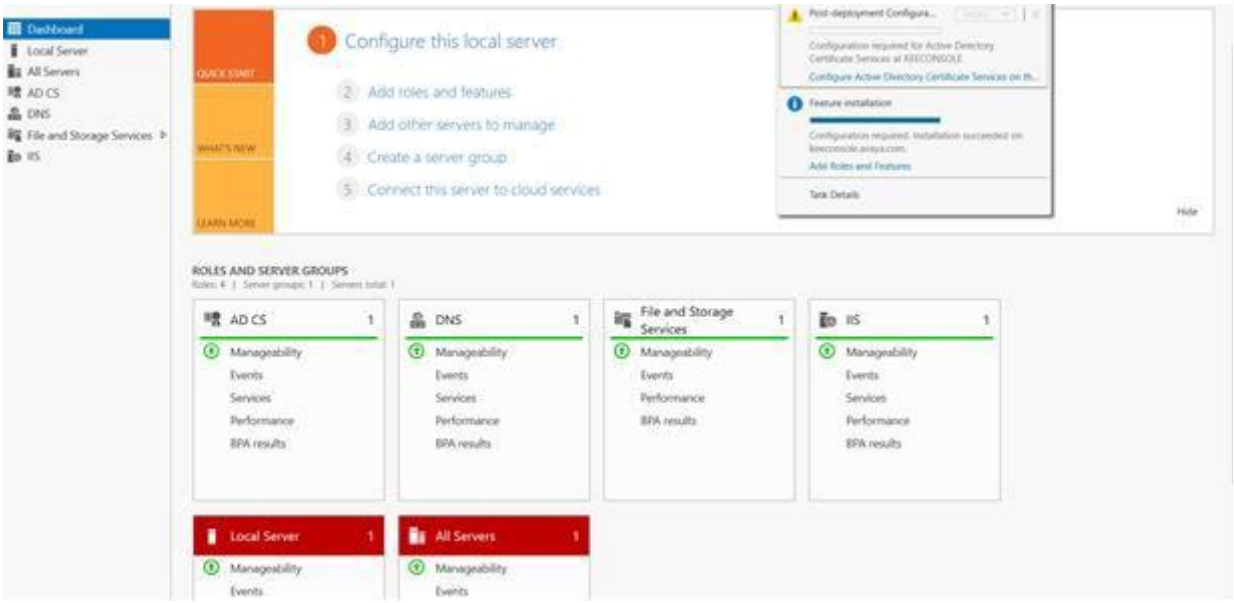
11. The installation of the ADCS starts.



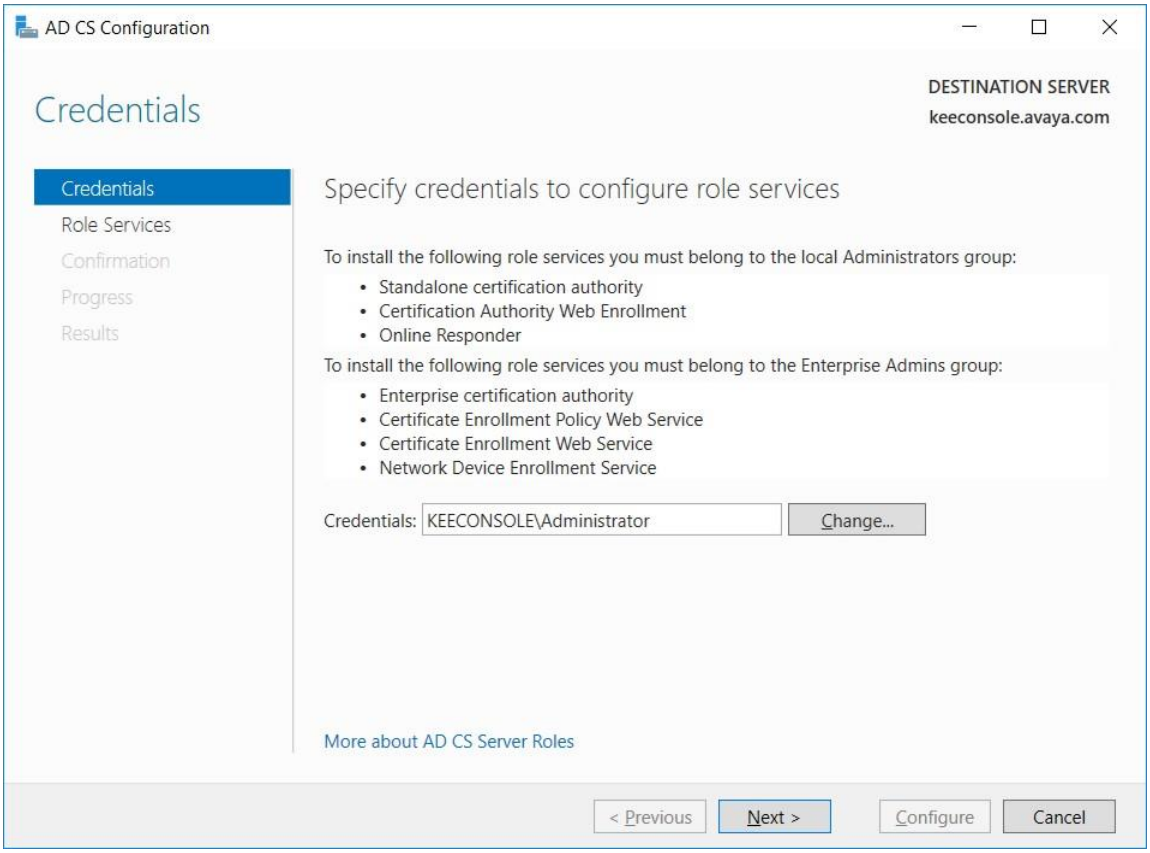
12. You can view the Installation progress. Click **Close** once the installation is complete. A fresh 2016 installation does not require a restart.



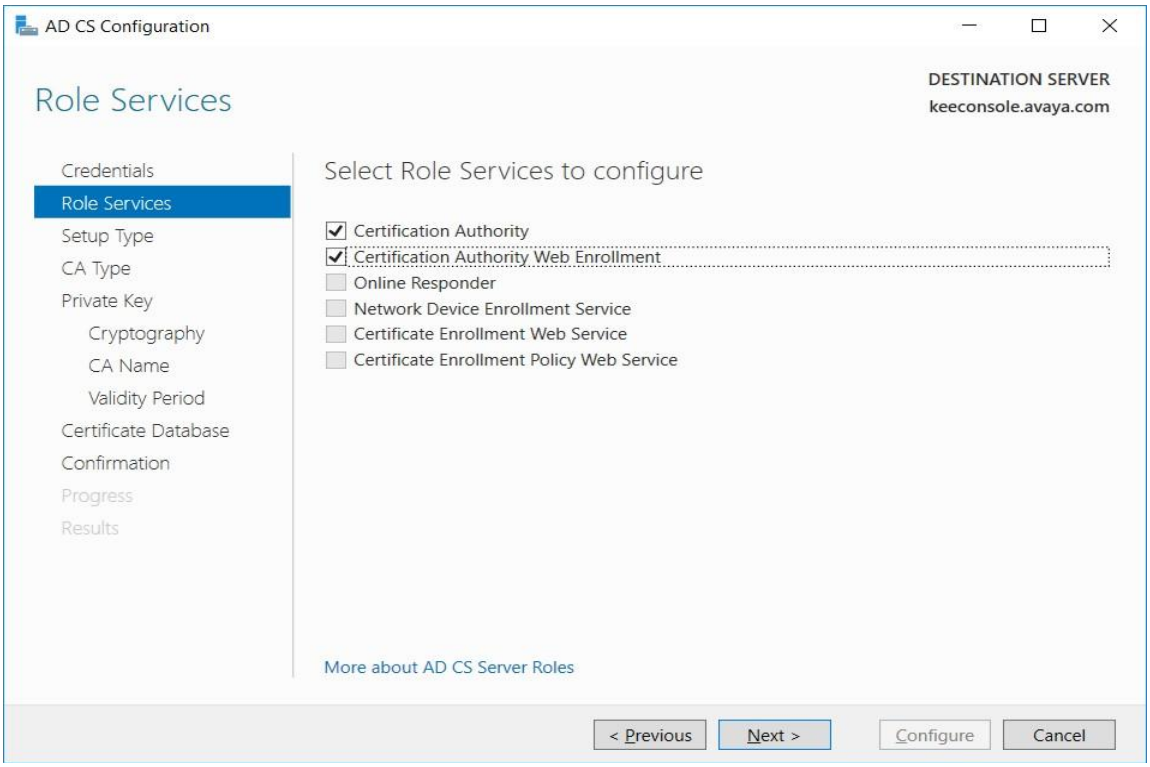
13. Return to your Server Manager Dashboard. The yellow exclamation mark indicates that you need to complete the ADCS configuration.



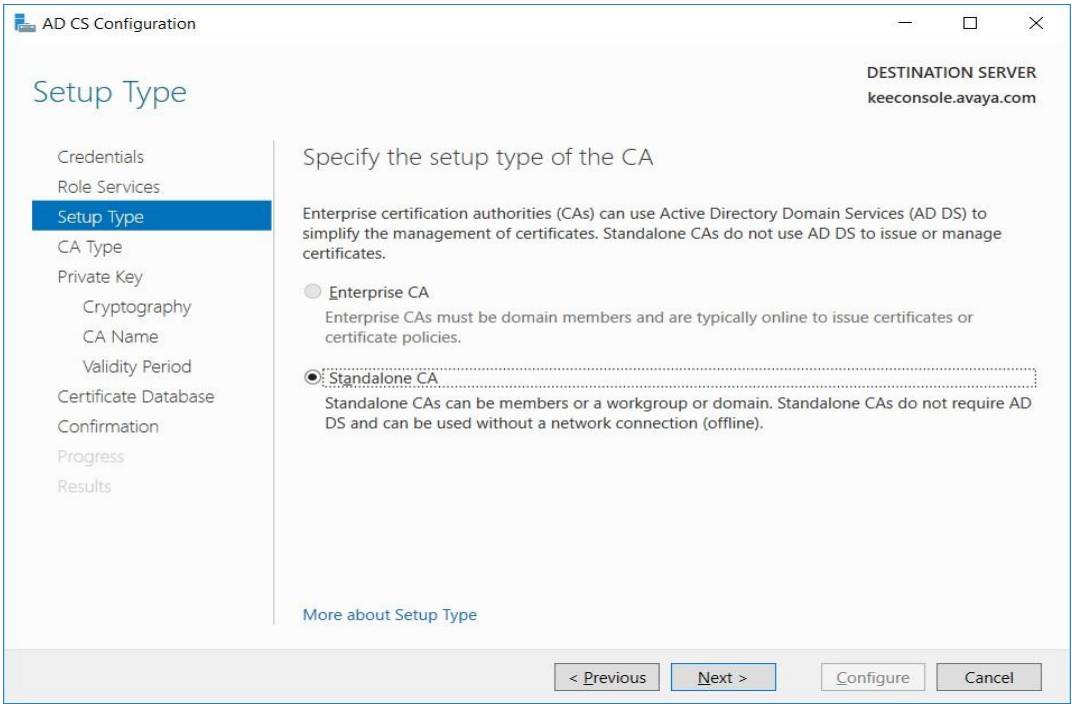
14. In the **Credentials** page, keep the default credentials and click **Next**.



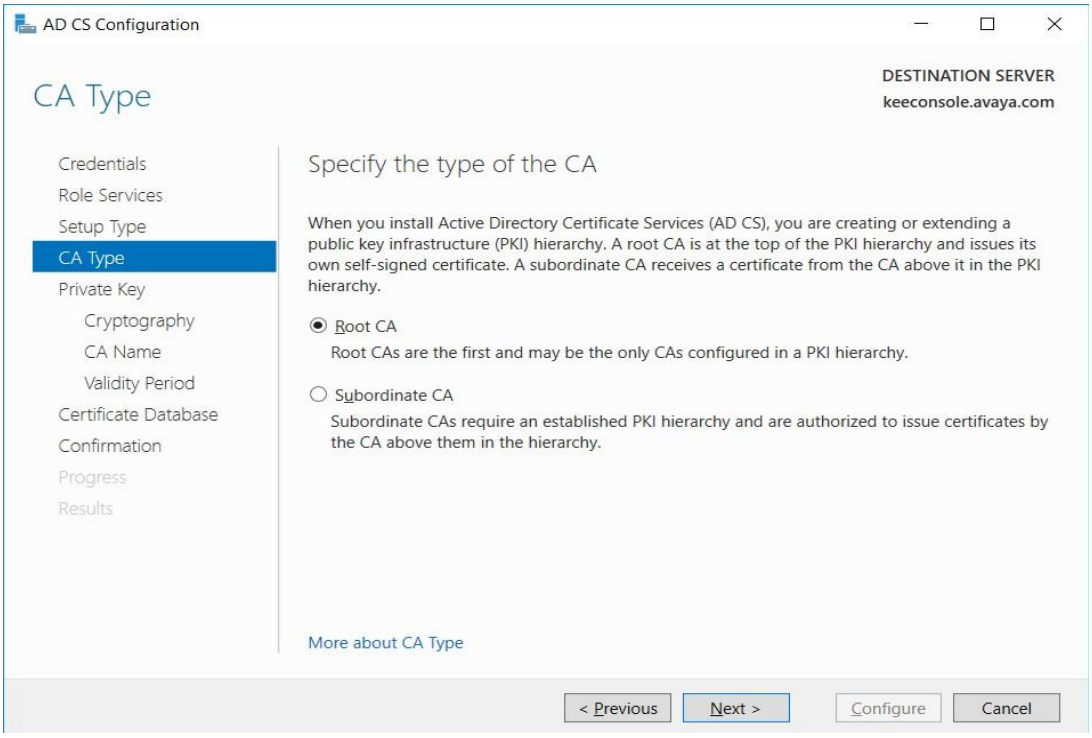
15. In **Role Services** page, select the **Certification Authority** and click **Next**.



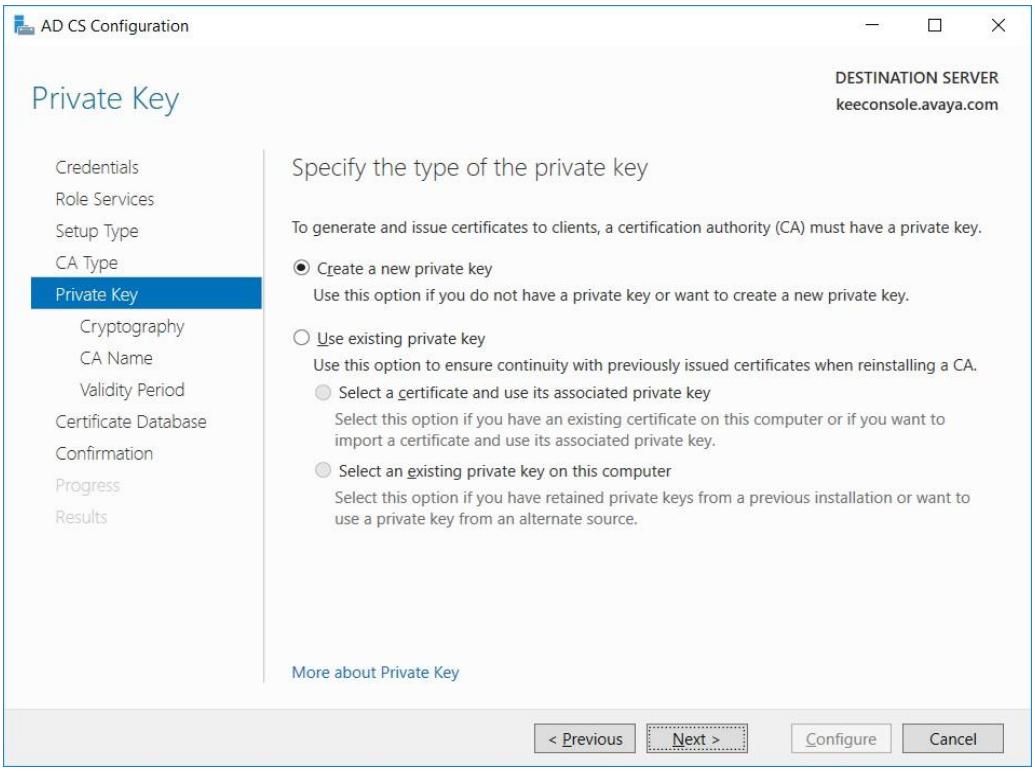
16. In **Setup Type** page, keep **Standalone CA** selected and click **Next**. For an Enterprise CA, you need to be connected to a domain.



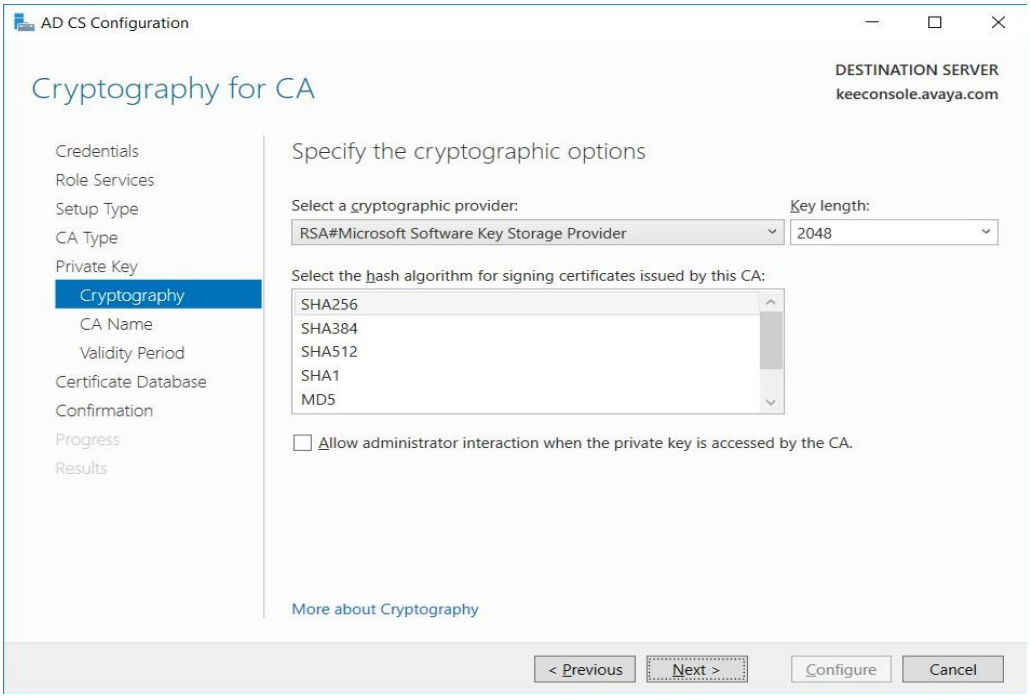
17. In **CA Type** page, select **Root CA**. Deploy a Root CA unless you have a Root CA which can be a subordinate. Click **Next**.



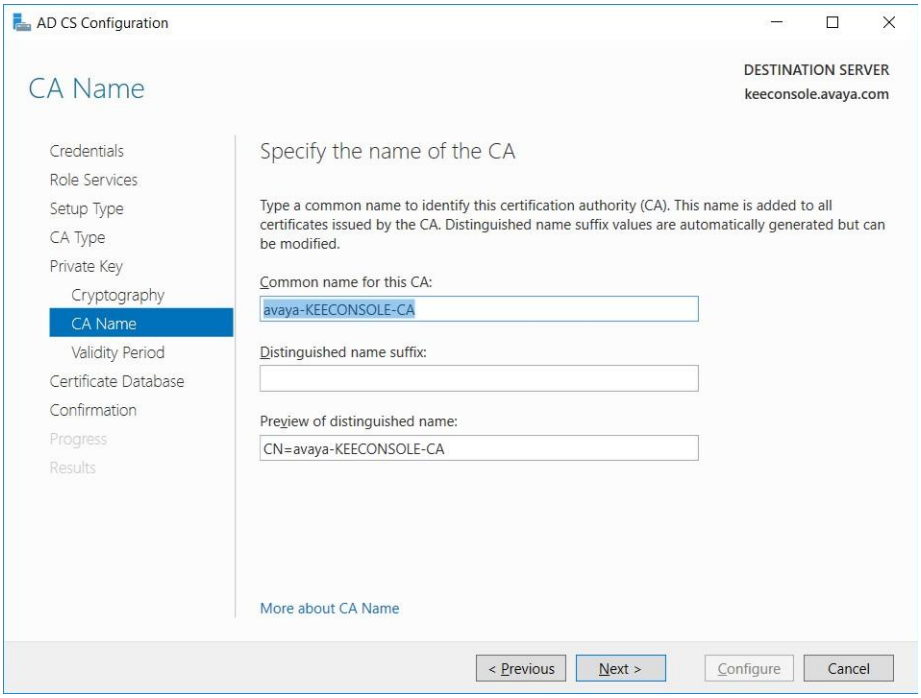
18. In **Private Key** page, keep **Create a new private key** selected and click **Next**.



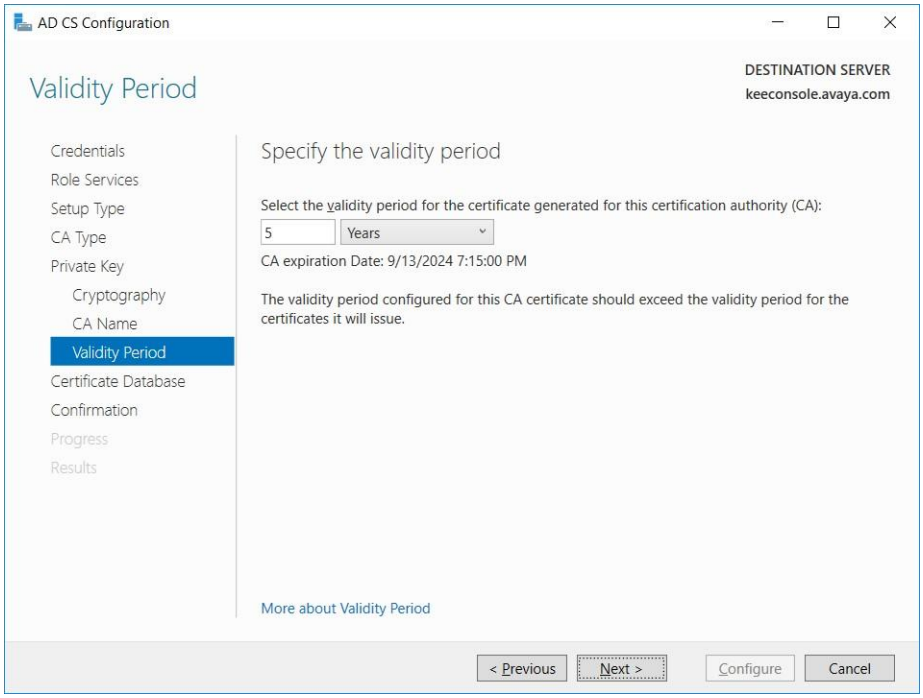
19. In **Cryptography** page, select **Cryptographic provider**. Ensure that the default Key Length and algorithm are sufficient for the lab needs. Click **Next**.



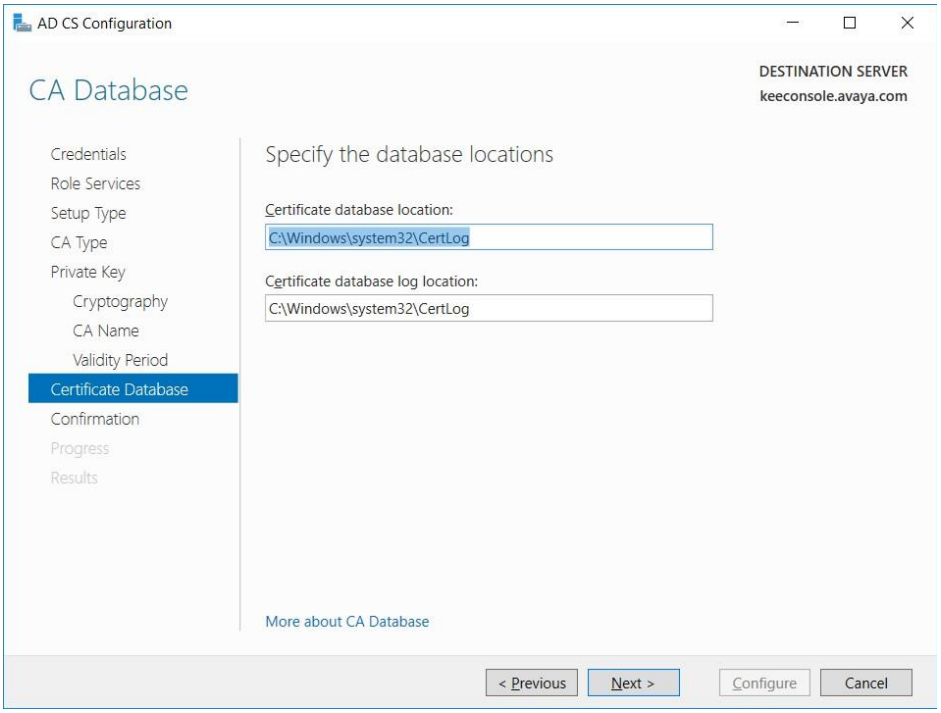
20. In the **CA Name** page, specify the name of the CA and click **Next**.



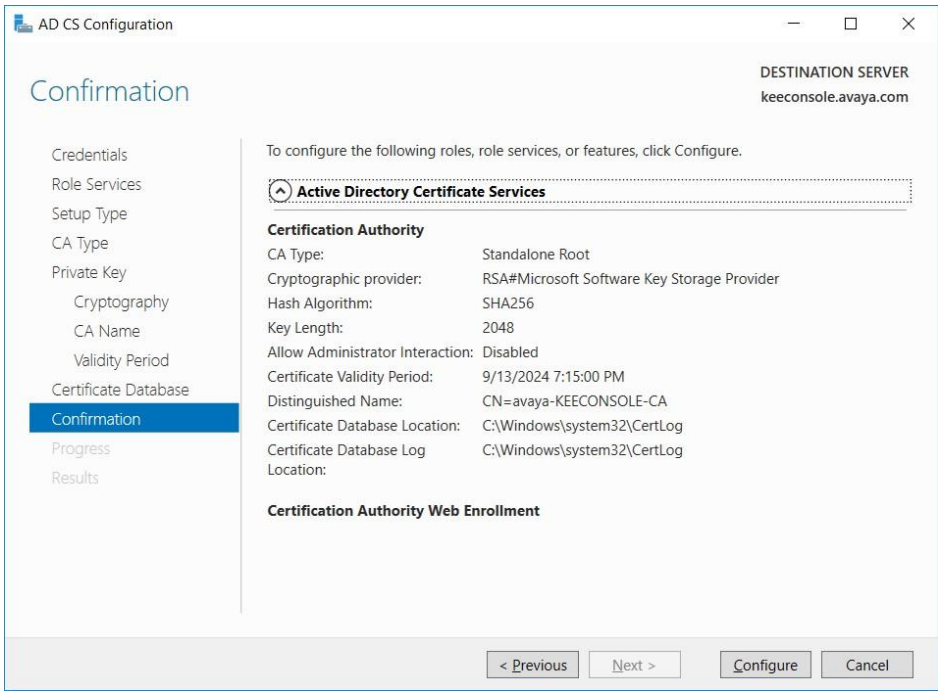
21. In the **Validity Period** page, specify the validity period to 5 years (default validity). Click **Next**.



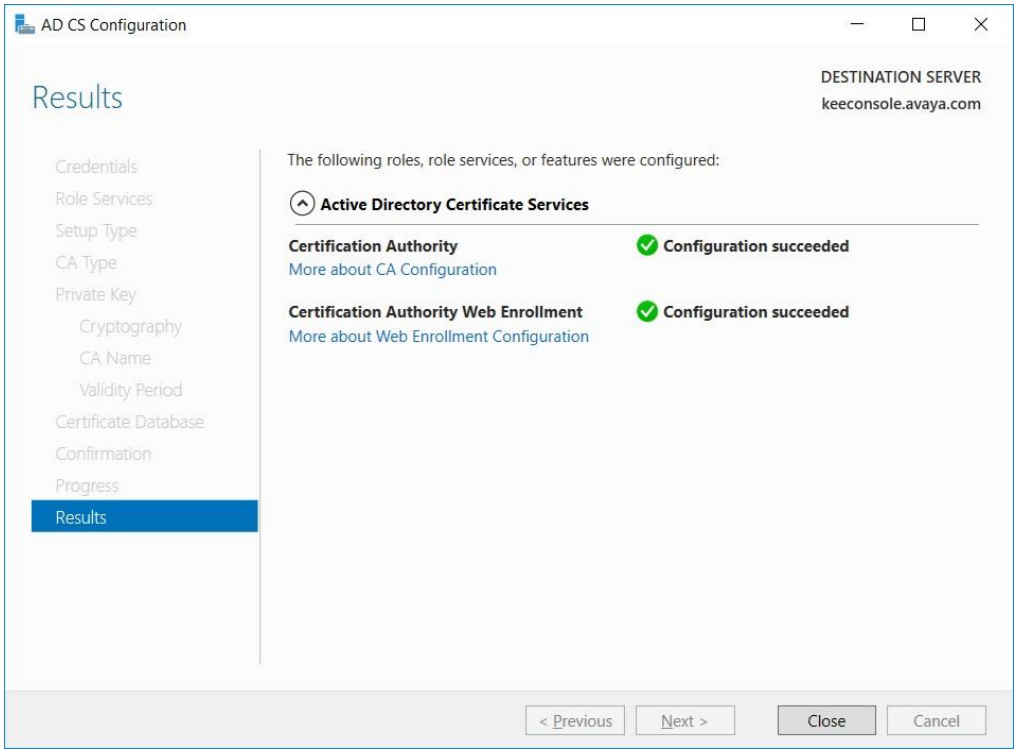
22. In **Certificate Database** page, leave the default database location unless you need to change. Click **Next**.



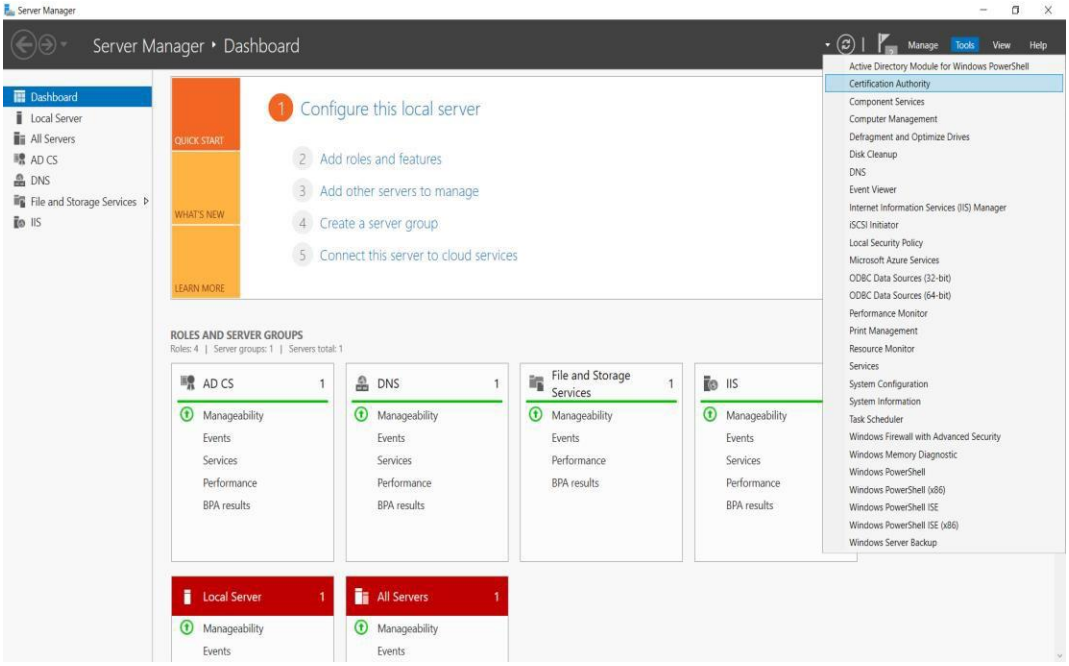
23. In **Confirmation** page, verify the selections you made and click **Configure**.



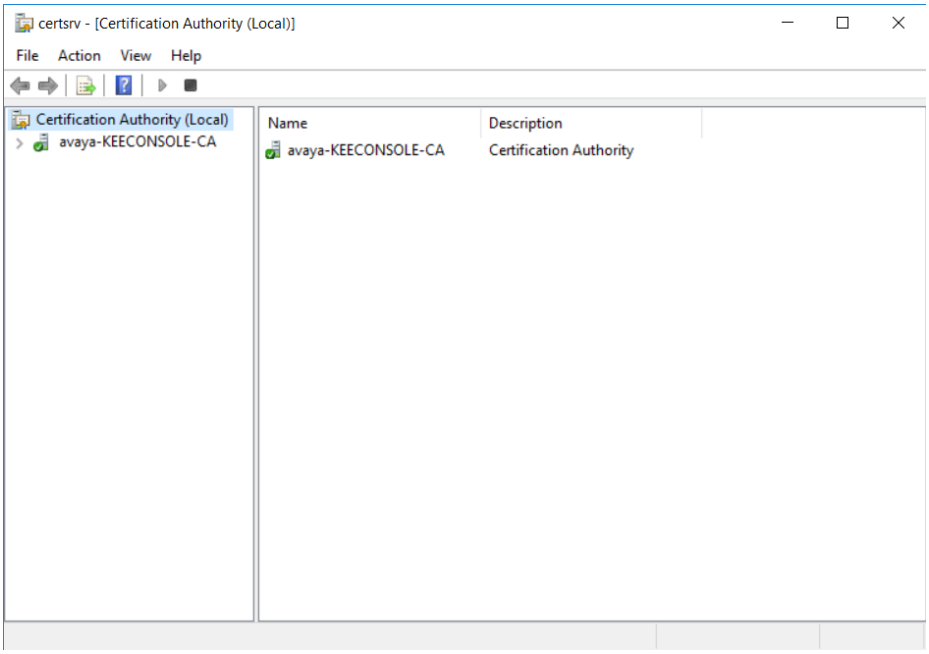
24. **Results** page shows whether your Certificate Services are configured successfully.



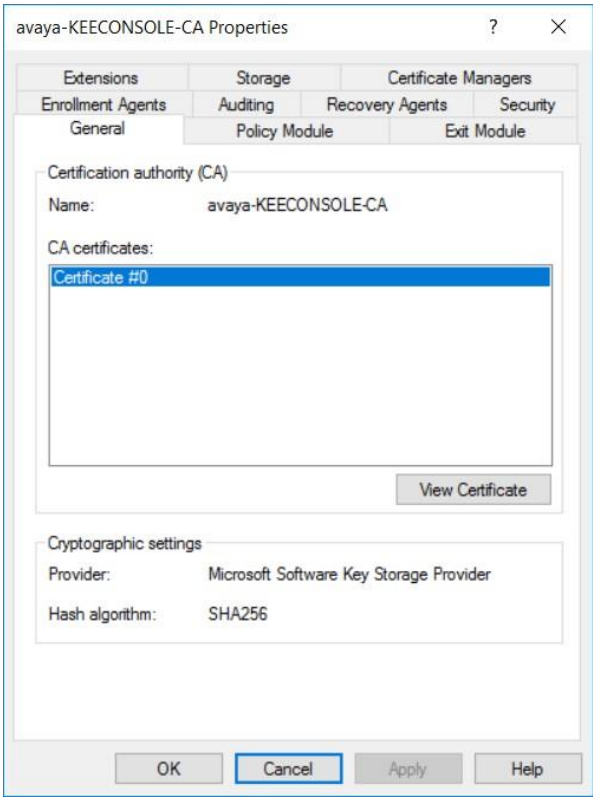
25. On the **Server Manager** Dashboard, click **Tools** > **Certification Authority**.



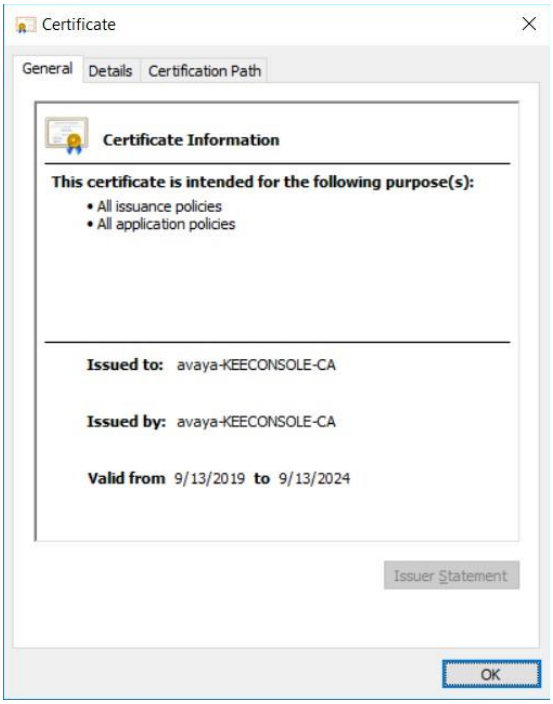
26. Your newly issued CA displays.



27. Right click the file `-ca` and select **Properties**. The CA Certificate shows **Certificate #0** which is the public certificate for the CA. Click **View Certificate**.



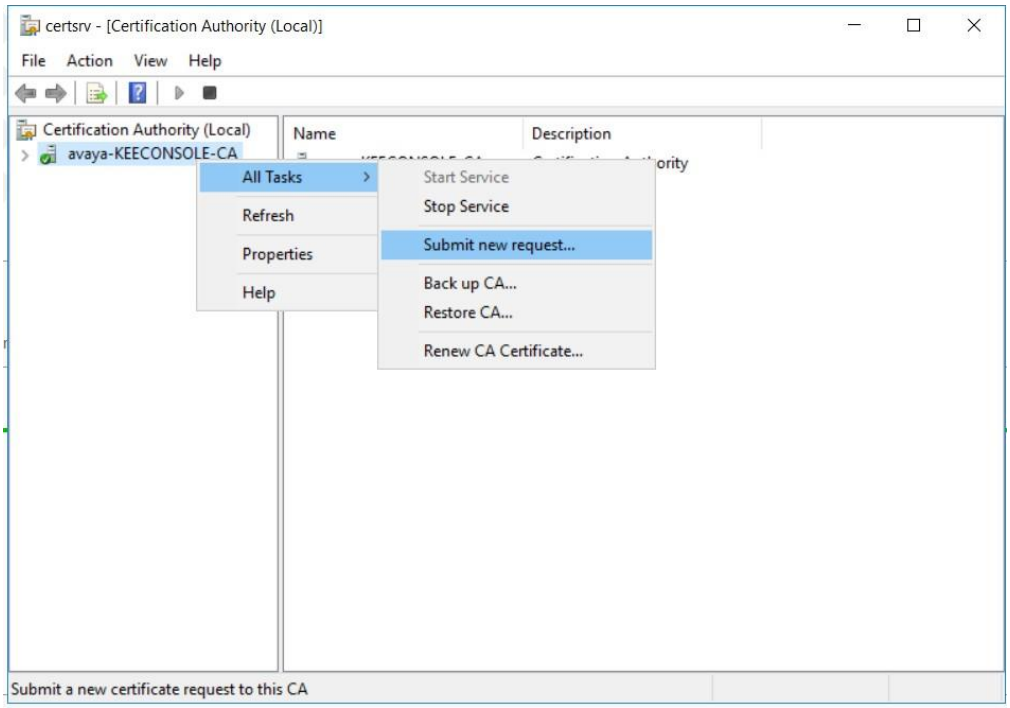
28. In the **General** page, the summary of the certificate displays. In this case, the Validity period shows 5 years as per your earlier seletion. This is the Root CA which needs to be installed on the client web browser.



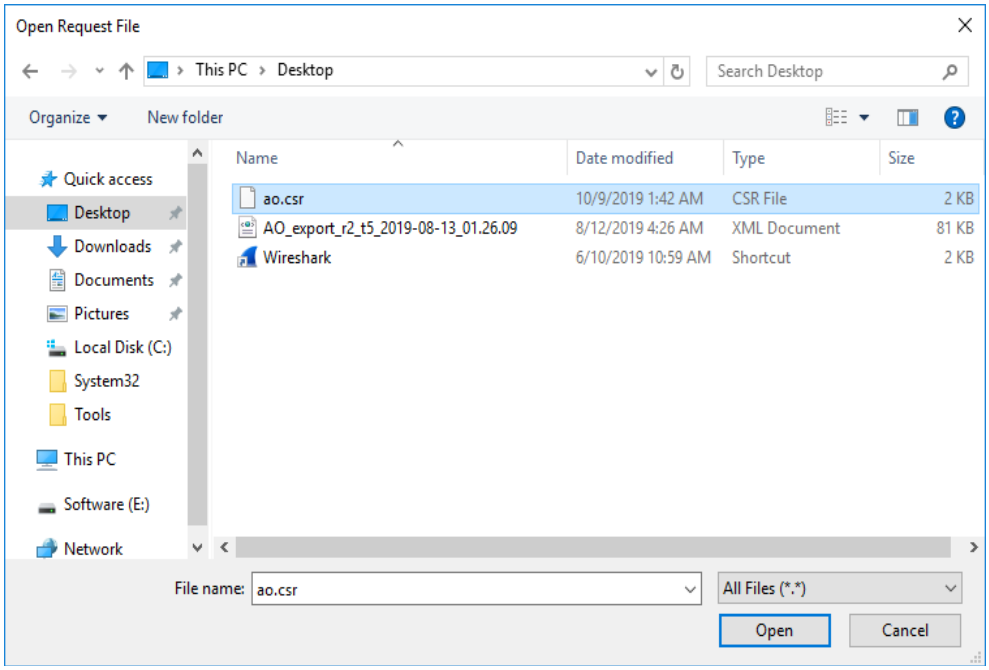
Signing Certificate Sign Request (CSR) with MSC as the Certificate Authority

Procedure

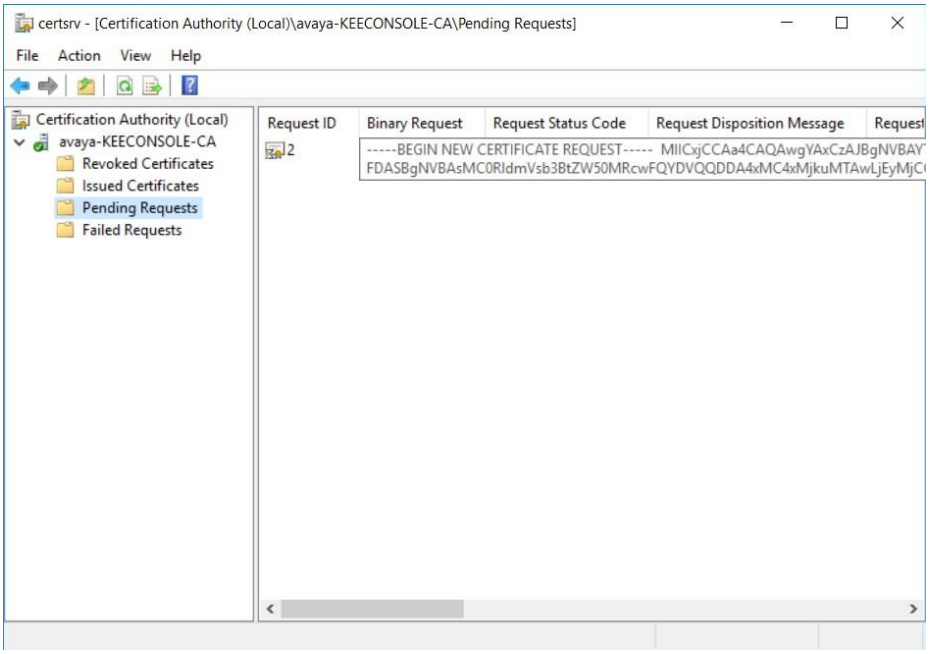
1. Copy your CSR file to the server running the CA and then open the **Certification Authority** configuration app. Right click the **CA** and select **All Tasks > Submit new request…**



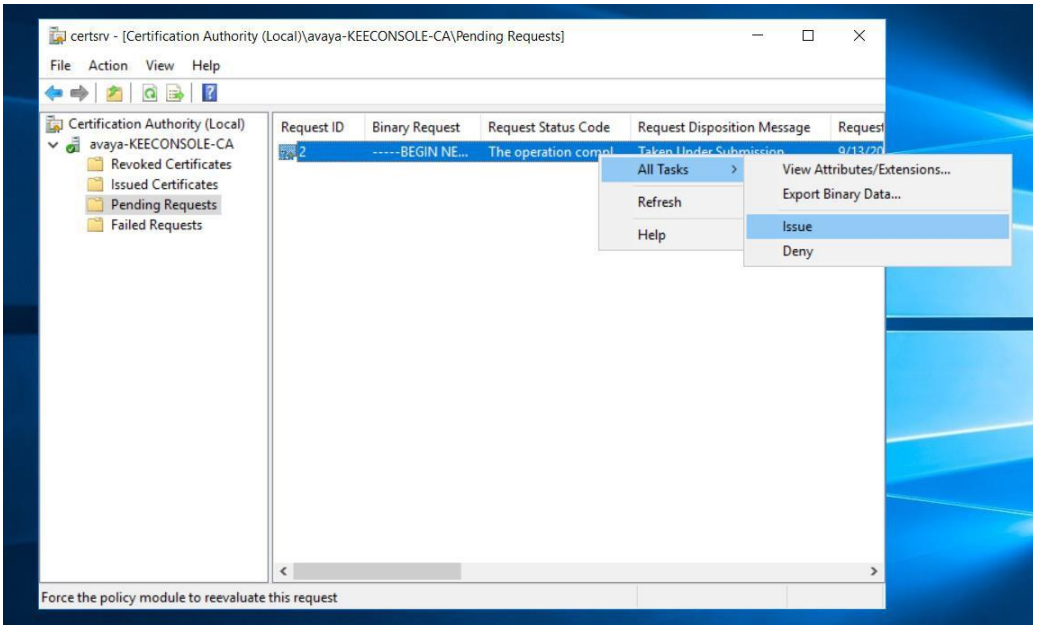
2. A file selector pops up and ask you for the `.CSR` file. Select the file and click **Open**.



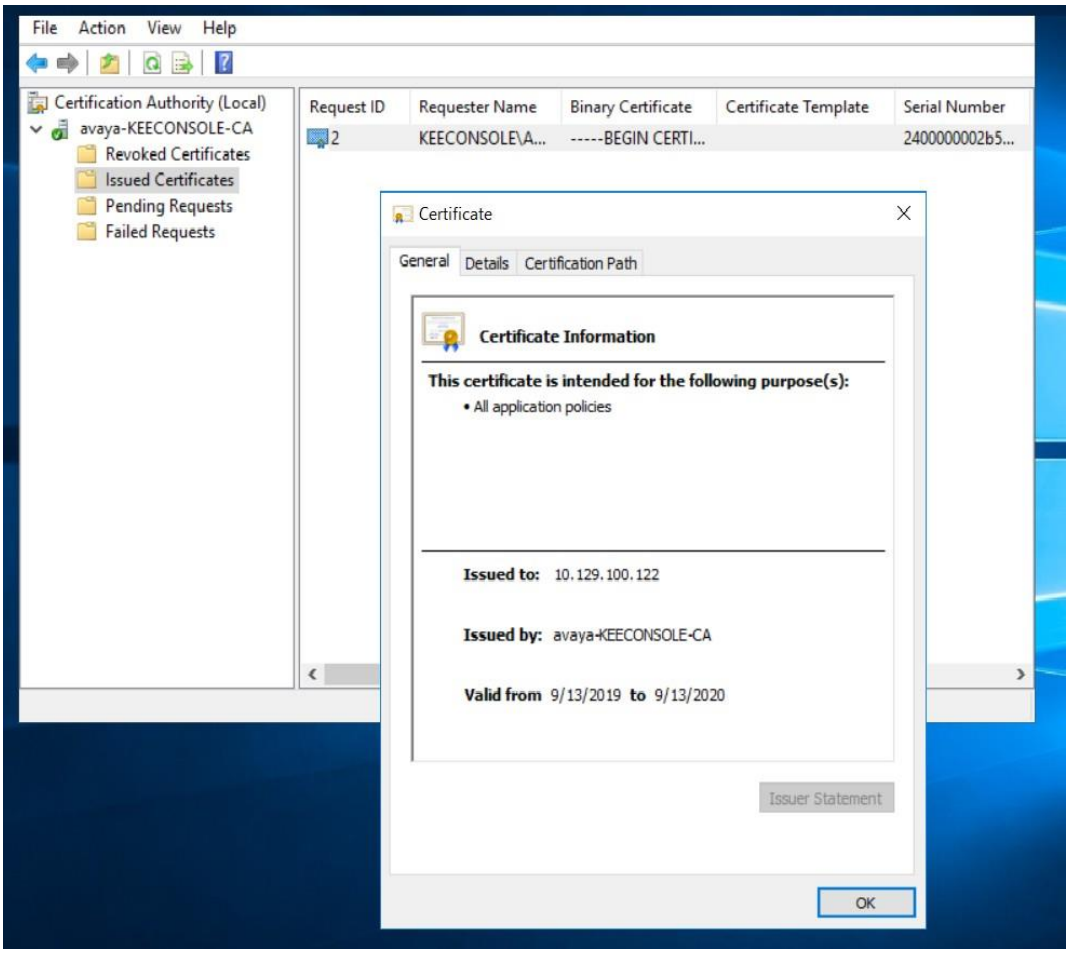
The CSR loads into the CA and then places a request into the **Pending Requests** folder.



3. Right click the request and select **All Tasks > Issue**.



The certificate is now placed in the **Issued Certificates** folder.



4. Export the Certificate in the form of DER, P7B extension which can be converted to `.crt` extension and include as part of the AO secure communication configuration.
5. Proceed to **Activating SSL certificate** section for secure connection between the browser and AO application.

Activating SSL certificate

Procedure

1. SSH to Avaya Orchestrator™ using the **aoadmin** credentials.
2. Run the following command to change user to superuser `root`:
   `su –`
   Enter the Password for the `root` account.
3. Run the following commands to set proper permissions for generated files:
   ```
   chown apache:apache /usr/local/nagiosxi/var/certs/*
   chmod 644 /usr/local/nagiosxi/var/certs/*
   ```
4. Perform the following steps to modify the SSL configuration settings:
   a. Run the command: `vi /etc/httpd/conf.d/ssl.conf`

b. Validate if the following entries are present:
SSLCertificateFile/usr/local/nagiosxi/var/certs/ao.crt
SSLCertificateKeyFile/usr/local/nagiosxi/var/certs/ao.key

c. Run the command: `vi /etc/httpd/conf.d/ssl.conf`
d. Press the down arrow key to get to the end of the configuration file.
e. Type `i` to enter to **INSERT** mode.
f. Position the cursor on Line `240 </VirtualHost>` and press **Enter**.



g. Copy the following content into the configuration file:

```
RewriteCond %{HTTPS} off
RewriteRule (.*) https://%{HTTP_HOST}%{REQUEST_URI}
```

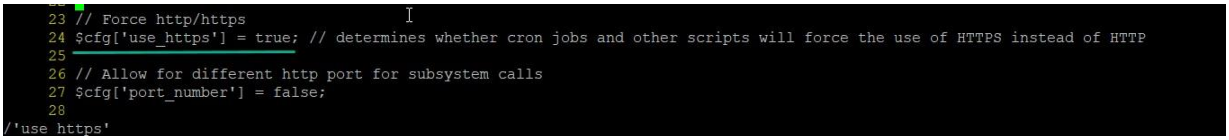
Note: Remove the empty lines after pasting content into the configuration file.



5. Enable HTTPS for Avaya Orchestrator™
`ao_https_enable`
6. Run the following command to restart the Apache web server:
`systemctl restart httpd`
7. Run the following command to modify the local firewall rules:
`firewall-cmd --zone=public --add-port=443/tcp`
`firewall-cmd --zone=public --add-port=443/tcp –permanent`

Note: If the following warning message appears, then proceed with the next step.
`Warning: ALREADY_ENABLED`

8. Run the command `vi /usr/local/nagiosxi/html/config.inc.php`.
Validate that the entry `$cfg['use_https']` is equal to `'true'`.



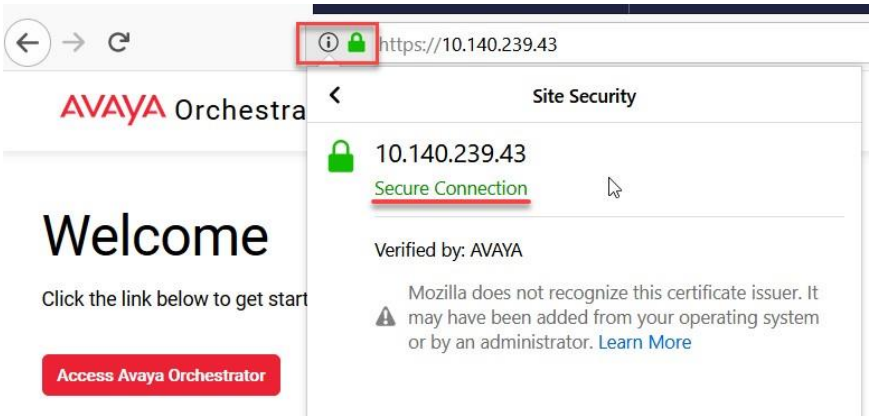
Validating the certificate

Procedure

1. Open a web browser and access Avaya Orchestrator™ using either the FQDN or IP Address.
2. Validate the certificate based on the web browser you are using:

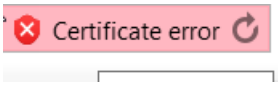
Using Firefox:

a. Lockbox icon displays in green.
b. (Optional) Click **Learn More** if you need to validate the information in the certificate.

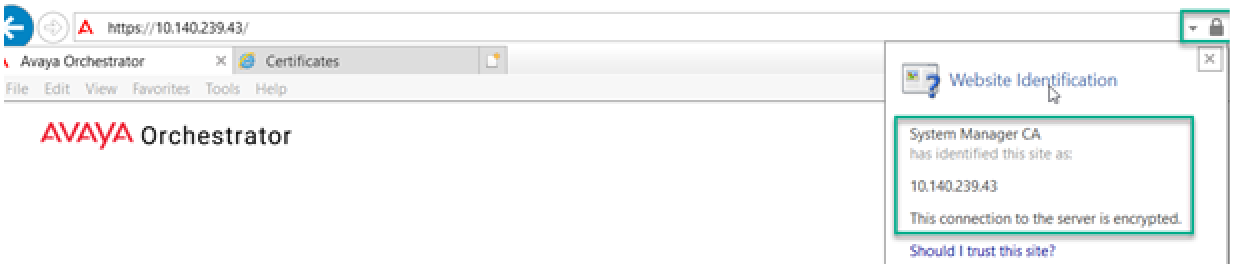


Using Internet Explorer:

a. If a valid certificate is present, the browser must not display any certificate error when trying to connect to AO.

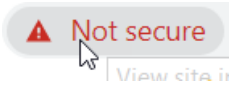


b. (Optional) Select lockbox icon to validate the connection and the certificate.

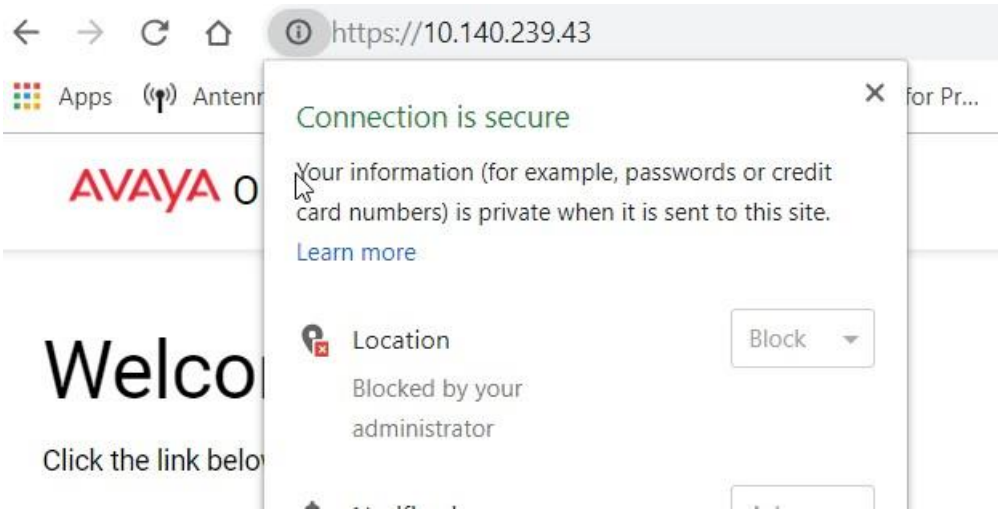


Using Chrome:

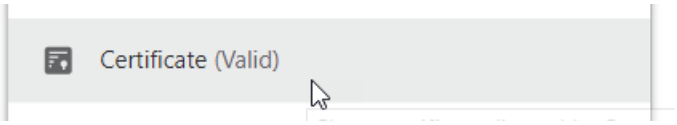
a. If a valid certificate is present, the browser must not display the message **Not secure** when trying to connect to AO.



b. (Optional) Click icon to check if it displays the message: `Connection is secure.`



c. You can validate the installed certificate by selecting **Certificate**.



Note: When you log in to Avaya Orchestrator™ after restarting the apache services, HTTPS will be set. You get the green lockbox for Firefox, and Certificate validation passed for Internet Explorer and Chrome.

Chapter 7: Avaya Orchestrator™ Dashboard Deployment

Overview

This chapter contains information about assigning static dashboard views to different users.

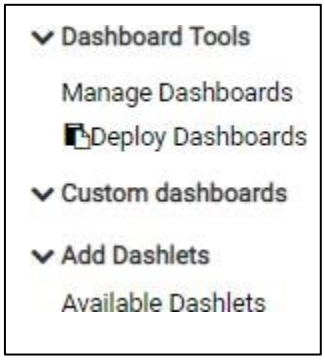
Accessing the Avaya Orchestrator™ dashboard

Note:
In Avaya Orchestrator™ Release 1.5, there are options for customizing dashboards. An Enhanced license will be required for building your own custom view.

The primary ACP Home Dashboard is still the “go to” view for identifying the solution state-of-health and is available with a basic license.

Procedure

1. Log on to the Avaya Orchestrator™ interface.
2. Click **Dashboards** to view the available menu options.

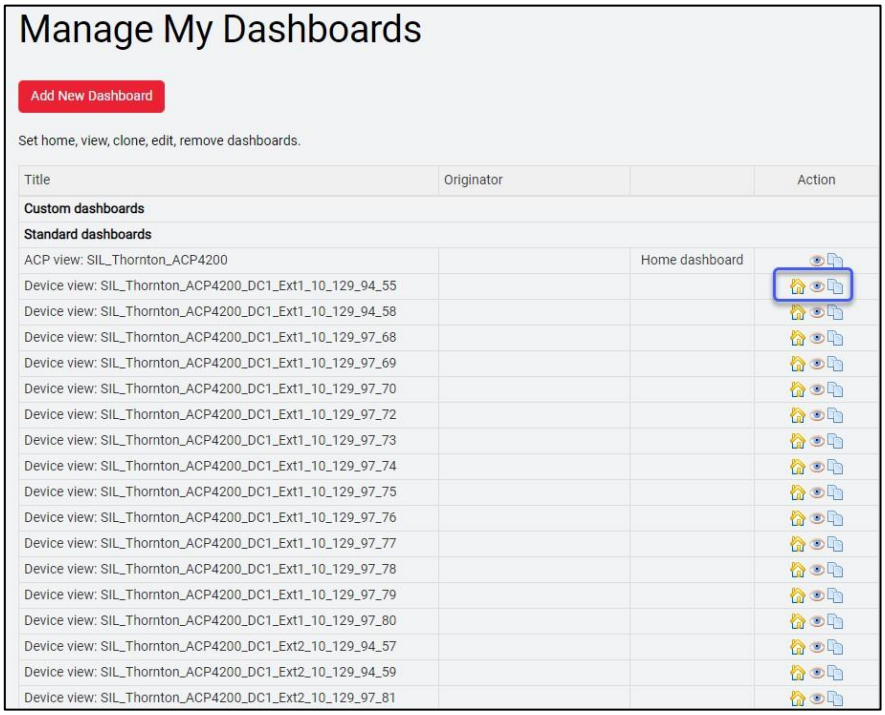


3. Click **Dashboard Tools** > **Manage Dashboards.**

Manage Dashboards

About this task

Use this procedure to create a new dashboard assign dashlet elements to an existing dashboard, or, if an enhanced license is in place, you may assign dashlets to a new “home” dashboard of your creation.

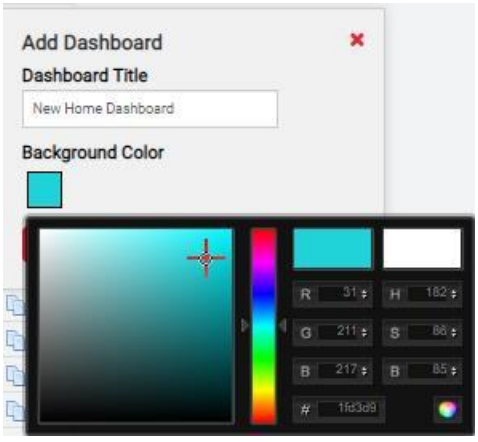


Within the blue square above, you may select the house icon to set a dashlet/dashboard as your official “home dashboard” or click the eye icon to view the dashlet and its content, or select the paper icons to clone the dashlet.

In this example, we can see that the “ACP view SIL_Thornton_ACP4200” is the Home dashboard. From the line-up of dashlets down the page, we can also learn which dashlets are part of the home dashboard view. In this example, all are part of the home dashboard – as is evident from the house icon association.

If a new, custom dashboard were created, you would use the Manage Dashboard form to assign it as your new Home Dashboard view.

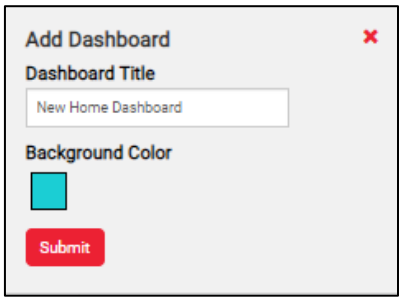
To add a new dashboard, click the Add New Dashboard button.



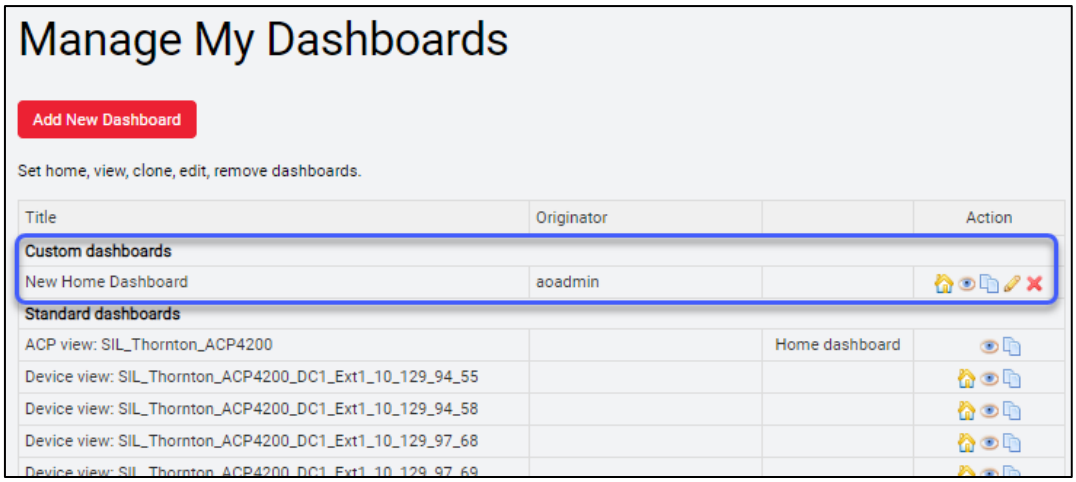
Give the new dashboard a name and then, if a different background color than white is desired,

click the **Background Color** square to open the color palette for selection. Slide the mouse pointer over the color bar until the preferred spectrum is shown in the window to the left. Then move the cross bar around the square until the desired color is displayed in the top level box to the right – the selected color will also appear in the Background Color box.

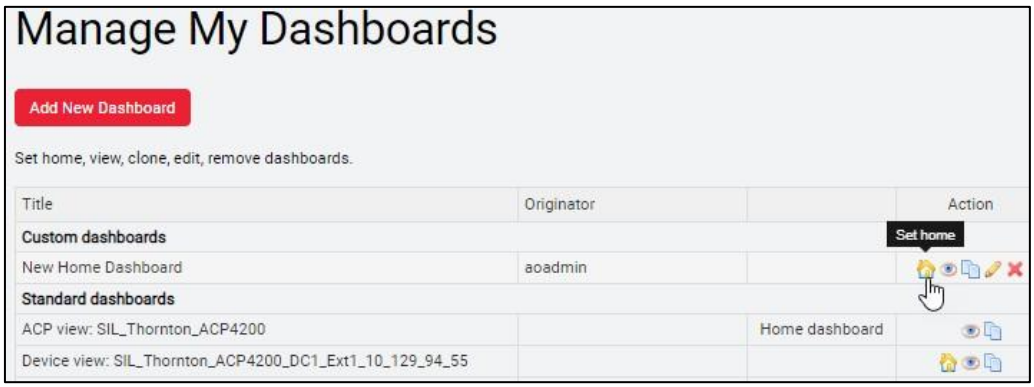
Then click **Submit**.



The new dashboard is then incorporated and is labeled as being originated by the login that created it.

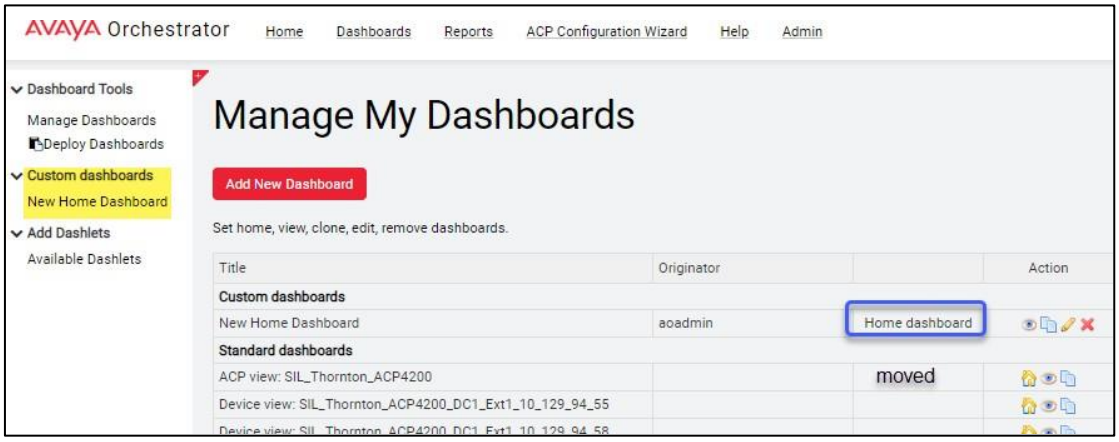


Click on the house icon to set the new dashboard as the new preferred Home Dashboard.



The Home Dashboard label is associated to the new element accordingly and the new

dashboard becomes part of the **Custom dashboards** menu.

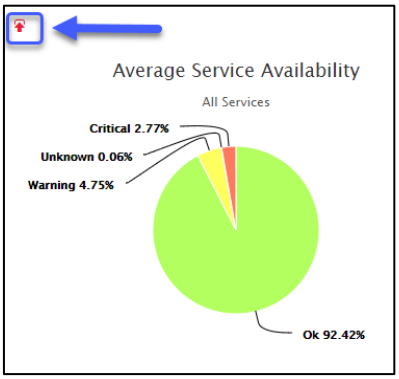


Now add some items into your new dashboard.

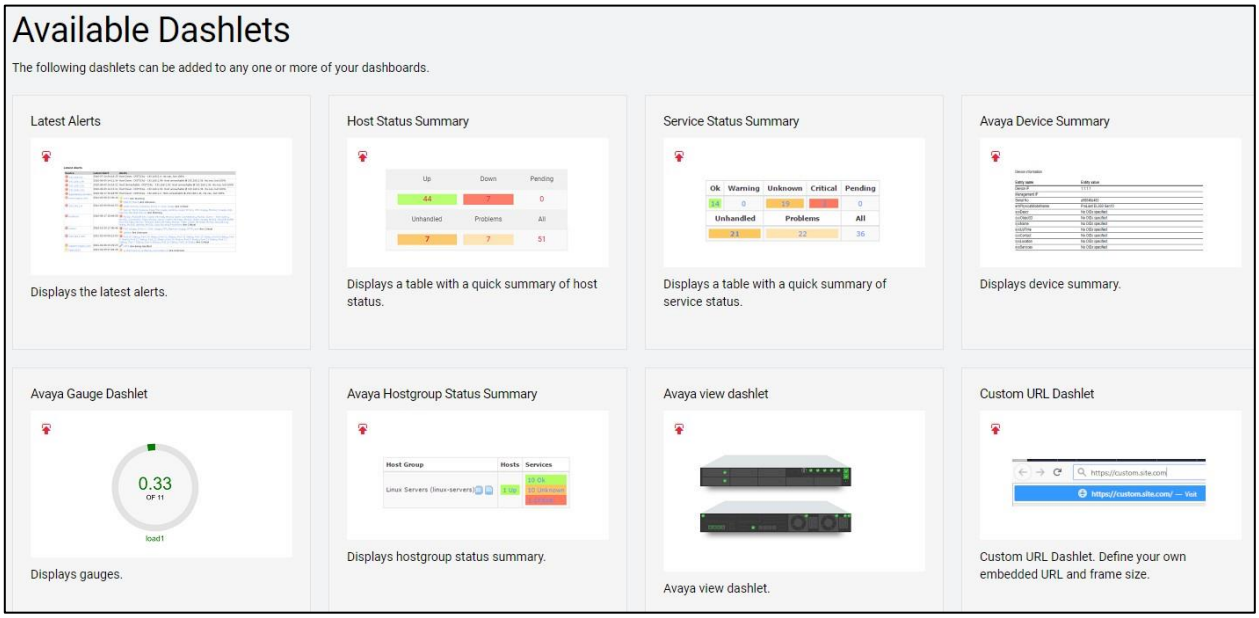
Add Dashlets

About this task
Use the information in this section to build a Dashboard “home page” monitoring view.

All dashboards are comprised of dashlets. A dashlet is easily recognized as a viewable reporting element that has a red arrow in the upper-left corner of its reporting screen.

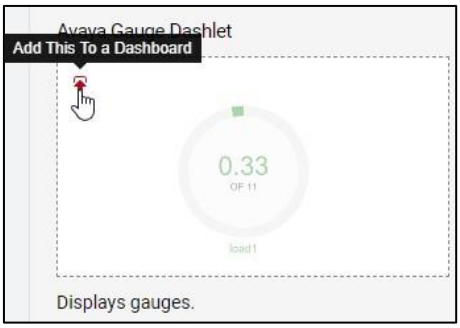


Dashlets can be found under a variety of menu options, such as the ACP Dashboard Home, Reports, and Admin submenus. The composite selection is located under **Dashboards** > **Add Dashlets** > **Available Dashlets** menu.

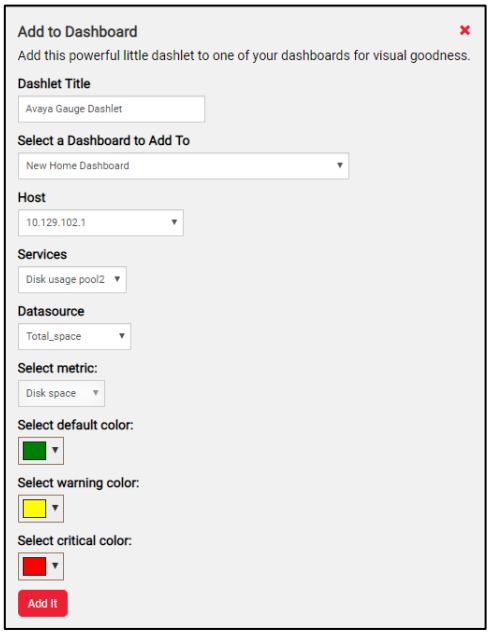


Add a dashlet to a specific dashboard.

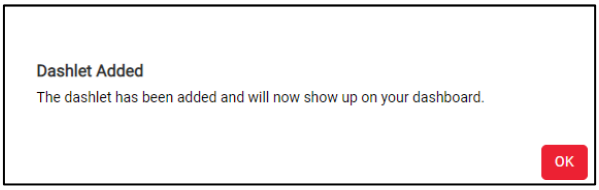
1. Click on the red arrow on the desired dashlet.



2. Provide a Dashlet Title – a default is provided but you may assign a new name. From the **Select a Dashboard to add to** drop down menu, locate your new dashboard title and select it. Complete the other selections for each dashlet, and then click the **Add it** button.

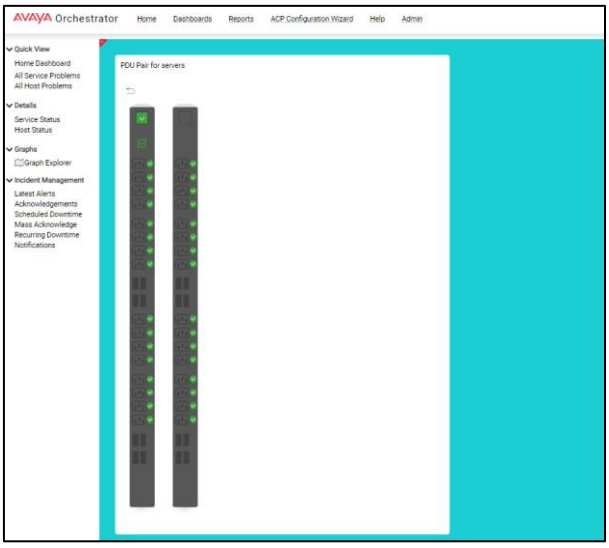


3. The dashlet is added to your dashboard.

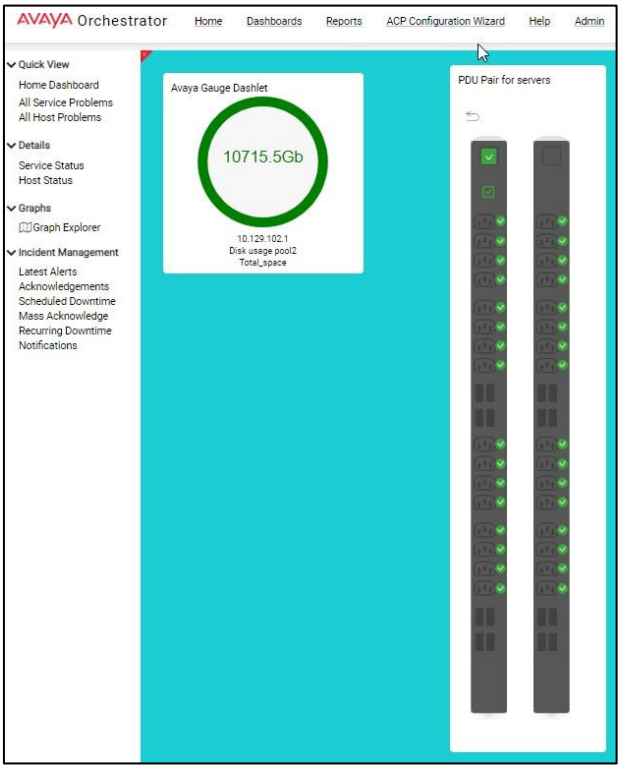


4. Add another to view the layout of multiple dashlets.

5. Open your new dashboard by clicking **Home** on the top menu bar. The Home Dashboard page opens to reveal your new dashboard.



6. All dashlets will be layered one atop the other. You must relocate the elements annually, placing them where you want them on the dashboard page. You may resize the dashlet boxes to better suite the elemental views.



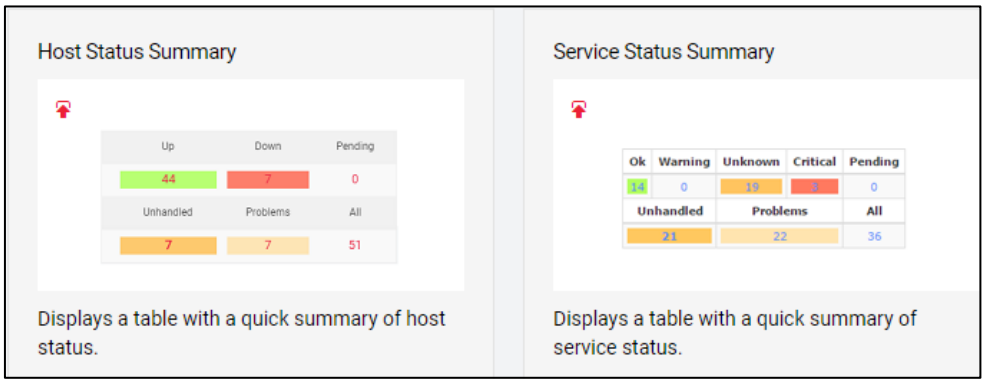
Any time you want to change the Home Dashboard view back to the standard view, or to a new dashboard view, use the Manage Dashboard page to select the desired home view.

The Dashlets

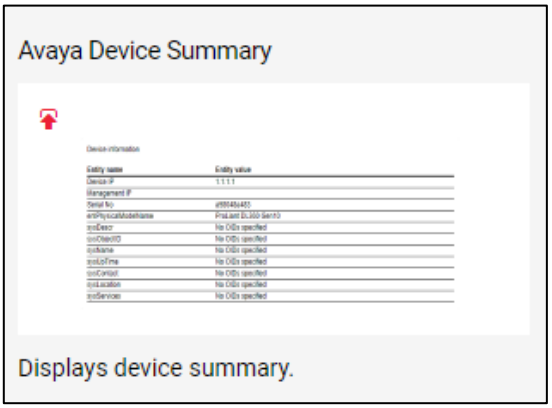
- **Latest Alerts**
  This dashlet will produce a top 20 list of the latest alerts received by AO. The dashlet will be updated as new alert information is processed.



- **Host and Service Status Summary**
  These are the solution collective data points that provide the 30k view. These dashlets provide drill down options and continually update as new information is learned and processed by AO.



- **Avaya Device Summary**
  The information provided by this dashlet is specific to each device. The listed details related to serial numbers, device IP, management IP and other contact and support information. A collection of these dashlets on the same dashboard page, representing all servers, for example, could provide a quick one-stop view for gathering specific device group related information for services activities.

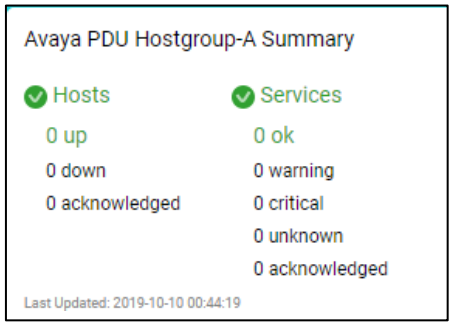


- **Avaya Gauge Dashlet**
  The gauge dashlet can provide a variety of elemental views per hosts and services. For example, select a storage device and monitor a gauge on storage capacity available, or used.



- **Avaya Hostgroup Status Summary**

  This dashlet allows you to build a more specific variety of the same host summary groups seen on the default Home Dashboard page – from Compute Group, Storage, Network and Power groups. You can opt to monitor servers from a specific cabinet, or build a server group representing UC production and then another group representing CCE activities specifically, for a more meaningful monitoring view for your business needs.

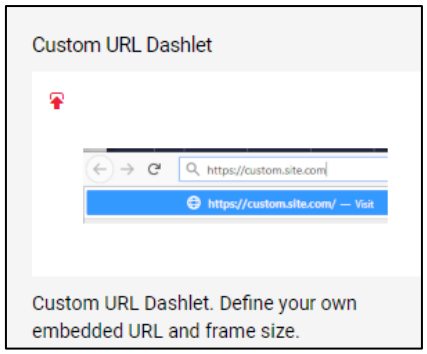


- **Avaya View Dashlet**

This is a device gui specific view dashlet. It could be useful for elements that have recently been upgraded or had parts replaced, or some other conditional state, like capacities that are running high as you await the arrival and deployment of additional devices. Use this dashlet to more closely monitor devices that need focus, even if only temporarily.



- **Custom URL Dashlet**
  Use this dashlet to reach out to applications that allow this type of access point through a browser.



Deploying dashboard

About this task

Use this procedure to deploy your dashboard for other Avaya Orchestrator™ users.

There is no need to deploy the default Home Dashboard for any users. All users get the basic license dashboard view, unless restricted through the user level permissions by a system administrator.

Before you begin

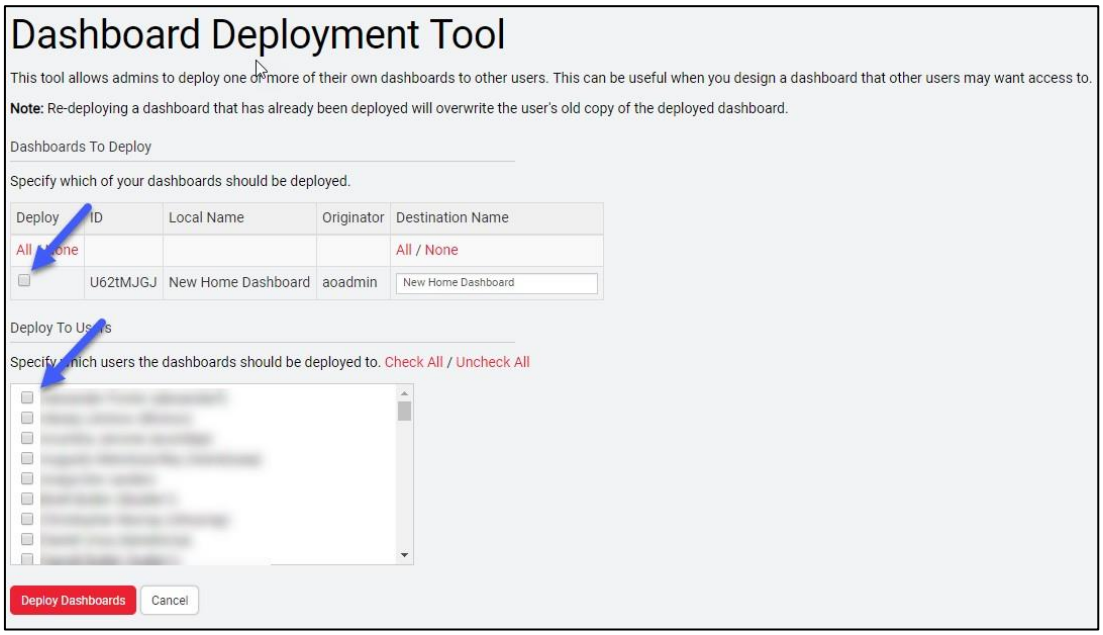
You must have administrative user rights to perform this task. The default login of aoadmin provides this permission.

Procedure

1. After building dashboards you wish to share, go to **Dashboards > Dashboard Tools > Deploy Dashboards.**

   From the list of available dashboards, select the ones you would like others to have access to run. You may select a single one at a time, or click the “All” to have all reports in the custom list checked.

2. Select the users you want to have access to the checked/selected dashboards.
3. Click **Deploy Dashboards.**

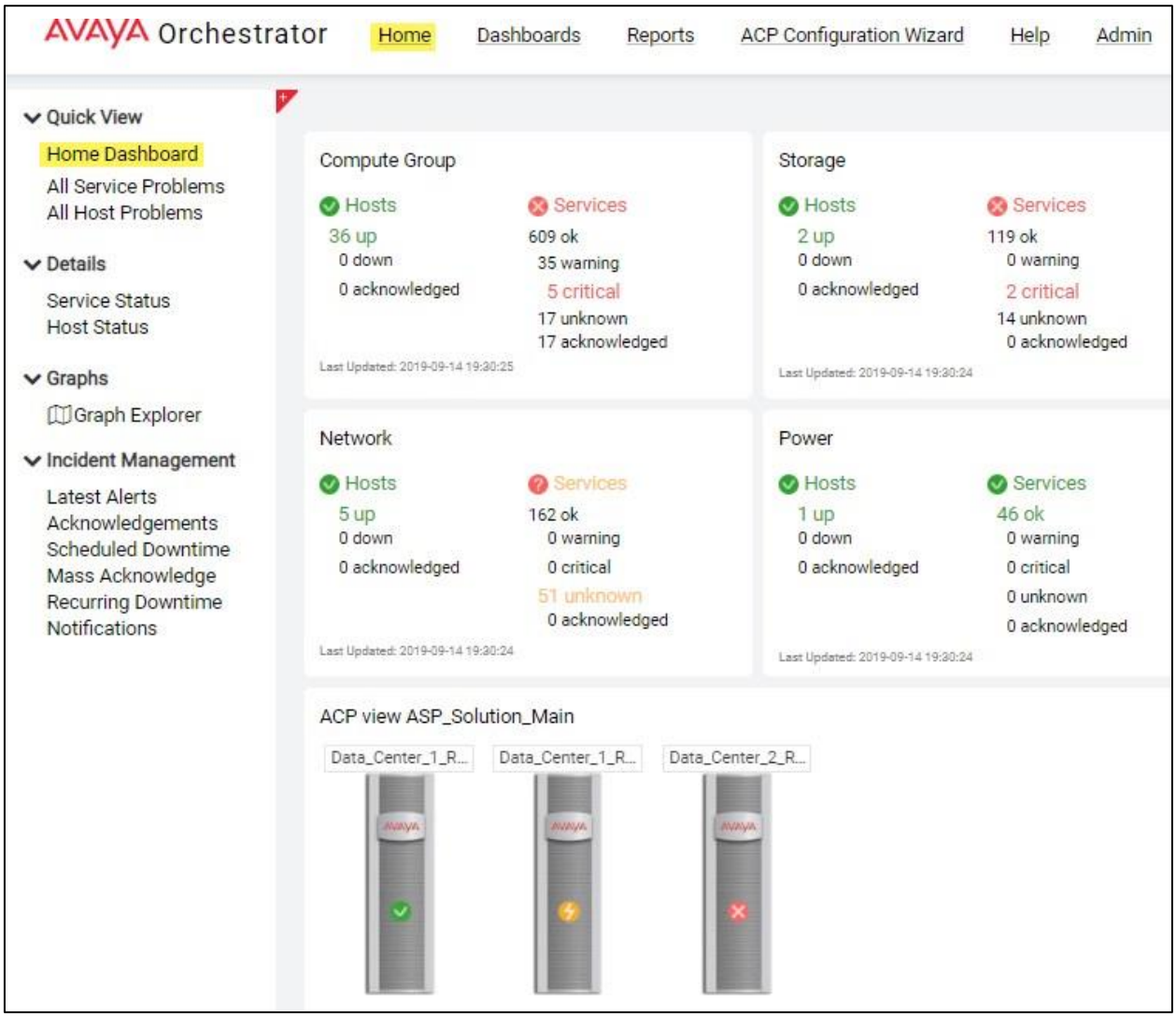


Chapter 8: Dashboard Overview

This chapter provides information about how to use and interpret the various dashboard options in Avaya Orchestrator™.

Avaya Converged Platform (ACP) Dashboard

The ACP dashboard is available on **Home** > **Quick View** > **Home Dashboard**.



The main dashboard displays summary information about the devices and related services installed in a solution. There are two perspectives represented on the primary dashboard. The

first provides a one-stop glance at the state-of-health per device group, and the second presents the relationship of those states within each rack.

Home Dashboard Dashlets

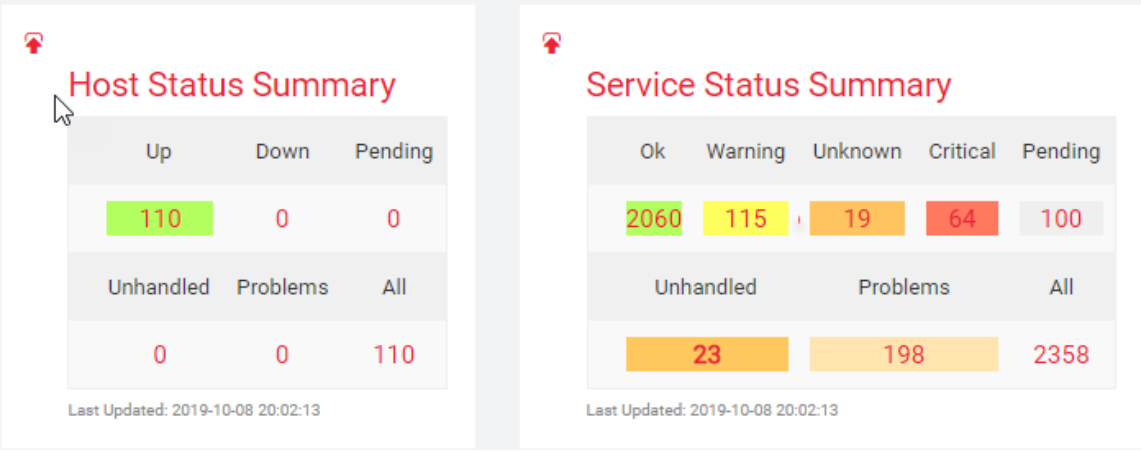
Each dashlet summarizes information for the corresponding group of devices:

Compute group: Compute servers
Storage: Storage devices
Network: Network switches
Power: PDUs

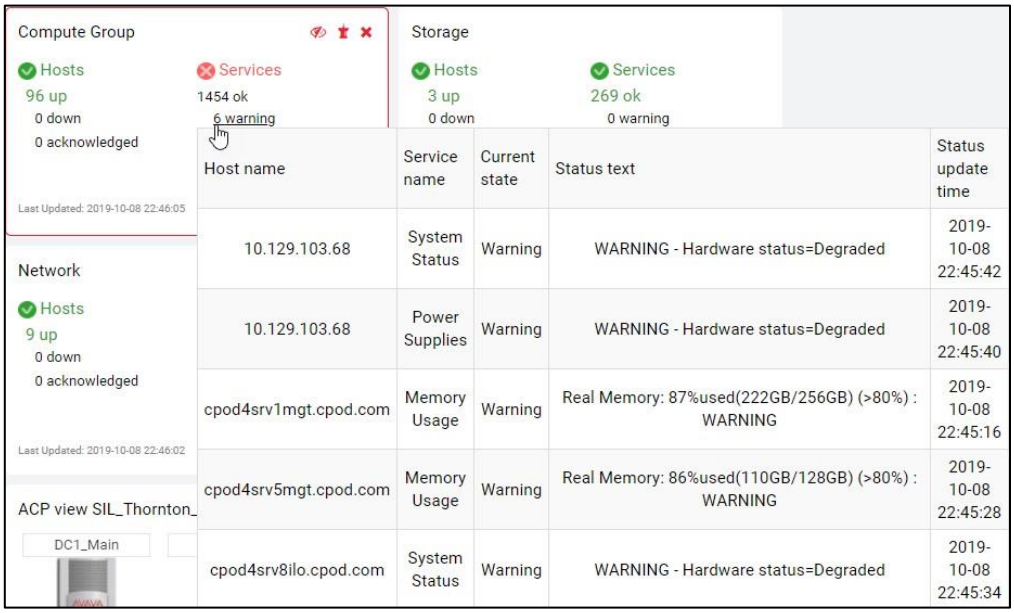
The related information displayed for each group depends on the specific view being monitored. For example, on the main dashboard below, the dashlets provide group information for the entire ACP solution. However, in the drill-down rack views, the dashlet groups and their representative information show status for a specific rack only.

Within each dashlet group is a run-down of the various active states for each host and related service state: Up, Down, Unreachable, Ok, Warning, Critical, Unknown, and Acknowledged. You can hover the mouse over each of the dashlet's green, amber, or red state-of-health links to view a summary of the most recent and high runner related events.

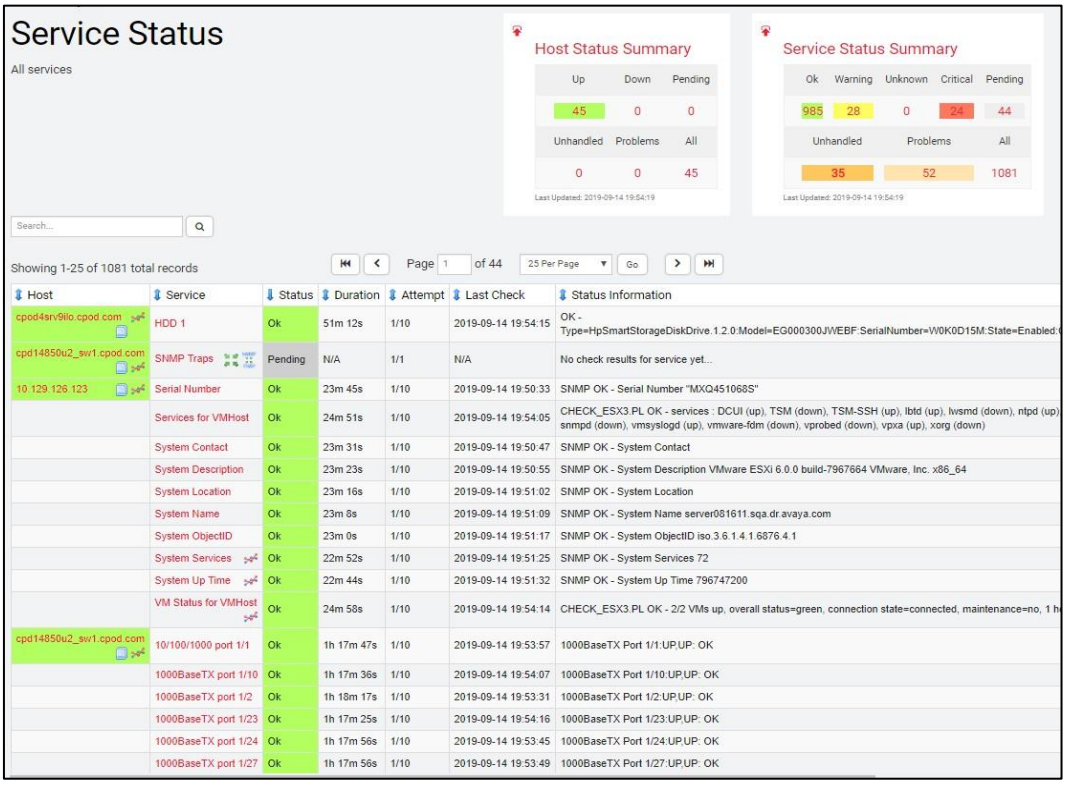
The **Host Status Summary** and **Service Status Summary** dashlets are presented across the top of many report views. They provide a collective bird's eye view of overall solution state-of-health and are automatically updated every 60 seconds. These dashlets are visible from the service and host problem reports as well as the service and host status reports.



The following is an example of a dashlet summary:



The preceding dashlet view shows the six Warnings in the Compute Group device node grouping. If there are more issues than can be easily displayed and read in the pop-up window, you can click on the numerical values, in this case the **6 warning** link, for a drill-down view of all the **Serv vice Status** report incidents, as can be seen in the following screenshot. This report provides a variety of options for prioritizing the list by allowing you to click any of the blue arrows within the list header: Host, Service, Status, Duration, Attempt, Last Check or Status Information prioritization.

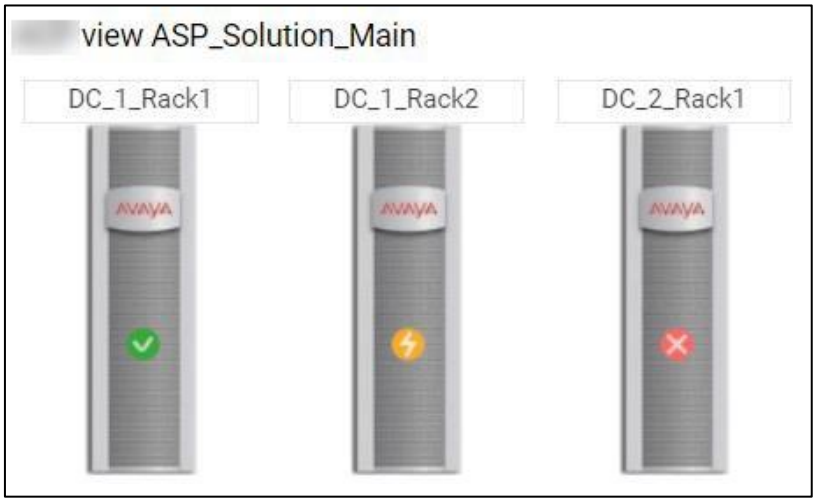


You can view a similar **Service Status** report through a menu option on the far-left side of the AO Home menu page under **All Service Problems**. However, the default view reported within each selection is different and is based on the intent of each menu selection. In the **All Service Problems** view, all issues for all device services are presented – no OK status states are represented. In the previous example, by clicking on the link for **6 warning** within the Compute Group box, only the specific warning alarms/traps for the server group are presented. By contrast, all *status* reports will provide all host and service-related information – all known issues plus all known OK states.

State-of-health information is also shown in the rack view. At the bottom of the Home Dashboard view are rack icons that provide state-of-health indications for the hardware devices deployed within each rack.

For example, if the Network dashlet reports a critical alarm in the Storage block, the rack containing the alarming storage array reports the critical alarm also. Thus, targeting the location of the alarmed device. You can click on the rack that contains the device to get a more detailed view of the device.

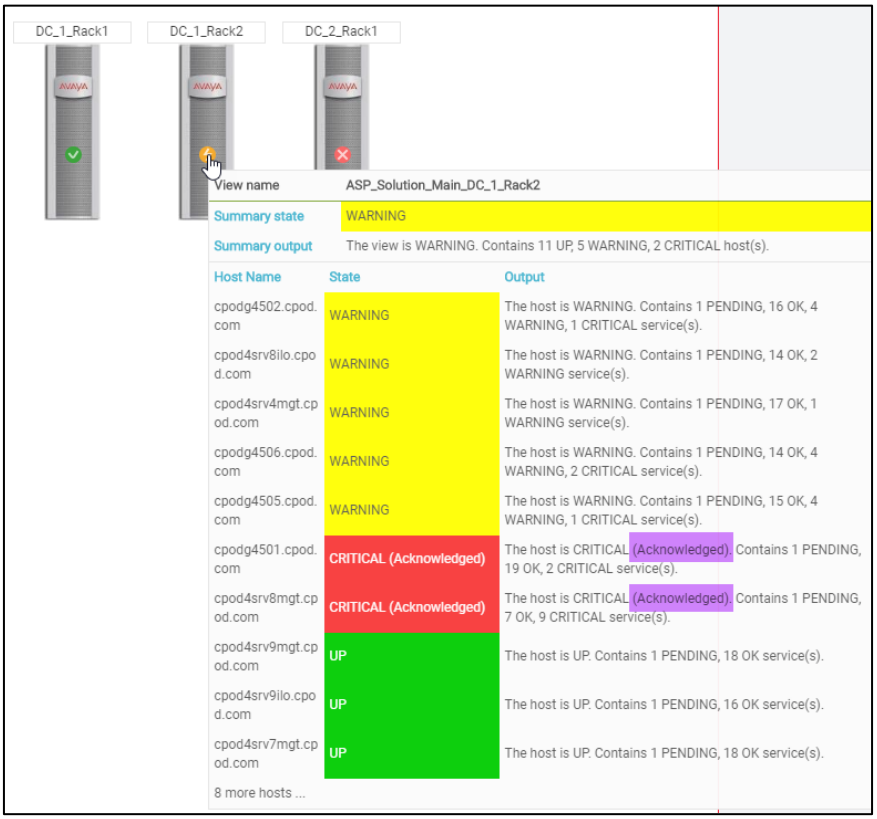
The rack status icon reflects the highest level of trap. For example, if the alarms for devices inside DC_2_Rack1 are represented by four warnings and one critical trap received, the rack icon shows a red icon that represents the highest-level critical alarm. In the following example, DC_1_Rack1 has no warnings and no critical alarms, DC_1_Rack2 has at least one warning on a deployed device and no critical alarms, and DC_2_Rack1 has at least one critical alarm.



You can hover over a rack status icon to view the state summary. Similar to the dashlet links, you can drill down into each specific area for a complete view.

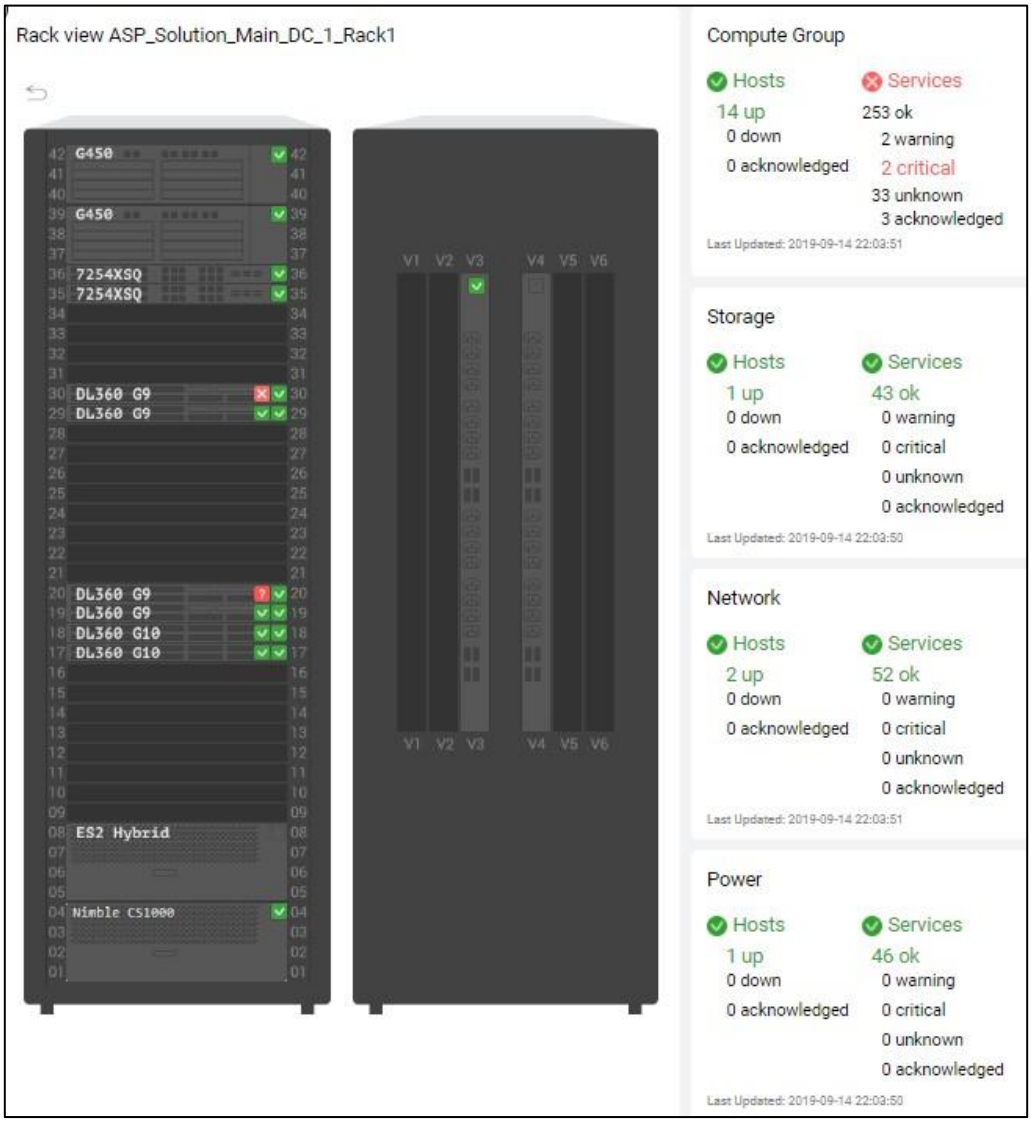
In the example hover-view below, the information is taken from the middle cabinet. You will see the Warning alarms are placed at the top of the alerting list and the Critical alarms are below them. This is because the Critical alarms have been *Acknowledged.*

An acknowledge alarm is one that is already known by the support team and is, therefore, identified and being worked. The Warning alarms that are yet to be acknowledged are considered unknown and will be represented as a higher priority. When acknowledgements are selected, the default is to disable the visual notifications from the high-level Home Dashboard view. By doing so, the visual slate is cleared of known issues, making any new incoming alarms more easily recognizable. This is why, in the previous example, Warning alarms are placed at the top of a hover-view listing over Critical alarms and why the cabinet reflects a Warning (yellow) status and not a Critical (red) status icon.



Rack dashboard

The Rack dashboard contains detailed information about the rack elements. This is the best area to begin any investigative work when reviewing issues with devices. The dashboards available within the rack view offer more than just a visual reference. You can use the administrative controls within the drill-down option to edit service settings, send notifications, and even control the representation of alarms to the user communities.



The same familiar group of dashlets are present to provide a high-level state-of-health status. Each dashlet summarizes information of the corresponding group of devices within the rack bring viewed: Compute group, Storage, Network, and Power.

Within a server device in the view above, where the icon for the iLO port is located, you will see a ? symbol. This represents an *unknown* state. When Avaya Orchestrator™ is unable to access any IP port for a proactive state-of-health check, the failure reflects as unknown rather than the previous known state. This is a truthful reflection of the current status and if such a symbol is consistently seen across the device, that indicates an unstable network.

Within each grouping, two process areas are monitored: Hosts and Services.

Hosts Status

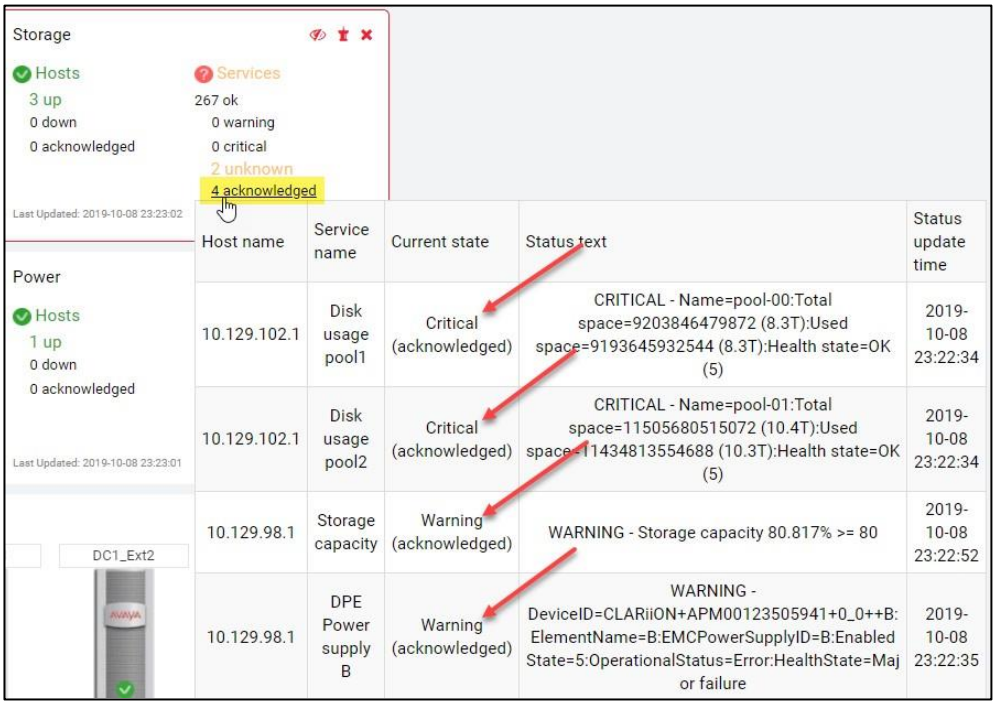
The Host status represents the accessibility of the IP address of each node/device. A device is either up (accessible), or down (not accessible). If it is down, the service elements within an inaccessible device will be reported with *unknown* states. Without access through the IP interface, there is no way for AO to inquire from the device about the internal service elements – their state of health will be *unknown*.

Service Status

The Service Status represents the individual function on each device that provides state-of-health information through received SNMP trap information, or through a proactive check via a REST or CLI API information exchange with AO. For example, the iLO IP port on a server represents a *Host* element. Within that Host element – on the server, exists fans, CPUs, temperature readings, NICs, etc., that report their state of health through the iLO Host element; these components are the *Service* elements on that Host.

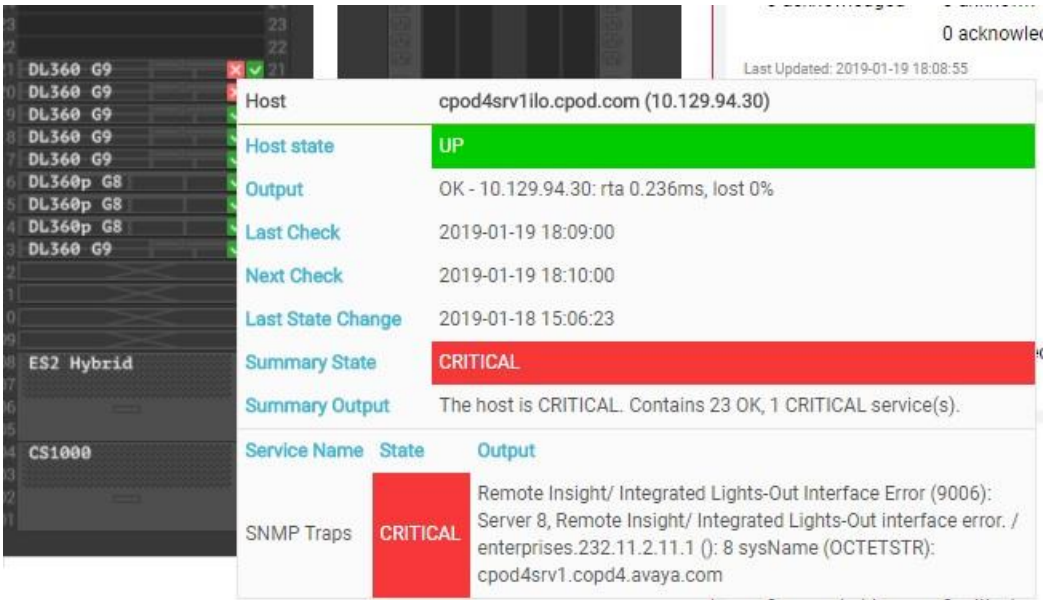
Each status area can have an *acknowledged* state; this represents an intentional and manual intervention on the part of users. Acknowledgements is a key status-flag area to review, because it can explain what appears to be a conflict in the representation of alarms on devices. For more information about the status area, see Service Status Detail. As previously noted, if an alarm is acknowledged, the Home Dashboard will report the alarm under the “acknowledged” category and will remove it from the critical or warning category – on the birds-eye-view only. This allows any new alarms to become more visually eye catching and obvious to data center administrators.

In the example, below, the 4 acknowledged alarms are still visible through the hovering mechanism.



You can hover over each dashlet or drill down into the colored dashlet links to view a reporting window. The interactive reports provide the state-of-health for the selected element group in the rack being viewed.

The colored status icons on each device in the rack image provide a similar high-level view when hovering your mouse over a green, amber, or red status lamp. The following is an example when you hover over a critical indicator on a Compute Group element (server).

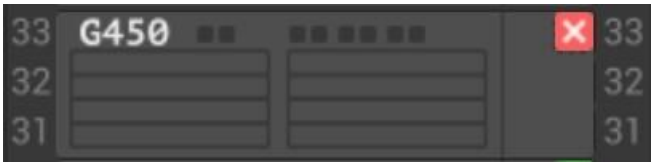


You can also click directly on a device to drill down into a more detailed view of a specific component. For more information, see Device dashboard.

The Rack dashboard also contains a visual representation of the elements in the rack. The following table contains information about the icons that represent various element states.

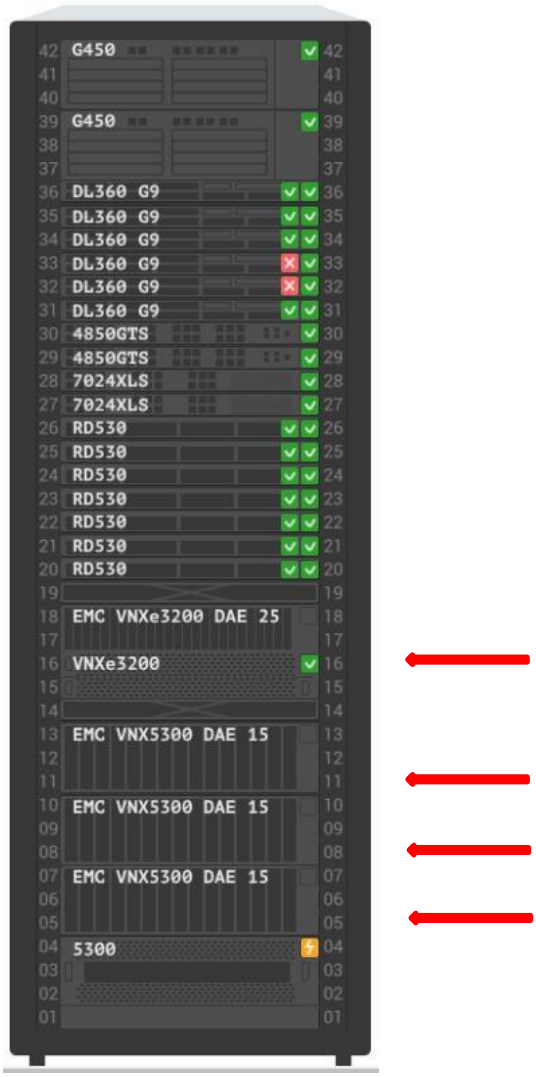
Element state	Icon
Operational and running without warnings	
Operational but some warnings present	
Not operational or critical issues present	
Unreachable	
Unchecked	

The following is an example of a representation of a G450 that is not operational or has critical issues.



Some rack slots contain fillers, storage extensions, and other elements that do not have detailed information to display. When you click these elements, the Device Dashboard is not displayed.

In the following example, the storage extensions for the EMC 3200 and 5300 Storage Arrays represent filler-elements. They do not have their own IP addresses, and therefore, cannot report their state-of-health status to AO. Instead, their status is reported by the EMC Controller, seen at the bottom of the rack. However, it is important to have representation for the expansion units in their proper rack position. The expansion components are added during the administration process, which is covered later in this guide. The same type of configuration is true for the CS1000 Nimble Array and its expansion units.



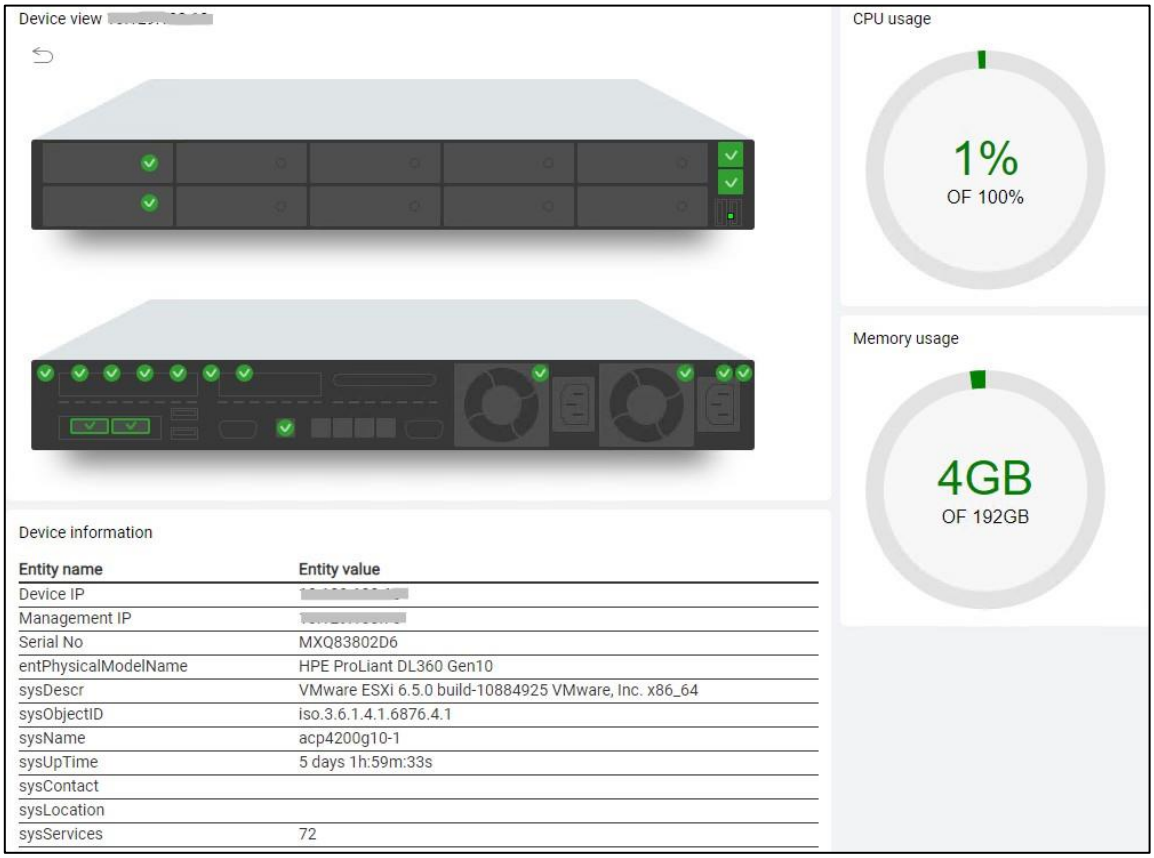
Device dashboard

You can click any element in the Rack dashboard to view the Device dashboard[2].

The following is an example of the Device dashboard for a compute server:

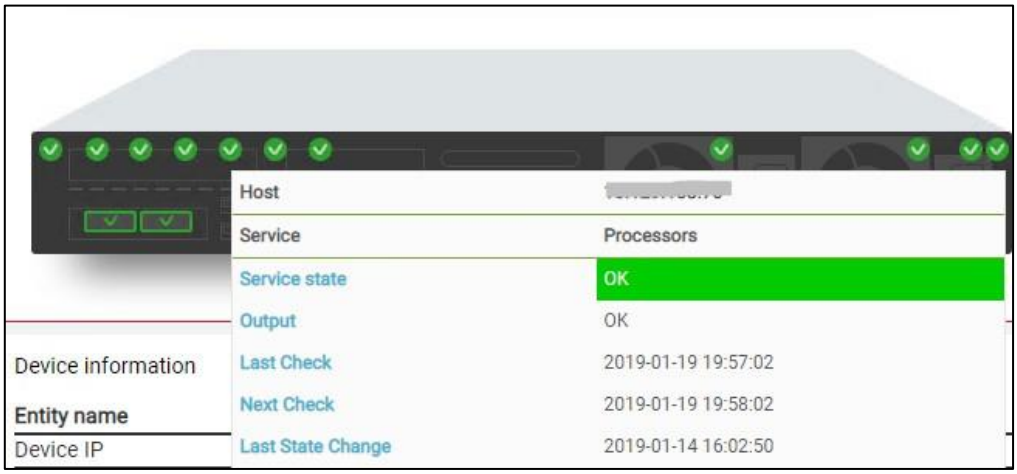
HPE Gen10 Compute Server

[2] This applies to device elements that are not fillers for slots or media devices, or expansion units for storage arrays.



The compute server has two IP addresses assigned: ESXi and iLO interfaces. The Device IP represents the ESXi element and the Management IP represents the iLO element. Other helpful product information is also captured in this dashboard, such as, product serial number, product model number, vendor product description, and host name. Additionally, there is a bird's eye view of the CPU and Memory usage consumption along with the total available memory footprint displayed alongside the device view.

You can hover over each individual status icon to view high-level service description, state-of-health report, IP address of the "host" providing the service status, and the time stamp of the last health check-in.



Services Status Detail

Each hardware device has a unique set of service icons represented in the GUI image. Some are located, where possible, atop or near the elements they are monitoring. Others, such as the ones seen on the upper left of the compute server, represent key hardware functions that are proactively monitored by AO. For example, memory, processors, temperature, and fans.

Other status details, such as the icons on the lower left of the compute server, monitor the Ethernet connections or the power supplies. There are always icons present for SNMP trap receipt reporting. The status changes for the SNMP icon relate to several areas of elemental changes on the device. For more information about this icon, see Chapter 16: Maintenance and Troubleshooting.

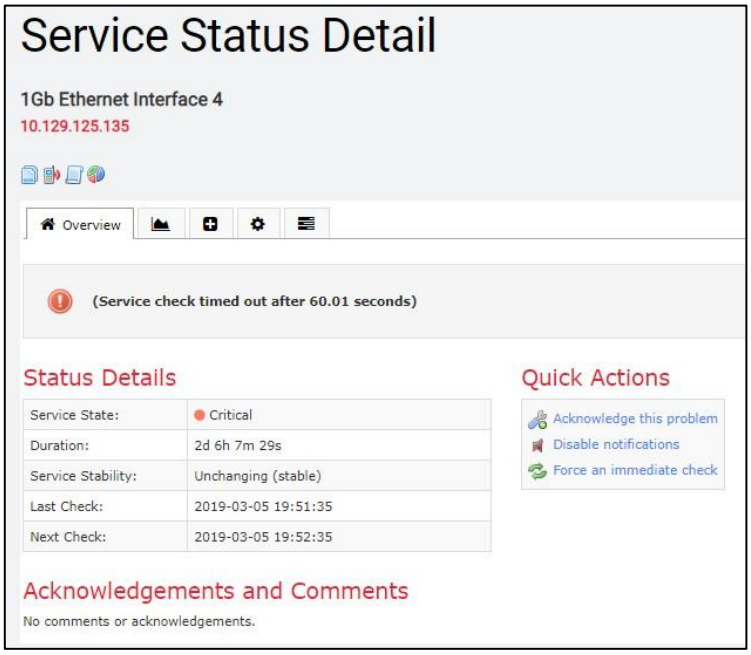
Clicking on the service icon as shown in the preceding example, that is, the “Processors” related green-check icon, opens an additional level of detail about the specific service state.

Overview tab

The following screen shot shows the view of a healthy processor. The highlighted icons provide additional drill-down:

From left to right, the icons represent one-click redirection to the following reports:

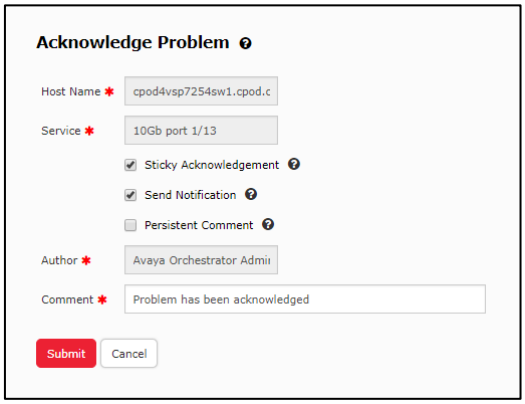
- Current Status for Host Service (Service Status report)
- View Service Notifications
- View Service History
- View Service Availability



Quick Actions

a. **Acknowledge this problem**

When a user is handling a specific issue, understands the nature of the alarm and is ready to post information about it and stop the associated Email/SMS notification process for the issue, the acknowledgement process is an appropriate selection. This function can stop notifications until the problem is resolved as well as provide notes for other users about the nature of the issue as well as flag the name of the person working the issue via the login of the one acknowledging the issue. This flagging of the logged in user's handle demonstrates the importance of assigning each user a unique login for AO.



The following are the options for an acknowledgement message:

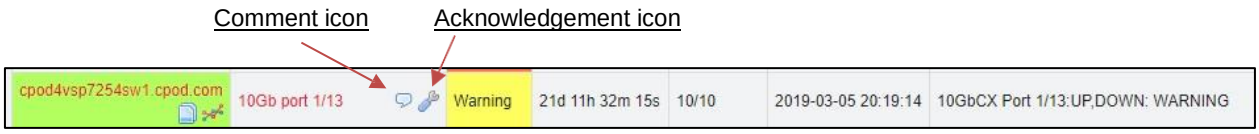
- **Sticky Acknowledgement**:
  - Selecting the **Sticky Acknowledgement** check box causes the acknowledgement to consistently stop any further notification Email/SMS messages until the problem is resolved. At that time, the acknowledgement is removed and is no longer required.

- Clearing the **Sticky Acknowledgement** check box causes notifications to continue to be sent until the associated problem is resolved.

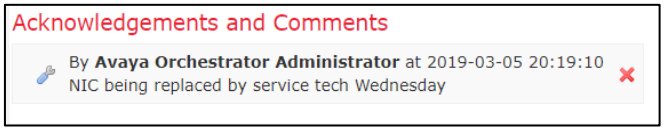
- **Send Notification**:
  - Selecting the **Send Notification** check box creates an Email/SMS notification stating the specific problem has been acknowledged.

- **Persistent Comment**:
  - Select the **Persistent Comment** check box to retain the comment after the problem is resolved or the acknowledgement is removed.

Acknowledging a problem provides the ability to associate a comment to the problem and creates a wrench icon next to the service or host problem that is acknowledged.



After you add a comment, the comment appears at the bottom of the Host or Service Detail Overview tab.



b. **Disable notifications**

If the processor in this example is serviced and taken down, you can click on the **Disable notifications** option to prevent Email and SMS notifications from being sent while the processor is unavailable. After you click the **Disable notifications** option, the option changes to **Enable notifications**, so that when the processor is brought back into service, you can click the **Enable notifications** option to re-establish alerting notifications.

When you click the **Disable notifications** option, the associated icon appears next to the service or host that has the notifications disabled by using this method. The following is an example from the All Service Problems report.



c. **Force an Immediate Check**

This option applies to passive alarms only, or SNMP Traps only. When an SNMP trap is received, it must be manually cleared. Many HW devices do not provide proper SNMP messages to notify when specific alarms are cleared. To provide a more consistent and

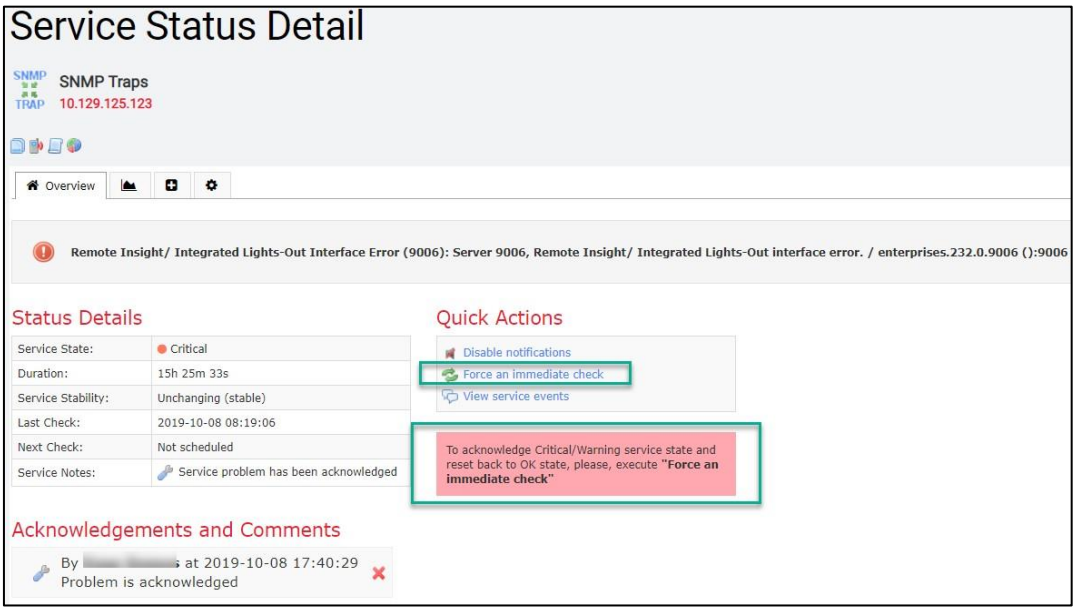
certain behavior, AO will report the alarm, but you must reset the trap to an OK state once the alarm is cleared.

When an SNMP alarm has been addressed and the you are ready to reset the status to OK:

- Navigate to the All Service Problems menu item.
- In the search window, enter the IP address or FQDN of the host that is reporting the SNMP trap.
- Find the SNMP Traps alarm and click on the SNMP symbol.



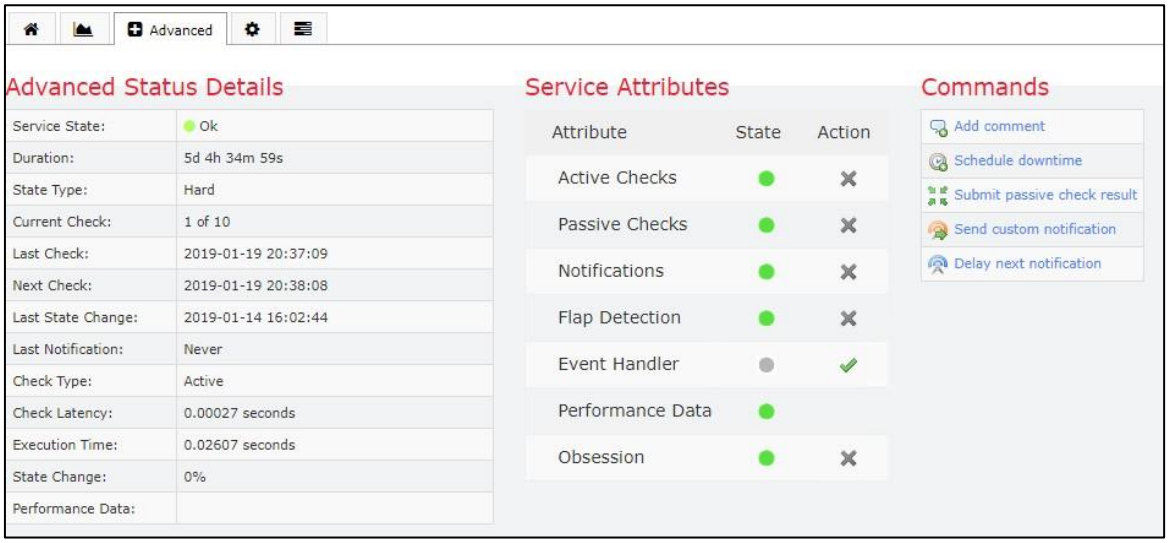
This click will drill down to the SNMP Service Status Detail page. Here is where you may click on the *Force Immediate Check* option to reset the trap status.



Once reset, the previously displayed SNMP trap will be removed from view.

Advanced tab

The following is an example of the **Advanced** tab that is provided in the service drill-down option.



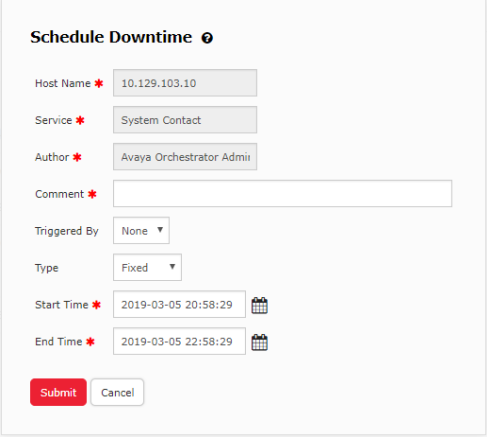
Service Attributes

These elements control the data collection process. There should be no need to change any of the settings in this area. These are more for Avaya services personnel to use during debug timeframes.

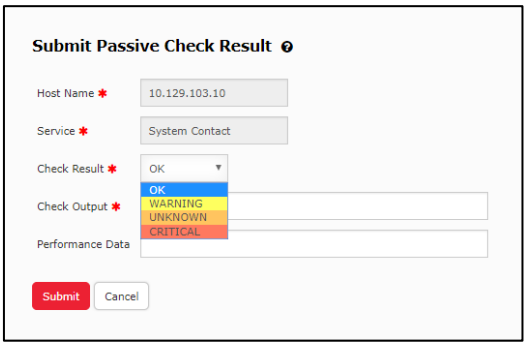
Commands options

The ***Commands*** area has options to configure the required downtime for the service.

- **Add comment**: Use this option to add a comment for the problem, without acknowledging the problem.
- **Schedule downtime**: There is a separate menu item for this activity, but it is also accessible here in the **Advanced** tab. You can add comments as well as administer a specific window of downtime that stops all notifications during that maintenance period.



- **Submit passive check result**: Use this option to change the reference alarm level and the associated alarm out message for problems. The option that you select in the **Check Result** field is the new reflected level of alarm, and the option that you select in the **Check Output** field is the associated alarm verbiage represented in reports.



- **Send customer notification**: Use this option to send an updated comment to an Email or SMS notification. Select the “Forced” option to send the notifications immediately, regardless of the users’ administered selected Time-of-Day preferences for notification receipt.

- **Delay next notification**: Use this option to delay notifications for up to 999 minutes instead of acknowledging an issue and stopping notifications all together.

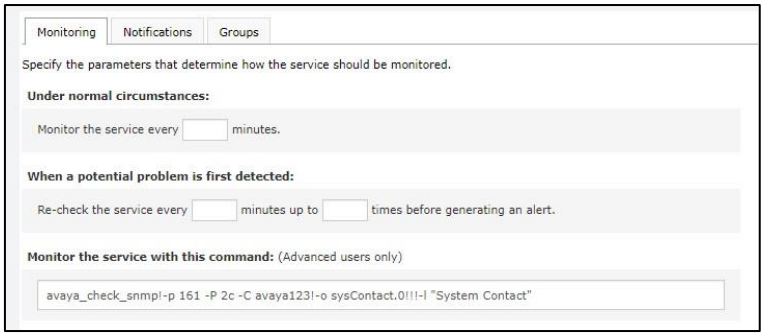
Configure tab



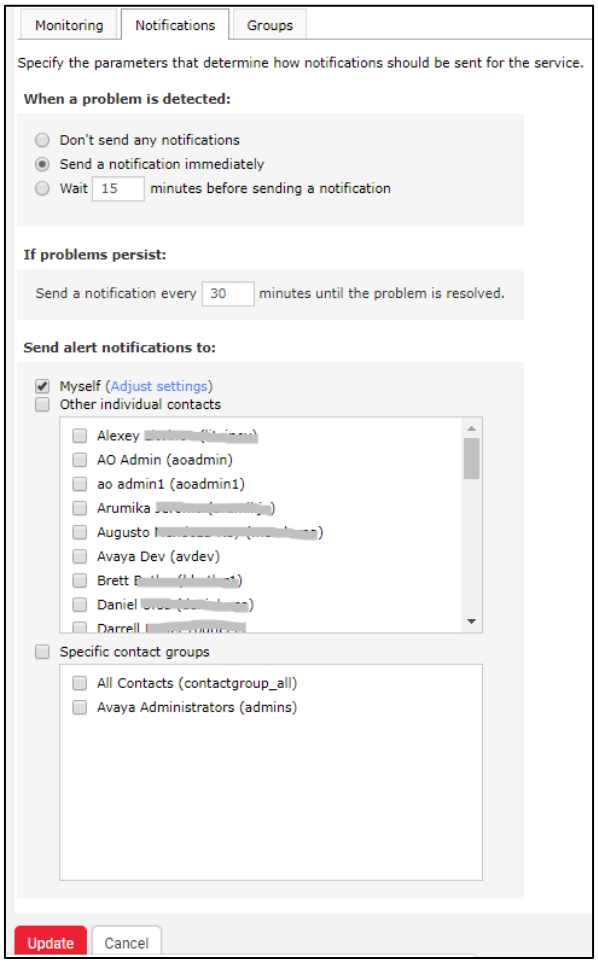
On the **Configure** tab, you can delete the service from the device, or edit some of the service settings.

The following are examples of settings available under **Re-configure this service**.

- **Monitoring**: Administer the time/rate the service is monitored by AO.



- **Notifications**: Stop notifications, delay notifications, or set specific time frames for consistent notifications when alarms for the service are received. Select the users and/or groups to receive notifications related to the service.



Chapter 9: Host and Service Details

Overview

This chapter contains information about how to use the different features of the Avaya Orchestrator™ interface to view information about hosts and services. The **Details** menu offers different ways to view the status of the hosts and services. For example, in larger environments, users may want to view status by host or service group, but in smaller environments users may prefer to view status by device.

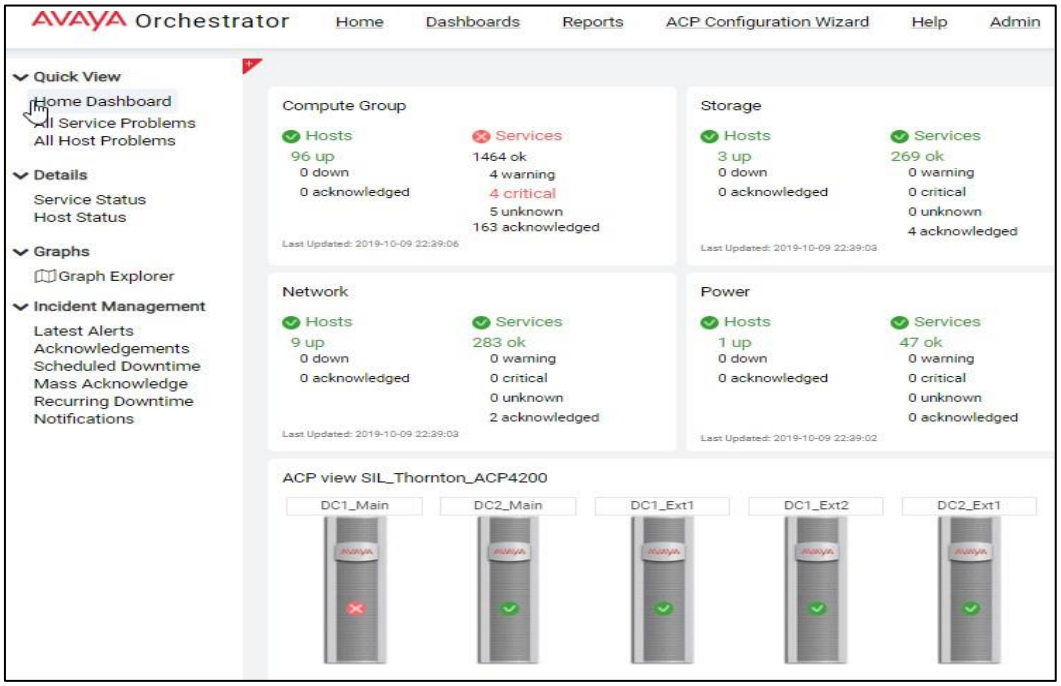
Avaya Orchestrator™ provides the following options to view host and service details:

- Individual hosts or services
- Host or service group summaries
- Host or service group overviews
- Host or service group grids

Service Status overview

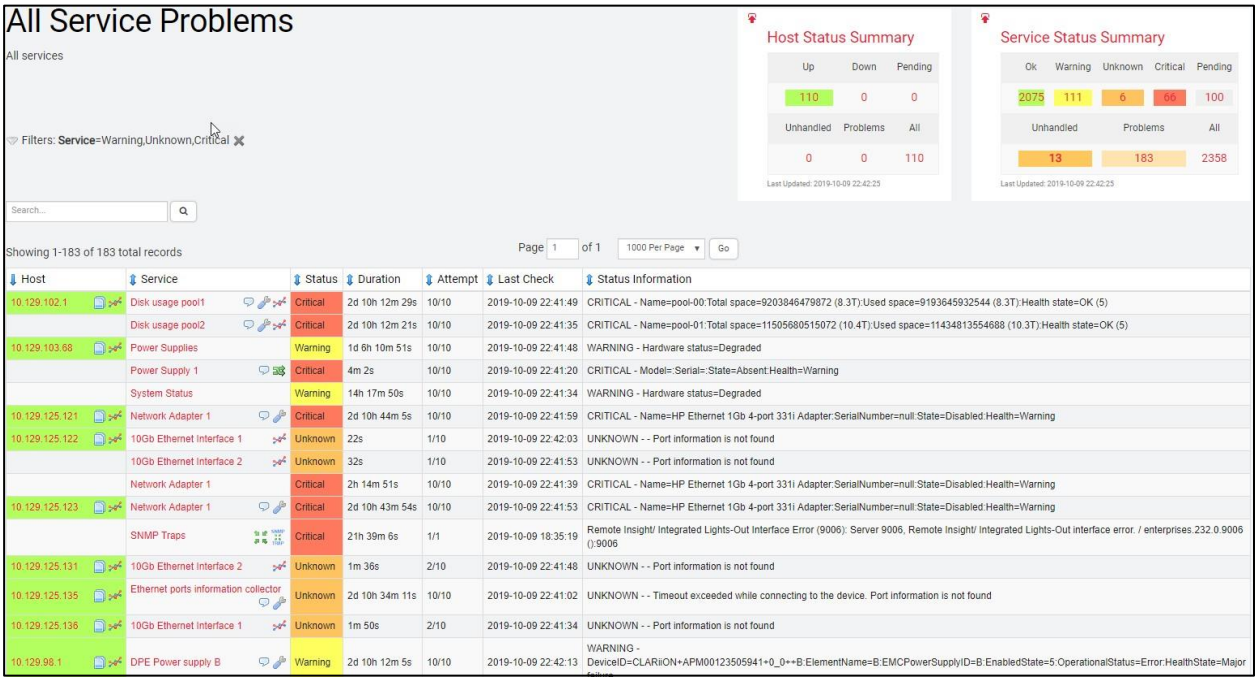
There are two high-level service related real-time reports

- **Home** > **Quick View** > **All Service Problems**.
- **Home** > **Details** > **Service Status**.



All Service Problems

Purpose
This report provides a view only of all warnings and problems associated with the reported devices. There is no information provided for hosts services in an OK state.



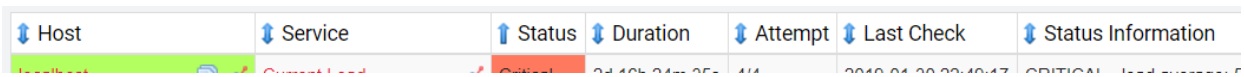
You can click the sort icon at top of the column to sort the alarms by the data in that column.

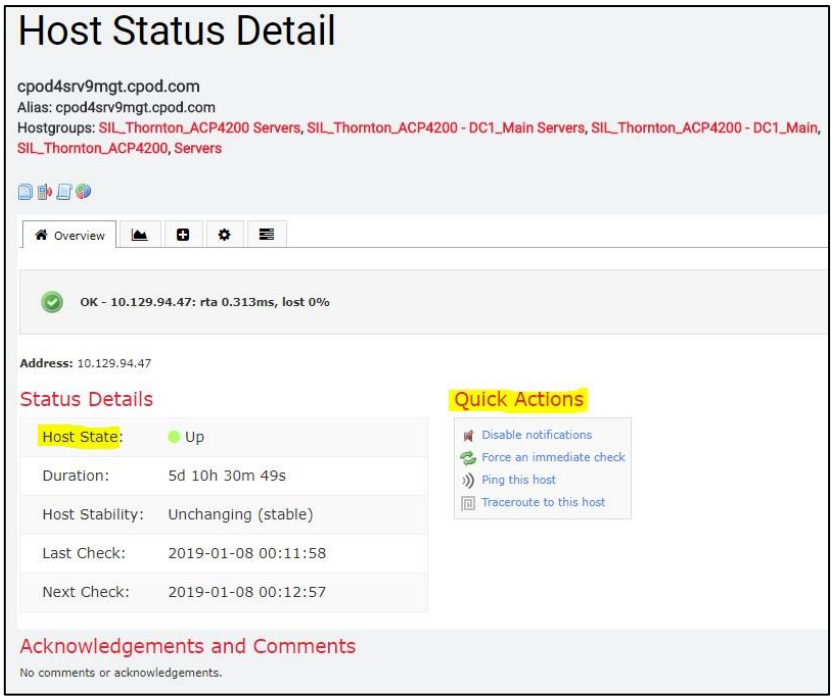
Service Problems

- **Host**: The specific device reporting an alarm event.
- **Service**: The specific function within the host that is reporting an alarm event.
- **Status**: Sort alarm events by “critical” events or “warning” events.
- **Duration**: Sort alarm events based on the length of time in the particular state.
- **Attempt**: List reports based on the number of successful checks and responses.
- **Last Check**: Sort alarms in sequence based on the last updated status.
- **Status Information**: Sort alarm events based on the type of service/host event reported.

You can click each host and service in the **Host** and **Service** columns respectively to view more information about that specific device or service. For example, if you click a host in the **Host** column, the **Host Status Detail** page for that host device appears.

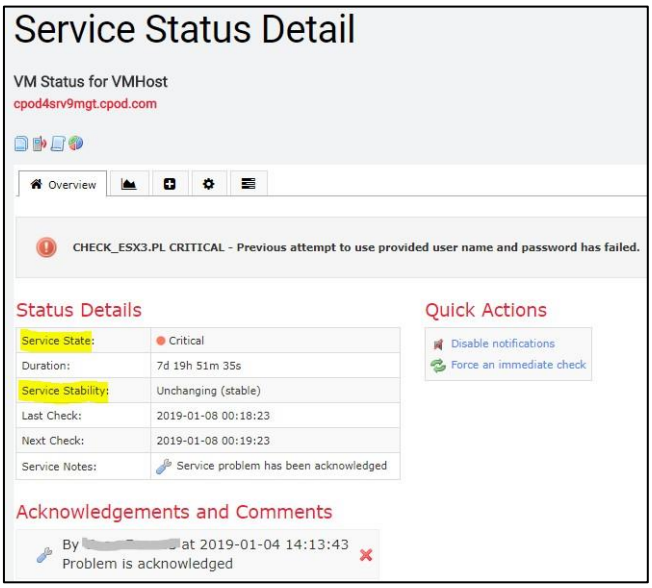
To determine how the specific view is sorted, look at the blue arrows corresponding to each of the sortable columns. The column with the single-direction arrow represents the sorted view. In the following example, the **Status** column represents the sorted view.





The **Host State** is **Up**, which confirms to the green (OK) status color of the host device. There are several **Quick Actions** available, as needed, to provide quick insight into potential problems with a host.

If you click a service in the **Service** column corresponding to the host, the **Service Status Detail** page for that service item appears.

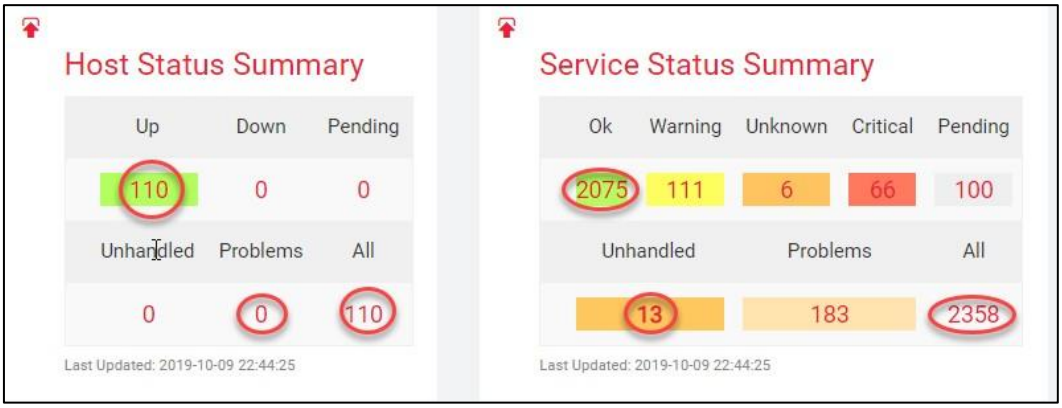


In the above image, the **Service State** is Critical, confirming the corresponding red color of the service state on the primary report page. The **Service Stability** is Unchanging, indicating that the problem still exists for the AO tool. At the top of the detailed information, a description of the issue is provided. In the preceding example, Avaya Orchestrator™ is unable to access the ESXi host. The message “Previous

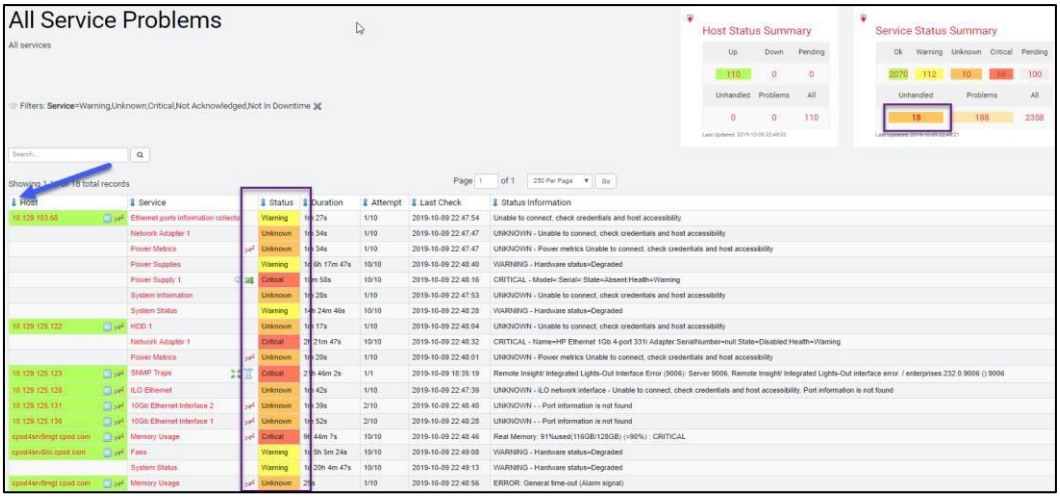
attempt to use provided user name and password has failed" appears. You can resolve this problem by confirming and re-administering the proper host and/or service credentials in the ACP Configuration Wizard.

Additional views of all device states, including healthy device services, are available when you click the respective links. You can click the available links to become more familiar with how to navigate to the desired data points.

For example, in the upper-right corner of each report are the high-level Summary overviews of Hosts and Services. This is consistent across the host-related and service-related reports and provides the ability to navigate from this problem-related report page to a device-related summary that displays all service and host specific status, both alarming and healthy states.



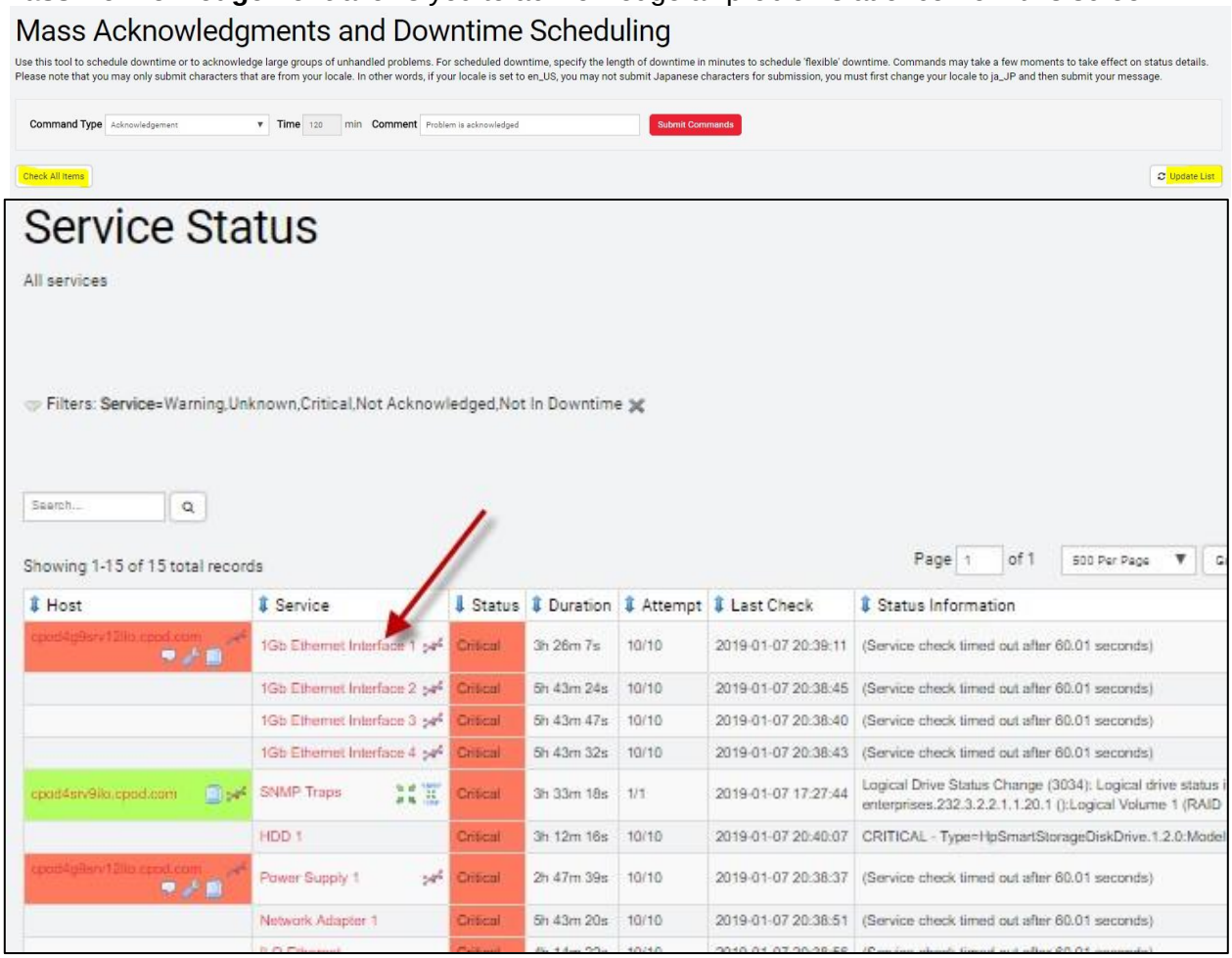
You can also click on any field/integer within the **Host Status Summary** and **Service Status Summary** areas for a more detailed view of the respective components. For example, in **Service Status Summary**, the **Unhandled** items represent those that are not yet acknowledged. You can click in the **Unhandled** area to view the Service Status for those reported items.



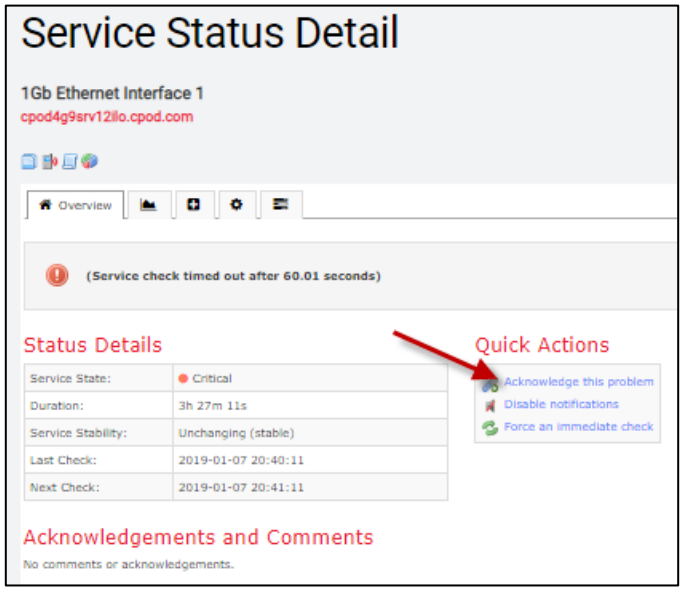
As each Service represented is acknowledged, the number of **Unhandled** items decrement.

Note:

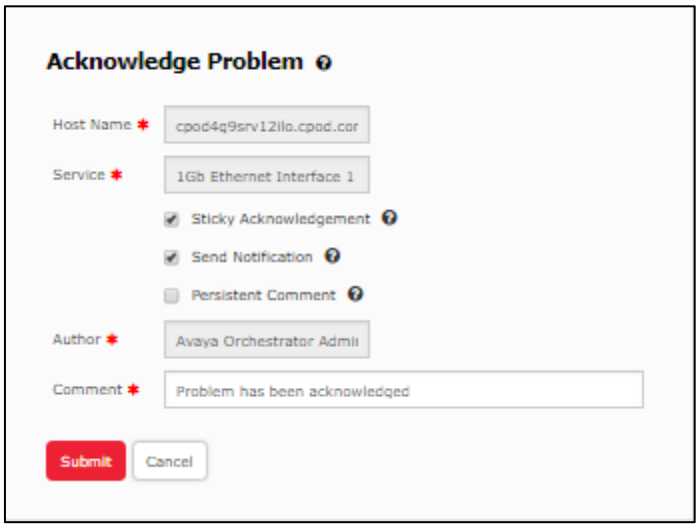
If appropriate for the nature of a solution-wide outage and recovery, **Home** > **Incident Management** > **Mass Acknowledgement** allows you to acknowledge all problems at once from this screen.

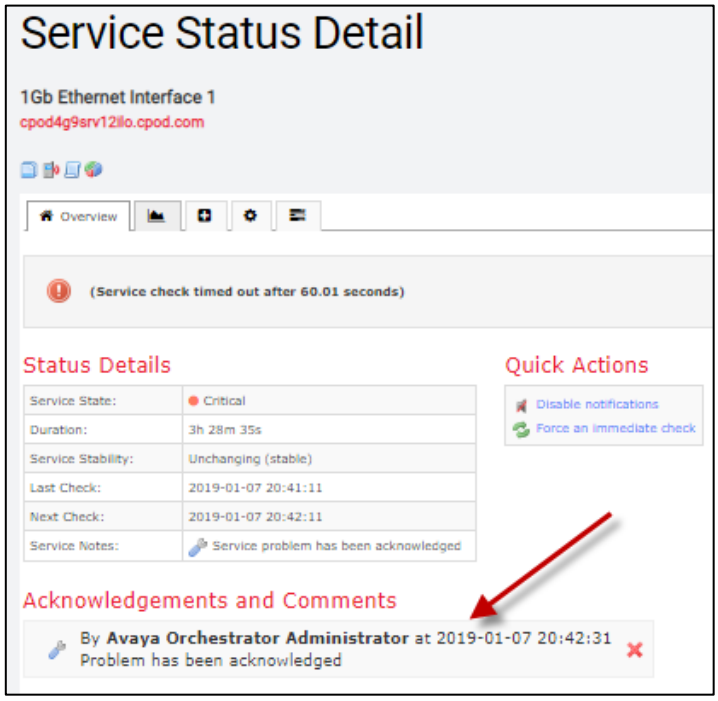


In the above image, the *1Gb Ethernet Interface 1* is selected. After you click on that service, the service detail for that service is displayed.

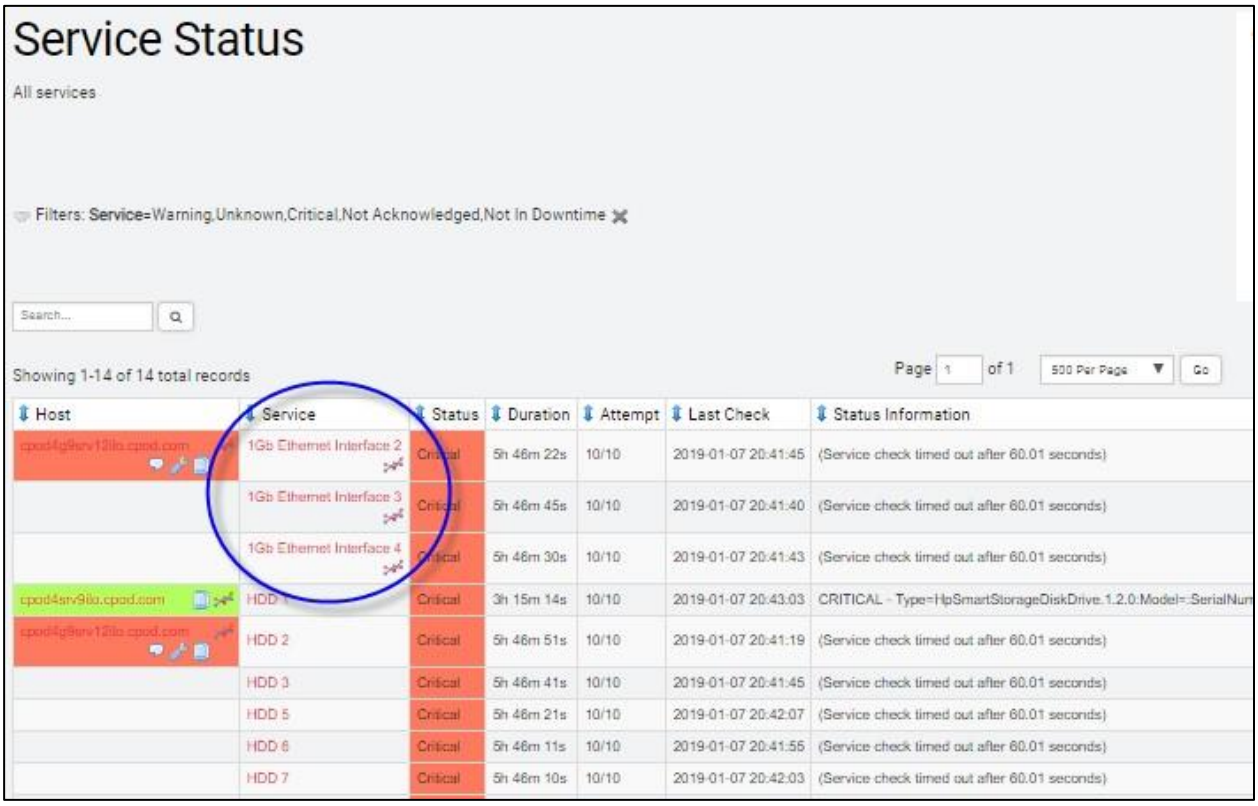


On the **Service Status Detail** page, click **Acknowledge this problem** to resolve the **Unhandled** state, if appropriate.





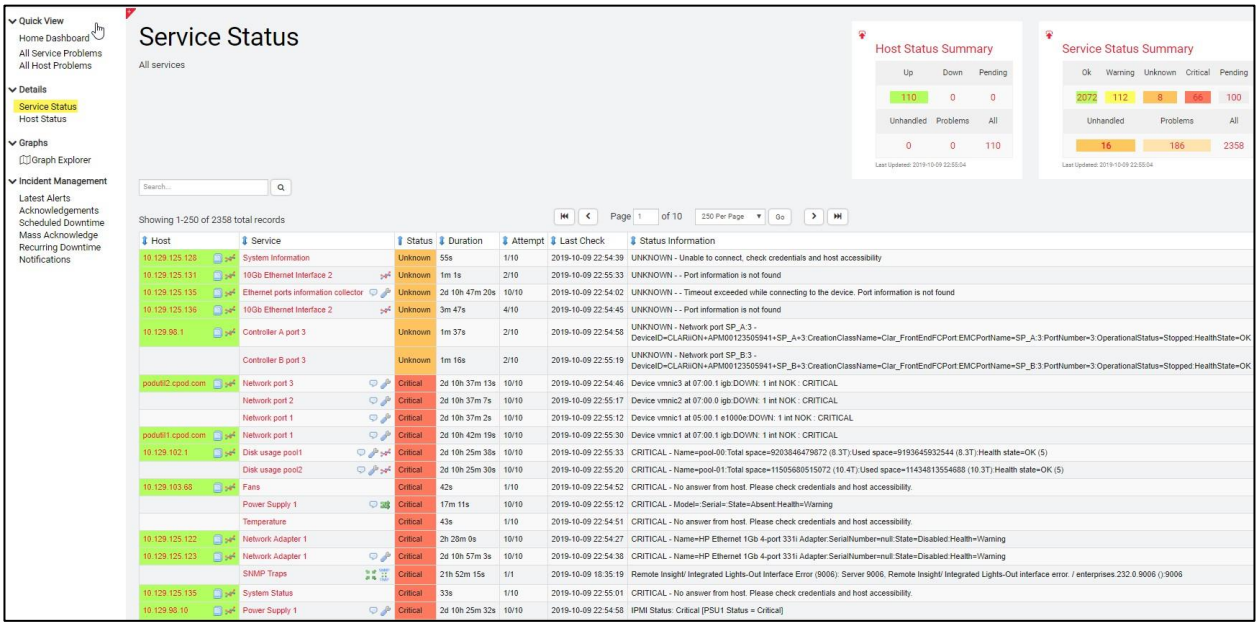
After you acknowledge the problem, AO reports the acknowledgement as a comment, decrements the **Unhandled** report value at that time, and the specific host's Service Status removes the previously reported unhandled service item.



The above image shows how you can easily navigate from a high-level problem view to a specific device view, and with a third click, navigate to the specific service of a device.

Service Status

The **Service Status** option displays a complete list of all monitored services. Services are color-coded based on their current status. You can click an entry in the **Service** column to view detailed information about that service on the **Service Status Detail** page. You can click an entry in the **Host** column to view detailed information about that host on the **Host Status Detail** page.



Service Status Detail

The **Service Status Detail** page contains detailed statistical information about a service operating in the solution. To view this page, click a service on the **Service Status** page. The **Service Status Detail** page contains the following tabs:

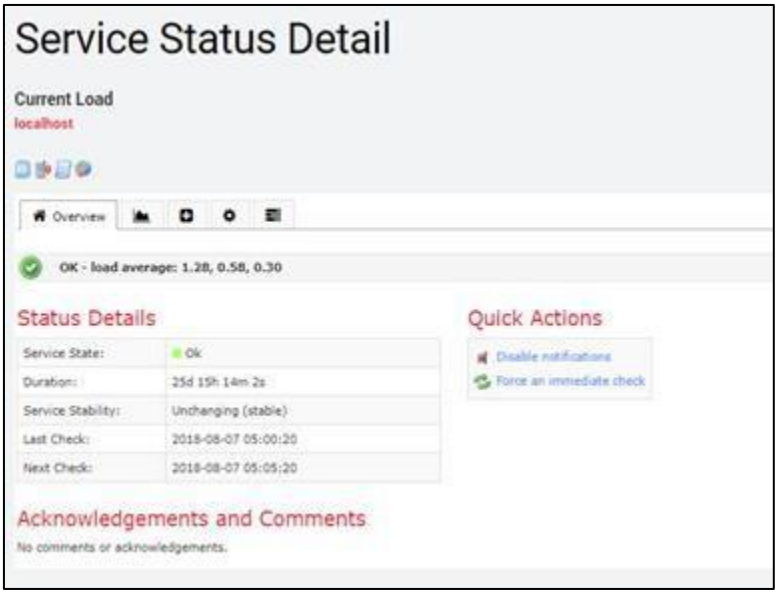
- Overview
- Performance Graphs
-
- Advanced
- Configure
- Free Variables

Overview

The **Overview** tab displays basic service information such as state, duration a service is in this state, stability, last checked time, and next check time.

You can use the links in **Quick Actions** to enable and disable notifications as well as force an immediate check. Other actions defined in the **Actions** component appear in this list.

Acknowledgments and comments also appear on this tab.



Performance Graphs

The **Performance Graphs** tab displays graphical information about the service. By default, information for the last 24 hours is displayed.

A Gauge is displayed if the performance data contains warning or critical thresholds.

The graph data is derived from the round robin database (RRD). The values are averaged if you generate performance graphs for larger time periods such as weeks and months.

The gauge data is derived from the last check result received by the service when it was populated into the RRD file. The data is in an accompanying XML file in the same directory where the RRD file resides.

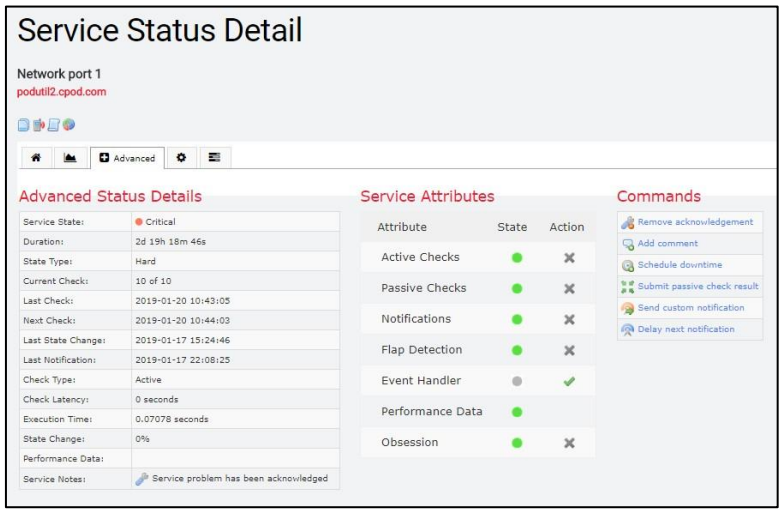
If the service does not produce performance data, the **Performance Graphs** tab still appears but no graphs are shown. Note that most services currently do not provide performance graphs. This function is more widely offered for Host detail reports.

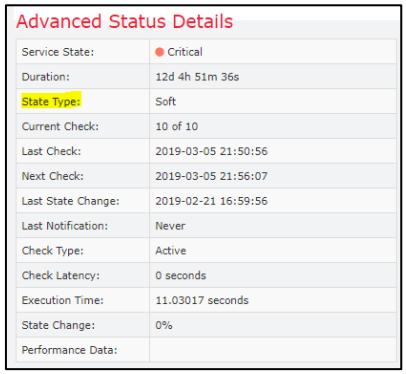
Advanced

The **Advanced** tab displays more detailed information about the service.

The **State** column of the **Service Attributes** area displays the current state of each attribute. You can click and in the **Action** column to enable or disable the attributes.

By changing any state here, you can significantly change the monitoring of your AO application. However, you must have administrative rights if you want to stop or start these processes to debug a problem.





The **State Type** can be either hard or soft and is shown in other reporting and display areas in AO.

Hard type: Represents an SNMP trap receipt. SNMP notifies only one time per issue. Hence, such alerts are considered hard, that is, confirmed. This is also the state available for proactive monitoring type alarms that are validated to be in the same state across 10 checks, of one per minute.

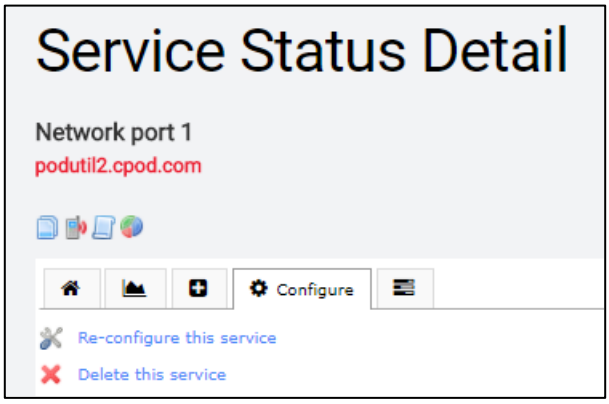
Soft type: Represents a proactive alarm that has not been in the same state for 10 checks.

Configure

The **Configure** tab allows you to re-configure or delete standard services.

If the service uses any advanced features, such as being assigned to multiple hosts, you cannot use either option.

When re-configuring a service, the options available are similar to a configuration wizard.



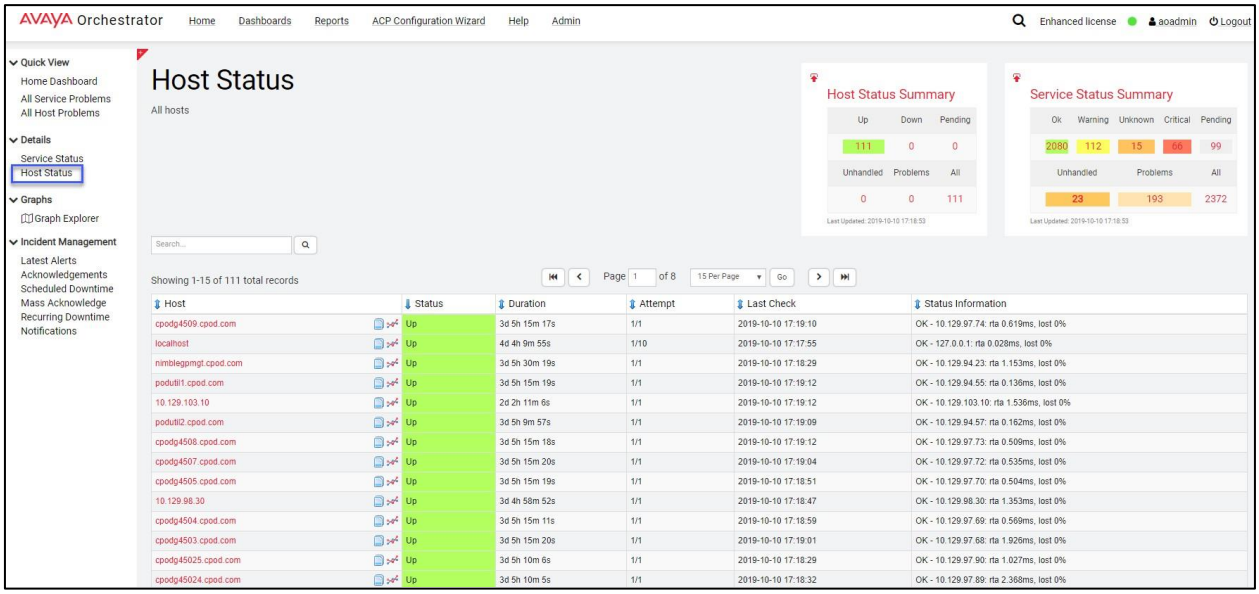
Free Variables

Free Variables is an advanced feature of Core that allows custom directives with values to be stored in a service object.

If your service has any free variables defined, the free variables appear here in a table for your reference.

Host Status

The **Host Status** option displays a complete list of all monitored hosts. Hosts are color-coded based on their current status. You can click an entry in the **Host** column to view detailed information about that host on the **Host Status Detail** page.



Host Status Detail

The **Host Status Detail** page contains detailed statistical information about a host operating in the solution. To view this page, click a host on the **Host Status** page. The **Host Status Detail** page contains the following tabs:

- Overview
- Performance Graphs
- Advanced
- Configure
- Free Variables

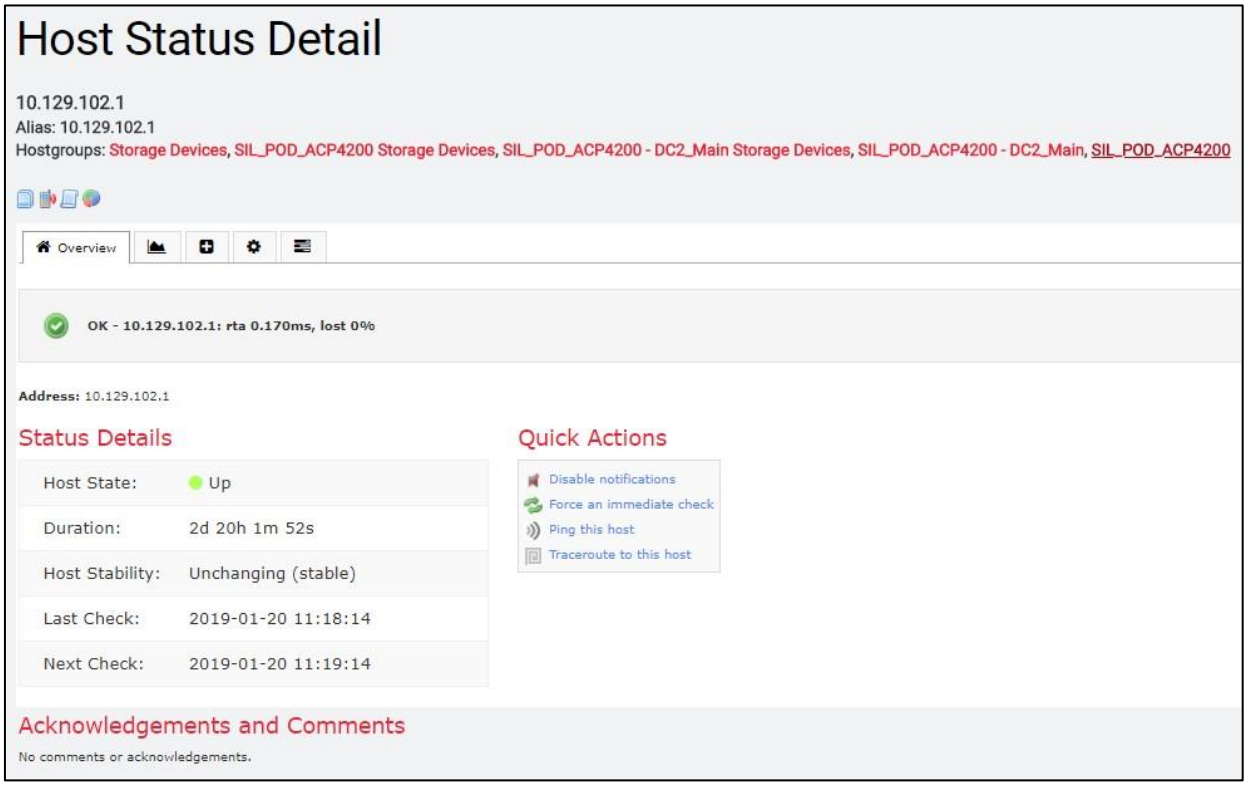
Overview

The **Overview** tab displays basic host information such as state, duration a host is in this state, stability, last checked time, and next check time.

The following host **Quick Actions** are available on this tab:

- Enable or disable notifications.
- Force an immediate check.
- Ping the host.
- Traceroute the host.

Acknowledgments or comments also appear on this tab.



Performance Graphs

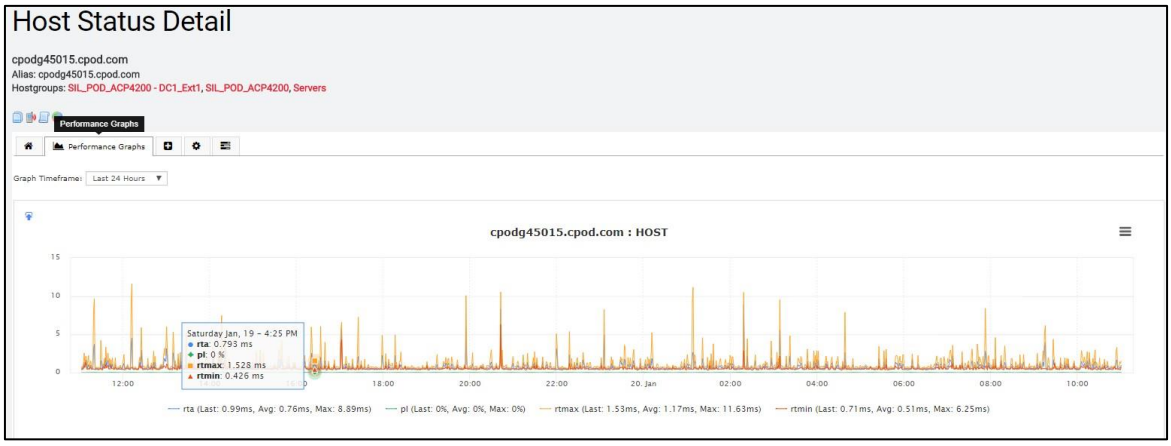
The **Performance Graphs** tab displays graphs for the host object and the first four services for the host. By default, information for the last 24 hours is displayed. Use the link at the bottom for more performance graphs that allow you to browse through all the performance graphs of the services assigned to the host.

A gauge is displayed if the host object performance data contains warning or critical thresholds.

The graph data is displayed from the round robin database (RRD). The values are averaged if you generate performance graphs for larger time periods such as weeks and months.

The gauge data is derived from the last check result received by the host when it was populated into the RRD file. The data is in an accompanying XML file in the same directory where the RRD file resides.

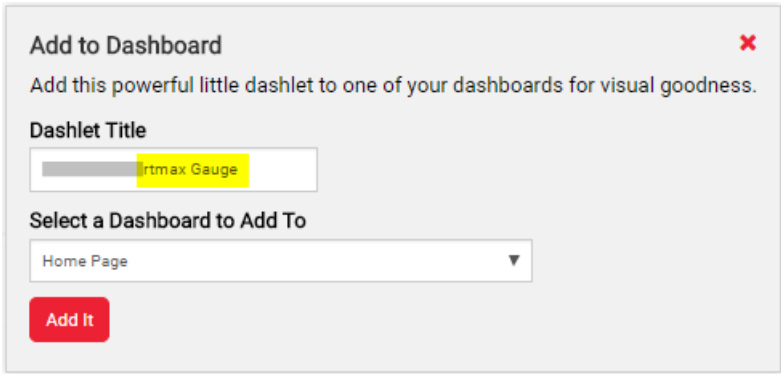
If the host does not produce performance data, the tab still appears but no host graphs are shown. The service graphs are shown if they exist.



Toward the bottom of the performance graphs are gauges. These provide the same information that is contained in the graphical format, but display it in a different visual reference form. You can click the blue icon located at the upper-left of each round gauge to place the item on a specific dashboard. These dashlets can be seen by all users, wherever they are placed.

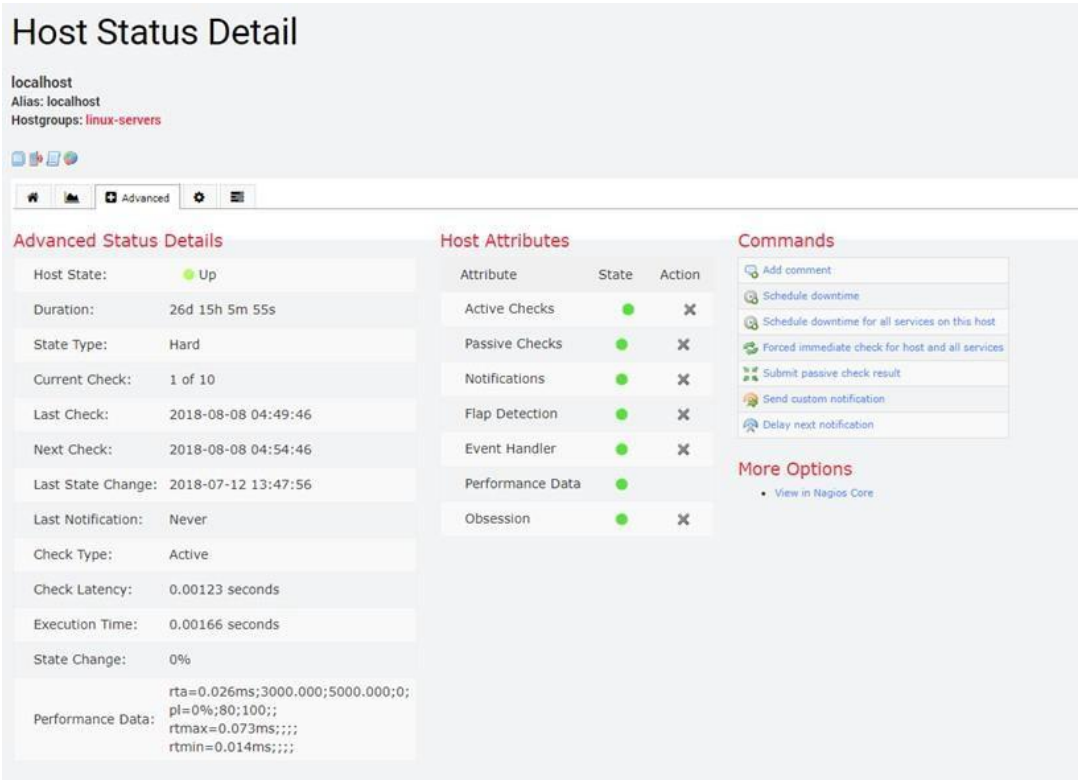


After you click the blue icon, the following dialog box appears. The **Dashlet Title** field shows the IP address associated with the Host dashlet along with the service source of the data. In the following example, the storage array is reporting *round trip max time gauge.*



Advanced

The **Advanced** tab shows more detailed information about the host.



The **Host Attributes** area displays the current state of each attribute and allows you to enable or disable the attributes.

In the **State** column:

- If an attribute is enabled, the circle is in green color. In the **Action** column, click  to disable the attribute.
- If an attribute is disabled, the circle is in gray or red color. In the **Action** column, click the check mark  to enable the attribute.

The **Commands** table allows you to:

- **Add comment**

  The comment that you add appears on the **Overview** tab.

- **Schedule downtime**

  Define scheduled downtime for the host.

- **Schedule downtime for all services on this host**

  Define scheduled downtime for all the services on the host instead of defining it for each service individually.

- **Forced immediate check for host and all services**

  Force Avaya Orchestrator™ to immediately perform host check and all service checks.

- **Submit passive check result**

  Manually define the state of the host. This is most useful with Passive hosts. For an Active host, the check result that you submit is overwritten by the check results of the next host check interval.

- **Send custom notification**

  Send a custom notification to all the contacts that are configured to receive notifications for the host.

- **Delay next notification**

  Delay the next problem notification that is sent for the specified host. The notification delay is disregarded if the host changes state before the next notification is scheduled to be sent.

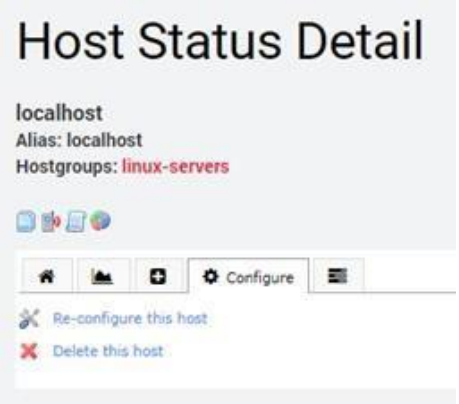
  This has no effect if the host is currently in an operational state.

Configure

The **Configure** tab allows you to re-configure or delete a host.

If the host uses any advanced features, you cannot use either option. You cannot delete a host object until all the services assigned to the host are deleted.

When re-configuring a host, the options available are similar to a configuration wizard.



Free Variables

Free Variables is an advanced feature of Core that allows custom directives with values to be stored in a host object.

If your service has any free variables defined, the free variables appear here in a table for your reference.

Chapter 10: Event handlers and Reports

About event handlers

This chapter contains information about how to use event handlers in Avaya Orchestrator™ to take predefined actions when the hosts or services that you are monitoring change state. Avaya Orchestrator™ uses event handlers to automate processes when a specific host or service changes state. This reduces the amount of manual work when something changes in your environment.

Event handlers are optional system commands. They are scripts or executables that are run when a host or service changes state. These commands include, but are not limited to, restarting services, parsing logs, checking other host or service states, and making database calls. These scripts proactively run every five minutes on all hardware devices, providing alarms and state color changes for service and host problems.

Event handlers are called whenever a state change occurs. This includes HARD, SOFT, OK, WARNING, CRITICAL, and UNKNOWN states. When a state change occurs, the logic behind the executed action, if any, is performed by the script or executable that is called by Avaya Orchestrator™ when the state change occurs. The script can parse these states through macros passed to it by the event handler and is readable on various web pages.

Ensure that the ACP Configuration Wizard is properly administered for each rack with the necessary IP addresses and protocols. This is the core basis for Event Handlers to function properly.

Modifying Event Handlers is not supported in Avaya Orchestrator™ Release 1.5 because of the complexity involved, the required expertise in programming knowledge, and the required familiarity with Avaya Orchestrator™. Customization of event handling will be supported in a future release.

Reports

The Avaya Orchestrator™ reporting engine is a multi-faceted tool that will review vast amounts of information prior to consolidating the requested information into an historical report.

Report generation time depends on the size of data file being requested and the output format (pdf, jpg or svc); depending on choices, a report can take few seconds or minutes to generate.
If a user tries to generate “heavy” reports then AO starts report building in background and prints the message “Exported report generation requests some time, please wait and check My Exported Reports”.

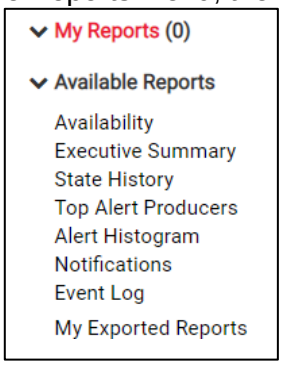
Page **My Exported Reports** contains:

- Exported reports list with the following information and actions for each report:
  - Report date
  - Report name
  - Report size (or status “In progress”)
  - Action “Download”
  - Action “Delete”
- Exported reports setting:

- Checkbox “Send email about exported report readiness”. If one is ON then AO sends email to user after requested report building is completed.
- The amount of exported reports you'd like to keep before replacing the oldest reports. You can enter 0 to keep unlimited reports.



From the Reports menu, the following varieties are available in AO.



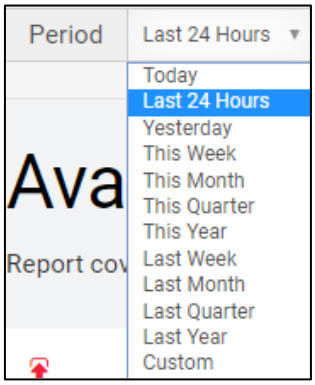
Availability Report

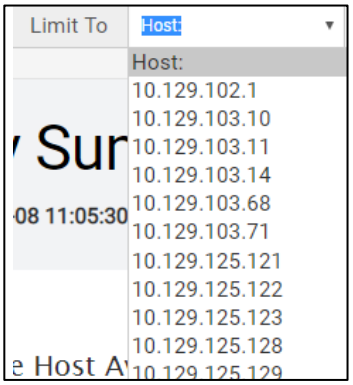
A breakdown across specified reporting criteria of functional and non-functional percentages. This report is available for custom dashboard viewing (Enhanced license required).

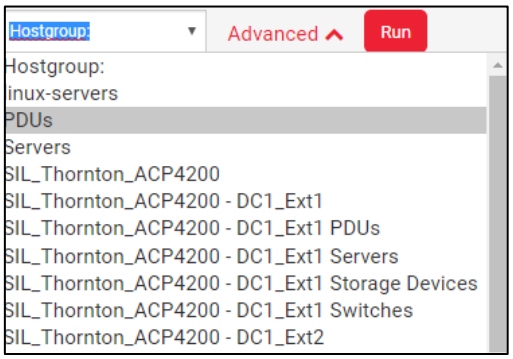
For the Host area, the breakdown targets up time and down time.

For the Services area, breakdowns include OK, Waring, Unknown and Critical timeframes.

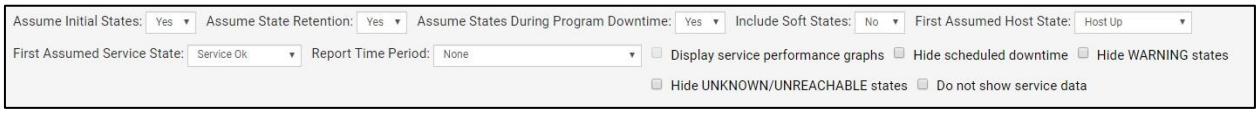
Menu options for Availability report presentation are as follows:

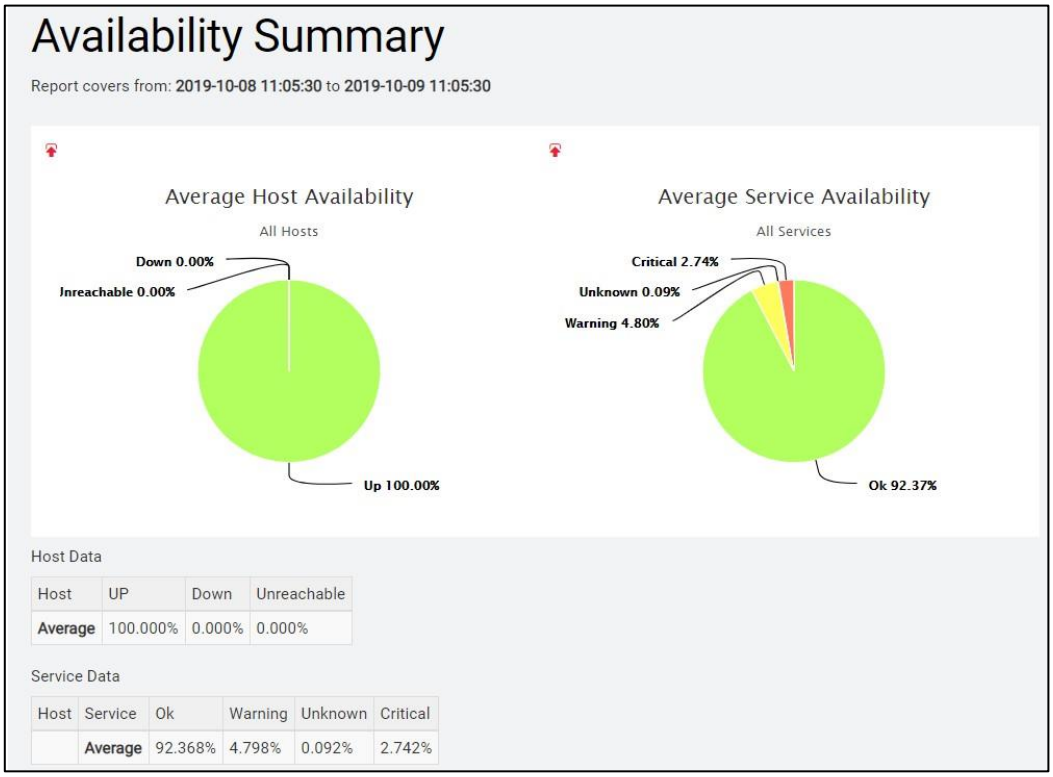




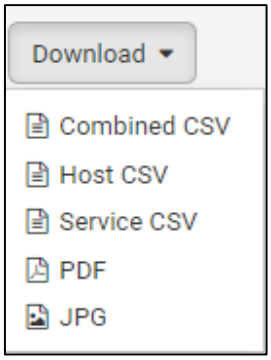


Some Advanced reporting criteria include the following options.





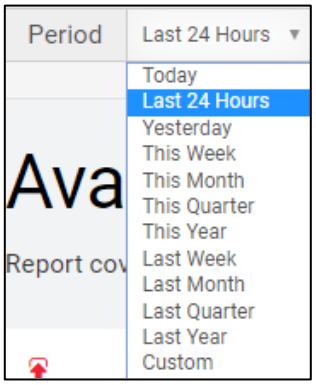
The Availability Report may be downloaded using the following formats:

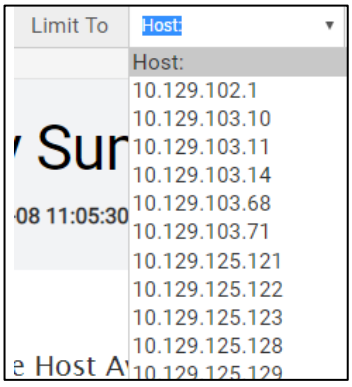


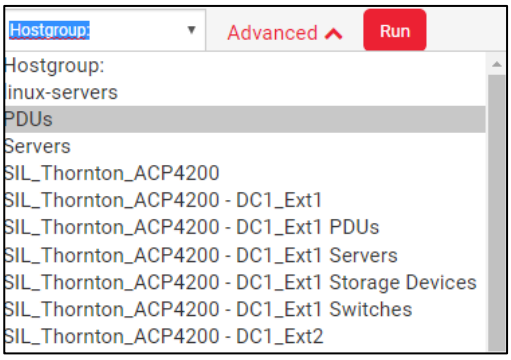
Executive Summary

This report is a collection of a variety of other reports that comprise the more critical monitoring aspects of AO.

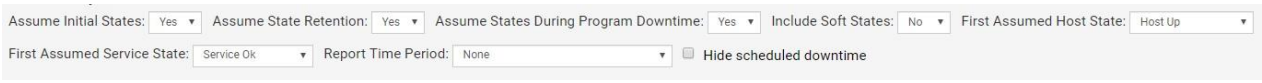
Menu options for Executive Summary report presentation are as follows:

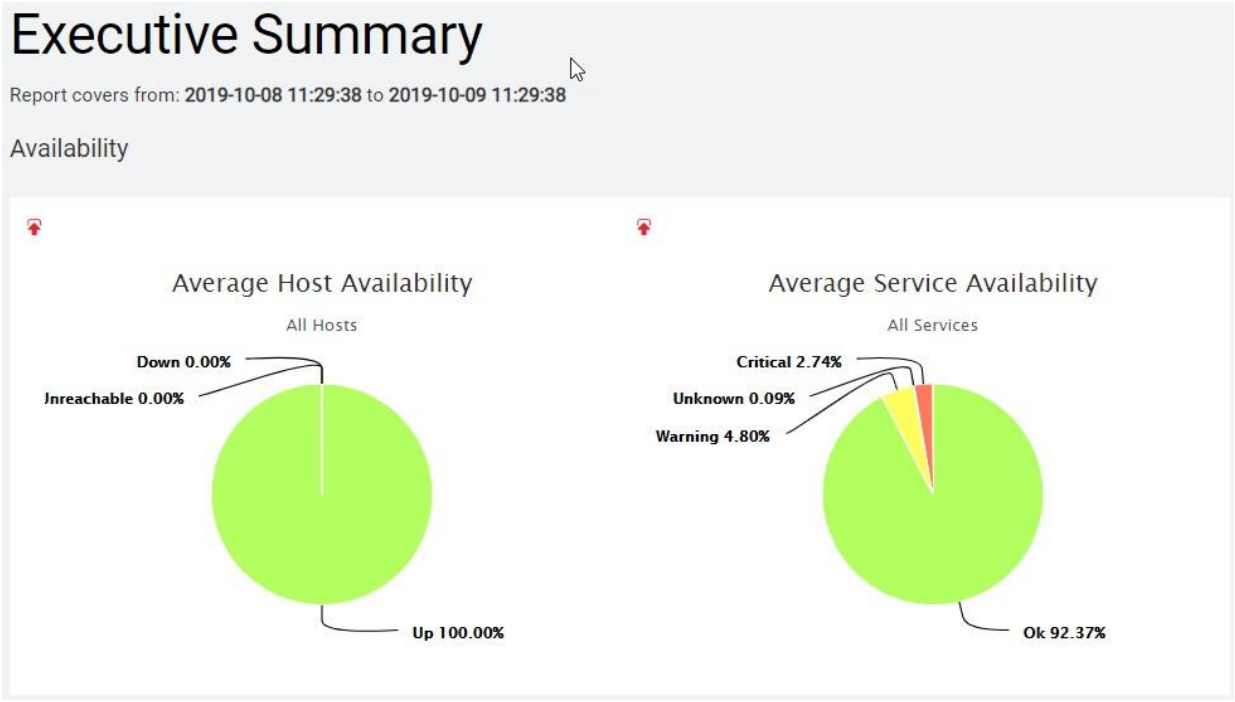






Some Advanced reporting criteria include the following options.

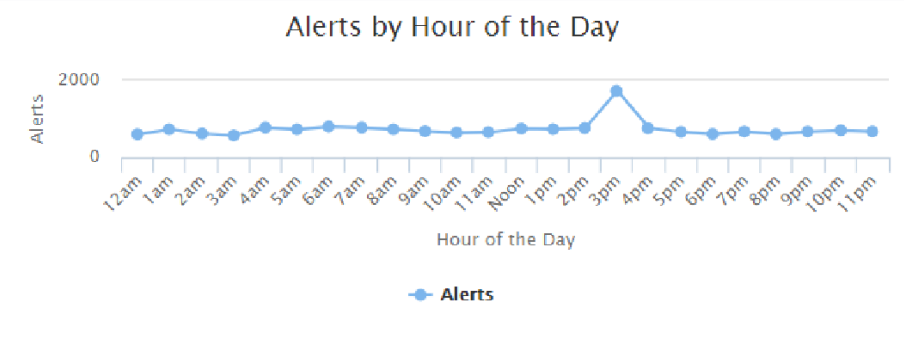




Top Alert Producers

Total Alerts	Host	Service	Latest Alert
314	10.129.103.68	Power Supply 1	2019-10-09 11:28:49
38	10.129.125.122	Network Adapter 1	2019-10-09 10:25:49
29	cpod4srv1mgt.cpod.com	Memory Usage	2019-10-09 11:07:46
8	cpod4srv7mgt.cpod.com	Memory Usage	2019-10-08 16:33:07
8	10.129.98.1	Controller B port 3	2019-10-09 08:54:21
6	localhost	Connection to WebLM servers	2019-10-09 10:08:16
6	10.129.98.1	Controller A port 3	2019-10-09 08:54:42
2	10.129.103.68	System Status	2019-10-09 08:24:35
2	10.129.125.122	10Gb Ethernet Interface 1	2019-10-09 04:12:48
2	10.129.125.123	SNMP Traps	2019-10-09 01:03:20

Alert Histogram



Latest Alerts

Source	Latest Alert	Alerts
cpod4srv1ilo.cpod.com	2019-10-09 11:29:46	10Gb Ethernet Interface 2 is Unknown
10.129.103.68	2019-10-09 11:28:31	Power Supply 1 is Critical Power Supplies, System Status are Warning Ethernet ports information collector is Unknown
10.129.125.129	2019-10-09 11:28:23	Ethernet ports information collector is Warning System Information, Power Supply 1 are Unknown
10.129.125.128	2019-10-09 11:27:28	10Gb Ethernet Interface 1 is Unknown
10.129.125.122	2019-10-09 10:25:42	Network Adapter 1 is Critical
10.129.125.123	2019-10-09 01:03:19	SNMP Traps is Critical Network Adapter 1 Is Being Handled
cpod4srv8ilo.cpod.com	2019-10-08 17:43:57	System Status, Fans are Warning
cpod4srv7mgt.cpod.com	2019-10-08 16:33:07	Memory Usage Is Being Handled
cpod4srv4mgt.cpod.com	2019-10-07 19:20:17	Memory Usage, Datastore usage for VMHost Are Being Handled
cpod4srv8mgt.cpod.com	2019-10-07 13:00:08	System Location, System Name, System ObjectID, System Services, System Up Time, System Contact, Entity Physical Model Name, Serial Number, System Description Are Being Handled

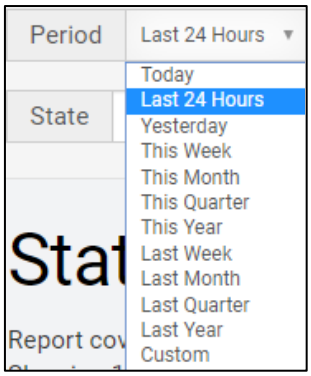
The Executive Summary Report may be downloaded using the following formats:

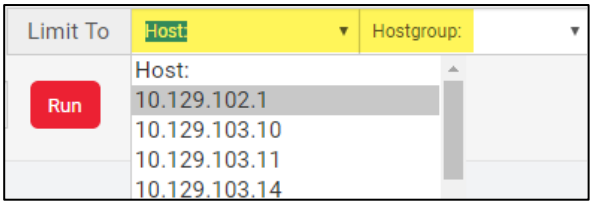


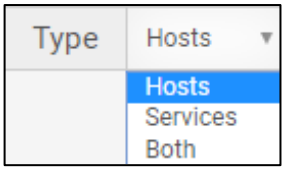
State History

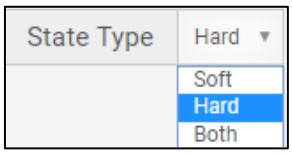
The State History report tracks specific host/service states, both hard and soft states, based on specific time stamps and dates reported by the devices/elements. For example, as AO checks hosts and services proactively every minute, it will be able to determine if 5:10 checks produced an alarm (soft) as opposed to 10:10 checks produced an alarm (hard).

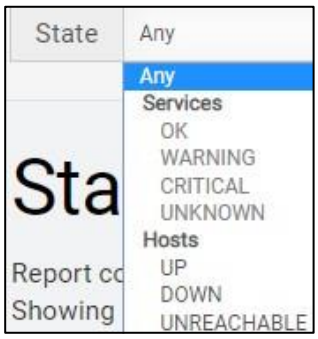
Menu options for State History report presentation are as follows:

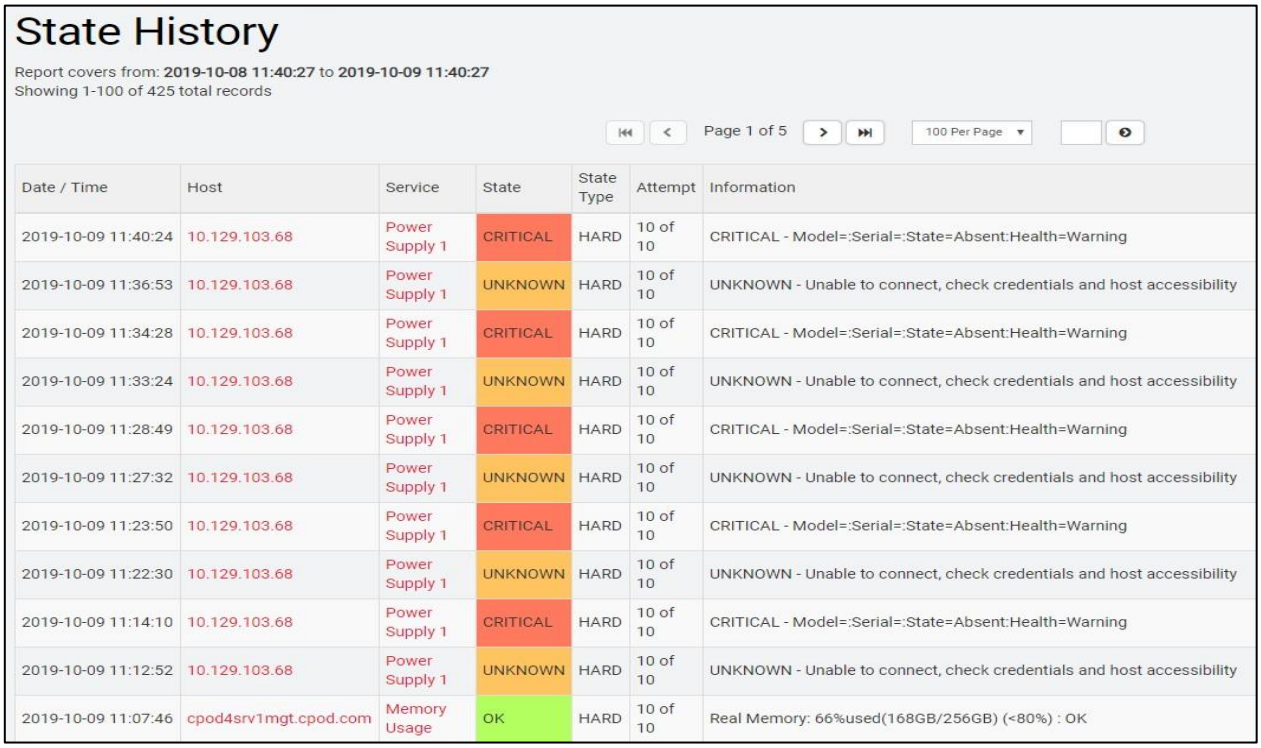












State History

Report covers from: **2019-10-08 11:40:27** to **2019-10-09 11:40:27**
Showing 1-100 of 425 total records

Page 1 of 5 | 100 Per Page

Date / Time	Host	Service	State	State Type	Attempt	Information
2019-10-09 11:40:24	10.129.103.68	Power Supply 1	CRITICAL	HARD	10 of 10	CRITICAL - Model=:Serial=:State=Absent:Health=Warning
2019-10-09 11:36:53	10.129.103.68	Power Supply 1	UNKNOWN	HARD	10 of 10	UNKNOWN - Unable to connect, check credentials and host accessibility
2019-10-09 11:34:28	10.129.103.68	Power Supply 1	CRITICAL	HARD	10 of 10	CRITICAL - Model=:Serial=:State=Absent:Health=Warning
2019-10-09 11:33:24	10.129.103.68	Power Supply 1	UNKNOWN	HARD	10 of 10	UNKNOWN - Unable to connect, check credentials and host accessibility
2019-10-09 11:28:49	10.129.103.68	Power Supply 1	CRITICAL	HARD	10 of 10	CRITICAL - Model=:Serial=:State=Absent:Health=Warning
2019-10-09 11:27:32	10.129.103.68	Power Supply 1	UNKNOWN	HARD	10 of 10	UNKNOWN - Unable to connect, check credentials and host accessibility
2019-10-09 11:23:50	10.129.103.68	Power Supply 1	CRITICAL	HARD	10 of 10	CRITICAL - Model=:Serial=:State=Absent:Health=Warning
2019-10-09 11:22:30	10.129.103.68	Power Supply 1	UNKNOWN	HARD	10 of 10	UNKNOWN - Unable to connect, check credentials and host accessibility
2019-10-09 11:14:10	10.129.103.68	Power Supply 1	CRITICAL	HARD	10 of 10	CRITICAL - Model=:Serial=:State=Absent:Health=Warning
2019-10-09 11:12:52	10.129.103.68	Power Supply 1	UNKNOWN	HARD	10 of 10	UNKNOWN - Unable to connect, check credentials and host accessibility
2019-10-09 11:07:46	cpod4srv1mgt.cpod.com	Memory Usage	OK	HARD	10 of 10	Real Memory: 66%used(168GB/256GB) (<80%) : OK

The State History Report may be downloaded using the following formats:

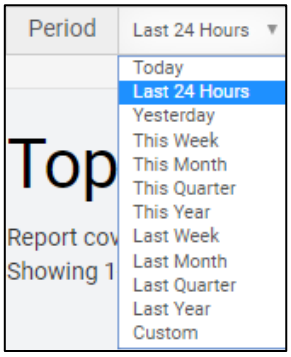


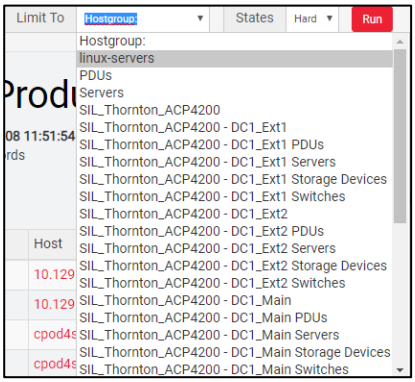
Top Alert Producers

This report provides a sorted list based on the sum of all alarms received from devices/elements selected in the report presentation criteria. The type of alerts/alarms are not separated. This would include all trap updates received from Hosts and Services including OK status updates.

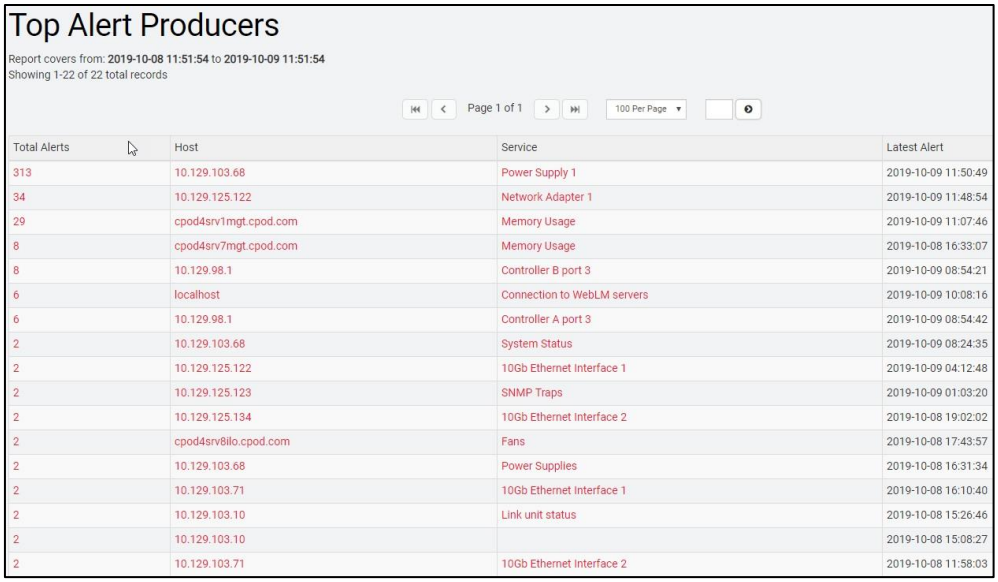
The purpose of this report is to help users identify those elements that may have consistent state changes, representing an unstable performance.

Menu options for Top Alert Producers report presentation are as follows:

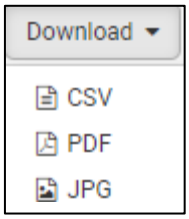








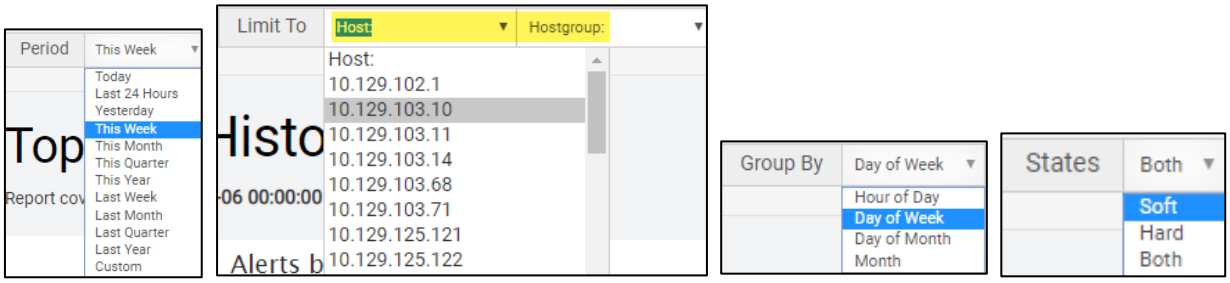
The State History Report may be downloaded using the following formats:

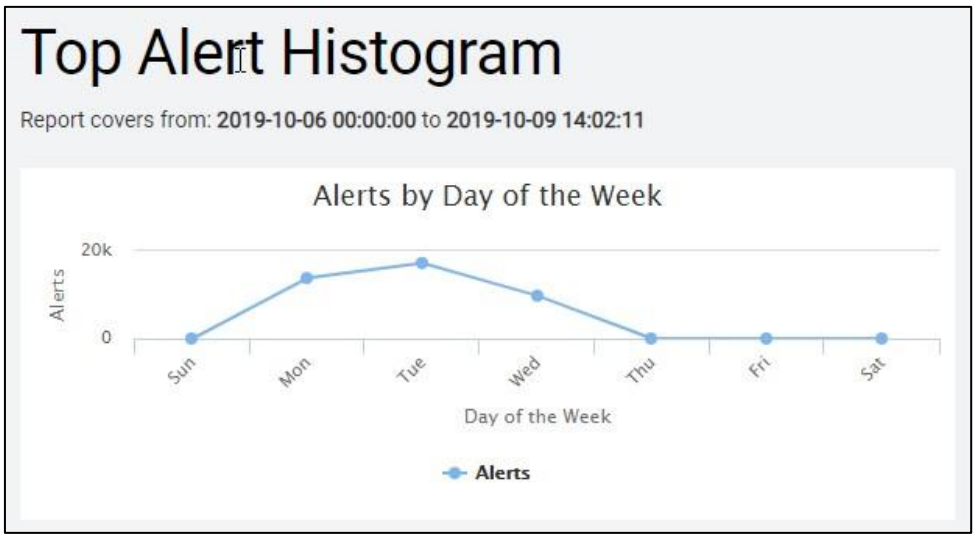


Alert Histogram

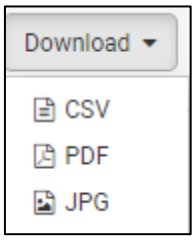
The Alert Histogram report provides a broad spectrum review of all alarms – based on specific Hosts or Host Groups, and presents them across a specified spectrum of time that is designated in the report presentation menu options.

Menu options for Alert Histogram report presentation are as follows:





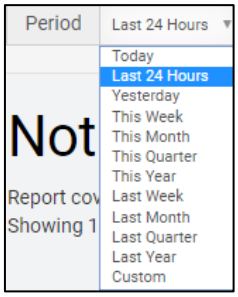
The Alert Histogram Report may be downloaded using the following formats:

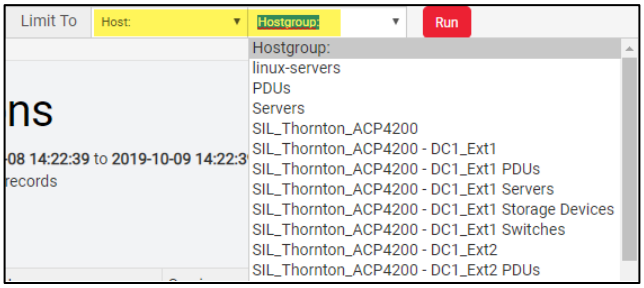


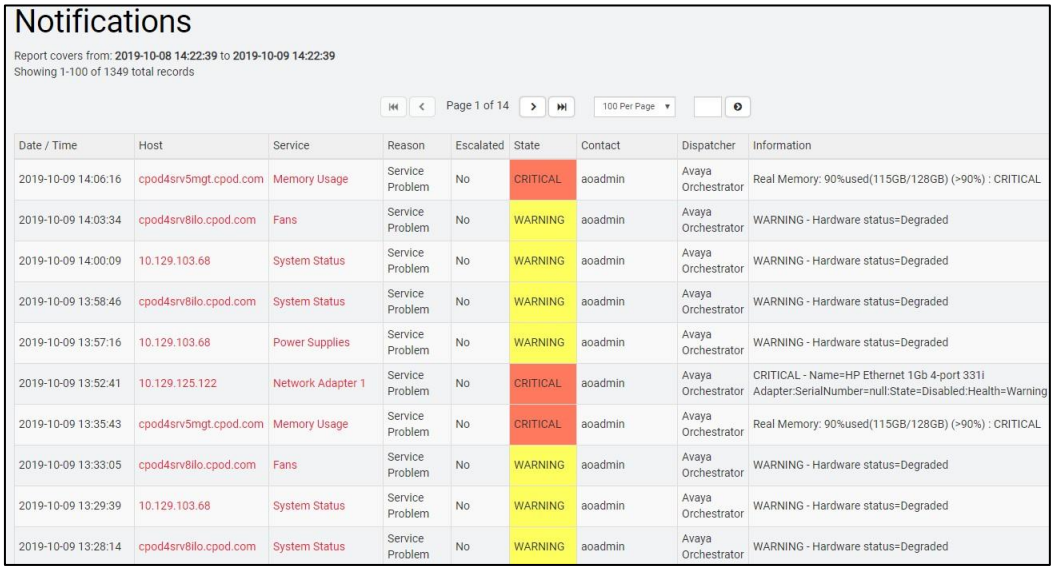
Notifications

This report provides a listing of alarms that created a notification activity, i.e., Email or SMS text, along with the time stamp and nature of the escalation; each line is presented by individual recipient. There is an ability to search on a specific recipient; the menu of report presentation view options does not include this option, but each report type does allow searches for all possible fields so that sorting through hundreds or thousands of entries is made easier.

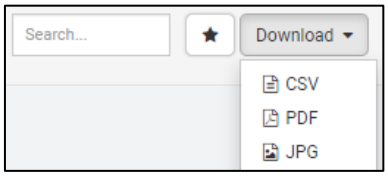
Menu options for Notifications report presentation are as follows:







The Alert Histogram Report may be downloaded using the following formats:



Event Log

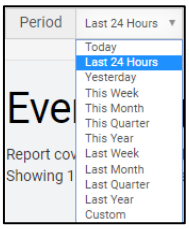
The Event Log report is a collection of all state-of-health events collected by AO. This comprises the largest report output in the AO database. Using the search capability for the report will allow a faster sort on specific types of alarms.

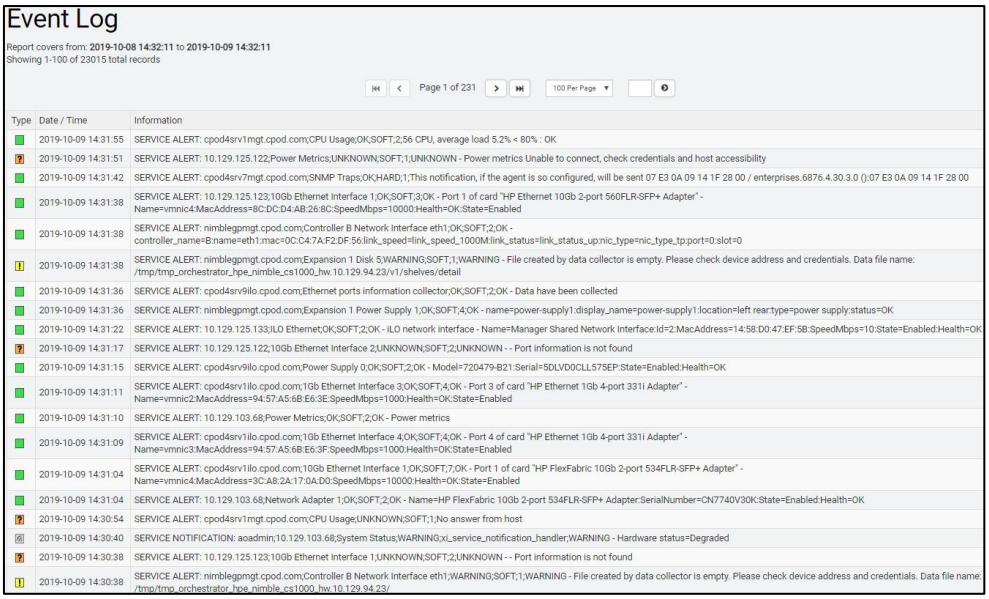
The event type is represented by symbolic representation of each type of alarm.

- represents “unknown” status.
- represents OK.

- represents a warning alert.
- represents a critical alarm.
- represents a notification.

Menu options for Event Log report presentation are as follows:

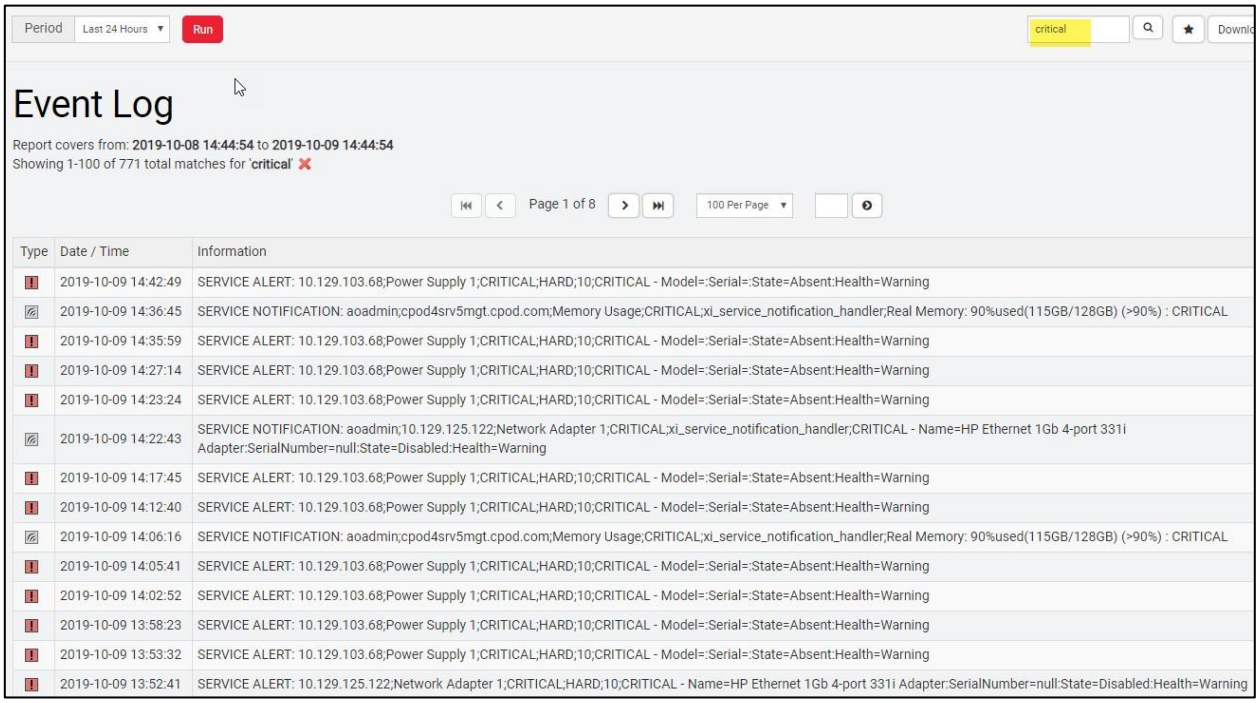




The Event Log Report may be downloaded using the following formats:



You may target an Event Log report to a specific alarm type by entering the word of the alarm in the search window.


Period
Last 24 Hours
Run
critical
Event Log
Report covers from: 2019-10-08 14:44:54 to 2019-10-09 14:44:54
Showing 1-100 of 771 total matches for 'critical'
Page 1 of 8
100 Per Page
Type
Date / Time
Information
2019-10-09 14:42:49
SERVICE ALERT: 10.129.103.68;Power Supply 1;CRITICAL;HARD;10;CRITICAL - Model=:Serial=:State=Absent:Health=Warning
2019-10-09 14:36:45
SERVICE NOTIFICATION: aoadmin;cpod4srv5mgt.cpod.com;Memory Usage;CRITICAL;xi_service_notification_handler;Real Memory: 90%used(115GB/128GB) (>90%) : CRITICAL
2019-10-09 14:35:59
SERVICE ALERT: 10.129.103.68;Power Supply 1;CRITICAL;HARD;10;CRITICAL - Model=:Serial=:State=Absent:Health=Warning
2019-10-09 14:27:14
SERVICE ALERT: 10.129.103.68;Power Supply 1;CRITICAL;HARD;10;CRITICAL - Model=:Serial=:State=Absent:Health=Warning
2019-10-09 14:23:24
SERVICE ALERT: 10.129.103.68;Power Supply 1;CRITICAL;HARD;10;CRITICAL - Model=:Serial=:State=Absent:Health=Warning
2019-10-09 14:22:43
SERVICE NOTIFICATION: aoadmin;10.129.125.122;Network Adapter 1;CRITICAL;xi_service_notification_handler;CRITICAL - Name=HP Ethernet 1Gb 4-port 331i Adapter:SerialNumber=null:State=Disabled:Health=Warning
2019-10-09 14:17:45
SERVICE ALERT: 10.129.103.68;Power Supply 1;CRITICAL;HARD;10;CRITICAL - Model=:Serial=:State=Absent:Health=Warning
2019-10-09 14:12:40
SERVICE ALERT: 10.129.103.68;Power Supply 1;CRITICAL;HARD;10;CRITICAL - Model=:Serial=:State=Absent:Health=Warning
2019-10-09 14:06:16
SERVICE NOTIFICATION: aoadmin;cpod4srv5mgt.cpod.com;Memory Usage;CRITICAL;xi_service_notification_handler;Real Memory: 90%used(115GB/128GB) (>90%) : CRITICAL
2019-10-09 14:05:41
SERVICE ALERT: 10.129.103.68;Power Supply 1;CRITICAL;HARD;10;CRITICAL - Model=:Serial=:State=Absent:Health=Warning
2019-10-09 14:02:52
SERVICE ALERT: 10.129.103.68;Power Supply 1;CRITICAL;HARD;10;CRITICAL - Model=:Serial=:State=Absent:Health=Warning
2019-10-09 13:58:23
SERVICE ALERT: 10.129.103.68;Power Supply 1;CRITICAL;HARD;10;CRITICAL - Model=:Serial=:State=Absent:Health=Warning
2019-10-09 13:53:32
SERVICE ALERT: 10.129.103.68;Power Supply 1;CRITICAL;HARD;10;CRITICAL - Model=:Serial=:State=Absent:Health=Warning
2019-10-09 13:52:41
SERVICE ALERT: 10.129.125.122;Network Adapter 1;CRITICAL;HARD;10;CRITICAL - Name=HP Ethernet 1Gb 4-port 331i Adapter:SerialNumber=null:State=Disabled:Health=Warning

Chapter 11: User Administration

Overview

This chapter explains how to administer users in Avaya Orchestrator™ manually. Administering users using LDAP/ADS imports are discussed in a later chapter. You will also learn, as an administrator, how to interpret the Manage Users interface.

Users vs. contacts

- Users correspond to user accounts that are used to log on to the Avaya Orchestrator™ web interface.
- A user is typically connected to a contact for both enabling notifications and obtaining permissions to view and modify hosts and services.
- Contacts are definitions in Core that are normally used for directing host and service alerts to specific individuals.
- Contacts do have a relationship with users, in order to ensure that the users can use the Avaya Orchestrator™ web interface.

Adding a user

Procedure

1. Log on to the Avaya Orchestrator™ web interface by using administrative credentials.
2. Click **Admin**.
3. In the left navigation pane, click **Users** > **Manage Users**.
4. On the Manage Users page, click **Add New User** to add a new user.
5. In the **General Settings** area, do the following:
   a. In the **Username** field, type a user name for the user to log on to Avaya Orchestrator™. No spaces may be in the name field.
   b. In the **Password** field, type a password for the user to log on to Avaya Orchestrator™.
   c. In the **Repeat Password** field, retype the password.
   d. Select the **Force Password Change at Next Login** check box if you want the user to change the password when the user logs in the next time.
   e. Select the **Email User Account Information** check box to send the user's account information to the user through an email message.
   f. In the **Name** field, type the name of the user.
   g. In the **Email Address** field, type the email address of the user.

h. In the **Phone Number** field, type the phone number of the user.

i. Clear the **Create as Monitoring Contact** check box.

j. Select the **Enable Notifications** check box if you want to send notifications to the user.

k. Select the **Account Enabled** check box to enable the user account and allow the user to log on to Avaya Orchestrator™.

   If you clear this check box, the user cannot log on to Avaya Orchestrator™ by using the login credentials.

6. In the **Preferences** area, set the user preferences.

   For more information, see User preferences.

7. In the **Authentication Settings** area, set the authentication type for the user.

   For more information, see Linking existing Avaya Orchestrator™ users to Active Directory users and Linking existing Avaya Orchestrator™ users to LDAP users.

8. In the **Security Settings** area, set the security settings for the user.

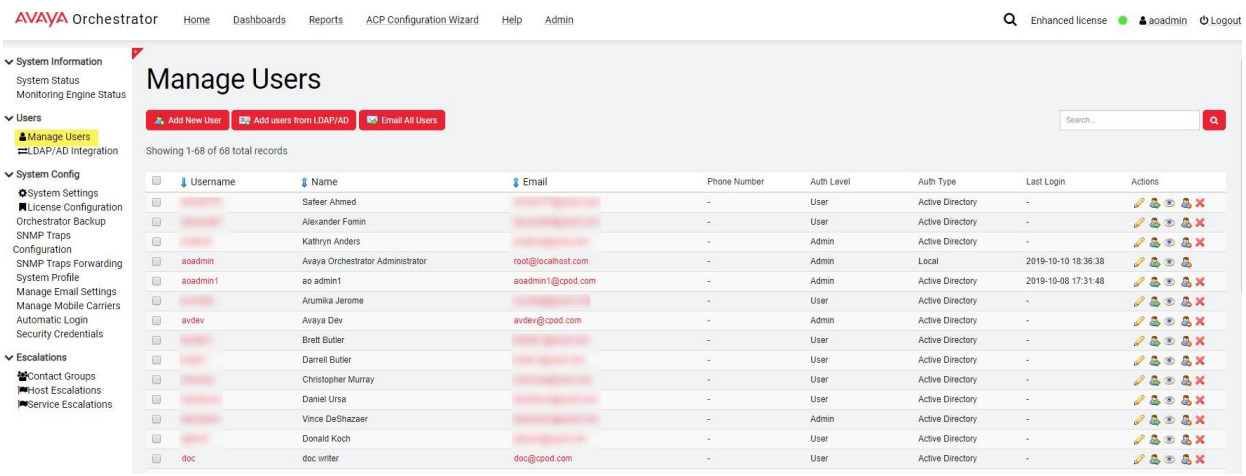
9. Click **Add User**.

User preferences

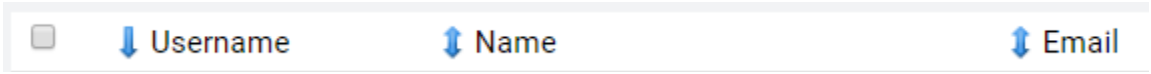
Preference	Description
Language	The language preference of the user.
Date Format	The Date format preference of the user.
Number Format	The number format preference of the user.
Week Format	The week format preference of the user.

Managing Users

Once the users are administered, either manually as a standalone AO user, or via an integrated LDAP/ADS enterprise user, their user accounts are managed from this form. You can also generate a system Email to all users from this form.



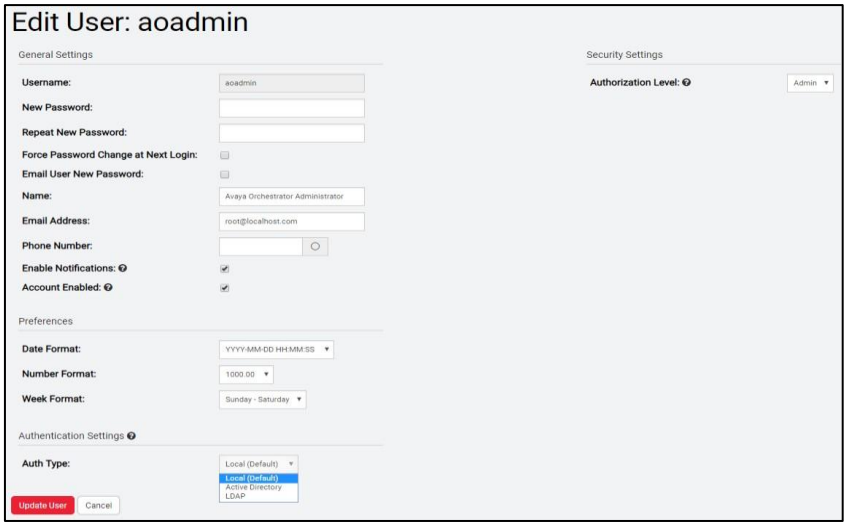
The user information can be sorted by user name, actual employee name or by email handle. The blue arrow pointing in a single direction, like the **Username** below, indicates the controlling sort mechanism. This example list is sorted by Username.



Username

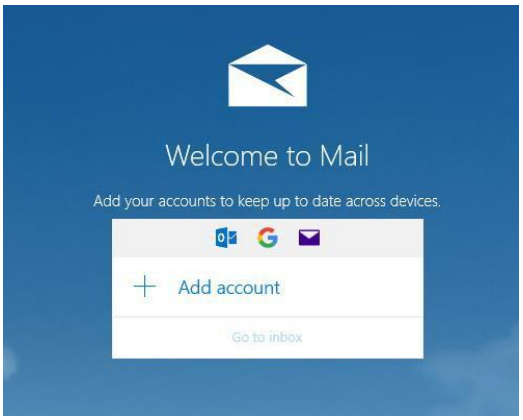
Clicking a user name drill into the original user admin page. Here you can change a variety of management settings, including the Auth Type and Authorization Level.

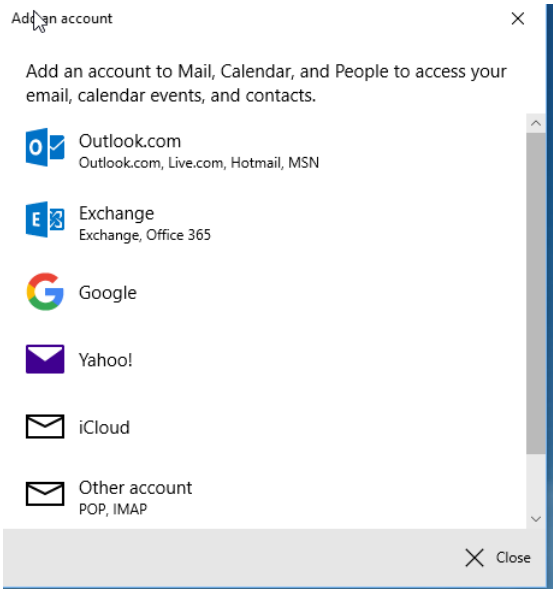
The Local (Default) Auth Type requires passwords to be tied locally. If a user is blocked from access, due to forgotten/incorrect password, the password would be changed on this form. If the user has an ADS/LDAP account, the password would be addressed via the enterprise tool, and would not be addressed locally.



Email

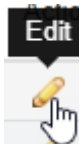
Clicking a user email allows you to set up an account for them using your preferred corporate methodology or using the user's preferred Email account.



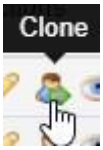


Actions

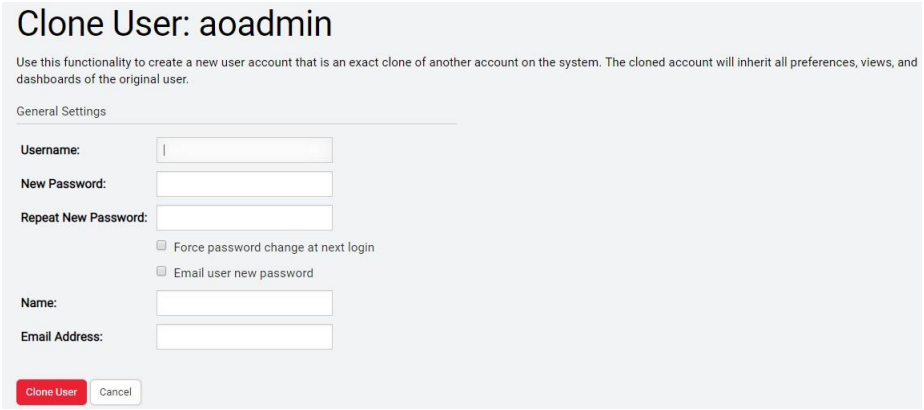
The following section explains action column icons and how to use them.

1. 

Click the **Edit** option to drill down to the user admin form, just as clicking the username does.

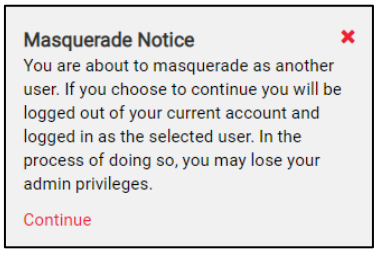
2. 

Click the **Clone** option to provide the opportunity to repeat the same permissions and administrative settings across other users in a similar support level community. See the following image for details.

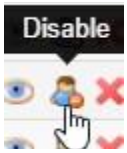


3. 

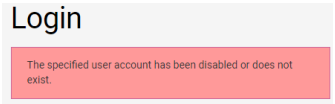
The **Masquerade** option provides the ability for administrators to switch between their login to the user selected. This function might be used for debug purposes, to assume a specific user identity and experience the abilities a specific user may or may not have available to them. The user could be a generic “User1” variety, that would be used to clone other users. Before assigning such a generic core user, an administrator would want to be certain of all abilities and expected outcomes.



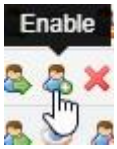
By clicking **Continue**, the login being used will be swapped out for the selected user.

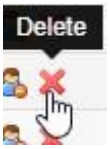
4. 

Click the **Disable** option to prevent the elected user from being allowed to login to AO. The following error is presented when a login is attempted.



After disabling an account, the Clone option disappears from the icon options and a new **Enable** option appears as follows:



5. 

Click the **Delete** option to delete a user. All associated admin will be removed from AO.

Chapter 12: Alarm Notifications

Overview

This chapter provides instructions on configuring alarm notifications that are available through the Basic License, and notification escalation options available with the Enhanced License.

Users vs. Contacts

Notifications can be emails or SMS text messages and are sent to users when hosts and services change states. This keeps users updated on the health of their monitoring environment.

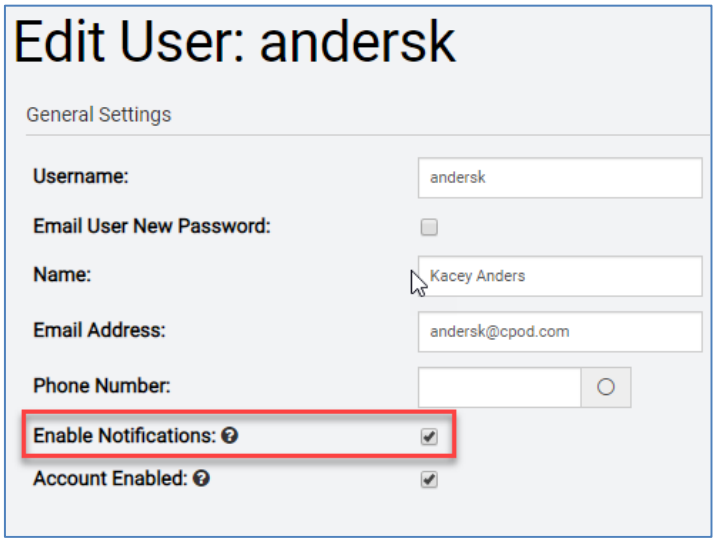
Users and contacts are two separate entities.

- AO creates and uses *contacts* to send notifications.
    - When a user is created, a contact is simultaneously created for it. It is the contact element that becomes available with the Enhanced License.
    - Contacts are assigned to host and service objects. AO uses this information to track which contacts receive notifications.
    - Contacts that are assigned specific escalation administration within the higher level notification escalation functions cannot modify those notification preferences, such as the format and timing of the email being sent or what type of notifications they receive.
- Avaya Orchestrator™ creates user accounts to receive notifications.
    - Provides an authentication mechanism so that end users can access Avaya Orchestrator™.
    - Allows end users to define their notification preferences, such as the format of the email messages being sent, or the type of notifications they receive.
    - Allows end users to do other activities such as email reports.
    - Provide users with the ability to receive email and text notifications with different notification preferences for each method.

Note: If you want to send notifications to the users that are imported from ADS/LDAP, ensure that the preceding notification configuration is completed.

Configuring user notifications

A user must first be administratively configured to receive notifications. Go to Admin > Manage Users to enable this capability. Find the user you wish to check and click on the name to drill down into the user administrative fields.



Confirm *Enable Notifications* is checked.

User Notification Administration

This function is available to any properly administered user with the Basic License suite.

Procedure

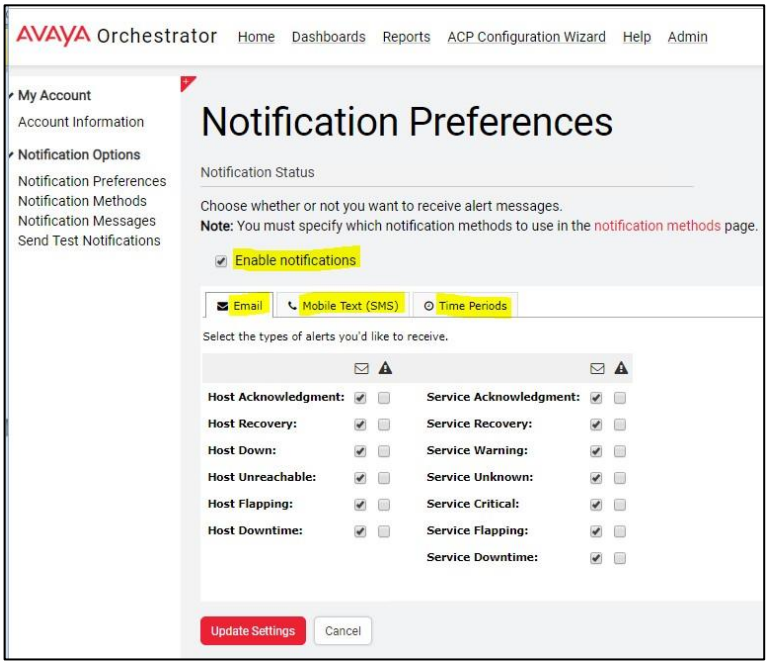
1. Log on to Avaya Orchestrator™ with the user credentials for which you want to configure user notifications.
2. Click the user name in the upper-right corner of the interface.



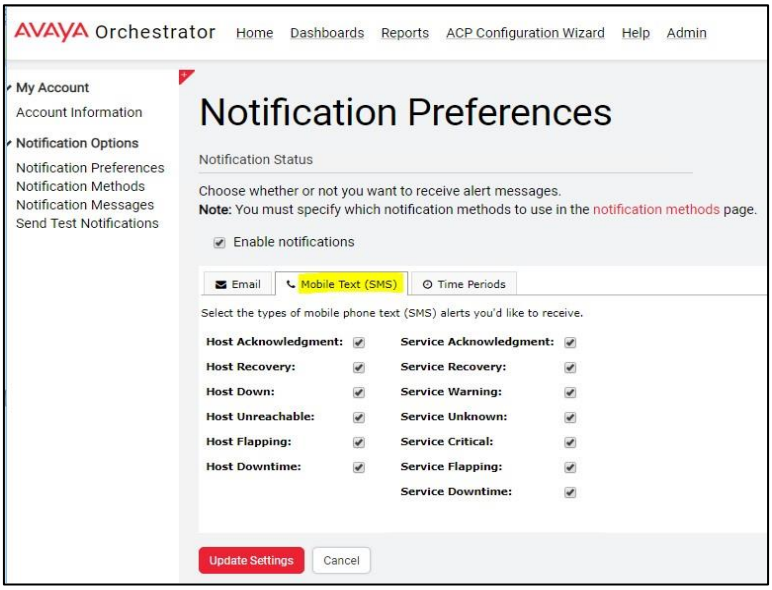
3. In the left navigation pane, click **Notification Options** > **Notification Preferences**.

4. On the Notification Preferences page, select the **Enable notifications** check box and do the following:

   a. On the **Email** tab, select the check boxes corresponding to the notifications that you want to enable.

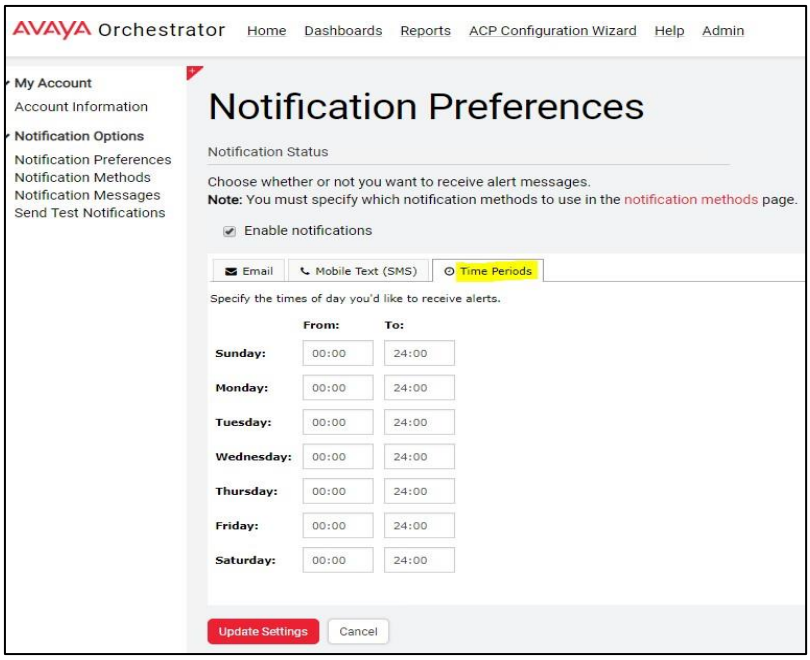


   b. On the **Mobile Text (SMS)** tab, select the check boxes corresponding to the notifications that you want to enable.

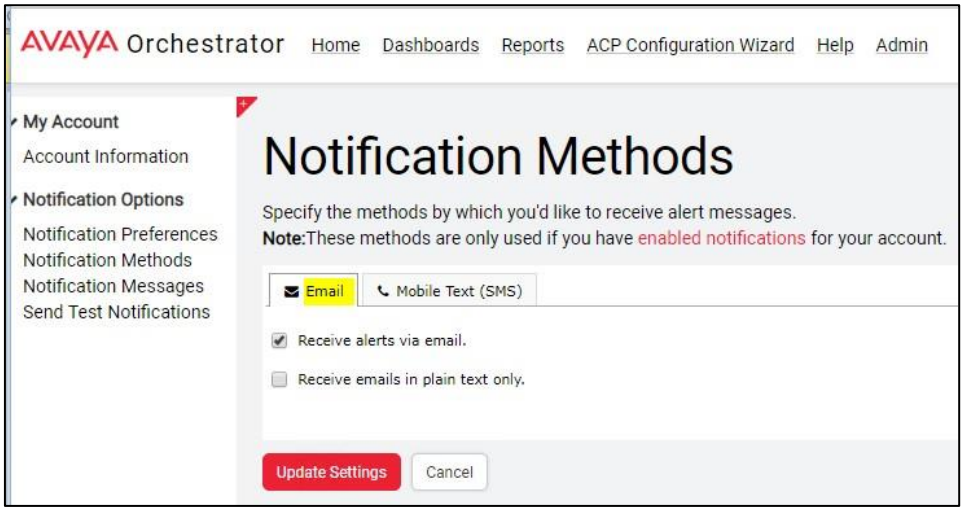


   c. On the **Time Periods** tab, configure the time of the day and days of the week for receiving

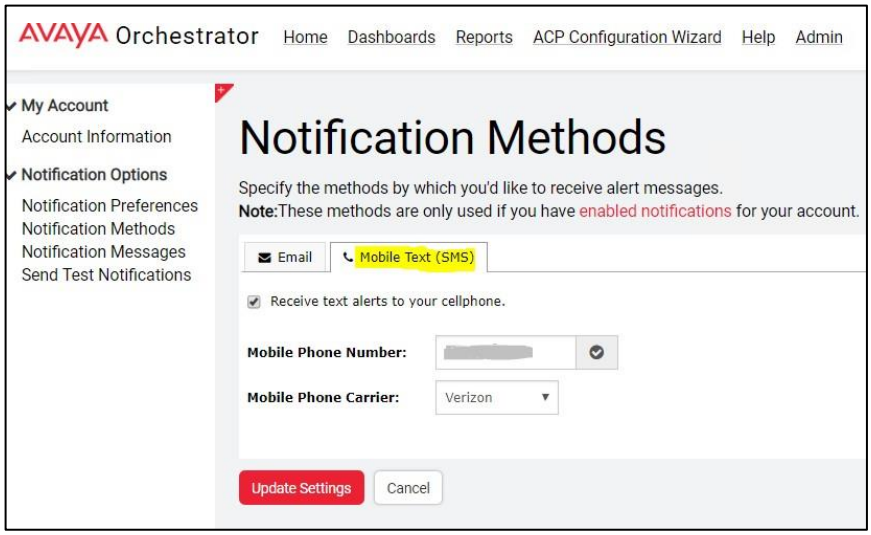
notifications.



5. In the left navigation pane, click **Notification Methods**.
6. On the Notification Methods page, do the following:
   a. On the **Email** tab, select the check box corresponding to the method by which you want to receive the notifications.



   b. On the **Mobile Text (SMS)** tab, select the **Receive text alerts to your cellphone** check box and specify the phone number and mobile phone carrier.



7. Click **Notification Messages**.
8. On the Notification Messages page, do the following:
   a. On the **Email** tab, configure the format of the email notifications.
   b. On the **Mobile Text (SMS)** tab, configure the format of the text notifications.
9. Click **Update Settings**.
10. **(Optional)** Avaya recommends that you use the **Send Test Notifications** option, located in the left navigation pane, to test the new notification settings.

Configuring Notification Escalations

Note: The following administration options require an Enhance License suite.

Administering Contact Groups

The purpose of a Contact Group is to provide a specific collection of 1 or more users who will be recipients of a specific type of alarm or set of alarms. You may create a contact group of 1 person or create a contact group comprised of several other contact groups for a more universal and urgent notification process.

Consider the following examples to better understand the creative options available.

- Create 2 or more tiers of contact groups that will sequentially receive notifications per a prescribed escalation path for weekend coverage.
- Build contact groups that are comprised of other contact groups as a “last resort” escalation point.
- Set notification delivery intervals for very short periods as notifications go unanswered after a

specific period of time.

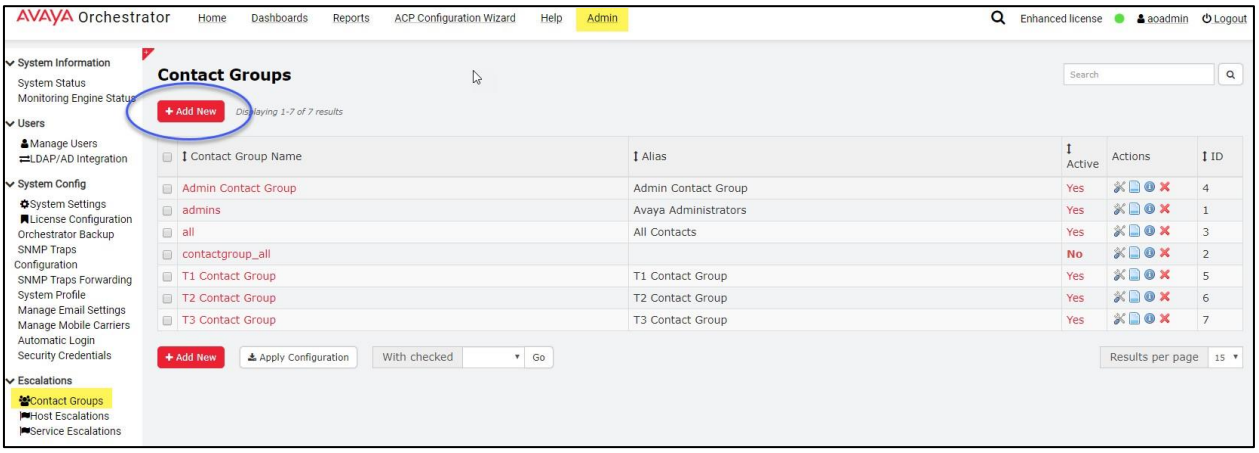
- Define contact groups based on alarms coming from devices in specific host groups, or specific data centers.

These are just a few ideas that touch on some of the key administrative variables that allow for a more controlled notification strategy in Avaya Orchestrator™ 1.5.

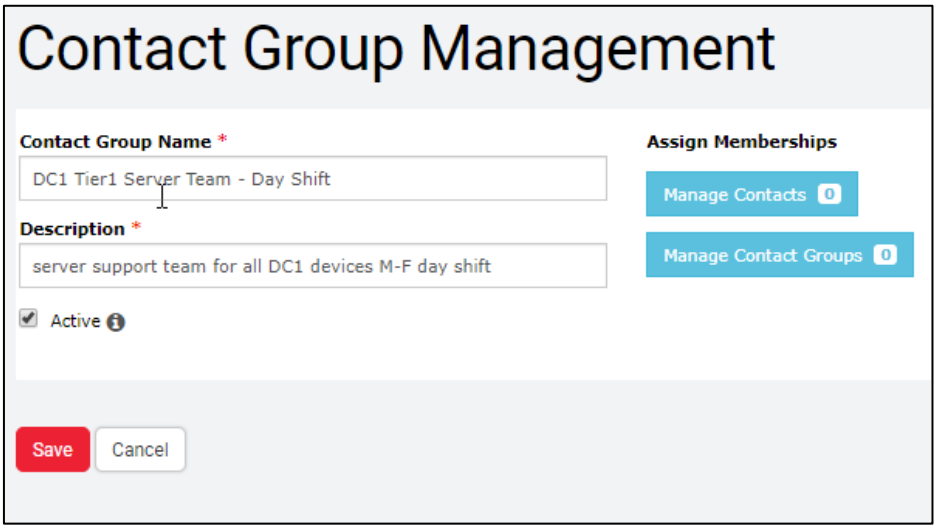
Building a matrix of administrable values could help organize and expedite the administrative process. Consider grouping as many users as possible when at the same tier, into the same alarm delivery timeframe to help limit the number of contact groups required.

Procedure

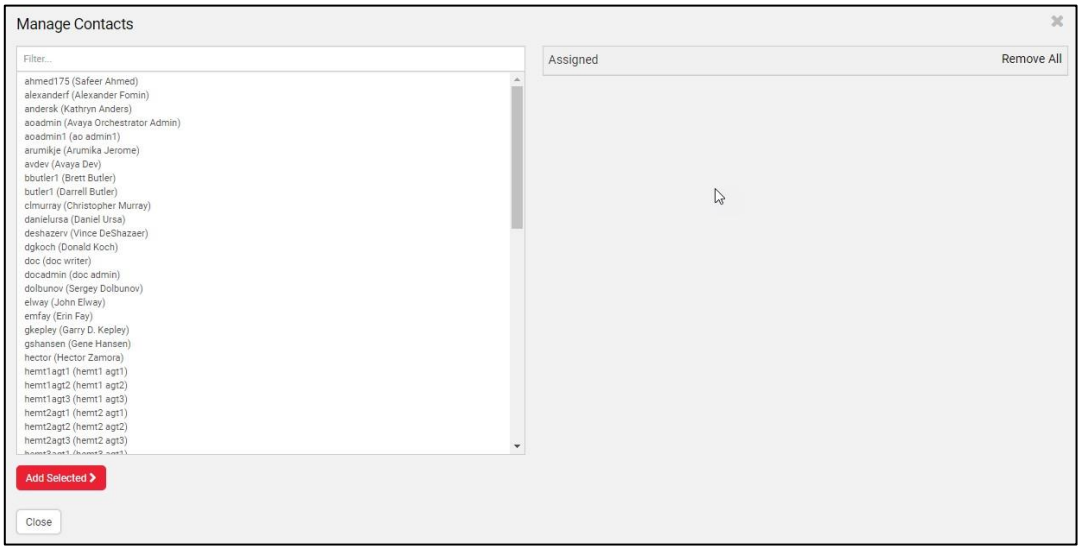
1. Go to *Admin* > *Escalations* > *Contact Groups* and click on + *Add New.*



2. Start by building Group 1 of the first Tier; create a meaningful label for the group so that you will be clear about its purpose when needing to possibly assign it for other areas later.



   a. Click Manage Contacts to locate and add specific user members to the contact group.

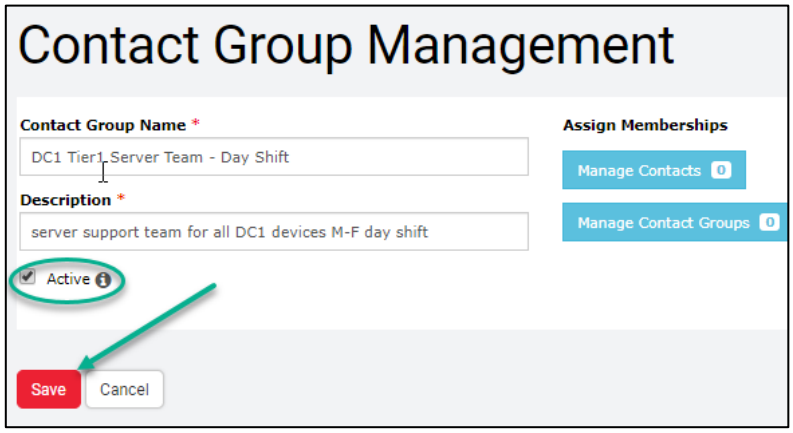


b. Another option is to add other contact groups as sub-members of a larger contact group.



c. When you have completed adding users into the contact group, click Save to accept the changes. When you are ready to start using the contact group, click the *Active* button to enable notifications to be sent to the specific group.

Note: To stop notifications to a specific contact group, disable the group by un-checking the *Active* box.



Administering Host Groups

This form is where Contact Groups may be applied to support specific Host and defined host alarm criteria.

1. Go to Admin > Escalations > Host Escalations.
2. Administer the Host and Services Escalation Management criteria.



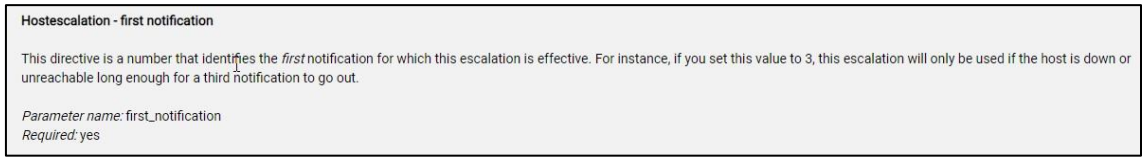
a. Config Name
The name in this example explains the specific elements supported – the servers deployed in Data Center 1. This will be comprised of specific host groups that can be collectively assigned the support of this contact group.

b. First Notification

The first notification represents when you want to start sending notifications to the contact group being identified. If this is a first tier group, you may want to begin with using 1. However, you have the option of waiting for the 2nd or 3rd alarm notification to allow systems to clear themselves before escalating notifications.

If you are in need of a clear definition of what each field means, you may click on the drop

down menu being in the upper right hand corner of this form, and an definition window will appear to explain how to administer each field.



c. Last Notification
This field represents when to stop notifying this particular contact group. If you enter 4, after the 4th notification is sent, based on the interval defined in the next field, AO will stop send notifications. A value of 0 represents infinity. If a 0 is entered, AO will continue to send notifications until the problem is resolved or acknowledged.

d. Notification Interval
The value of 30 present in this example means that after the first notification is sent, AO will wait 30 minutes before sending the second and 30 minutes before sending the third, etc.

e. Escalation Options
Select *Down* to be notified when a host is represented as down (Ip unreachable).
Select *Up* to be notified when a host has recovered and reports Up (IP reachable again).
Select both *Down* and *Up* to be notified if wither state is reported.

f. Host Notification Period
This value represents the span of time the contact group will receive notifications.

g. Host Escalation Period
Set the number of minutes you want to pass between each notification being sent.

h. Active (enable/disable)
As with the contact group administration, there is an *Active* box which enables and disables the administration for this form. If you wish to stop all notifications for a particular Host group, un-check the *Active* box and all alarm notifications for the specific host suite selected will be stopped.

i. Manage Hosts
Click the red Manage Hosts button to select the individual host(s) to be monitored for the specific escalation group being defined.



j. Manage Host Groups
This option allows you to build a supported host group collectively. These groups are presented as servers in specific racks and/or data centers.



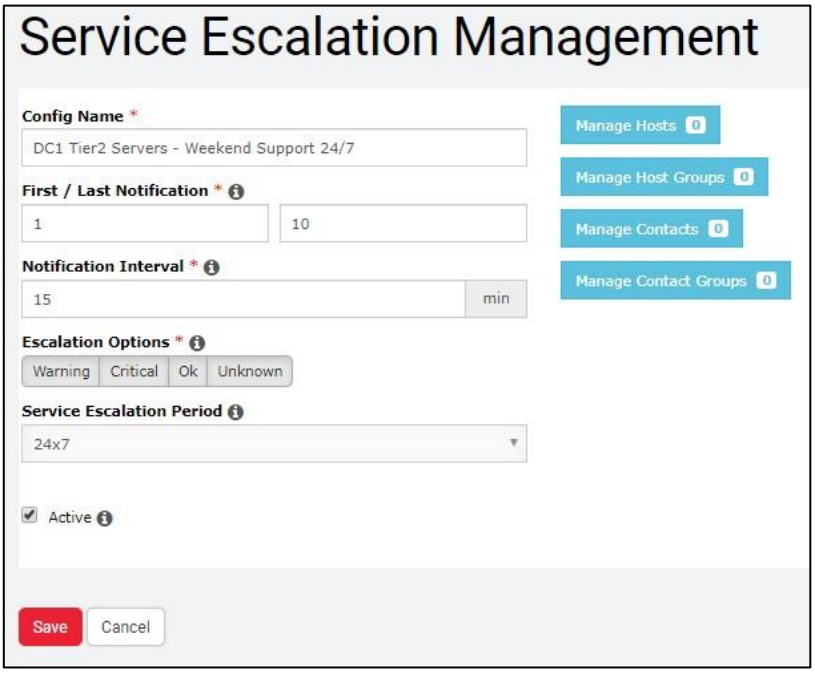
k. Manage Contacts
Rather than use a specific contact group, you may have urgent need to add support contacts manually, on the fly. You can add the individual contacts for an outlier/uncovered time frame, and then remove them later, in favor of the selected Contact Group that is once again staffed accordingly.

l. Manage Contact Groups
This is where you can select the Contact Group previously built to support specifically tiered host escalations. You can mix individual “Manage Contacts” additions with one or multiple selected groups.

m. Save
Once you’ve completed administering the configuration, click **Save**.

Administering Service Groups

In this form, Contact Groups may be assigned to specific Service alarms within specific hosts. One of the primary attractions to this form would be the ability to flag escalations based on more alarm variables, like *Unknown* status.



a. Config Name -> Notification Interval are no different from the Host Escalation Management options.

b. Escalation Options
The available options may all be selected at once, or only 1 status alert also be selected.

c. Service Escalation Period
As with the Host Escalation form, this field represents the cross-span of date/time contacts and contact groups will be eligible to receive notification alerts.

d. Active
Check the box for the administrative selections to go live and in service. Un-check the box to stop all notifications escalations.

Chapter 13: User rights

User rights

This chapter contains information about Avaya Orchestrator™ user rights or permissions and how to effectively manage permissions to ensure security and obtain a web interface tailored to various individual needs.

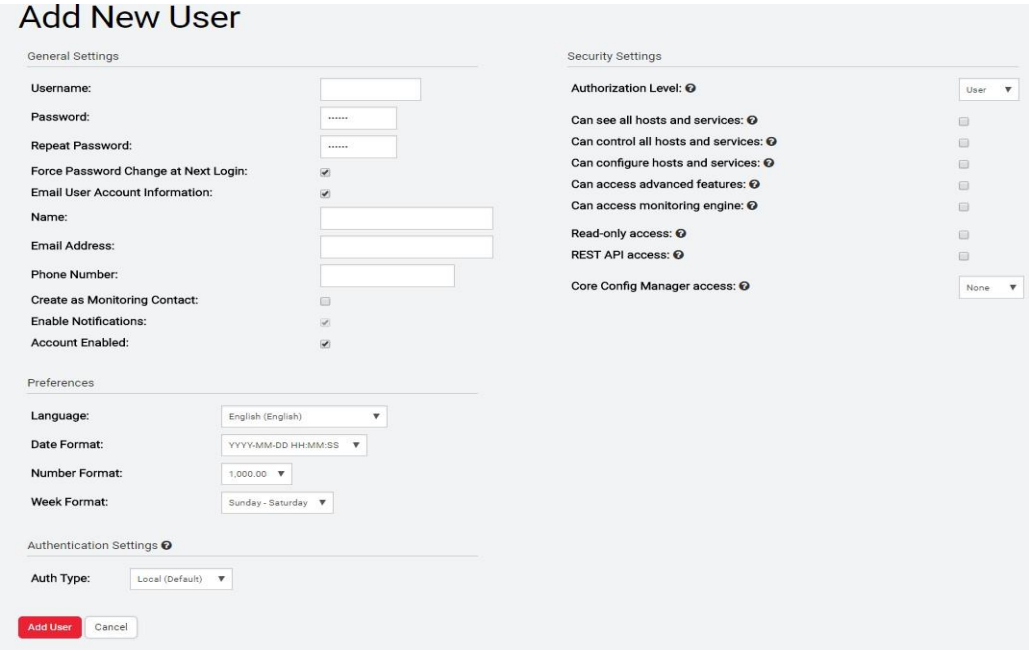
Managing permissions

About this task

You can configure permissions for individual users when adding a new user account to Avaya Orchestrator™ or modify the permission for an existing user on the Manage Users page.

Procedure

1. Log on to the Avaya Orchestrator™ web interface by using administrative credentials.
2. Click Admin.
3. In the left navigation pane, click Users > Manage Users.
4. On the **Manage Users** page, do one of the following:
   - Click the Edit icon corresponding to the user that you want to edit.
   - Click **Add New User** to add a new user.



5. Set the permissions.

Note:

- Clear the **Create as Monitoring Contact** check box.
- The options that you select in the **Security Settings** area of the **Add New User** or **Edit User: *<user name>*** page determine the permissions.
- By default, **Authorization Level** is set to **User**. This is the most restrictive permission in Avaya Orchestrator™.
- If you do not select any options, the user can only view the host and services that have the user defined as a contact.

Administrator privileges

Users with administrator privileges can access, add, and re-configure the following:

- Users
- Hosts
- Services
- Components
- Configuration wizards
- Dashlets
- Program settings
- Security credential

Note:

You must enable the **Rest API access** option when you select the **Authorization Level** as **Admin**. Failure to do so results in undesirable configuration outcomes when changes are done in the ACP Configuration Wizard, which may require saved XML translations to be imported for resolution.

For more information, see Managing permissions.

User security settings

You can grant various levels of security settings to users depending on the requirements. The following table contains information about the security setting options:

Setting	Description
Authorization Level	The authorization level for the user. The options are: • **User**: Security settings for users. • **Admin**: Security settings for administrators.

	Note: The **Admin** authorization level has all user rights except the **REST API access** right. By default, the **REST API access** option is not enabled for the **Admin** authorization level.
Can see all hosts and services	The user can see all hosts and services which are monitored and not just the ones they are in a direct or indirect notification contact.
Can control all hosts and services	The user can: • Acknowledge problems • Schedule downtime • Toggle notifications • Force checks on all objects
Can configure hosts and services	The user can: • Run configuration wizards. • Delete from Detail page. • Re-configure from Detail page.
Can access advanced features	The user can: • Edit check command on the Re-configure Host/ service page. • Show the **Advanced tab** and commands on the Host/service page. • Allow setting host parents in wizards and on the Re-configure Host/service page.
Can access monitoring engine	The user can: • View the monitoring process icon on the navigation bar. • Control the monitoring engine. For example, shutdown or restart. • Allow access to the event logs.
Read-only access	This option restricts the user to a read-only role and overwrites other options preceding it.
REST API access	The Avaya Orchestrator™ REST API allows users to create/query to read, write, delete, and update data in the Avaya Orchestrator™ system by using commands that are authenticated through the Avaya Orchestrator™ API keys.
Core Config Manager access	Option to provide user access to Core Config Manager (CCM). Leave this option at the default state of **None**. • **None**: No access. CCM is not visible to the user.

	• **Login**: The user can view the CCM links and must log in with a CCM user account. • **Limited**: The user has integrated CCM access. The user can view the objects specified under this option. Select the objects to allow a user to add, edit, and remove the objects. • **Full**: The user has integrated CCM access. The user can access all objects with no administrative features.

Avaya Orchestrator™ API

Avaya Orchestrator™ API is a REST API that includes feature rich control over the Avaya Orchestrator system. The API allows you to read, write, delete, and update data in the Avaya Orchestrator system through commands that are authenticated by using Avaya Orchestrator™ API keys.

For the following settings, each user has a unique API key:

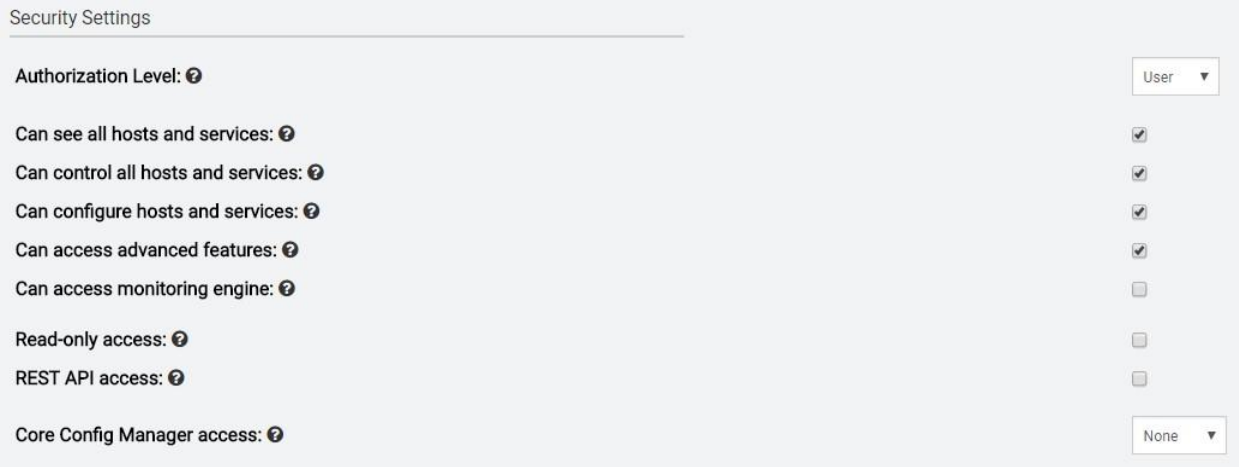
- Users have read access if the **REST API Access** setting is selected.
- Users can have access only to the **Objects API** endpoint and the relevant documentation.
- Administrators have full access to the API if the **REST API Access** setting is selected.

User privileges

Advanced user with change control

Common settings for an advanced user allow the user to view, control, and re-configure all existing hosts and services that are monitored, as well as, add new hosts and services to the monitoring configuration.

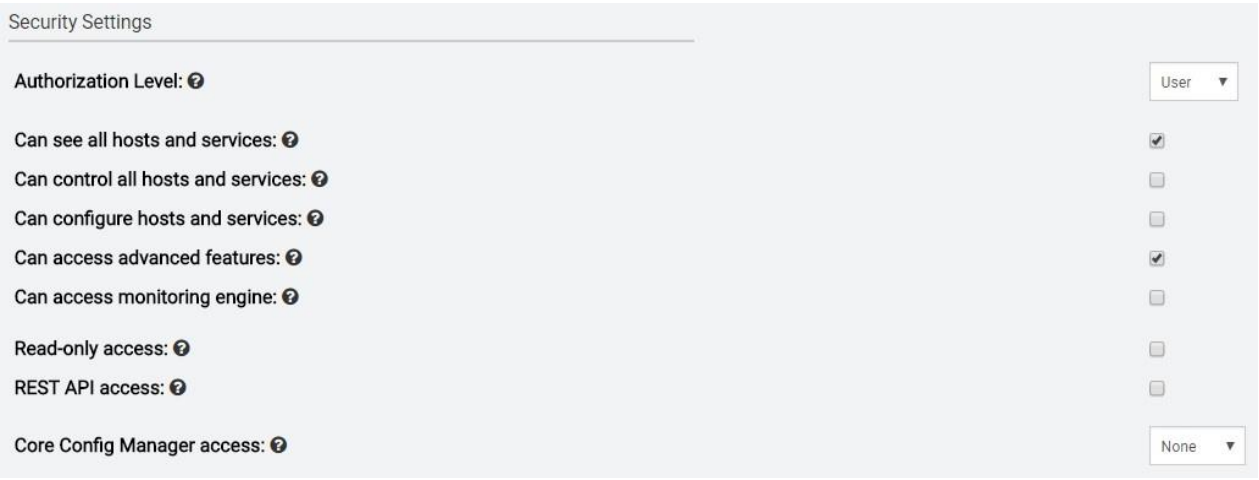
A user with these user rights has access to advanced information and commands related to hosts and services that are monitored. However, this user will not have access to control the monitoring engine. For example, shutdown and start the monitoring engine.



Basic read-only user

Common settings for a basic user allow the user to view all hosts and services that are monitored. However, the user cannot re-configure anything or submit commands to the monitoring engine.

These settings are often used when configuring user rights for IT managers or decision makers who need access only to view the monitoring information.



Chapter 14: User authentication and import

Authenticate and import users with Active Directory or LDAP

This chapter contains information about how to integrate Avaya Orchestrator™ with Active Directory (AD) or Lightweight Directory Access Protocol (LDAP) to allow user authentication and validation with an AD or LDAP infrastructure by using the Avaya Orchestrator™ interface.

This helps system administrators to simplify user management of large infrastructures and standardize credentials that are needed for Avaya Orchestrator™ by allowing users to authenticate with their AD or LDAP credentials.

Using a DNS server

About this task

This procedure assumes that the DNS settings for your Avaya Orchestrator™ server use DNS servers that are either of the following:

- Domain Controllers (DC) in your AD domain.
- Capable of resolving the DNS entries that are used to contact your LDAP servers.

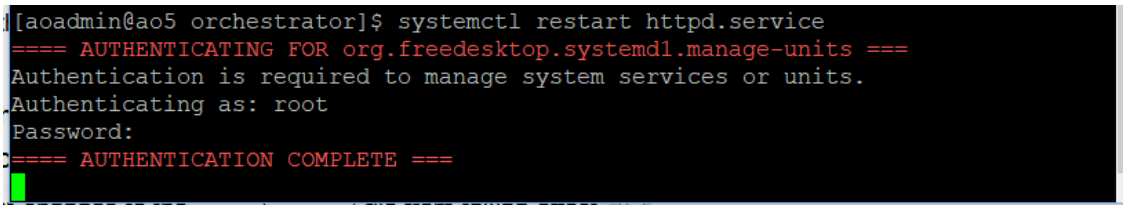
If you have problems with the DNS, use the following procedure to edit the `resolv.conf` file to use the DNS server within the AD infrastructure as the primary name server.

Procedure

1. Log in to Avaya Orchestrator™ by using SSH and the *aoadmin* login credentials.
2. Run the following command to edit the `resolv.conf` file in a text editor:
   sudo vi /etc/resolv.conf
3. Type the following before the lines that start with `nameserver`:

   i nameserver [DNS_server_IP] <ESC KEY>
   :wq!
   Caching options in PHP may prevent changes to the `resolv.conf` file from taking effect and require restarting the Apache service.
4. To edit the file, restart the Apache web server by running the following command:
   systemctl restart httpd.service

   The system prompts you to enter the root password to authenticate the permissions to perform this activity.



Note:

Be aware that the networking stack in RHEL can automatically overwrite the `/etc/resolv.conf` file.

Configuring authentication servers

About this task

Use this procedure to configure the authentication server that Avaya Orchestrator™ must use.

Procedure

1. Log on to Avaya Orchestrator™ by using administrative credentials.
2. Click **Admin**.
3. In the left navigation pane, click **Users** > **LDAP/AD Integration**.
4. To add an authentication server, click **Add Authentication Server**.
5. In the **Authentication Server Settings** area, select the **Enable this authentication server** check box.
6. In the **Connection Method** field, click one of the following:
   - **Active Directory**
   - **LDAP**
7. Do the following if you select **Active Directory** in the **Connection Method** field:
   a. In the **Base DN** field, type the LDAP formatted string where the users are located. For example, Orchestrator user are on POD Organizational Unit.

      For Example, OU=pod,DC=avaya,DC=com

   b. In the **Account Suffix** field, type the part of the full user identification that comes after the user name, in the format: @yourdomain.suffix.

      For example, `@avaya.com`.

   c. In the **Domain Controllers** field, type the domain controller servers that Avaya Orchestrator™ can use to authenticate against.

      This can be either IP addresses or fully qualified domain names.

      When you use SSL for security, this entry must match the Common Name (CN) in the SSL certificate that these domain controllers present to the Avaya Orchestrator™ server. TLS is not supported in Avaya Orchestrator™ Release 1.5.

For example, `dc1.avaya.com`

d. In the **Security** field, click the security method to connect to the server.

e. Click **Save Server**.

8. Do the following if you select **LDAP** in the **Connection Method** field:

a. In the **Base DN** field, type a LDAP formatted string where the users are located.

For example, `dc=avaya,dc=com`

b. In the **LDAP Host** field, type the IP address or the host name of the LDAP server that Avaya Orchestrator™ can use to authenticate against.

You can specify an IP address, short name, or fully qualified domain name. For example, `ldap01.avaya.com`

When you use SSL for security, this entry must match the Common Name (CN) in the SSL certificate that the LDAP server presents to the Avaya Orchestrator™ server.

For example, `ldap01.avaya.com`

c. In the **LDAP Port** field, type the TCP network port that you want to use to communicate with the LDAP server.

The default port is 389.

d. In the **Security** field, click the security method to connect to the LDAP server.

e. Click **Save Server**.

Importing users from Active Directory and LDAP

Procedure

1. Log on to Avaya Orchestrator™ by using administrative credentials.
2. Click **Admin**.
3. In the left navigation pane, click **Users** > **Manage Users**.
4. On the Manage Users page, click **Add Users from LDAP/AD**.
5. On the **LDAP / Active Directory Import Users** page, select the authentication server that you have defined and specify the user name and password to connect to the server.

   The account credentials that you provide are used only to authenticate against the Active Directory or LDAP to retrieve the directory contents. These credentials are not saved or used in the actual user authentication.
6. Click **Next**.

   After successful authentication, a node of your directory tree appears. This is relative to the Base DN that you specify.
7. Select the users that you want to import, and then click **Add Selected Users**.

8. Select the check boxes corresponding to the users for whom you want to configure the same preferences and security settings.
9. In the **Edit multiple** field, click **Preferences**.

   The **Preferences** dialog box appears.
10. Do the following to configure the preferences for the users:
    a. Clear the **Create as Monitoring Contact** check box.
11. In the **Edit multiple** field, click **Security Settings**.

    The **Security Settings** dialog box appears.
12. Configure the security settings for the users.
13. Click **Save**, and then click **Import**.

Result

After you import a user, Avaya Orchestrator™ queries the domain controllers or LDAP server to validate the credentials each time the user logs in.

Linking existing Avaya Orchestrator™ users to Active Directory users

About this task

If you have already created Avaya Orchestrator™ users, you can easily link these local accounts to Active Directory accounts.

Procedure

1. Log on to Avaya Orchestrator™ by using administrative credentials.
2. Click **Admin**.
3. In the left navigation pane, click **Users** > **Manage Users**.
4. On the Manager Users page, click the **Edit** icon corresponding to the user that you want to link to Active Directory.
5. On the Edit User: <*user name*> page, in the **Authentication Settings** area, do the following:
   a. In the **Auth Type** field, click **Active Directory**.
   b. In the **AD Server** field, select the authentication server that you have defined.
   c. In the **AD Username** field, type the user name that is configured in Active Directory for the user.

      For example, `jane.doe`
6. Select the **Allow local login if auth server login fails** check box to allow the user to use the local password that is created for the user.

Avaya Orchestrator™ uses the local login when the authentication server cannot be connected or times out, or the password provided is incorrect. This allows a secondary method of authentication if the authentication server is unreachable.

7. Click **Update User**.

Result

After these changes are made, the existing Avaya Orchestrator™ users can log in by using their Active Directory credentials.

Linking existing Avaya Orchestrator™ users to LDAP users

About this task

If you have created Avaya Orchestrator™ users, you can easily link these local accounts to LDAP accounts.

Procedure

1. Log on to Avaya Orchestrator™ by using administrative credentials.
2. Click **Admin**.
3. In the left navigation pane, click **Users** > **Manage Users**.
4. On the Manager Users page, click the **Edit** icon corresponding to the user that you want to link to LDAP.
5. On the Edit User: <*user name*> page, in the **Authentication Settings** area, do the following:
   a. In the **Auth Type** field, click **LDAP**.
   b. In the **LDAP Server** field, click the authentication server that you have defined.
   c. In the **User's Full DN** field, type the full distinguished name (DN) that is configured in LDAP for the user.

      For example, `uid=bobsmith,ou=People,dc=box293,dc=local`
   d. Select the **Allow local login if auth server login fails** check box to allow the user to use the local password that is created for the user.

      Avaya Orchestrator™ uses the local login when the authentication server cannot be connected or times out, or the password provided is incorrect. This allows a secondary method of authentication if the authentication server is unreachable.
6. Click **Update User**.

Result

After these changes are made, the existing Avaya Orchestrator™ users can log in by using their LDAP credentials.

LDAP account requirements

The following is an example of the required object classes and attributes that must exist for an LDAP user. If these attributes do not exist, it is likely that they do not appear in the list of users when you import from your LDAP server.

- dn: uid=bobsmith,ou=POD,dc=avaya,dc=com givenName: Bob
- sn: Smith
- cn: Bob Smith uidNumber: 10004
- gidNumber: 10004
- mail: bobsmith@avaya.com homeDirectory: /home/bobsmith objectClass: top
- objectClass: posixAccount objectClass: inetOrgPerson

Chapter 15: Email configuration

Email configuration

This chapter contains information about how Avaya Orchestrator™ sends email messages and how to configure your email settings. Avaya Orchestrator™ uses email to send notifications and reports.

Accessing the email settings

Procedure

1. Log on to Avaya Orchestrator™ by using administrative credentials.
2. Click **Admin**.
3. In the left navigation pane, click **System Config** > **Manage Email Settings**.

Web browser behavior

Important: There are some web browser behaviors you should be aware of that can cause unwanted behaviors in ways that are not obvious to detect.

Different web browsers auto-complete and auto-populate fields on a web page when the web page loads. This usually occurs only when the web browser identifies a common field that does not have a value. The web browser has a saved value for that named field. Hence, the web browser populates the field with the saved value. Therefore, if you open the Manage Email Settings page in Avaya Orchestrator™, the **Username** and **Password** fields are already populated, even when you visit the page for the first time after a fresh installation of Avaya Orchestrator™.

However, this can cause confusion. For example, you might define SMTP settings that do not require a user name or password. If you click **Update Settings** when the **Username** and **Password** fields are populated with the values that the web browser auto-completes, authentication is attempted with those values, even though your receiving server does not require credentials. Since the credentials are saved, they are used while sending email messages. As a result, sending of the email messages fails as the SMTP server is unaware about the credentials.

If you leave the **Username** and **Password** fields blank, and then click **Update Settings**, Avaya Orchestrator™ saves the settings and records that no user name or password is defined. However, when the web page refreshes, your web browser might re-populate those fields with the saved values.

Configuring the email address from which email messages are sent

About this task

Use the **Send Mail From** field to configure the email address from which email messages are sent. The format of the email address is: Plain Text Name <alias@your.email.domain>.

Note:

The brackets < > are required.

If you do not format the email address properly, the email is sent; however, in some circumstances the mail sending program switches to the system default. For example, Root User <root@localhost>.

If the receiver of the email message clicks the reply button in their email client, the reply is sent to the Root User <root@localhost>. Hence, ensure that you configure a valid email address.

Procedure

1. Log on to Avaya Orchestrator™ by using administrative credentials.
2. Click **Admin**.
3. In the left navigation pane, click **System Config** > **Manage Email Settings**.
4. On the Mail Settings page, in the **General Mail Settings** area, in the **Send Mail From** field, type the email address from which you want to send the email messages.

Methods for sending emails

Avaya Orchestrator™ provides the following two methods for sending email messages:

- Sendmail / Postfix
- SMTP

Configuring Sendmail / Postfix as the method for sending email messages

About this task

This mail method uses Postfix to send email. It is referred to in the interface as **Sendmail** because this is historically the most common mail sending method. In the operating system, the **`sendmail`** command is actually the **`sendmail.postfix`** command that allows Postfix to accept **`sendmail`** commands.

The Avaya Orchestrator™ server uses the **Sendmail** method to send email messages directly to all the recipients. It contacts the email server for the email recipient and sends the message through SMTP port 25. This means that the message is sent by using plain text. Hence, network sniffing programs can easily view the contents of the email messages.

Problems can arise when you send email messages to recipients that have spam or virus detection software. The receiving mail server detects that the email message it received is not from the mail server that is the owner of that domain. The mail server either discards the email message or moves it to a junk mail folder. This behavior is obviously not desired as you want to make sure that notifications are received.

You need not configure additional settings if you select **Sendmail**, on the Manage Email Settings page, as your method to send email messages.

Procedure

1. Log on to Avaya Orchestrator™ by using administrative credentials.
2. Click **Admin**.
3. In the left navigation pane, click **System Config** > **Manage Email Settings**.
4. On the Mail Settings page, in the **General Mail Settings** area, in **Mail Method**, click **Sendmail**.

Configuring SMTP as the method for sending email messages

About this task

You can use SMTP as the method for sending email messages if you want to configure Avaya Orchestrator™ to use an email server for mail delivery.

The email server can be:

- An internal email server in your organization, such as:
  - Microsoft Exchange
  - Postfix
- An external email server, such as:
  - Hosted email services
  - Internet service provider

Using an SMTP server for mail delivery is a more secure method of sending email messages. Also, the Avaya Orchestrator™ server can focus on monitoring activities and need not use computing resources for being an email server.

Procedure

1. Log on to Avaya Orchestrator™ by using administrative credentials.
2. Click **Admin**.
3. In the left navigation pane, click **System Config** > **Manage Email Settings**.
4. On the Mail Settings page, in the **General Mail Settings** area, in **Mail Method**, click **SMTP**.
5. In the **SMTP Settings** area, do the following:
   a. In the **Host** field, type the network address of the SMTP server.

      You can specify the IP address or FQDN of the SMTP server.

   b. In the **Port** field, type the network port that the SMTP server is listening on.

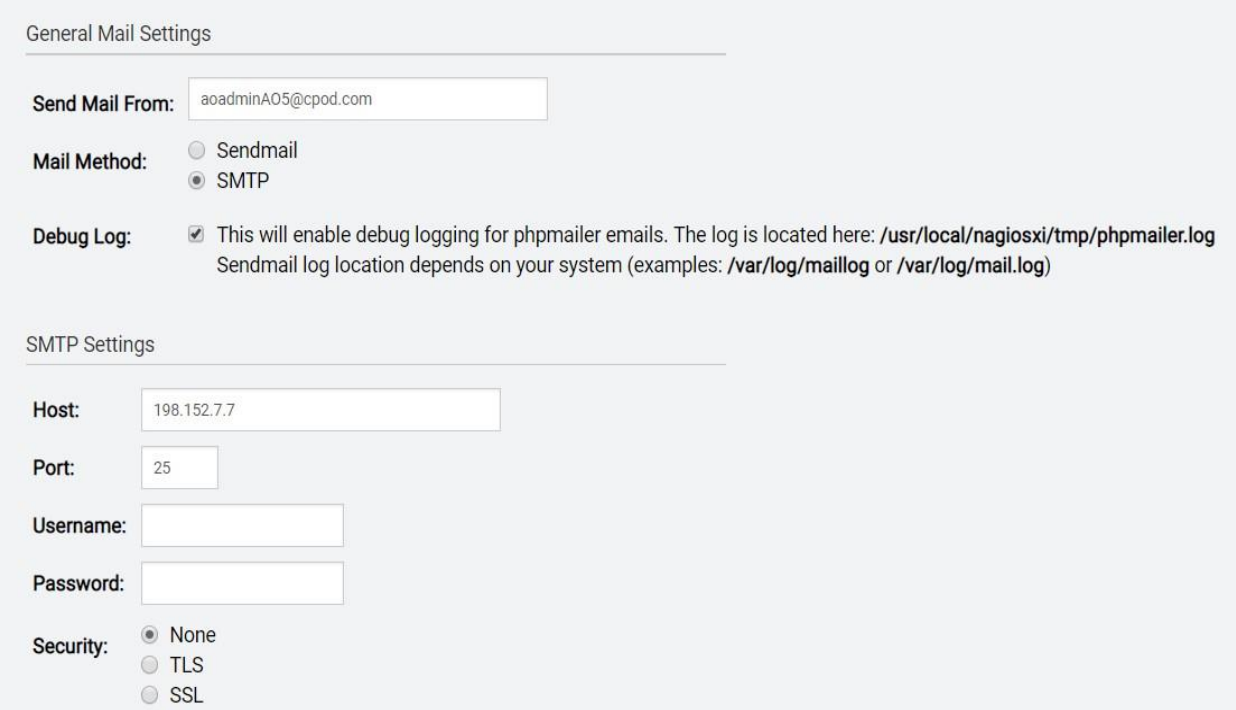
Common port to use is 25.

Note:

- The **Username** and **Password** fields are used in Avaya Orchestrator™ Release 1.5. Hence, not required.
- TLS and SSL are not supported in Avaya Orchestrator™ Release 1.5.

Example:

In the following example, the SMTP server is a Microsoft Exchange server that allows connections from the Avaya Orchestrator™ server IP address. It does not require authentication and the **Security** option is set to **None**.



Chapter 16: Maintenance and Troubleshooting

Overview

This chapter contains information and procedures for maintaining and troubleshooting an Avaya Orchestrator™ instance.

Log files

This section contains information about the logs that are available for troubleshooting Avaya Orchestrator™.

Standard log locations

The following locations contain alarm and application support activity logs in the Avaya Orchestrator™ server:

- `/var/log/orchestrator`
- `/var/log/snmptt`
- `/var`

These are system logs that provide helpful information when troubleshooting a problem in Avaya Orchestrator™ or within the server itself. By default, all the following logs are managed and rotated by rsyslog or by the system logger that the Avaya Orchestrator™ server is running.

Logs located in /var/log/orchestrator

```
[aoadmin@ao5 orchestrator]$ cd /var/log/orchestrator
[aoadmin@ao5 orchestrator]$ ls -ltr
total 2892
-rw-r--r--. 1 root   root         0 Jan 17 07:24 check_system_services.log
-rw-rw-r--  1 apache nagios 1164875 Jan 17 15:25 wizard-20190117.log
-rw-r--r--. 1 root   root       894 Jan 17 22:00 orchestrator_backup.log
-rw-rw-r--  1 apache nagios    3148 Jan 17 22:18 viewgen-20190117.log
-rw-rw-r--. 1 nagios nagios  943357 Jan 17 23:55 rediscovery-20190117.log
-rw-rw-r--  1 apache nagios     678 Jan 18 04:41 viewgen-20190118.log
-rw-rw-r--  1 nagios nagios    6407 Jan 18 07:15 rediscovery-20190118.log
-rw-r--r--. 1 nagios nagios  812347 Jan 18 07:15 orchestrator_rediscovery_cron.log
```

These are system logs that provide status details about the processes that support the administration wizard and the discovery of hardware in each of the designated racks.

Logs located in /var/log/snmptt

```
[aoadmin@ao5 snmptt]$ cd /var/log/snmptt
[aoadmin@ao5 snmptt]$ ls -ltr
total 6940
-rw-r--r--. 1 root   root    1384 Jan 17 15:04 snmpttsystem.log
-rw-rw-r--  1 snmptt root 7088318 Jan 18 07:39 snmptt.log
```

These are logs that collect the SNMP trap information received by Avaya Orchestrator™. The information that passes into the snmptt.log file is often used to monitor real-time, incoming trap activities. The following screen shot contains an example:



Logs located in /var

These are system logs that provide helpful information when troubleshooting a problem in Avaya Orchestrator™ or the server itself. By default, all the following logs are managed and rotated by rsyslog or by the system logger that the Avaya Orchestrator™ server is running.

You must have root level privilege to view the following log files:

- `/var/log/messages`

  This is the system messages log. Most hardware-related errors, nrpe information, segfaults, kernel msg limits, ulimit errors, and so on appear here. If you suspect intermittent hardware problems, use this log or run **`dmesg`**.

- `/var/log/httpd/error_log`

  This is the Apache error log. Problems and bugs in the PHP, authentication problems, and problems with broken URLs are logged here. Because Avaya Orchestrator™ is a LAMP application, many issues are logged here. You can use this log for troubleshooting.

- `/var/log/httpd/access_log`

  This is the Apache access log. Failed authentications, Ajax requests, and page views are logged here.

- `/var/log/maillog`

  This file logs email sent through sendmail. It is only applicable to core contact "notify-*-by-email" notification handlers and sendmail tests.

System time configuration

Use the information and procedures in this section to configure the system date, time, and time zone for the server.

Configuring the system time zone

Procedure

1. Log on to Avaya Orchestrator™ by using administrative credentials.
2. Click **Admin**.
3. In the left navigation pane, click **System Config** > **System Settings**.
4. On the **General** tab, in the **Timezone Settings** area, in the **Timezone** field, click the appropriate time zone.
5. Click **Update Settings**.

Verifying the configuration

About this task

Verify the system date and time configuration.

Procedure

1. Log on to Avaya Orchestrator™ by using administrative credentials.
2. Click **Admin** > **System Config** > **System Profile**.
3. On the System Profile page, click **View System Info**.

   Information about the system is displayed.
4. Locate the Date/Time section and verify that the information is correct.

Change passwords

Use the information and procedure in this section to change the password for an Avaya Orchestrator™ installation to ensure a safe and secure monitoring environment.

Default password considerations

All password changes are optional. Changing default passwords is a network security best practice that helps secure your Avaya Orchestrator™ installation from security threats and compromises.

Note: Avaya strongly recommends changing the default passwords of the product in production.

Changing the Linux aoadmin (super user) password

About this task

Use the following procedure to change the password for the Linux `aoadmin` account. It is through this login that users can access the *root* account permissions.

Procedure

1. Log in to Avaya Orchestrator™ VM by using SSH.
2. Use the following credentials:

   User name: *aoadmin*

   Password: `Avaya123$`
3. At the aoadmin prompt $, type the **`passwd`** command.
4. Follow the next prompt and type the current password, and then press `Enter`.
5. Type the new password at the next command prompt and press `Enter`.
6. Re-enter the new password at the next command prompt and press `Enter`.

   A message appears that the password is successfully changed.

Configuring downtime

About this task

Use the following procedure to schedule downtime for a service, host, host group, or service group. You can schedule downtime to avoid receiving unnecessary or unwanted notifications during a period of expected service interruption.

You can configure a Fixed or Flexible downtime.

Note:

Fixed downtime starts and stops at the exact start and end time that is specified when the downtime is scheduled.

Flexible downtime is intended for an event when a host or service is unavailable for an amount of time, but the time when that event will start is not known. Avaya Orchestrator™ starts the downtime sometime between the scheduled start and end times. The duration lasts for the scheduled amount of time.

Flexible downtime assumes that the host or service for which you have scheduled the flexible downtime either goes down, becomes unreachable, goes into a non-operational state sometime between the start and end times that you specify. The time at which a host or service transitions to a problem state determines the time at which Avaya Orchestrator™ actually starts the downtime. The downtime lasts for the duration that you specify, even if the host or service recovers before the downtime expires.

Procedure

1. Log on to Avaya Orchestrator™ by using administrative credentials.

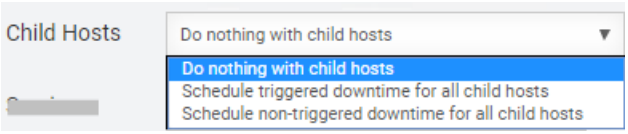
2. Click **Home.**
3. In the left navigation pane, click **Incident Management** > **Scheduled Downtime**.
4. On the Scheduled Downtime page, click **Schedule Downtime**.
5. Do one of the following:
   a. Click **For Host(s)** if you want to schedule downtime for hosts.
   b. Click **For Service(s)** if you want to schedule downtime for services.

      Use the **Filter** field to filter host and service names in large deployments.
6. Click **Add Selected**.

   The **Author** field displays the login ID of the user who has logged in.
7. In the **Comment** field, type a comment indicating the purpose of the downtime.
8. In the **Triggered By** field, specify if the downtime is started by another scheduled downtime event.
9. In the **Type** field, click **Fixed** or **Flexible** depending on the type of downtime and provide the required information.
10. In the **Duration** field, specify a duration for the downtime.

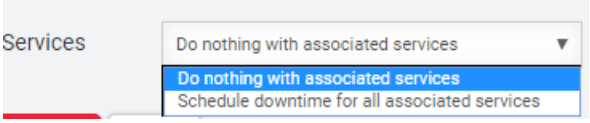
    The **Duration** field is available only when you schedule a Flexible downtime.
11. In the **Start Time** field, click the start time for the downtime.
12. In the **End Time** field, click the end time for the downtime.
13. In the **Child Hosts** field, click the child host behavior that matches the intended downtime situation.

    The **Child Hosts** field is available only when you schedule downtime for hosts.



14. In the **Services** field, click the effected services.

    The **Services** field is available only when you schedule downtime for hosts.



15. Click **Schedule**.

Configuring recurring downtime

About this task

Recurring downtime is useful when you have regular periods of downtime and you do not want to schedule those periods individually. You can configure recurring periods of downtime instead.

Procedure

1. Log on to Avaya Orchestrator™ by using administrative credentials.
2. Click **Home.**
3. In the left navigation pane, click **Incident Management** > **Recurring Downtime**.
4. On the Recurring Scheduled Downtime page, click the tab according to what you want to schedule the downtime for: **Hosts**, **Services**, **Hostgroups**, or **Servicegroups**.
5. Click **Add Schedule**.
6. On the **Add Recurring Downtime Schedule** page, do the following to schedule the recurring downtime:
   a. Specify the Host, Service, Hostgroup, or Servicegroup depending on the tab you have selected.
   b. If you are configuring a recurring downtime for hosts or hostgroups, select the check box corresponding to the **Services** field to include all services in the host or hostgroup.

      The check box is available only when you schedule recurring downtime for hosts and hostgroups.
   c. If you are configuring recurring downtime for services, in the **Services** field, type the associated services.

      The **Services** field is available only when you schedule recurring downtime for services.
   d. In the **Comment** field, type a comment that describes the recurring downtime.
   e. In the **Start Time** field, type a start time for the recurring downtime.

      Use a 24-hour time format.
   f. In the **Duration** field, type a duration, in minutes, for the recurring downtime.
   g. In the **Valid Months**, **Valid Weekdays**, and **Valid Days of Month** fields, specify the appropriate values for the recurring downtime.
7. Click **Submit Schedule**.

Scheduling downtime by using mass acknowledgement

About this task

You can use the *Mass Acknowledgments and Downtime Scheduling* page to schedule downtime for hosts and services that are already in a non-operational state.

Procedure

1. Log on to Avaya Orchestrator™.
2. Click **Home.**
3. In the left navigation pane, click Incident Management > Mass Acknowledge.
4. On the Mass Acknowledgments and Downtime Scheduling page, select all the hosts and services that you want to place in the scheduled downtime.

5. In **Command Type**, click **Schedule Downtime**.
6. In the **Time** field, specify the length of downtime in minutes to schedule flexible downtime.
7. In the **Comment** field, type a comment.
8. Click **Submit Commands**.

Notification configuration

This section contains information and procedures about how to configure and manage notifications. Notifications can be emails or SMS text messages and are sent to users when hosts and services change states. This keeps users updated on the health of their monitoring environment.

Users and contacts are two separate entities.

- Core process creates and uses contacts to send notifications.
  - When a user is created, a contact is created for it by the Core process.
  - Contacts are assigned to host and service objects. Core uses this information to track which contacts receive notifications.
  - In Avaya Orchestrator™ Release 1.5, end users cannot modify their notification preferences, such as the format of the email being sent or what type of notifications they receive.
- Avaya Orchestrator™ creates user accounts to receive notifications.
  - Provides an authentication mechanism so that end users can access Avaya Orchestrator™.
  - Allows end users to define their notification preferences, such as the format of the email messages being sent, or the type of notifications they receive.
  - Allows end users to do other activities such as email reports.
  - Provide users with the ability to receive email and text notifications with different notification preferences for each method.

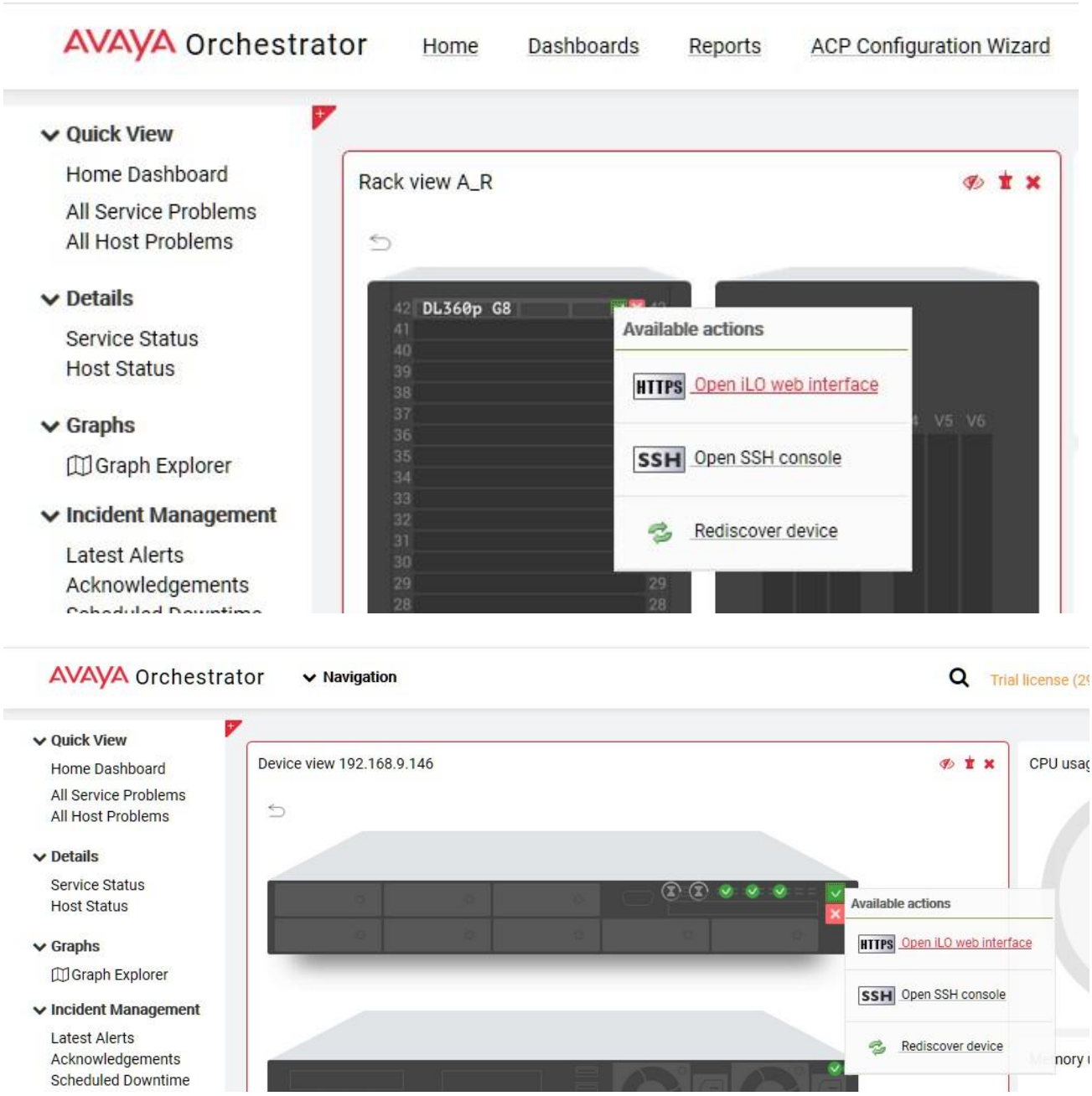
Note:
If you want to send notifications to the users that are imported from ADS/LDAP, ensure that the preceding notification configuration is completed.

Opening the iLO web interface from Rack view or Device view

1. Log in to Avaya Orchestrator™ by using administrative credentials.
2. Click **Home**.
3. Click the rack dashboard that contains the device that you want to open in the iLO web interface.
4. Do any of the following:
   a. In the Rack dashboard view, right-click the device status icon corresponding to the device, and then click **Open iLO web interface**.

b. In the Rack dashboard, click the rack that contains the device that you want to open in the iLO web interface. In the Device dashboard view, right-click the device status icon, and then click **Open iLO web interface**.

The login page of the ILO web interface appears.

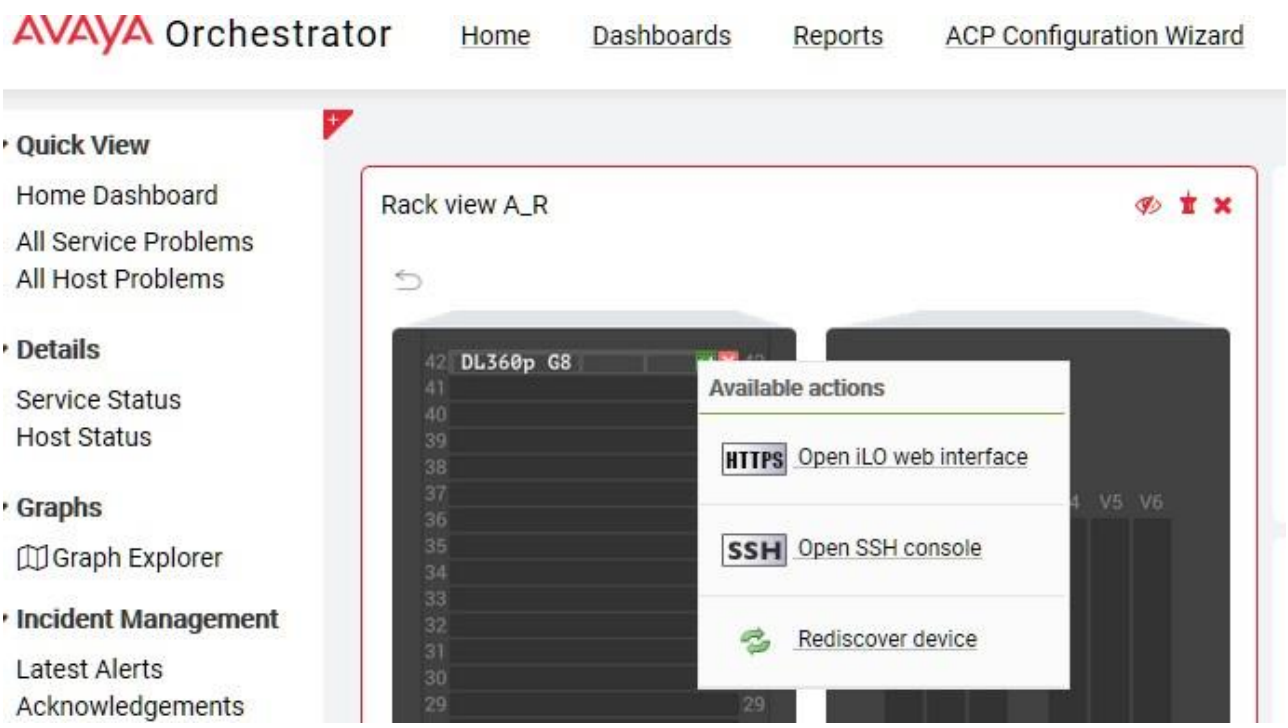


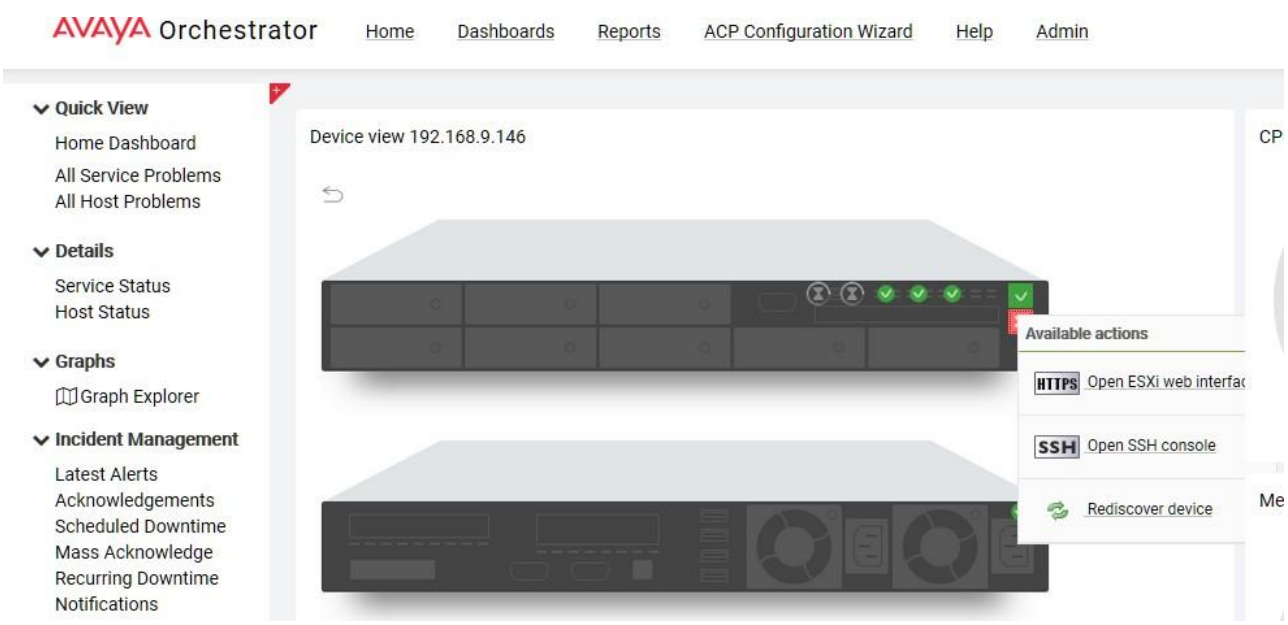
5. Specify the user name and password to log in to the ILO web interface.



Access the SSH terminal: Opening a device in the SSH console from a Rack view or Device view

1. Log in to Avaya Orchestrator™ by using administrative credentials.
2. Click **Home**.
3. Click the rack dashboard that contains the device that you want to open in the SSH console.
4. Do any of the following:
   a. In the Rack dashboard view, right-click the device status icon corresponding to the device, and then click **Open SSH console**.
   b. In the Rack dashboard, click the rack that contains the device that you want to open in the SSH console. In the Device dashboard view, right-click the device status icon, and then click **Open SSH console**.





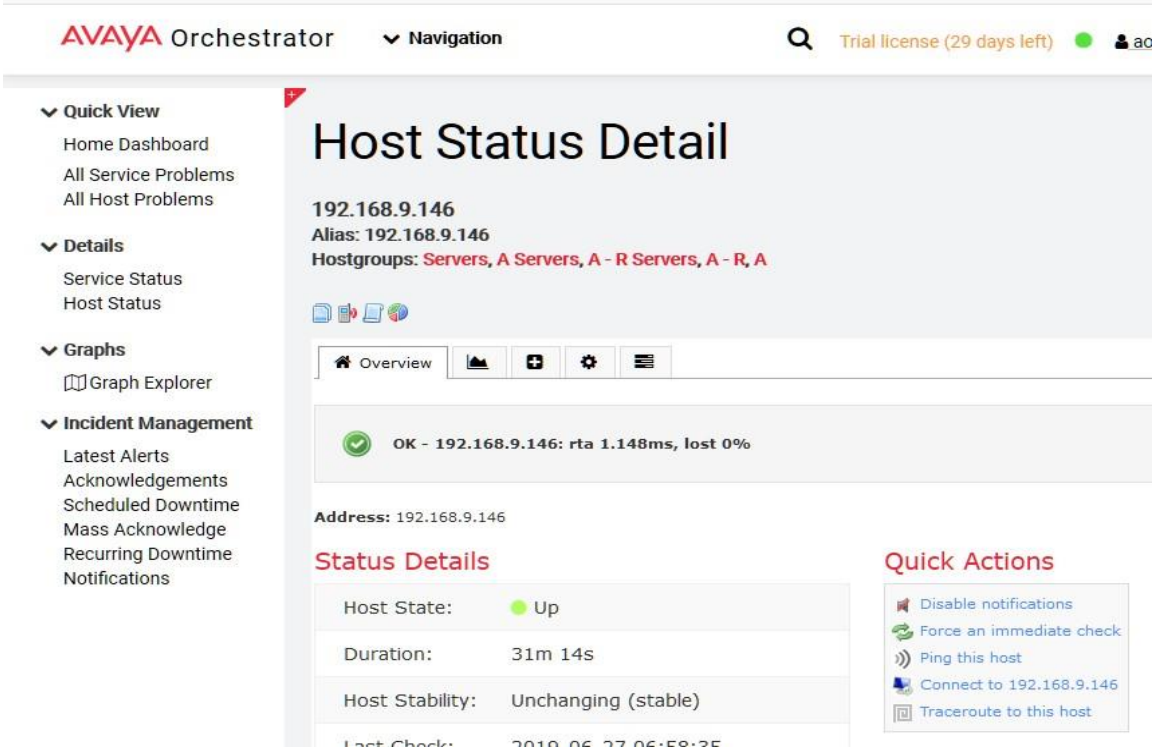
The SSH web console opens in a new browser.

5. Specify the user name and password to log in to the SSH web console.

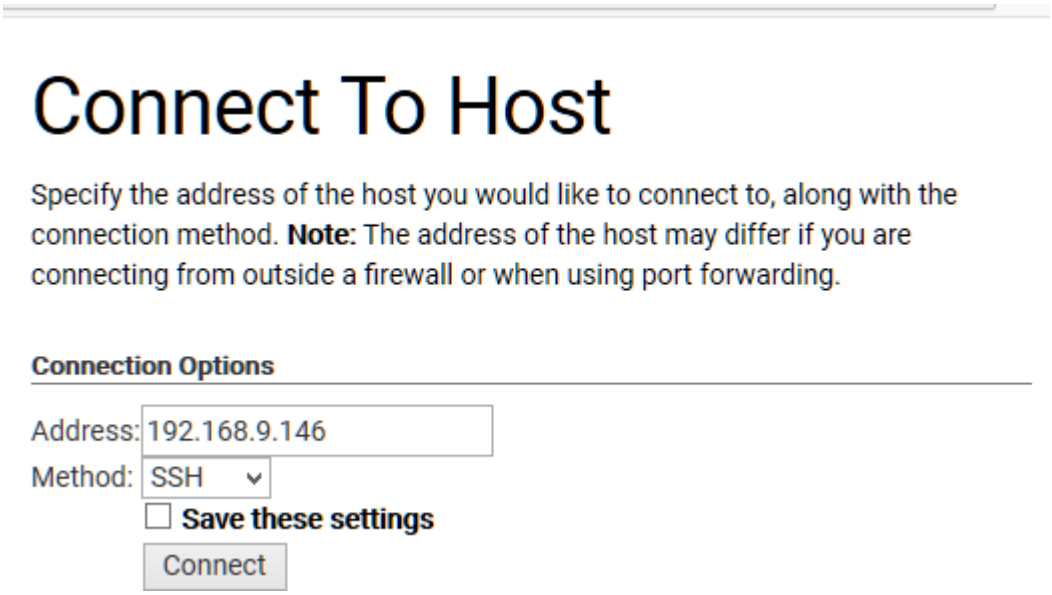
```
192.168.9.146 username: root
root@192.168.9.146's password:
Last login: Wed Jun 26 16:39:46 2019 from localhost
[root@themis ~]#
[root@themis ~]#
```

Opening a device in the SSH console from the Host Status Detail page

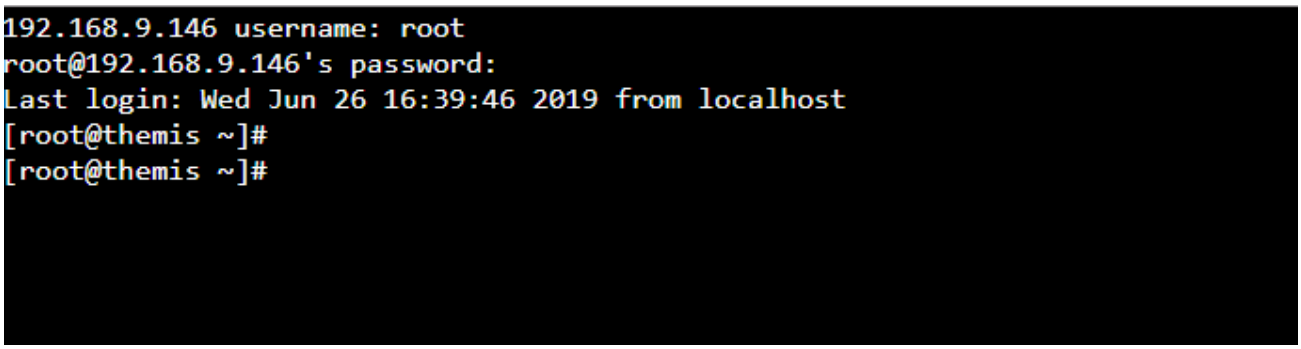
1. Log in to Avaya Orchestrator™ by using administrative credentials.
2. Click **Home**.
3. In the left navigation pane, click Details > Host Status.
4. On the Host Status page, in the Host column, click the device that you want to open in the SSH console.
5. On the Host Status Detail page, on the Overview tab, in Quick Actions, click Connect to <Device IP address>.



6. On the Connect To Host page, in the Method field, click SSH.



7. Click Connect.
The SSH web console appears.



8. Specify the user name and password to log in to the SSH web console.

Troubleshooting

Start with the bird’s eye view

Home Dashboard Assessment

Start by viewing the Home Dashboard. This is where all bird’s eye collective alarm information is presented. From here, you can drill down into many different reporting and action-oriented menus to learn more about problems and communicate status with other AO users who have opted to receive updates.

Host alarms

- The Host data in each category reflects the success or failure of AO to access the IP address of the administered devices.
- Alarms will be either *ok* or *critical.* Device ports will be either up or down.
- There is no need for *warning* level alarms for Hosts.
- *Unreachable* is not currently used in AO Release 1.5. It will be enabled in a future release and will relate to objects that are supported within a Host being monitored; for example, IP/SIP phones on a network host.

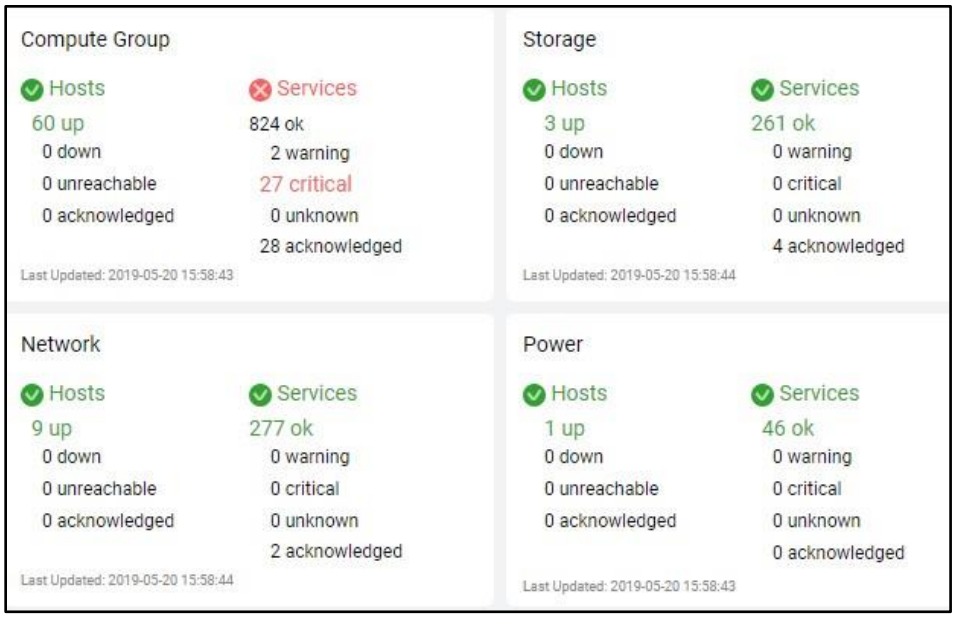
Service alarms

- Service data reflects the status of the monitored elements within each host.
- Alarms can be *ok, warning*, or *critical.*
- The *unknown* category reflects peg counts when hosts are down and reporting critical alarms. When a host is not accessible, AO cannot evaluate the internal services of that host. Therefore, the state of the services will be reported as *unknown.*

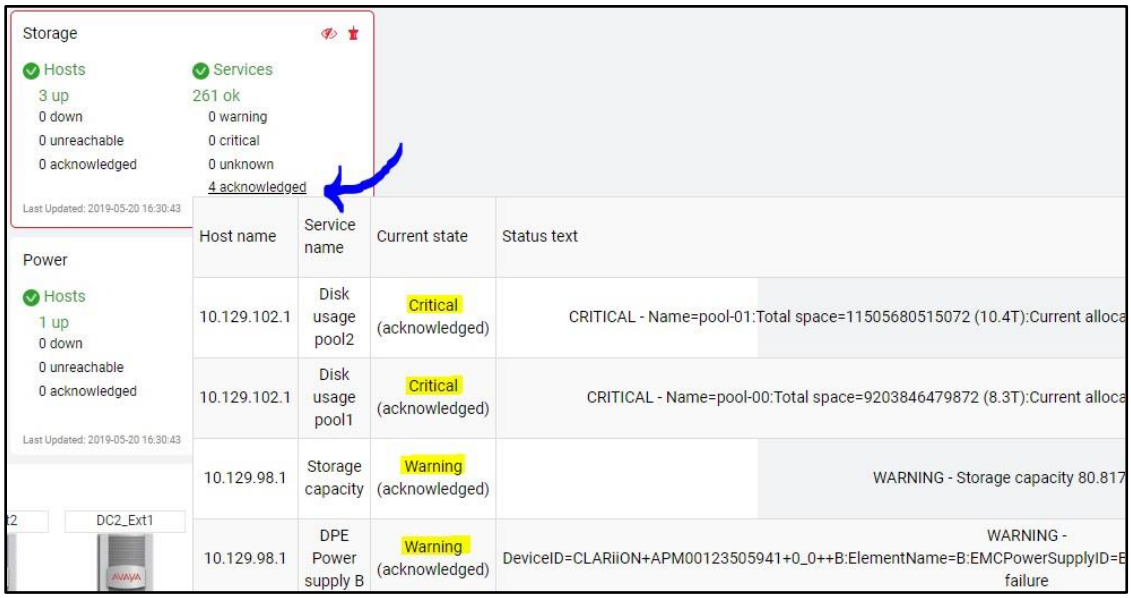
Acknowledged alarms

- When an administrative user has physically “acknowledged” an alarm in AO, alarm notification processing is stopped.
- On the Home dashboard view, as shown in the following screenshot, when an alarm is acknowledged, the associated *warning* or *critical* alarm is quiesced, or removed from this high-level view.
- An acknowledged alarm is the one already being attended and; therefore, should be removed from the collective alarm view to prevent potential visual distraction toward alarms already investigated. Removing such alarms states from the high-level overview allows the users who are monitoring the solution state of health to clearly view new alarms and new state changes.
- The acknowledged alarm(s) will remain present across all other reporting mechanisms, such as the Problems and Status reporting overviews, and they can be easily accessed by hovering over or clicking on the acknowledged link in each category.

In the following example, the *Storage* category reports no warnings and no critical alarms. There are 4 acknowledged alarms reported. A quick glance at this area would reveal no *new* issues. The same is true for the Network category, which reports no warnings, no critical alarms, and 2 acknowledged issues.



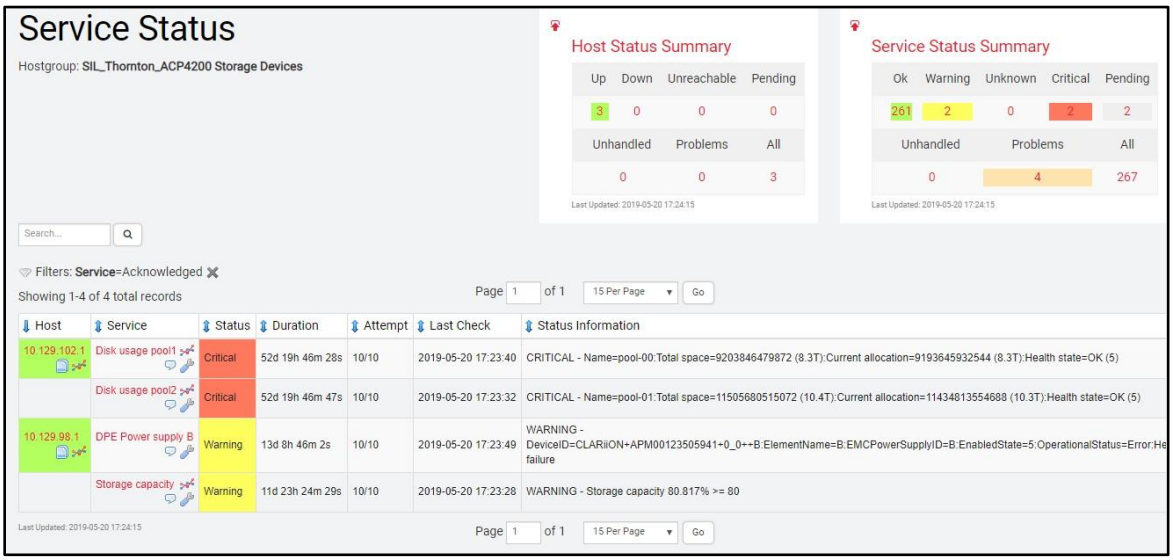
The following image shows that hovering over the acknowledge issues reveals the true state of the services in each category. In this example, there are still 2 critical and 2 warning type alarms for the Storage array. They have not yet been resolved and can still be viewed but are not flagged as red and amber alarms. Should a new warning or critical alarm arrive for the Storage area, the peg count in the warning or critical alarm area as well as the color change will grab the attention of those monitoring the solution.



Drilling down for information

Most elements in reports reveal information by hovering over fields and/or by drilling down into a specific area of concern.

In the following example, the Storage acknowledgement field was selected and clicked to drill down and view the details. The issues reported in the example represent the 2 critical and 2 warning alarms previously noted as being acknowledged.



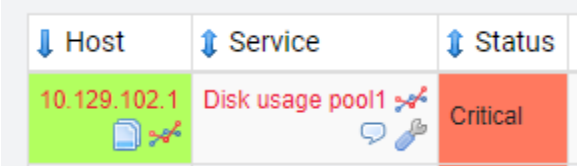
A closer look at the first item reveals icons communicating the other types of information available.

Under the Host column, the following icons are present:

- Stacked paper icon: To view the service status details.
- Graphical icon: To view the related performance graph for the associated host.[3]

Under the Service column, the following icons are present.

- Graphical icon: To view the related performance graph for the alarming service.
- Conversation bubble icon: Redirects you to the Service Status Detail page where there are acknowledgement comments noted.
- Wrench icon: This is present for all alarms that have been acknowledged (are being worked).

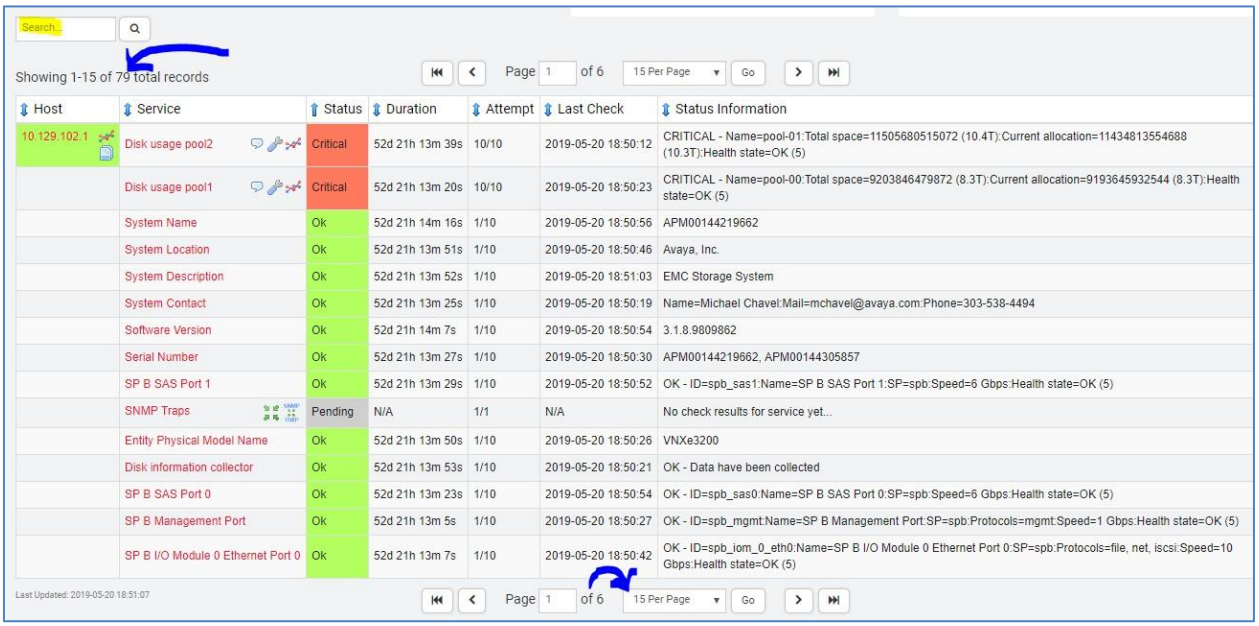


[3] Graphical representation is not often available for host elements.

Service Status icon 

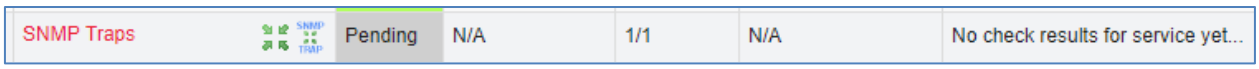
Drilling down into the paper stack displays the complete list of services associated with the host containing the services that are alarming, including those in a healthy state. This could provide needed insight into the source of a problem.

You may search for a specific service name for a specific sorted view or click on any of the blue arrows next to the column names for sorting according to that criteria. Verify the number of pages available and increase your view, as needed, at the bottom of each reporting page.



From this report, you may drill down into more specific view of each Service or Host item, or into the same type of icons as previously available on the upper-level form.

An important item to note on this form is the SNMP Traps item, located somewhere at the middle of the page.



The two icons associated with the SNMP Traps items are:

- Inbound 4-corners arrows: Passive check only, indicating the only way this item will alarm is if a service on the host sends a trap to AO.
- SNMP Trap: A link to drill down to Service Status Detail for SNMP traps.

With critical alarms present for services within this host, you might be curious as to why the SNMP trap

alarm is not reporting a critical or warning state, since the host should have sent an SNMP trap to AO in response to the state changes within the host.

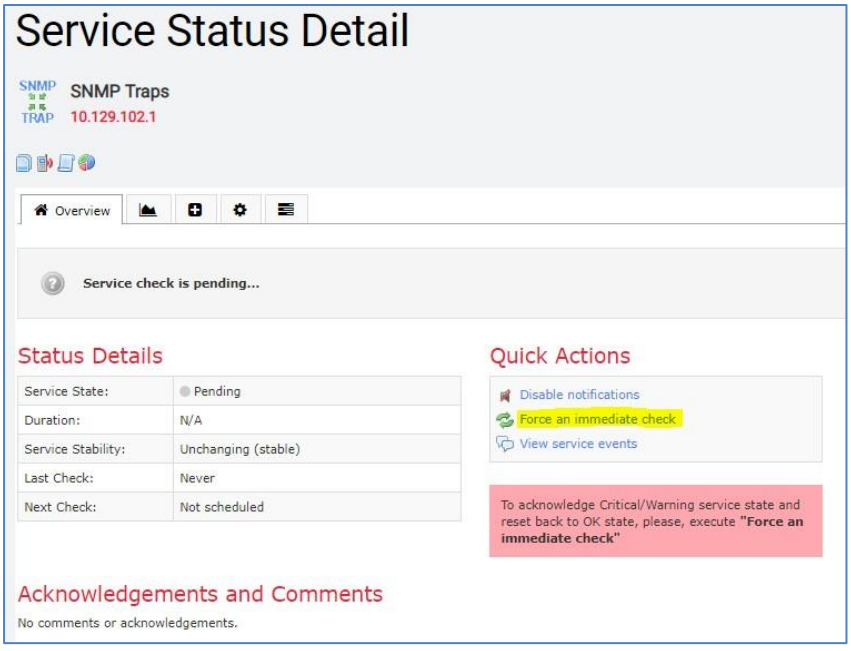
The current critical and warning alarms could also have been “learned” by AO through proactive monitoring. Still, SNMP should also be reporting an alarm state.

The reason this SNMP alarm is not reporting a critical or warning state is because it was reset to a “Pending” state, to await new SNMP trap information. It was cleared because the alarming state of the host was already reviewed and understood, each service alarm being “acknowledged” and cleared from the main solution view.

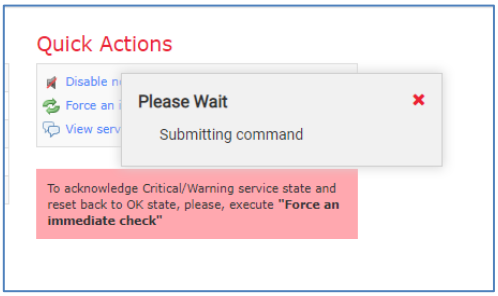
Important:
Clear the fields that are monitored after alarms are seen and understood.

After an alarm is acknowledged, AO clears the alarm status information from the main dashboard, creating a fresh view for new incoming alarms. You can perform the same kind of activity manually for the SNMP Trap element. After the SNMP alarm issues are recognized and are in the process of being resolved, you should clear the alarm field to identify new SNMP traps easily. Even if the issues are still open, they are tracked and monitored by proactive checks from AO.

To clear an SNMP Trap alarm, click on the SNMP Trap icon. You will be directed to the Service Status Detail page for SNMP Traps. The message in the red box instructs users how to reset the SNMP Trap field by selecting the **Force an immediate check** option in the **Quick Actions** area.



Clicking the **Force an immediate check** option, resets the SNMP Traps service field to a “Pending” state. When the next trap/alarm is sent to AO from the associated host, a state change will be reported.


Quick Actions
Please Wait
Submitting command
To acknowledge Critical/Warning service state and reset back to OK state, please, execute "Force an immediate check"

Chapter 17: Trap Forwarding

Overview

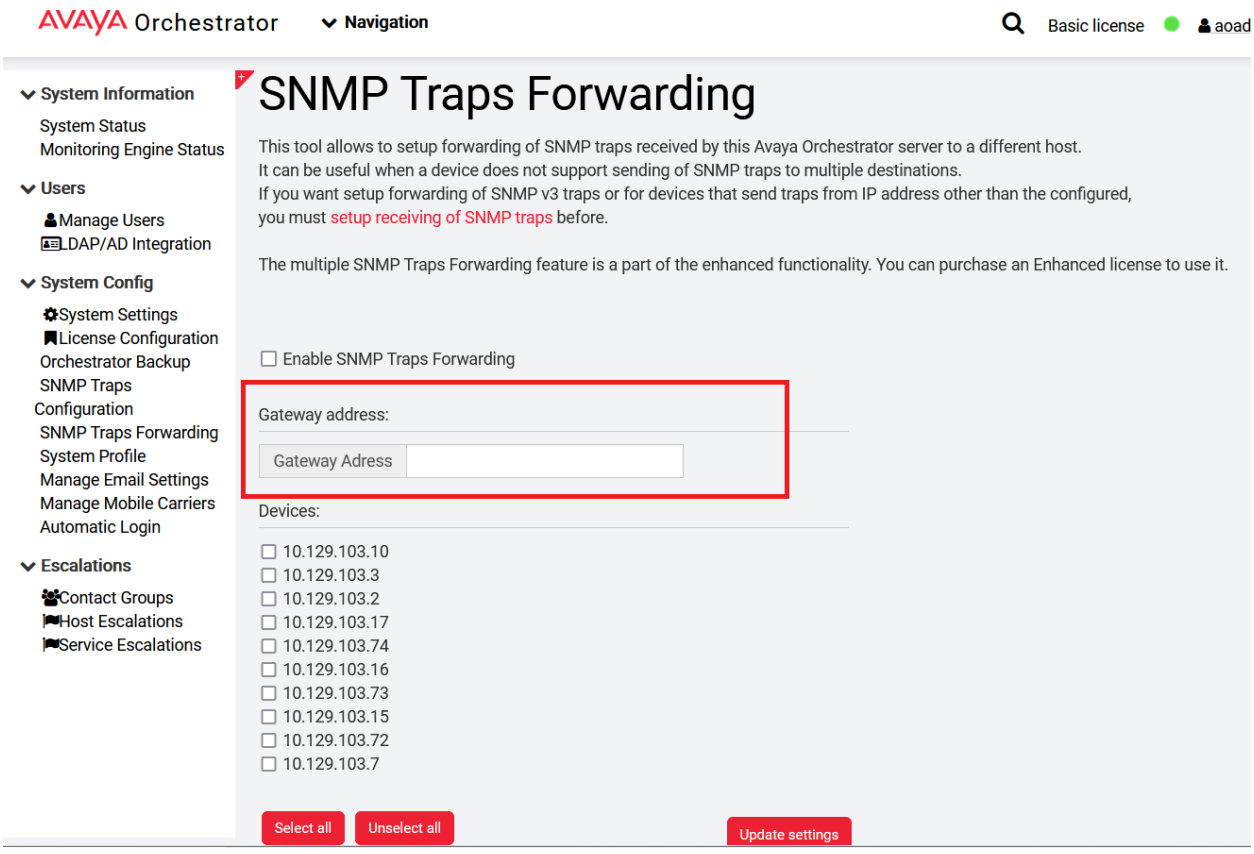
This chapter explains how to forward SNMP traps from Avaya Orchestrator™ to another trap receiver tool. Any SNMP alarm that is sent to AO from any administered device may be forwarded out from AO to another trap receiving device. When the information arrives, it will appear as if it is sent directly from the alarming device.

Menu Guidelines

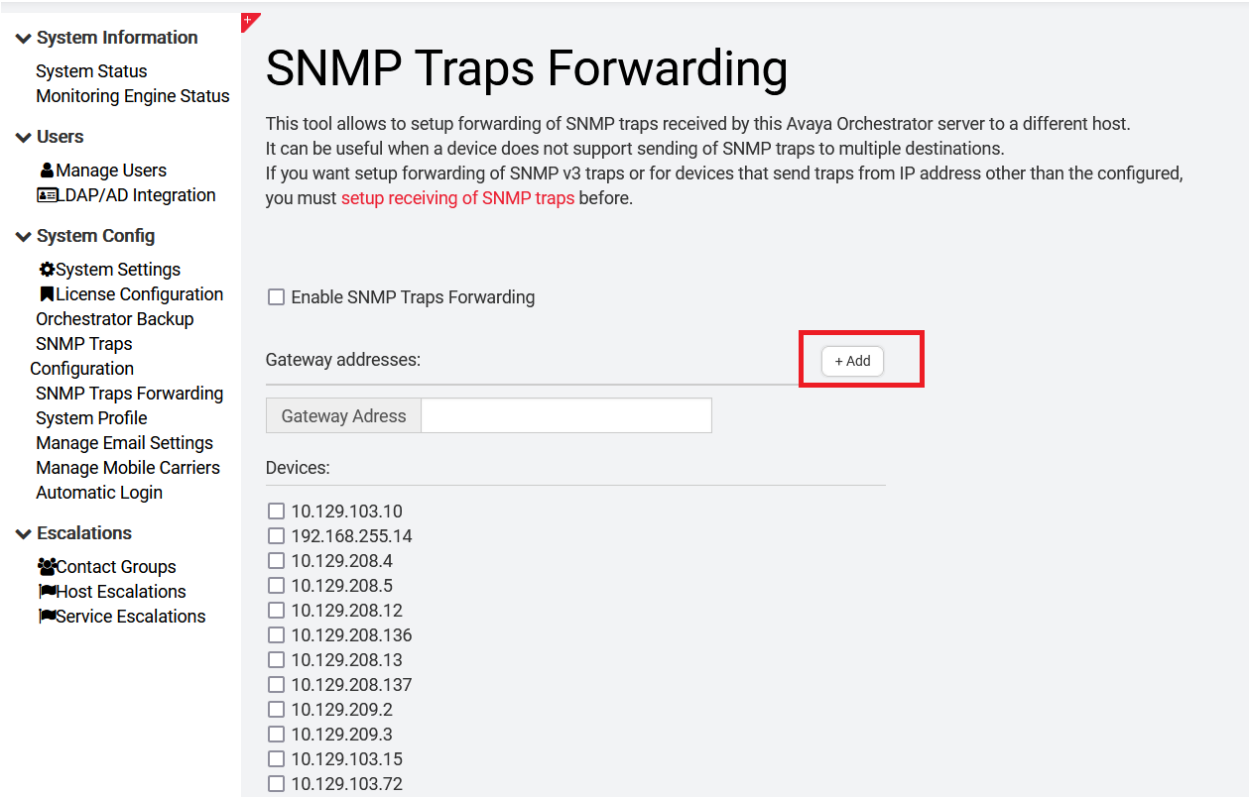
Note:

In Basic license single gateway is supported for trap forwarding.
In Enhanced License multiple gateways are supported for trap forwarding

Basic License



Enhance license:



Navigate to the Admin > System Config tabs and select **SNMP Trap Forwarding**.

On the subsequent pages, all devices that have been administered with an IP address in the ACP Configuration Wizard will be presented under the *Devices* listing.

Only those users with administrative privileges will have permission to configure this page.

Administration

Trap Receiver

Note: Only ONE far end trap receiver may be administered for trap forwarding.

It is important that the far end trap receiver must be administered with the same SNMP values configured in each device, just as Avaya Orchestrator™ has been administered to receive the SNMP trap information.

Once the far end trap receiver has been administered, enter the IP address for the target trap receiver in the field labeled *Gateway Address.*

Device Selection

Select the host devices that will have 100% of the “host” and “service” related warnings and critical alarms forwarded. The red *Select all* and *Unselect all* allow for rapid selection and disabling functionality.

Enabling Forwarding

When both the trap receiver gateway and the device selection have been administered/selected, click the red *Update Settings* button.

At this point, trap forwarding is configured but not yet enabled. To enable the forwarding activity to begin, click the *Enable SNMP Trap Forwarding* box and then select the *Update Settings* button to complete the process.

Chapter 18: Backup and restore

Backup configuration

This chapter contains information and procedures about how to back up the Avaya Orchestrator™ configuration.

Backups are an important aspect of administration and maintenance of your system. They can and should be automated for nightly archiving. If the alarm and maintenance data is critical to maintain, it is recommended that you store the backups at a location other than the AO server location.

The backup script saves the archived information in the `/store/backups/orchestrator/` directory. Backup names correspond to the `AO_backup_yyyy-mm-dd_hh-ii.tar.gz` pattern, where `yyyy-mm-dd_hh-ii` is the year, month, day, hour, and minute of the backup creation date and time.

The backup script:

- Gathers all data files into a temporary directory in `/store/backups/orchestrator/`.
- Creates the backup `.tar.gz` file after collecting all stored AO data.
- Deletes all the files previously collected, during the gathering process, after successfully creating the `.tar.gz` file.

Important:

Ensure that there is enough free disk space in `/store/backups/orchestrator/` for the data collection and processing activities. If not, the backup process fails and the server runs out of disk space. Lack of disk space can also cause other issues for the Avaya Orchestrator™ server.

There is 20 GB of capacity allocated for backup storage. A large and active application is projected to require approximately 420 MB of storage for seven days. The capacity available is sufficient for approximately one year of local storage for most customer solutions.

Note:

The backup script restarts the service at the beginning of the backup to ensure that the `retention.dat` file is up to date with the latest information. There is a slight interruption to the monitoring process when the restart occurs.

You can create and schedule backups by using the web interface.

Creating a backup by using the web interface

About this task

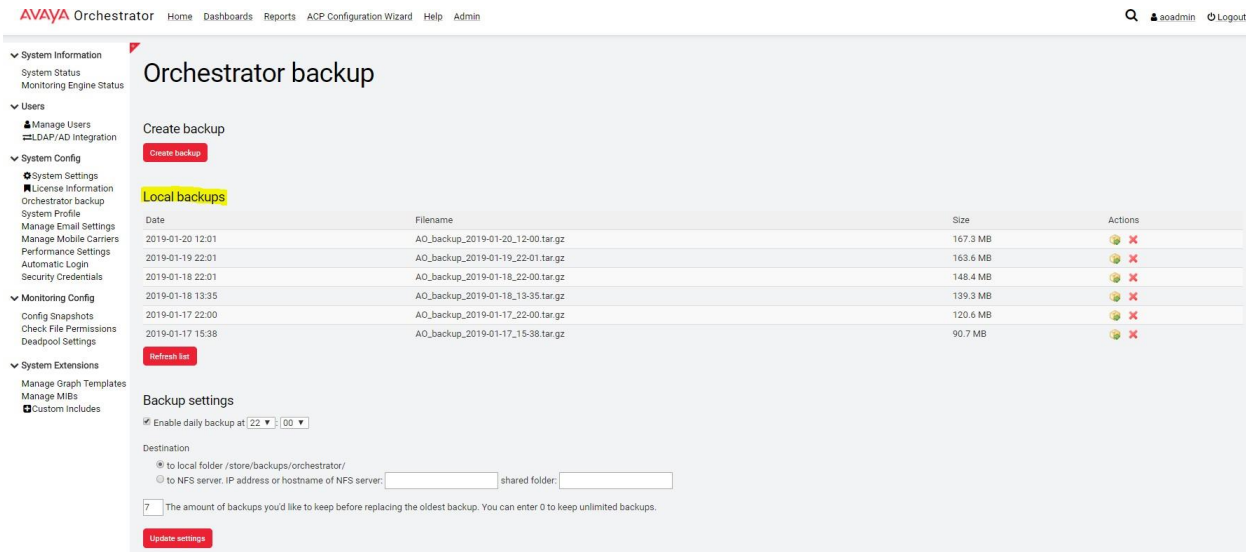
Use the following procedure to create a backup by using the Avaya Orchestrator™ web-based interface.

Procedure

1. Log on to Avaya Orchestrator™ by using administrative credentials.
2. Click **Admin**.
3. In the left navigation pane, click **System Config** > **Orchestrator backup**.
4. On the Orchestrator backup page, click **Create backup**.

Result

The new manually created backup file appears in *Local backups*.



Scheduling backups

Procedure

1. Log on to Avaya Orchestrator™ by using administrative credentials.
2. Click **Admin**.
3. In the left navigation pane, click **System Config** > **Orchestrator backup.**
4. On the Orchestrator backup page, navigate to the **Backup settings** area.
5. Select the **Enable daily backup at** check box and in the corresponding fields, click the hour and minute at which the daily backup must start.
6. Click **Update settings**.

Configuring backup retention

About this task

Use the following procedure to configure the retention of backup files.

Procedure

1. Log on to Avaya Orchestrator™ by using administrative credentials.
2. Click **Admin**.
3. In the left navigation pane, click **System Config** > **Orchestrator backup.**
4. On the Orchestrator backup page, navigate to the **Backup settings** area.
5. In **The amount of backups you'd like to keep before replacing the oldest backup. You can enter 0 to keep unlimited backups** field, type the number of backup files that you want to retain.

   The oldest backup file is deleted when the maximum number of backup files is reached.

6. Click **Update settings**.

Storing backup files

About this task

Avaya recommends that you store the configuration backups at a location other than the one located within the Avaya Converged Platform 4200 series SAN. Remote storage ensures that configuration backups are available in all failure circumstances.

You can configure Avaya Orchestrator™ to save the backup files to an NFS, FTP, or SFTP server storage.

Procedure

1. Log in to Avaya Orchestrator™ by using administrative credentials.
2. Click **Admin**.
3. In the left navigation pane, click **System Config** > **Orchestrator backup.**
4. On the Orchestrator backup page, navigate to the **Backup settings** area.
5. If you select to save the backup file to an NFS, FTP, or SFTP server storage, select the **Keep local backup copy** check box to save a local copy of the backup file in addition to saving it on the remote NFS, FTP, or SFTP server storage.
6. In **Destination**, do one of the following:
   - Click **Local folder** to save the backup files in the /store/backups/orchestrator/ folder, which is a locally allocated SAN storage of Avaya Orchestrator™.
   - Click **NFS server** and do the following:

a. In the **IP address or hostname** field, type the IP address or the hostname of the NFS server.

b. In the **Shared folder** field, type the shared folder name on the NFS server where you want to save the backup files. Be sure to prepend and append the location with the proper Linux or Windows / or \ markings. For example, a file location on a Linux server might be: /root/tftpbackup/AO/ao1/

- Click **FTP server** and do the following:

  a. In the **IP address or hostname** field, type the IP address or the hostname of the FTP server.

  b. In the **Remote folder** field, type the folder name on the NFS server where you want to save the backup files. Be sure to prepend and append the location with the proper Linux or Windows / or \ markings. For example, a file location on a Windows FTP server might be: \Downloads\backups\AO/ao1\

  c. In the **User name** field, type the user name to access the FTP server.

  d. In the **Password** field, type the password to access the FTP server.

  If the FTP server is anonymous, do not specify the user name and password.

- Click **SFTP server** and do the following:

  a. In the **IP address or hostname** field, type the IP address or the hostname of the SFTP server.

  b. In the **Remote folder** field, type the folder name on the SFTP server where you want to save the backup files. Be sure to prepend and append the location with the proper Linux or Windows / or \ markings. For example, a file location on a Linux SFTP server might be: /root/tftpbackup/AO/ao1/

  b. In the **User name** field, type the user name to access the SFTP server.

  c. In the **Password** field, type the password to access the SFTP server.

7. Click **Update settings**.

Downloading the backup files

About this task

Avaya Orchestrator™ supports downloading of configuration backup files so that you can move the backup files to a remote location or alternate storage medium.

Procedure

1. Log on to Avaya Orchestrator™ by using administrative credentials.
2. Click **Admin**.
3. In the left navigation pane, click **System Config** > **Orchestrator backup**.
4. On the Orchestrator backup page, navigate to the **Local backups** area.
5. Click the **Download** icon corresponding to the backup file that you want to download.

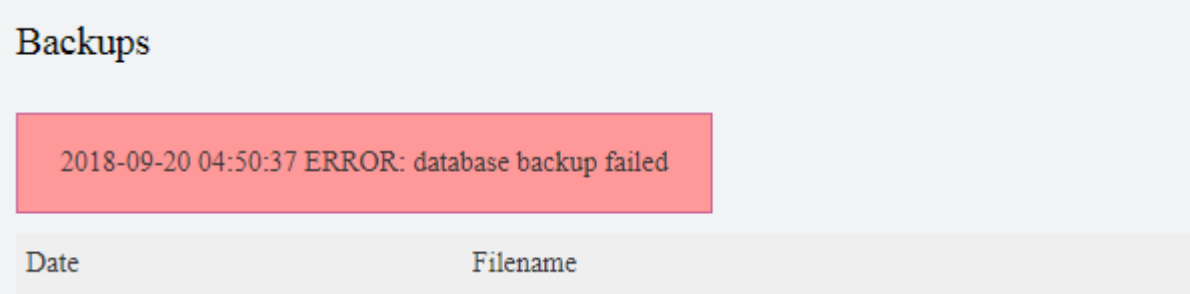
6. Move the backup file to a remote storage location or alternate storage medium. For example, the local computer.

Troubleshooting backups

The backup script writes high-level backup process information to the `/var/log/orchestrator/orchestrator_backup.log` log file.

An error message is displayed on the Backups page if an error occurred during the last backup. Click **Admin** > **Orchestrator backup** > **Backups** to navigate to the Backups page.

The following is an example of an error message:



Avaya Orchestrator™ system restore

You can perform an Avaya Orchestrator™ system restore by using the Avaya Orchestrator™ web GUI or by running the restore script at the Avaya Orchestrator™ CLI command prompt.

You can use the restore script or the Restore feature in the following scenarios:

- Restoring an Avaya Orchestrator™ VM that has experienced disk/storage issues and fails.
- Redeploying a VM after a failed upgrade. If the new feature behaviors are undesired, you can redeploy the previous AO OVA and restore the former translations.

In Avaya Orchestrator™ Release 1.5, restore functions are available only for exact matches between the software version of AO and the software version on the backup to be restored. For example, a backup of an AO application running load ABC can be restored only to an AO application running load ABC.

Important: The restore script and the Restore feature overwrite any existing configurations and data on the target server.

Restoring a backup file by using the Avaya Orchestrator™ CLI

Note:
Avaya recommends creating a VMware snapshot of the Avaya Orchestrator™ virtual machine before

proceeding. This provides a fallback to the earlier image in case the outcome of any restoration results in undesired product behaviors.

Procedure

1. Log in to Avaya Orchestrator™ by using SSH and *aoadmin* credentials.
2. At the aoadmin admin prompt $, type ***su – root***, and then type the root password.
3. To restore a local backup, do the following:
   a. At the root # prompt, type the following command:

      cd /store/backups/orchestrator

   b. In the backup directory, identify the file that you want to restore and note the file name.
   c. Move to Step 5.
4. To restore a backup from an external device, do the following:
   a. From the remote backup media location, copy the backup file that you want to restore into the `/tmp` directory in Avaya Orchestrator™.
   b. At the root # prompt, type the following command:

      cd /tmp

   c. Follow Step 5.
5. At the root prompt, type the following command:

   restore_orchestrator <AO backup file name>

   The following messages appear indicating the start and completion of the restoration process.

```
[root@ao4 tmp]# restore_orchestrator AO_backup_2019-01-22_19-00.tar.gz
Log file is /var/log/orchestrator/restore_orchestrator.log
Restoration is started.
Restoration is completed.
[root@ao4 tmp]#
```

   Contact the Avaya Services Support team in case you come across any problems during the restoration process.

Restoring a backup file by using the Avaya Orchestrator™ web GUI

Procedure

1. Log on to Avaya Orchestrator™ by using administrative credentials.
2. Click **Admin**.
3. In the left navigation pane, click **System Config** > **Orchestrator backup**.
4. On the Orchestrator backup page, navigate to the **Local backups** area.

5. Click the **Restore**  icon corresponding to the backup file that you want to restore.
   The restoration process takes a few minutes to complete. After the restoration process is complete, Avaya Orchestrator™ displays a message for restoration completion.

Export and Import ACP Configuration Wizard-Administration

One of the most critical and time consumptive aspects of restoration is the administration of all solution components in the AO Wizard. This administration can be easily and quickly restored through this functionality. Any exports of the Wizard Administration, from an Avaya Orchestrator™ 1.5 software load, can be imported on to any AO 1.5 software load. An exact match of load software is not necessary for this activity, as long as both AO and the export file data are based on the same AO release, that is, 1.5.

This functionality is most often used after a redeployment of AO. For example, part of the upgrade process. However, it can be applied to existing systems once the items needing to be refreshed or restored with the import data have been removed.

Exporting rack configuration

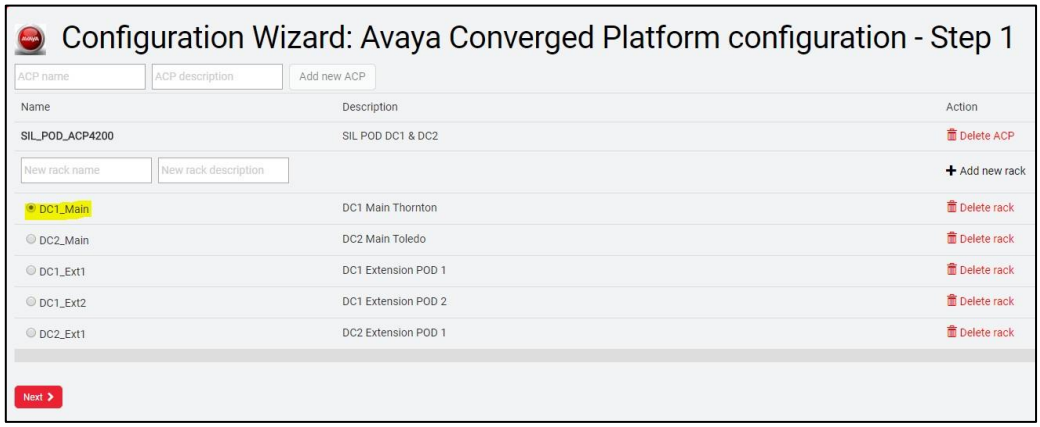
Note:

The import process will depend on you adding back the exact same racks, with the exact naming convention used during the export. At some point, before or after the export process, grab a screen capture of the list of racks and name so that you will be able to rebuild the prober base for the import files.

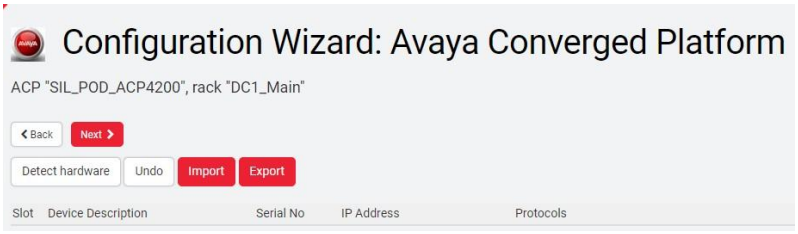
Procedure

1. Log on to the Avaya Orchestrator™ web interface by using administrative credentials, and then click **ACP Configuration Wizard**.

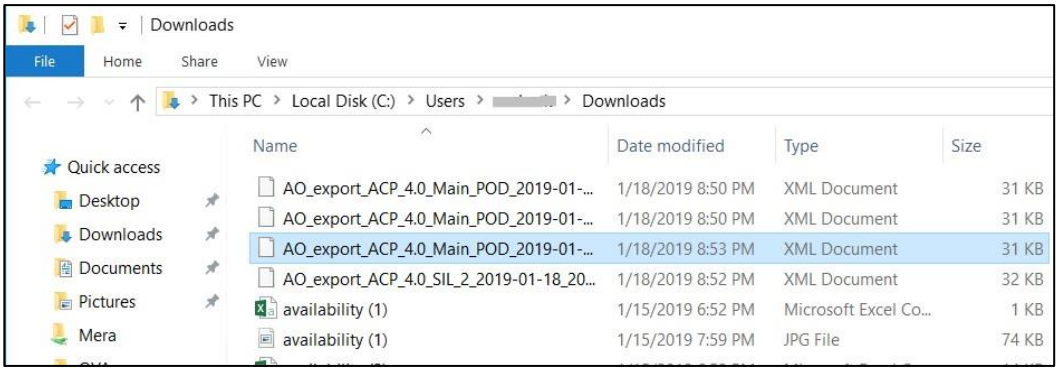
2. On the Configuration Wizard: Avaya Converged Platform configuration – Step 1 page, select a rack, and then click **Next**.



3. On the Configuration Wizard: Avaya Converged Platform configuration – Step 2 page, click **Export.**



The Export function creates a file for the rack translations in the `Downloads` directory of the local machine.



4. Export each rack information one at a time.
   When finished, you can keep these files on the local computer, or copy them to other media or storage locations.

Importing rack configuration

About this task

To import the configuration of a specific rack, the configuration of the rack must first exist.

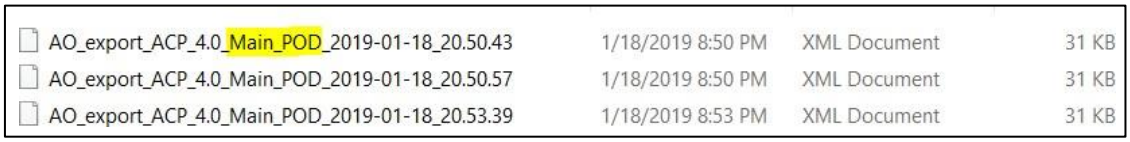
Note: The import process overwrites the configuration that is present in a rack. Using the screen capture previously taken, add the same racks, with the exact same rack names.

Procedure

1. Log on to the Avaya Orchestrator™ web interface by using administrative credentials, and then click **ACP Configuration Wizard**.

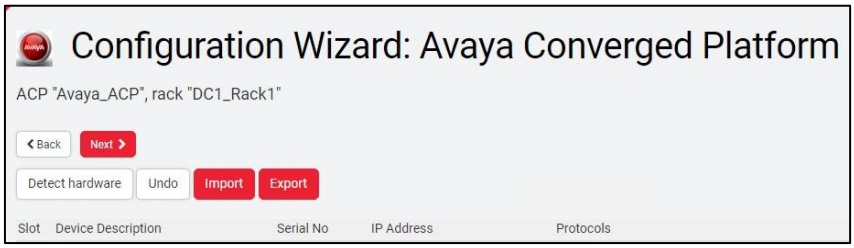
2. On the Configuration Wizard: Avaya Converged Platform configuration – Step 1 page, select a rack.

   Ensure that the name of the rack that you select is the same as that of the exported XML data file that you want to import.
   The following screen shot provides an example of the XML file names:



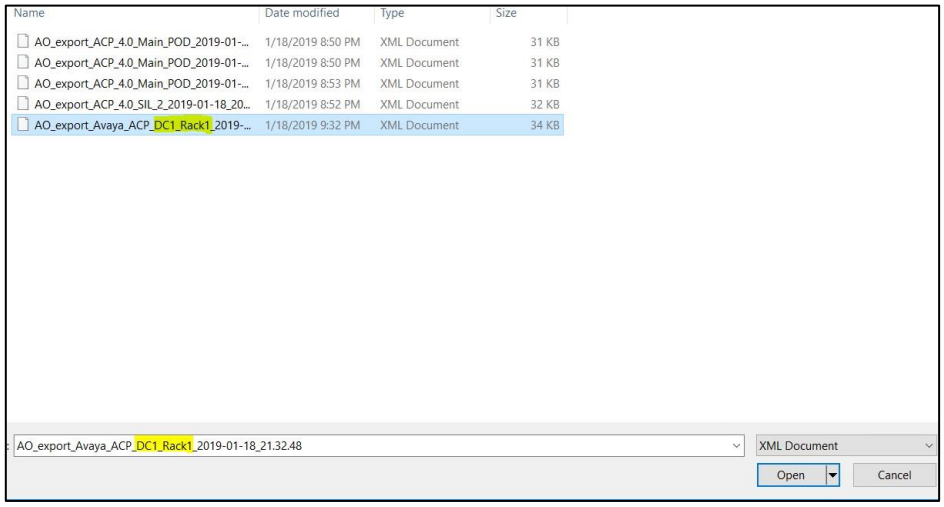
3. Click **Next**.

4. On the Configuration Wizard: Avaya Converged Platform configuration – Step 2 page, click **Import.**



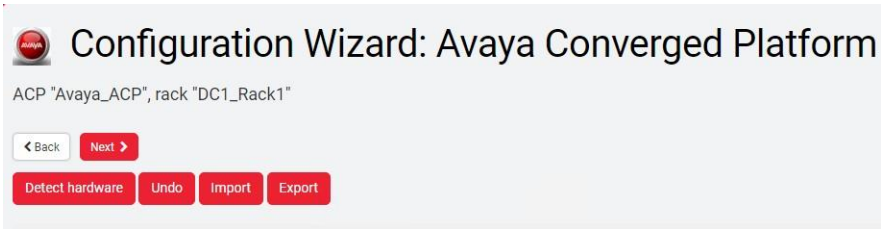
   The `Downloads` directory on the local device is displayed.

5. Browse to the file that you want to import, click the file, and then click **Open**.



The file is imported. Note that the **Detect Hardware** button is now red, indicating that the devices must be rediscovered.

6. Click **Detect Hardware**.



7. After hardware detection is complete, click **Next**.
8. Click **Finish** to complete the import and rediscovery process for the rack.
9. Repeat this procedure for all racks as needed.

Chapter 19: Upgrade and update Avaya Orchestrator™

Overview

This chapter provides information and procedures about how to upgrade and update Avaya Orchestrator™.

Important: Prior to beginning any upgrade, it is important to have a means of VM restoration should it be needed. Confirm a recent backup of the application has successfully completed. Another possible option would be a temporary vCenter snapshot of the VM; this could be held until the AO upgrade has been confirmed successful. AT that point, the snapshot should be removed immediately.

Verifying the installed version of Avaya Orchestrator™

1. Log in to Avaya Orchestrator™ by using SSH.
2. Run the following command to verify the version number of the currently installed Avaya Orchestrator™:

   `cat /orchestrator_version.txt`

   `1.4.`*`x.z.yymmddrr`*
   or
   `1.5.`*`x.z.yymmddrr`*

Upgrading Avaya Orchestrator™

Avaya Orchestrator upgrades to AO 1.5 B51 will now follow the below supported upgrade path:

Customers upgrading from Avaya Orchestrator **1.4** to **1.5 B51**

Initial Build	Intermedia Build	Upgrade to AO 1.5 Build 50	Upgrade to AO 1.5 Build 51
AO 1.4 Build **39** + Patch **43** (No Exceptions/Only supported Initial build)	AO 1.5 Build **46**	AO 1.5 B50	AO 1.5 B51

Important Note:

Customers with Avaya Orchestrator **1.4 must be** at the latest supported release, that is AO 1.4 build 39 + Patch 43 (**Version: 1.4.0.0.19081643**). If the current AO 1.4 is not at the expected release plan accordingly to have AO 1.4 at the required version prior to upgrading to AO 1.5 B51. Additionally, a **Three-step upgrade** procedure must be followed to get to AO 1.5 Build 51.

Customers upgrading from Avaya Orchestrator **1.5 Build <46, Two-step-upgrade** procedures 2 and 3 must be followed to get to AO 1.5 Build 51.

Initial Build	Intermedia Build	Upgrade to AO 1.5 Build 51
1.5 Build 33	AO 1.5 B50	AO 1.5 B51
1.5 Build 38	AO 1.5 B50	AO 1.5 B51
1.5 Build 45	AO 1.5 B50	AO 1.5 B51

Customers upgrading from Avaya Orchestrator **1.5 Build >45** (Follow only procedure 3)

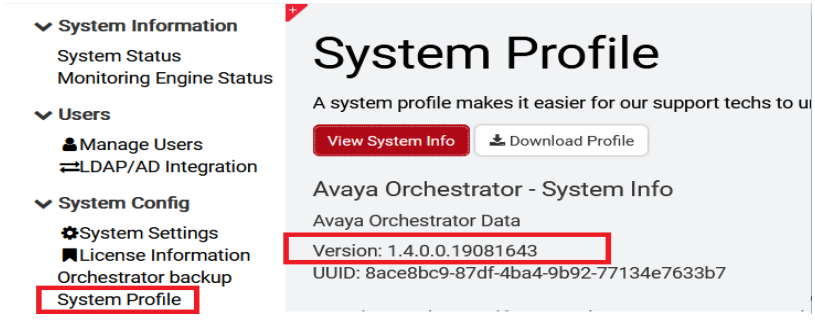
Initial Build	Upgrade to AO 1.5 Build 51
1.5 Build 46	Direct upgrade supported.
1.5 Build 47	Direct upgrade supported.
1.5 Build 50	Direct upgrade supported.

Upgrades to Avaya Orchestrator 1.5 Build 51

1. Avaya Orchestrator 1.4 upgrades to AO 1.5 Build 51

Important Note:

Customers with Avaya Orchestrator **1.4 must be** at the latest supported release, that is AO 1.4 build 39 + Patch 43 (**Version: 1.4.0.0.19081643**). If the current AO 1.4 is not at the expected release plan accordingly to have AO 1.4 at the required version prior to upgrading to AO 1.5 B51. Additionally, a Three-step upgrade procedure must be followed to get to AO 1.5 Build 51.



Warning: Avaya Orchestrator must be in a healthy state prior to attempting any upgrade. Resolve or acknowledge present alarms an ensure all expected hardware components are properly configured in the ASP 4200 rack. Also validate that proactive monitoring on every device works accordingly.

1.1. Step-up upgrade procedure from 1.4 build 39 + Patch 43 to 1.5 release build 51.

Note: The following upgrade path is the only method supported without exception. Step-up upgrades to a different AO build could leave the solution in an unsupported state and generate undesired upgrade failures.

1.1.1 Procedure to reset 1.4 build license.

Note: The Avaya Orchestrator internal license for release 1.4 has expired in March 2019. Customers that have not upgraded to AO 1.5 any build by March 2019 and later dates must reset the internal AO license prior to upgrading to AO 1.5 Build 46.

1.1.1.1 Start a remote desktop connection to the Management Server Console. Authenticate using the *administrator* credentials.

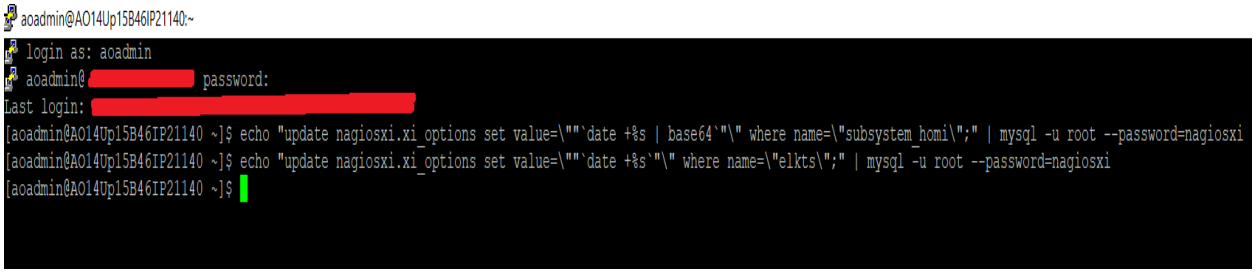
1.1.1.2 Using Putty, initiate an SSH session to Avaya Orchestrator™ and authenticate using the *aoadmin* credentials.

1.1.1.3 Run the following commands to reset the license on the Avaya Orchestrator 1.4 release.

Note: root access is not required

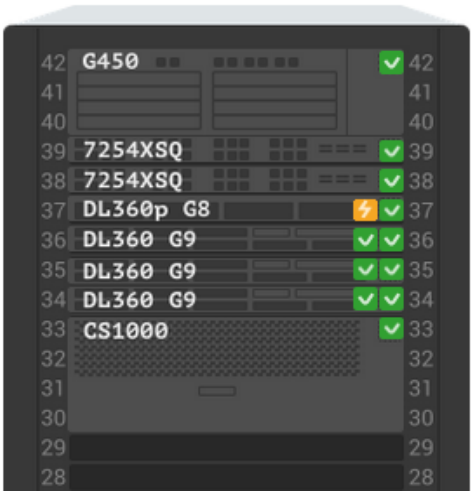
```
#  echo "update nagiosxi.xi_options set value=\""`date +%s | base64`"\" where name=\"subsystem_homi\";" | mysql -u root --password=nagiosxi

#  echo "update nagiosxi.xi_options set value=\""`date +%s`"\" where name=\"elkts\";" | mysql -u root --password=nagiosxi
```



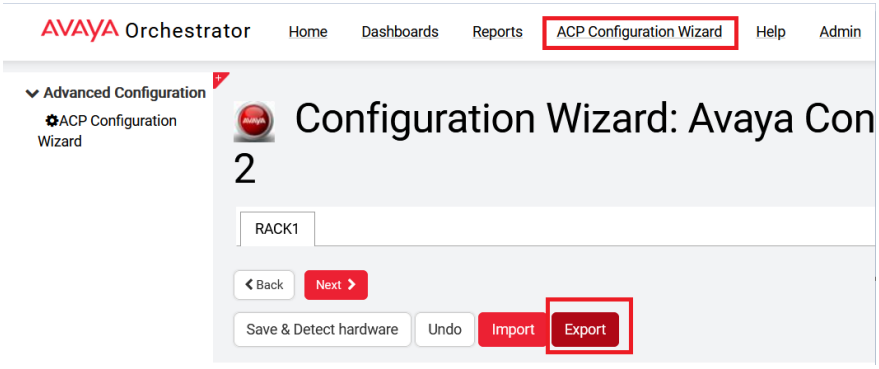
1.1.1.4 Open a Web browser and navigate to the Avaya Orchestrator GUI e.g., https://AO_ip_or_fqdn . Authenticate using the *orchestratoradmin* credentials.

1.1.1.5 Perform a health check of the system to ensure the configured data is intact.



Note: Based on the current hardware status in your POD, Avaya orchestrator might show different monitor status.

1.1.1.6 Import config wizard from Avaya orchestrator→ACP Configuration Wizard→ Select the Rack→Click Next→Click on Export button.



1.1.2 Upgrading from AO 1.4 build 39 + Patch 43 to AO 1.5 build 46

Warning: This is the only supported upgrade path. **DO NOT** attempt to upgrade to other 1.5 builds when at AO 1.4 as this will put the solution in an unsupported state. Any upgrade failures will not be handled by Avaya Support.

Prerequisite

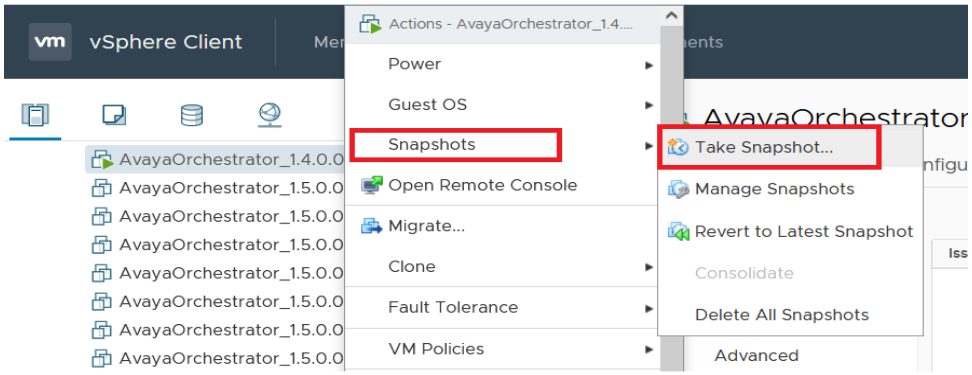
Download from PLDS the Avaya Orchestrator 1.5 build 46 ISO image. Transfer the ISO image to the Management Server console prior to the maintenance windows.

Procedure

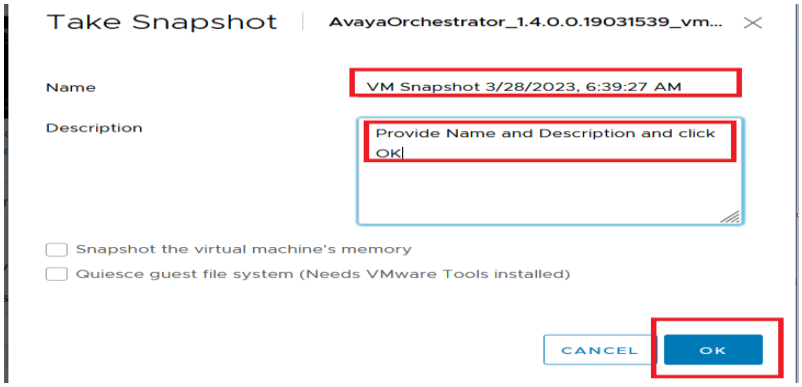
1.1.2.1 Start a remote desktop connection to the Management Server Console. Authenticate using the *administrator* credentials.

1.1.2.2 Open a new browser tab and navigate to the vCenter Server Web client e.g., https://vCenter_ip_or_fqdn. Authenticate using the administrator@vsphere.local credentials.

1.1.2.3 From the Hosts and Clusters view, locate the Avaya Orchestrator VM ➔ Right Click ➔ Snapshots➔ Take a snapshot.



1.1.2.4 Provide Name and Description and click Create.



1.1.2.5 Connection to vCenter can be closed.

1.1.2.6 Using Putty, initiate an SSH session to Avaya Orchestrator™ and authenticate using the *aoadmin* credentials.

1.1.2.7 Run the following command to escalate to root:

su – root

Enter root password.

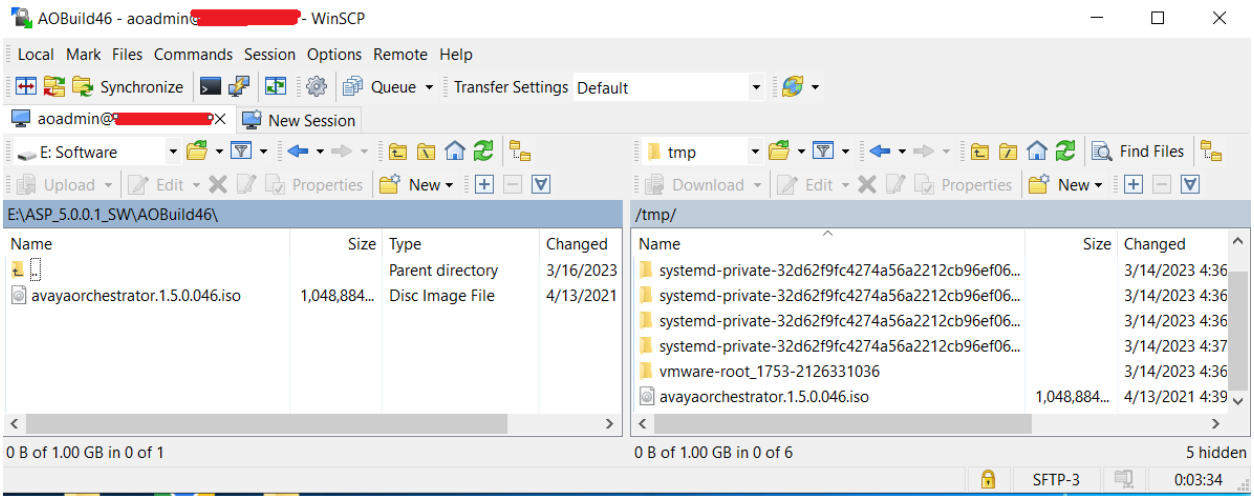
1.1.2.8 Run the following command to remove other versions of the Avaya Orchestrator™ ISO image fromthe /tmp/ folder:

```
# rm -f /tmp/avayaorchestrator.*.iso
```

1.1.2.9 Leave the Putty session a side and Open WinSCP.

1.1.2.10 Initiate a SCP session to Avaya Orchestrator and authenticate using the *aoadmin* credentials.

1.1.2.11 Transfer the previously downloaded Avaya Orchestrator™ 1.5 build 46 ISO image to the /tmpfolder on the Avaya Orchestrator™host.



1.1.2.12 WinSCP session can be closed.

1.1.2.13 Return to the SSH session opened in previous steps to Avaya Orchestrator.

1.1.2.14 Run the following command to create the mount folder:

```
# mkdir -p /tmp/iso
```

1.1.2.15 Run the following command to mount the uploaded Avaya Orchestrator™ ISO image:

```
# mount -t iso9660 -o loop,ro /tmp/avayaorchestrator.1.5.0.046.iso  /tmp/iso
```

1.1.2.16 Run the following command to create the repository definition file:

```
# echo -e "[AO]\nname=AO\nbaseurl=file:///tmp/iso\ngpgcheck=0\nenabled=1" >
/etc/yum.repos.d/ao.repo
```

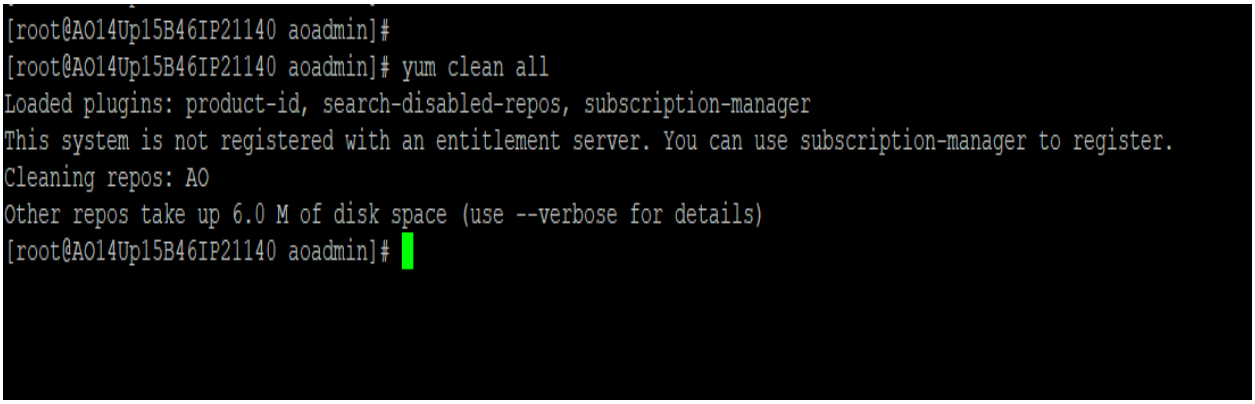


1.1.2.17 Run the following command to clean up the repository:

yum clean all

The following messages appear:

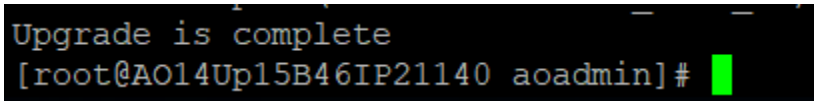
```
This system is not registered ...
Cleaning repos: ...
```



1.1.2.18 Run the following command to upgrade Avaya Orchestrator™ from version 1.4 to version 1.5:

/tmp/iso/upgrade_from_1_to_2.sh

Note: **DO NOT** kill the upgrade process even if there is no visible progress being displayed as in some cases it can take up to 30-40 minutes for the upgrade script to complete. An '`Upgrade is Complete`' message is exhibited once the upgrade process from AO 1.4 B39 + Patch 43 to AO 1.5 B46 is successfully completed.



1.1.2.19 Run the following command to remove the repository definition file:

```
# rm -f /etc/yum.repos.d/ao.repo
```

1.1.2.20 Run the following command to unmount the ISO image:

```
# umount /tmp/iso
```

1.1.2.21 Run the following command to remove the ISO image:

```
# rm -f /tmp/avayaorchestrator.*.iso
```

1.1.2.22 Restart the Avaya Orchestrator™ host:

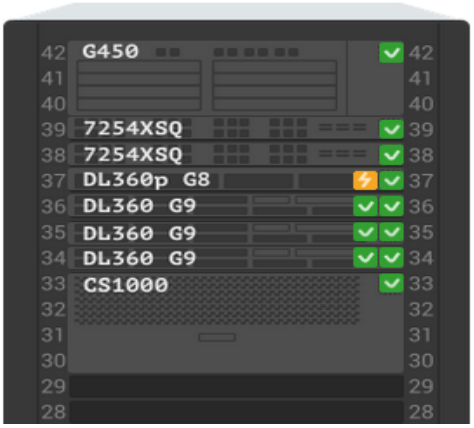
```
# reboot
```

1.1.3 Validating Avaya orchestrator health after upgrade

1.1.3.1 Before accessing the Avaya Orchestrator Web UI, clear the browser cache and history from every browser used in the past.

1.1.3.2 Open a browser and navigate to the Avaya Orchestrator GUI e.g., https://AO_ip_or_fqdn . Authenticate using the *aoadmin* credentials.

1.1.3.3 Perform a health check of the system to ensure the configured data is intact.



Note: Based on the current hardware status with the ASP 4200 rack, Avaya orchestrator might show a different monitor status.

2. Upgrades to Avaya Orchestrator 1.5 Build 50.

Prerequisite

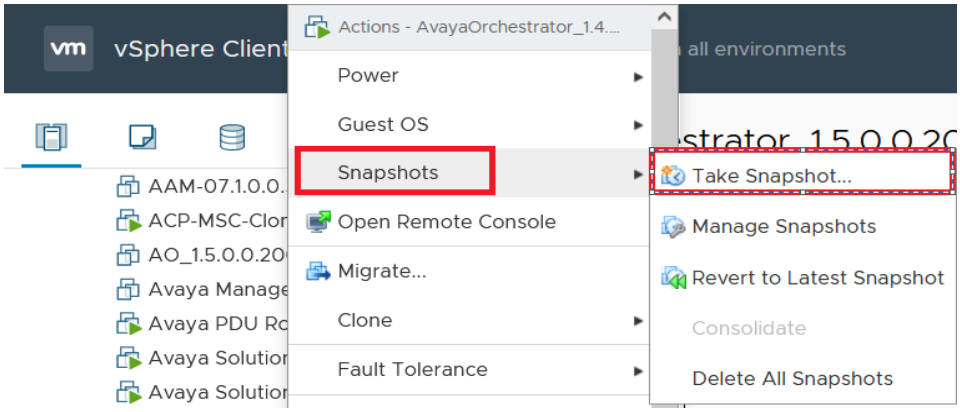
Download from PLDS the Avaya Orchestrator 1.5 build 50 ISO image. Transfer ISO image to the Management Server console prior to the maintenance windows.

Procedure

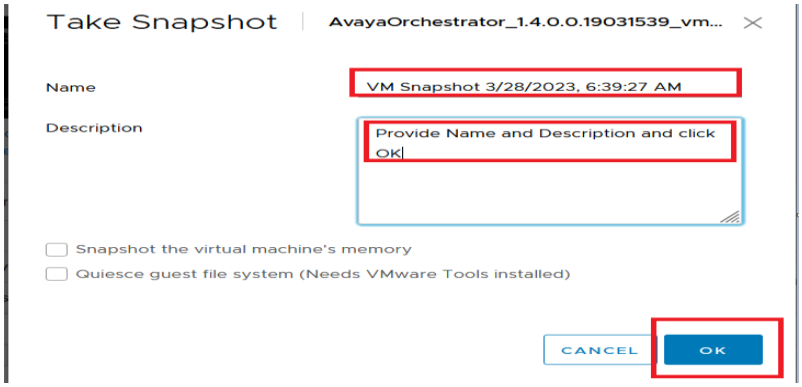
2.1 Start a remote desktop connection to the Management Server Console. Authenticate using the *administrator* credentials.

2.2 Open a new browser tab and navigate to the vCenter Server Web client e.g., https://vCenter_ip_or_fqd/ui. Authenticate using the administrator@vsphere.local credentials.

2.3 From the Hosts and Clusters view, locate the Avaya Orchestrator VM→ Right Click→ Snapshots→ Take a snapshot.



2.4 Provide Name and Description and click Create.



2.5 Connection to vCenter can be closed.

2.6 Using Putty, initiate an SSH session to Avaya Orchestrator™ and authenticate using the *aoadmin* credentials.

2.7 Run the following command to escalate to root:

su – root

Enter root password.

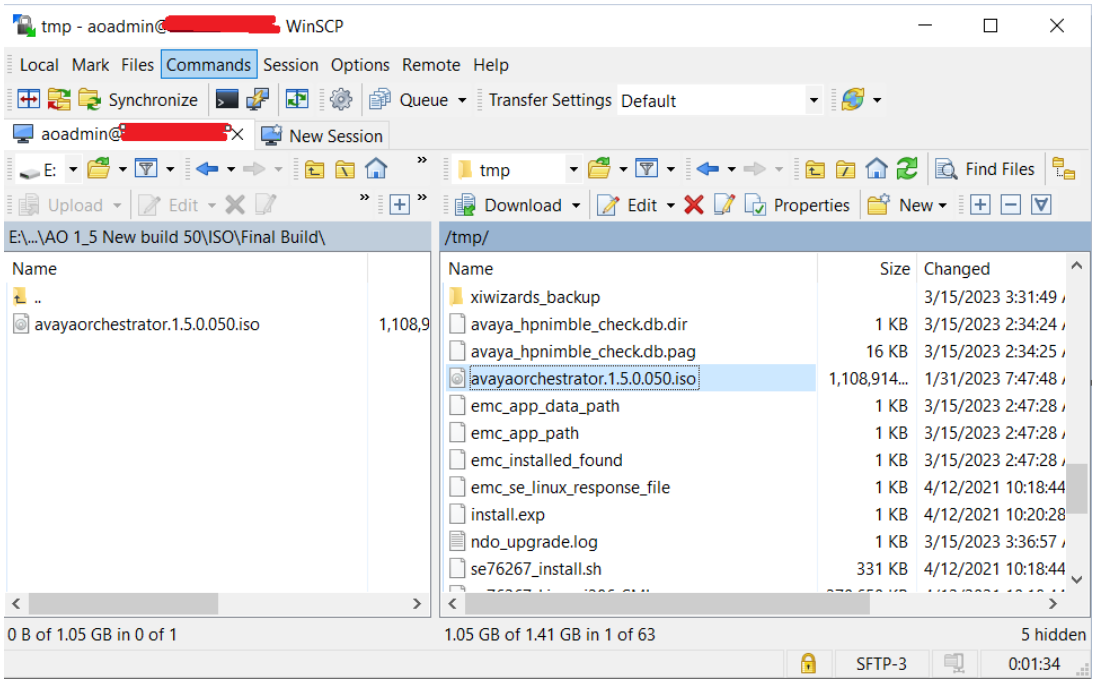
2.8 Run the following command to remove other versions of the Avaya Orchestrator™ ISO image fromthe /tmp/ folder:

- **`# rm -f /tmp/avayaorchestrator.*.iso`**

2.9 Leave Putty session a side and Open WinSCP.

2.10 Initiate a SCP session to Avaya Orchestrator and authenticate using the *aoadmin* credentials.

2.11 Transfer the previously downloaded Avaya Orchestrator™ 1.5 build 50 ISO image to the /tmpfolder on the Avaya Orchestrator™host. Confirm the file name ends with *.iso* and not *.vmx*. The *.iso* is used for upgrades and the *.vmx* file is an OVA used for fresh deployments.



2.12 WinSCP session can be closed.
2.13 Return to the SSH session opened in previous steps to Avaya Orchestrator.

2.14 Run the following command to create the mount folder:

```
# mkdir -p /tmp/iso
```

2.15 Run the following command to mount the uploaded Avaya Orchestrator™ ISO image:

- `# mount -t iso9660 -o loop,ro /tmp/avayaorchestrator.1.5.0.050.iso /tmp/iso`

2.16 Run the following command to create the repository definition file:

- `# echo -e "[AO]\nname=AO\nbaseurl=file:///tmp/iso\ngpgcheck=0\nenabled=1" > /etc/yum.repos.d/ao.repo`

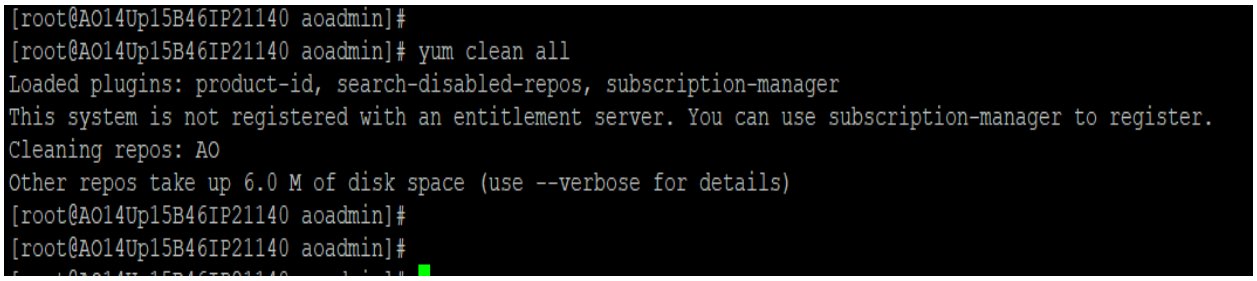


2.17 Run the following command to clean up the repository:

```
# yum clean all
```

The following messages appear:

```
This system is not registered ...
Cleaning repos: ...
```



2.18 Run the following command to update the currently installed Avaya Orchestrator™:

```
# bash /tmp/iso/ao_yum_upgrade.sh
```

Note: **DO NOT** kill the upgrade process even if there is no visible progress being displayed as in some cases it can take up to 30-40 minutes for the upgrade script to complete depending on the version getting upgraded. The following message is displayed after the upgrade is successfully completed from AO 1.5 build x to AO 1.5 build 50:

```
Complete!
Avaya Orchestrator upgrade is completed with no errors
```

When upgrading from AO 1.5 build x to AO 1.5 build 50 the following message is expected and can be ignored:

```
Failed:
python-urllib3.noarch 0:1.10.27.el7
Complete!
Avaya Orchestrator upgrade is completed with no errors
```



2.19 Run the following command to remove the repository definition file:

rm -f /etc/yum.repos.d/ao.repo

2.20 Run the following command to unmount the ISO image:

umount /tmp/iso

2.21 Run the following command to remove the ISO image:

rm -f /tmp/avayaorchestrator.*.iso

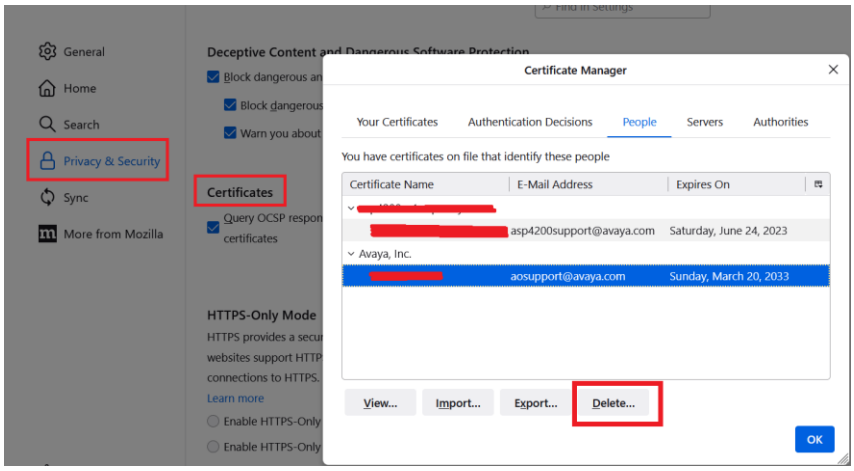
2.22 Restart the Avaya Orchestrator™ host:

reboot

2.2. Validating Avaya orchestrator health after upgrade.

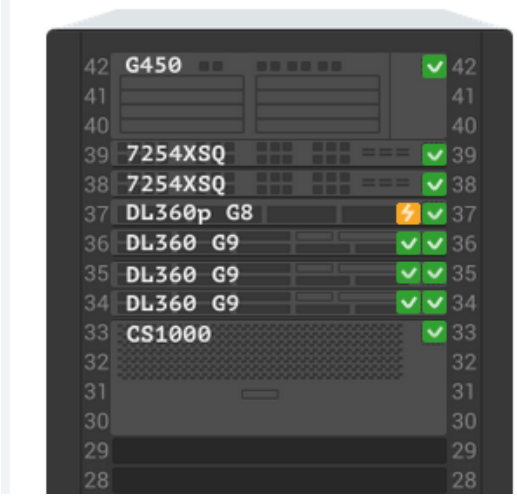
2.2.1 Before accessing the Avaya Orchestrator Web UI, clear the browser cache, history

from every browser and old certificates used in the past.



2.2.2 Open a web browser and navigate to the Avaya Orchestrator GUI e.g., https://AO_ip_or_fqdn . Authenticate using the *aoadmin* credentials.

2.2.3 Perform a health check of the system to ensure the configured data is intact.



Note: Based on the current hardware status in the ASP 4200 rack, Avaya orchestrator might show a different monitor status.

3. Upgrades to Avaya Orchestrator 1.5 Build 51.

Prerequisite

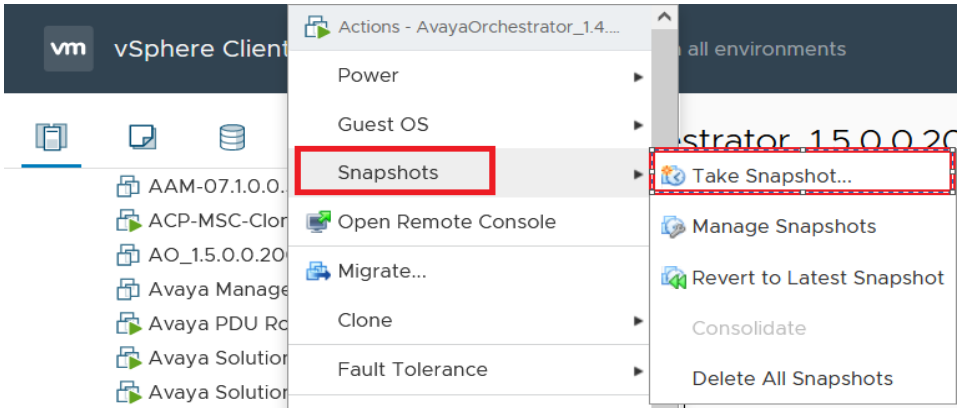
Download from PLDS the Avaya Orchestrator 1.5 build 51 ISO image. Transfer ISO image to the Management Server console prior to the maintenance windows.

Procedure

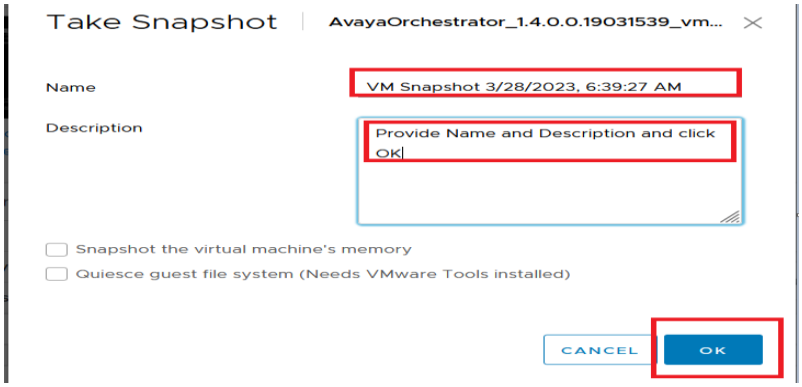
3.1 Start a remote desktop connection to the Management Server Console. Authenticate using the *administrator* credentials.

3.2 Open a new browser tab and navigate to the vCenter Server Web client e.g., https://vCenter_ip_or_fqd/ui. Authenticate using the administrator@vsphere.local credentials.

3.3 From the Hosts and Clusters view, locate the Avaya Orchestrator VM→ Right Click→ Snapshots→ Take a snapshot.



3.4 Provide Name and Description and click Create.



3.5 Connection to vCenter can be closed.

3.6 Using Putty, initiate an SSH session to Avaya Orchestrator™ and authenticate using the *aoadmin* credentials.

3.7 Run the following command to escalate to root:

```
# su – root

# Enter root password.
```

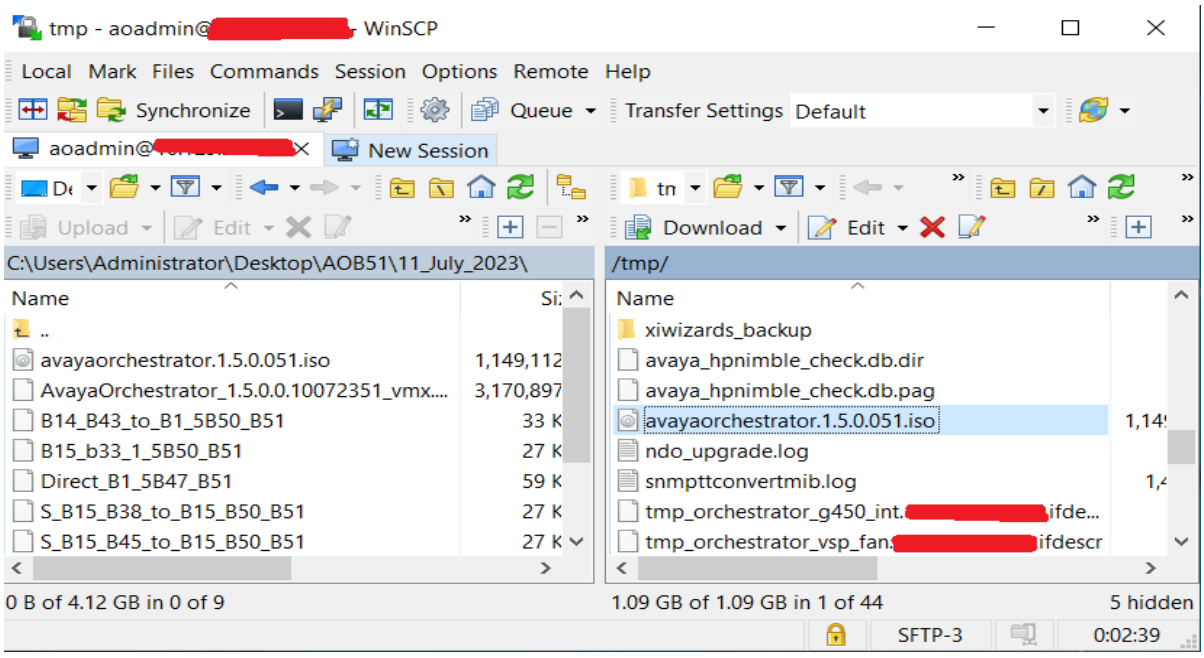
3.8 Run the following command to remove other versions of the Avaya Orchestrator™ ISO image fromthe /tmp/ folder:

- **`# rm -f /tmp/avayaorchestrator.*.iso`**

3.9 Leave Putty session a side and Open WinSCP.

3.10 Initiate a SCP session to Avaya Orchestrator and authenticate using the *aoadmin* credentials.

3.11 Transfer the previously downloaded Avaya Orchestrator™ 1.5 build 51 ISO image to the /tmpfolder on the Avaya Orchestrator™host. Confirm the file name ends with *.iso* and not *.vmx*. The *.iso* is used for upgrades and the *.vmx* file is an OVA used for fresh deployments.



3.12 WinSCP session can be closed.
3.13 Return to the SSH session opened in previous steps to Avaya Orchestrator.
3.14 Run the following command to create the mount folder:

```
# mkdir -p /tmp/iso
```

3.15 Run the following command to mount the uploaded Avaya Orchestrator™ ISO image:

- **# mount -t iso9660 -o loop,ro /tmp/avayaorchestrator.1.5.0.051.iso /tmp/iso**

3.16 Run the following command to create the repository definition file:

- **# echo -e "[AO]\nname=AO\nbaseurl=file:///tmp/iso\ngpgcheck=0\nenabled=1" > /etc/yum.repos.d/ao.repo**

```
[root@AO14Up15B46IP21140 aoadmin]#
[root@AO14Up15B46IP21140 aoadmin]# mkdir -p /tmp/iso
[root@AO14Up15B46IP21140 aoadmin]#
[root@AO14Up15B46IP21140 aoadmin]#
[root@AO14Up15B46IP21140 aoadmin]#  mount -t iso9660 -o loop,ro /tmp/avayaorchestrator.1.5.0.051.iso /tmp/iso
[root@AO14Up15B46IP21140 aoadmin]#
[root@AO14Up15B46IP21140 aoadmin]# echo -e "[AO]\nname=AO\nbaseurl=file:///tmp/iso\ngpgcheck=0\nenabled=1"> /etc/yum.repos.d/ao.repo
[root@AO14Up15B46IP21140 aoadmin]#
[root@AO14Up15B46IP21140 aoadmin]#
```

3.17 Run the following command to clean up the repository:

yum clean all

The following messages appear:

```
This system is not registered ...
Cleaning repos: ...
```

```
[root@AO14Up15B46IP21140 aoadmin]#
[root@AO14Up15B46IP21140 aoadmin]# yum clean all
Loaded plugins: product-id, search-disabled-repos, subscription-manager
This system is not registered with an entitlement server. You can use subscription-manager to register.
Cleaning repos: AO
Other repos take up 6.0 M of disk space (use --verbose for details)
[root@AO14Up15B46IP21140 aoadmin]#
[root@AO14Up15B46IP21140 aoadmin]#
```

3.18 Run the following command to update the currently installed Avaya Orchestrator™:

bash /tmp/iso/ao_yum_upgrade.sh

Note: **DO NOT** kill the upgrade process even if there is no visible progress being displayed as in some cases it can take up to 30-40 minutes for the upgrade script to complete depending on the version getting upgraded. The following message is displayed after the upgrade is successfully completed from AO 1.5 build x to AO 1.5 build 51

```
Replaced:
     python-pymssql.x86_64 0:2.1.1-1.el7   python-simplejson.x86_64 0:3.3.3-1.el7

Complete!

     Avaya Orchestrator upgrade is completed with no errors
```

3.19 Run the following command to remove the repository definition file:

```
# rm -f /etc/yum.repos.d/ao.repo
```

3.20 Run the following command to unmount the ISO image:

```
# umount /tmp/iso
```

3.21 Run the following command to remove the ISO image:

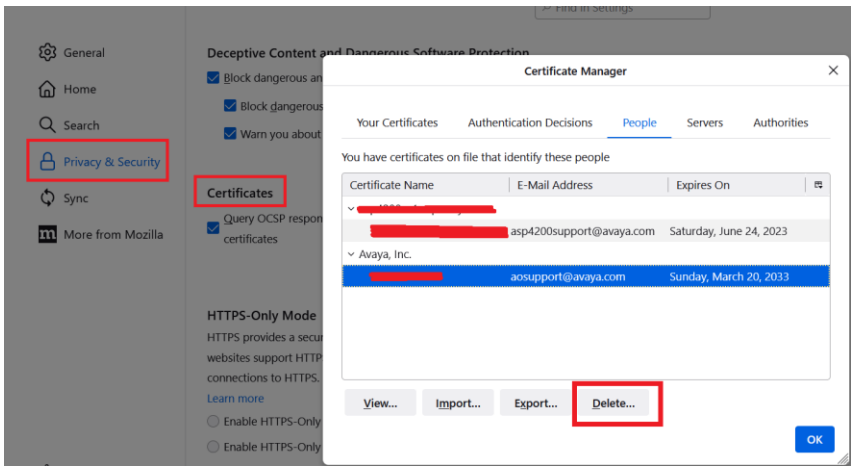
```
# rm -f /tmp/avayaorchestrator.*.iso
```

3.22 Restart the Avaya Orchestrator™ host:

```
# reboot
```

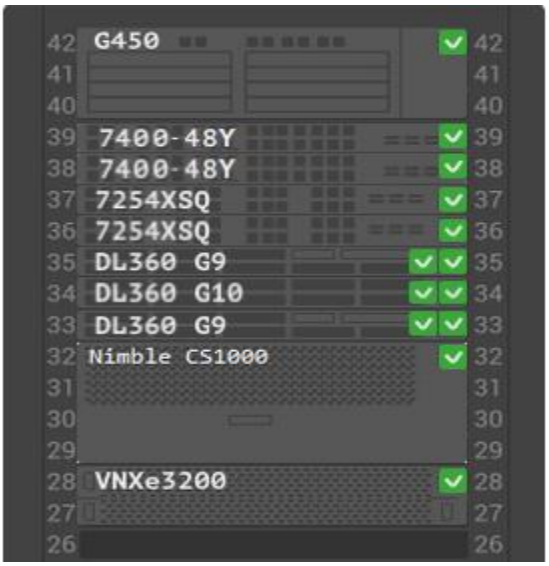
3.2 Validating Avaya orchestrator health after upgrade.

3.2.1 Before accessing the Avaya Orchestrator Web UI, clear the browser cache, history from every browser and old certificates used in the past.



3.2.2 Open a web browser and navigate to the Avaya Orchestrator GUI e.g., https://AO_ip_or_fqdn . Authenticate using the *aoadmin* credentials.

3.2.3 Perform a health check of the system to ensure the configured data is intact.

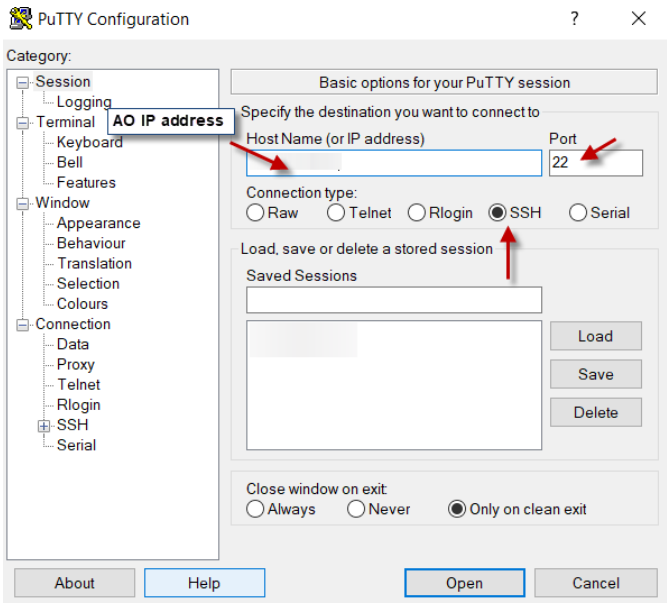


Note: Based on the current hardware status in the ASP 4200 rack, Avaya orchestrator might show a different monitor status.

Chapter 20: Altering Trap Severity

The procedure written below explains altering SNMP trap severity levels in Avaya Orchestrator.

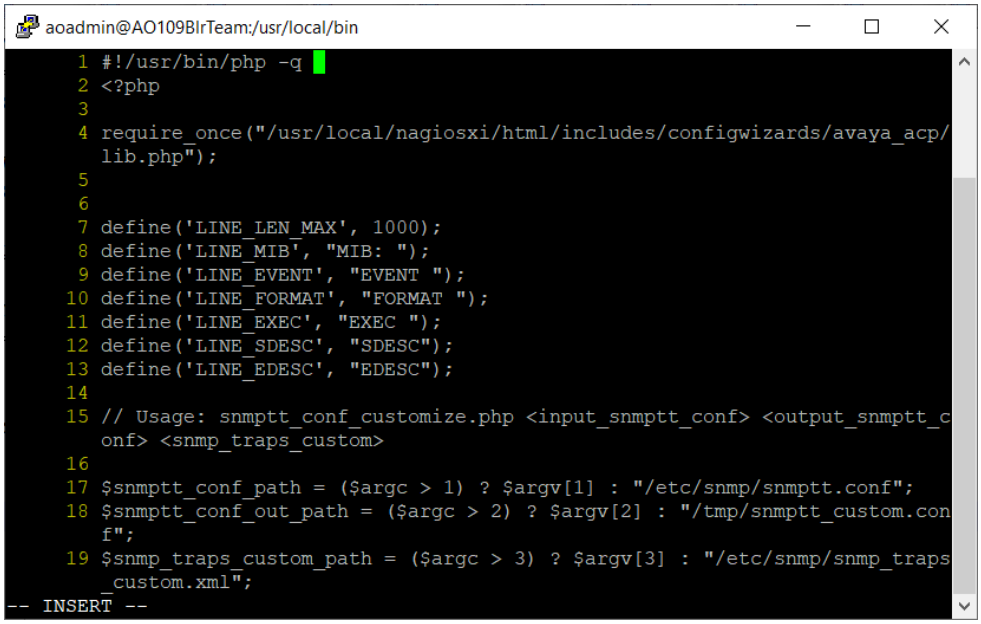
1. Log into the MSC and open Putty to start an SSH session with Avaya Orchestrator.
   Note: Refer to *Customer Lifecycle Workbook* for MSC and AO login details.



2. Log into AO via SSH with the **aoadmin** user credentials.
3. Change the user to **root** by typing the **su** command and provide the root password when prompted.
4. Capture the OID information of the trap for the appropriate ASP 4200 component from the Events and Alert Messages chapter.
5. Take backup of the **snmp_traps_custom.xml** file before editing it using the following command:
   cp *<u>/etc/snmp/snmp_traps_custom.xml</u> /etc/snmp/snmp_traps_custom.old*
6. Edit the **snmp_traps_custom.xml** file using the command shown below.
   vi /etc/snmp/snmp_traps_custom.xml
7. Press Insert button on the keyboard.
8. To modify the severity level of an existing OID, scroll through the **snmp_traps_custom.xml** file and find a section where the OID is listed.
   The syntax of a trap section is shown below:
   <trap_custom>
   <oid>OID_String</oid>
   <severity>Severity_level</severity>
   </trap_custom>
   Note: The following severity levels are available in AO. Only choose one of the following severity levels while altering the severity level of a trap.
   - **INFORMATIONAL**

- **NORMAL**
- **SEVERE**
- **MAJOR**
- **CRITICAL**
- **WARNING**
- **MINOR**

9. Change the severity level to the desired level as per the note above.
   An example of a trap section is shown below:
   <trap_custom>
   <oid>.1.3.6.1.4.1.37447.2.1.2.14401</oid>
   <severity>CRITICAL</severity>
   </trap_custom>
10. Press ESC key, type **wq!** and press Enter to save the changes.
11. Change directory using the command **cd /usr/local/bin/**
12. Take backup of the **snmptt_conf_customize.php** file before editing it using the following command:
    cp *snmptt_conf_customize.php snmptt_conf_customize.old*
13. Edit the **snmptt_conf_customize.php** file located in the bin directory using the following command:
    vi snmptt_conf_customize.php
14. Press Insert button on the keyboard.
15. As shown in the screenshot below, add **#!/usr/bin/php -q** as the first line in the file.



16. Press ESC key, type **wq!** and press Enter to save the changes.
17. The command format shown below is an example of executing a standard php file:
    ./snmptt_conf_customize.php <input_snmptt_conf> <output_snmptt_conf> <snmp_traps_custom>

Variables:

- input_snmptt_conf = /etc/snmp/snmptt.conf
- output_snmptt_conf = /tmp/snmptt_custom.conf
- snmp_traps_custom = /etc/snmp/snmp_traps_custom.xml

18. Ensure that the variables mentioned above correctly match with the respective filenames and execute the command shown below.
    Command:
    ./snmptt_conf_customize.php/etc/snmp/snmptt.conf/tmp/snmptt_custom.conf/etc/snmp/snmp_traps_cust.xml
19. Open the /tmp/snmptt_custom.conf file using the command -
    vi /tmp/snmptt_custom.conf
20. Verify the changes made earlier in the procedure have successfully been saved.
21. Rename the /etc/snmp/snmptt.conf file as /etc/snmp/snmptt.conf.bak
    Command: ***mv /etc/snmp/snmptt.conf /etc/snmp/snmptt.conf.bak***
22. Replace the /etc/snmp/snmptt.conf file with /tmp/snmptt_custom.conf
    Command: ***mv /tmp/snmptt_custom.conf /etc/snmp/snmptt.conf***
23. Restart the snmptt daemon to make it re-read the configuration file.
    Command: ***service snmptt restart***
24. Once the trap is generated the severity level is automatically changed in AO.
25. Generate a trap or when a trap gets generated, it should now be visible in AO UI with the updated severity level.
    Note: Only the digits after the last decimal point in an OID string will be displayed in the SNMP event log page in the Avaya Orchestrator web interface.



Chapter 21: Events and Alert Messages

The tables shown below display the OID information of ACP/ASP 4200 components supported in Avaya Orchestrator:

EMC VNX5300:

Name	OID	Severity
eventMonitorTrap	.1.3.6.1.4.1.1981.0.2	Normal
eventMonitorTrapInfo	.1.3.6.1.4.1.1981.0.3	Normal
eventMonitorTrapWarn	.1.3.6.1.4.1.1981.0.4	Normal
eventMonitorTrapError	.1.3.6.1.4.1.1981.0.5	Critical
eventMonitorTrapFault	.1.3.6.1.4.1.1981.0.6	Critical

PDU:

Name	OID	Severity
branchLoadEvent	.1.3.6.1.4.1.1718.3.100.0.15	Critical
branchStatusEvent	.1.3.6.1.4.1.1718.3.100.0.14	Critical
contactClosureEvent	.1.3.6.1.4.1.1718.3.100.0.13	Critical
envMonADCEvent	.1.3.6.1.4.1.1718.3.100.0.9	Critical
envMonStatusEvent	.1.3.6.1.4.1.1718.3.100.0.7	Critical
envMonWaterSensorEvent	.1.3.6.1.4.1.1718.3.100.0.8	Critical
infeedLoadEvent	.1.3.6.1.4.1.1718.3.100.0.3	Critical
infeedStatusEvent	.1.3.6.1.4.1.1718.3.100.0.2	Critical
outletChangeEvent	.1.3.6.1.4.1.1718.3.100.0.6	Informational
outletLoadEvent	.1.3.6.1.4.1.1718.3.100.0.5	Critical
outletStatusEvent	.1.3.6.1.4.1.1718.3.100.0.4	Critical
st4AdcSensorEvent	.1.3.6.1.4.1.1718.4.100.0.24	Critical
st4BranchCurrentEvent	.1.3.6.1.4.1.1718.4.100.0.14	Critical
st4BranchStatusEvent	.1.3.6.1.4.1.1718.4.100.0.13	Critical
st4CcSensorStatusEvent	.1.3.6.1.4.1.1718.4.100.0.23	Critical
st4FanSensorEvent	.1.3.6.1.4.1.1718.4.100.0.25	Critical
st4HumidSensorEvent	.1.3.6.1.4.1.1718.4.100.0.21	Critical
st4InputCordActivePowerEvent	.1.3.6.1.4.1.1718.4.100.0.3	Critical
st4InputCordApparentPowerEvent	.1.3.6.1.4.1.1718.4.100.0.4	Critical
st4InputCordOutOfBalanceEvent	.1.3.6.1.4.1.1718.4.100.0.6	Critical
st4InputCordPowerFactorEvent	.1.3.6.1.4.1.1718.4.100.0.5	Critical
st4InputCordStatusEvent	.1.3.6.1.4.1.1718.4.100.0.2	Critical
st4LineCurrentEvent	.1.3.6.1.4.1.1718.4.100.0.8	Critical
st4LineStatusEvent	.1.3.6.1.4.1.1718.4.100.0.7	Critical
st4OcpStatusEvent	.1.3.6.1.4.1.1718.4.100.0.12	Critical
st4OutletActivePowerEvent	.1.3.6.1.4.1.1718.4.100.0.18	Critical
st4OutletCurrentEvent	.1.3.6.1.4.1.1718.4.100.0.17	Critical
st4OutletPowerFactorEvent	.1.3.6.1.4.1.1718.4.100.0.19	Critical
st4OutletStateChangeEvent	.1.3.6.1.4.1.1718.4.100.0.16	Informational

Name	OID	Severity
st4OutletStatusEvent	.1.3.6.1.4.1.1718.4.100.0.15	Critical
st4PhasePowerFactorEvent	.1.3.6.1.4.1.1718.4.100.0.11	Critical
st4PhaseStatusEvent	.1.3.6.1.4.1.1718.4.100.0.9	Critical
st4PhaseVoltageEvent	.1.3.6.1.4.1.1718.4.100.0.10	Critical
st4TempSensorEvent	.1.3.6.1.4.1.1718.4.100.0.20	Critical
st4UnitStatusEvent	.1.3.6.1.4.1.1718.4.100.0.1	Critical
st4WaterSensorStatusEvent	.1.3.6.1.4.1.1718.4.100.0.22	Critical
tempHumidSensorHumidEvent	.1.3.6.1.4.1.1718.3.100.0.12	Critical
tempHumidSensorStatusEvent	.1.3.6.1.4.1.1718.3.100.0.10	Critical
tempHumidSensorTempEvent	.1.3.6.1.4.1.1718.3.100.0.11	Critical
towerStatusEvent	.1.3.6.1.4.1.1718.3.100.0.1	Critical

Nimble CS1000:

Name	OID	Severity
nimbleDsdRedEntry0101Deprecated	.1.3.6.1.4.1.37447.2.1.2.101	Informational
nimbleDsdSpaceRedExit	.1.3.6.1.4.1.37447.2.1.2.102	Informational
nimbleDsdSpaceCrit0103Deprecated	.1.3.6.1.4.1.37447.2.1.2.103	Normal
nimbleDsdSpaceUtilizationHigh	.1.3.6.1.4.1.37447.2.1.2.104	Major
nimbleDsdSpaceUtilizationOk	.1.3.6.1.4.1.37447.2.1.2.105	Informational
nimbleDsdSpaceUtilizationCrit	.1.3.6.1.4.1.37447.2.1.2.106	Critical
nimbleDsdSpaceRedEntry0107Deprecated	.1.3.6.1.4.1.37447.2.1.2.107	Normal
nimbleDsdSpaceCrit0110Deprecated	.1.3.6.1.4.1.37447.2.1.2.110	Normal
nimbleDsdSpaceRedEntry	.1.3.6.1.4.1.37447.2.1.2.111	Critical
nimbleDsdSpaceCrit	.1.3.6.1.4.1.37447.2.1.2.112	Critical
nimbleCtrlrException	.1.3.6.1.4.1.37447.2.1.2.2001	Critical
nimbleCtrlrTakeover	.1.3.6.1.4.1.37447.2.1.2.2002	Major
nimbleCtrlrStandbyAvail	.1.3.6.1.4.1.37447.2.1.2.2003	Informational
nimbleCtrlrStandbyUnavail	.1.3.6.1.4.1.37447.2.1.2.2004	Critical
nimbleCtrlrExcessiveRestarts	.1.3.6.1.4.1.37447.2.1.2.2005	Normal
nimbleServiceReboot	.1.3.6.1.4.1.37447.2.1.2.2006	Normal
nimbleUserReboot	.1.3.6.1.4.1.37447.2.1.2.2007	Normal
nimbleUserRebootFailed	.1.3.6.1.4.1.37447.2.1.2.2008	Normal
nimbleUserHalt	.1.3.6.1.4.1.37447.2.1.2.2009	Normal
nimbleUserHaltFailed	.1.3.6.1.4.1.37447.2.1.2.2010	Normal
nimbleCtrlrStandbyUnavailInfo	.1.3.6.1.4.1.37447.2.1.2.2011	Critical
nimbleCtrlrStandbyUnavailWarn	.1.3.6.1.4.1.37447.2.1.2.2012	Major
nimbleCtrlrExceptionWarn	.1.3.6.1.4.1.37447.2.1.2.2013	Major
nimbleCtrlrExceptionCrit	.1.3.6.1.4.1.37447.2.1.2.2014	Critical
nimbleCtrlrStandbyUnavailWarnTimeDeprecated	.1.3.6.1.4.1.37447.2.1.2.2015	Normal
nimbleCtrlrStandbyUnavailWarnTime	.1.3.6.1.4.1.37447.2.1.2.2016	Major
nimbleCtrlrTakeoverWarn	.1.3.6.1.4.1.37447.2.1.2.2017	Major
nimbleCtrlrFailoverDeprecated	.1.3.6.1.4.1.37447.2.1.2.2018	Normal
nimbleCtrlrFailover	.1.3.6.1.4.1.37447.2.1.2.2019	Major
nimbleServiceStarted	.1.3.6.1.4.1.37447.2.1.2.2101	Normal
nimbleServiceDeadRestart	.1.3.6.1.4.1.37447.2.1.2.2102	Normal
nimbleServiceDeadNoRestart	.1.3.6.1.4.1.37447.2.1.2.2103	Normal

Name	OID	Severity
nimbleServiceCreateTunnel	.1.3.6.1.4.1.37447.2.1.2.2104	Normal
nimbleServiceTerminateTunnel	.1.3.6.1.4.1.37447.2.1.2.2105	Normal
nimbleServiceEssentialStoppedDeprecated	.1.3.6.1.4.1.37447.2.1.2.2106	Normal
nimbleServiceEssentialStopped	.1.3.6.1.4.1.37447.2.1.2.2107	Normal
nimbleServiceEmailAlertFailedDeprecated	.1.3.6.1.4.1.37447.2.1.2.2108	Normal
nimbleServiceEmailAlertFailed	.1.3.6.1.4.1.37447.2.1.2.2109	Normal
nimbleTestDbg	.1.3.6.1.4.1.37447.2.1.2.5000	Normal
nimbleTestInfo	.1.3.6.1.4.1.37447.2.1.2.5001	Normal
nimbleTestErr	.1.3.6.1.4.1.37447.2.1.2.5002	Normal
nimbleTestNot	.1.3.6.1.4.1.37447.2.1.2.5003	Normal
nimbleTestNoteDeprecated	.1.3.6.1.4.1.37447.2.1.2.5004	Normal
nimbleTestWarn	.1.3.6.1.4.1.37447.2.1.2.5005	Normal
nimbleTestCrit	.1.3.6.1.4.1.37447.2.1.2.5006	Normal
nimbleTestNote	.1.3.6.1.4.1.37447.2.1.2.5007	Normal
nimbleUpdateUnpackFail	.1.3.6.1.4.1.37447.2.1.2.6000	Normal
nimbleUpdateStartedDeprecated	.1.3.6.1.4.1.37447.2.1.2.6001	Normal
nimbleUpdateRevert	.1.3.6.1.4.1.37447.2.1.2.6002	Normal
nimbleUpdateSuccessDeprecated	.1.3.6.1.4.1.37447.2.1.2.6003	Normal
nimbleUpdateRollback	.1.3.6.1.4.1.37447.2.1.2.6004	Normal
nimbleUpdatePrecheckFail	.1.3.6.1.4.1.37447.2.1.2.6005	Normal
nimbleUpdateFailMsg	.1.3.6.1.4.1.37447.2.1.2.6007	Normal
nimbleUpdateUnpackStarted	.1.3.6.1.4.1.37447.2.1.2.6008	Normal
nimbleUpdateUnpackDone	.1.3.6.1.4.1.37447.2.1.2.6009	Normal
nimbleUpdateSwitchRoot	.1.3.6.1.4.1.37447.2.1.2.6010	Normal
nimbleUpdateDownloadFailed	.1.3.6.1.4.1.37447.2.1.2.6011	Normal
nimbleUpdateFailTmpFsFull	.1.3.6.1.4.1.37447.2.1.2.6012	Normal
nimbleUpdateFailScratchFsFull	.1.3.6.1.4.1.37447.2.1.2.6013	Normal
nimbleUpdateFailVarFsFull	.1.3.6.1.4.1.37447.2.1.2.6014	Normal
nimbleUpdateFailConfigFsFull	.1.3.6.1.4.1.37447.2.1.2.6015	Normal
nimbleUpdateFailUsbFsFull	.1.3.6.1.4.1.37447.2.1.2.6016	Normal
nimbleUpdatePkgNotFound	.1.3.6.1.4.1.37447.2.1.2.6017	Normal
nimbleUpdatePkgWrongSig	.1.3.6.1.4.1.37447.2.1.2.6018	Normal
nimbleUpdatePkgWrongCksum	.1.3.6.1.4.1.37447.2.1.2.6019	Normal
nimbleUpdateNetDegradeDeprecated	.1.3.6.1.4.1.37447.2.1.2.6020	Normal
nimbleUpdateDisallowSoloDeprecated	.1.3.6.1.4.1.37447.2.1.2.6021	Normal
nimbleUpdateDisallowSolo	.1.3.6.1.4.1.37447.2.1.2.6022	Normal
nimbleUpdateNetDegrade	.1.3.6.1.4.1.37447.2.1.2.6023	Normal
nimbleUpdateRaidDegrade	.1.3.6.1.4.1.37447.2.1.2.6024	Normal
nimbleUpdateStarted	.1.3.6.1.4.1.37447.2.1.2.6025	Normal
nimbleUpdateSuccess	.1.3.6.1.4.1.37447.2.1.2.6026	Normal
nimbleUpdateArrayUnreachable	.1.3.6.1.4.1.37447.2.1.2.6501	Normal
nimbleUpdateArrayFailed	.1.3.6.1.4.1.37447.2.1.2.6502	Normal
nimbleUpdateArrayTimedOut	.1.3.6.1.4.1.37447.2.1.2.6503	Normal
nimbleArrayUnreachableDeprecated	.1.3.6.1.4.1.37447.2.1.2.10010	Normal
nimbleArrayReachableDeprecated	.1.3.6.1.4.1.37447.2.1.2.10011	Normal
nimbleArrayUnreachable	.1.3.6.1.4.1.37447.2.1.2.10012	Critical
nimbleArrayReachable	.1.3.6.1.4.1.37447.2.1.2.10013	Informational

Name	OID	Severity
nimbleUserClearedSysCache	.1.3.6.1.4.1.37447.2.1.2.10101	Normal
nimbleVolSpcCurWarningUp	.1.3.6.1.4.1.37447.2.1.2.10200	Normal
nimbleVolSpcCurWarningDown	.1.3.6.1.4.1.37447.2.1.2.10201	Normal
nimbleVolSpcCurQuotaUp	.1.3.6.1.4.1.37447.2.1.2.10202	Normal
nimbleVolSpcCurQuotaDown	.1.3.6.1.4.1.37447.2.1.2.10203	Normal
nimbleVolSpcSnapWarningUp	.1.3.6.1.4.1.37447.2.1.2.10204	Normal
nimbleVolSpcSnapWarningDown	.1.3.6.1.4.1.37447.2.1.2.10205	Normal
nimbleVolSpcSnapQuotaUp	.1.3.6.1.4.1.37447.2.1.2.10206	Normal
nimbleVolSpcSnapQuotaDown	.1.3.6.1.4.1.37447.2.1.2.10207	Normal
nimbleGmVolSpcCurCritUp	.1.3.6.1.4.1.37447.2.1.2.10208	Normal
nimbleGmVolSpcCurCritDown	.1.3.6.1.4.1.37447.2.1.2.10209	Normal
nimbleGmSnapSpcCurCritUp	.1.3.6.1.4.1.37447.2.1.2.10210	Normal
nimbleGmSnapSpcCurCritDown	.1.3.6.1.4.1.37447.2.1.2.10211	Normal
nimbleGmVolSpcCurQuotaOffline	.1.3.6.1.4.1.37447.2.1.2.10212	Normal
nimbleGmVolSpcCurQuotaSet	.1.3.6.1.4.1.37447.2.1.2.10213	Normal
nimbleGmVolSpcSnapQuotaOffline	.1.3.6.1.4.1.37447.2.1.2.10214	Normal
nimbleGmVolSpcSnapQuotaSet	.1.3.6.1.4.1.37447.2.1.2.10215	Normal
nimbleGmVolSpcCurReserveOffline	.1.3.6.1.4.1.37447.2.1.2.10216	Normal
nimbleGmVolSpcCurReserveSet	.1.3.6.1.4.1.37447.2.1.2.10217	Normal
nimbleGmVolSpcSnapReserveOffline	.1.3.6.1.4.1.37447.2.1.2.10218	Normal
nimbleGmVolSpcSnapReserveSet	.1.3.6.1.4.1.37447.2.1.2.10219	Normal
nimbleGmVolSpcCurWarningUp	.1.3.6.1.4.1.37447.2.1.2.10220	Normal
nimbleGmVolSpcCurWarningDown	.1.3.6.1.4.1.37447.2.1.2.10221	Normal
nimbleGmVolSpcCurQuotaUp	.1.3.6.1.4.1.37447.2.1.2.10222	Normal
nimbleGmVolSpcCurQuotaDown	.1.3.6.1.4.1.37447.2.1.2.10223	Normal
nimbleGmVolSpcSnapWarningUp	.1.3.6.1.4.1.37447.2.1.2.10224	Normal
nimbleGmVolSpcSnapWarningDown	.1.3.6.1.4.1.37447.2.1.2.10225	Normal
nimbleGmVolSpcSnapQuotaUp	.1.3.6.1.4.1.37447.2.1.2.10226	Normal
nimbleGmVolSpcSnapQuotaDown	.1.3.6.1.4.1.37447.2.1.2.10227	Normal
nimbleVolAttrSyncDelay	.1.3.6.1.4.1.37447.2.1.2.10228	Normal
nimbleGmPoolArrAssgnDeprecated	.1.3.6.1.4.1.37447.2.1.2.10229	Normal
nimbleGmPoolArrUnassgnDeprecated	.1.3.6.1.4.1.37447.2.1.2.10230	Normal
nimbleGmVolSpcCurCritUpUnlim	.1.3.6.1.4.1.37447.2.1.2.10231	Normal
nimbleGmSnapSpcCurCritUpUnlim	.1.3.6.1.4.1.37447.2.1.2.10232	Normal
nimbleGmVolSpcReserveUp	.1.3.6.1.4.1.37447.2.1.2.10233	Normal
nimbleGmVolSpcReserveDown	.1.3.6.1.4.1.37447.2.1.2.10234	Normal
nimbleGmSnapSpcReserveUp	.1.3.6.1.4.1.37447.2.1.2.10235	Normal
nimbleGmSnapSpcReserveDown	.1.3.6.1.4.1.37447.2.1.2.10236	Normal
nimbleGmPoolMrgDeprecated	.1.3.6.1.4.1.37447.2.1.2.10240	Normal
nimbleVolAttrSyncSuccess	.1.3.6.1.4.1.37447.2.1.2.10241	Normal
nimbleSnapAttrSyncDelay	.1.3.6.1.4.1.37447.2.1.2.10242	Normal
nimbleSnapAttrSyncSuccess	.1.3.6.1.4.1.37447.2.1.2.10243	Normal
nimbleGroupAttrSyncDelay	.1.3.6.1.4.1.37447.2.1.2.10244	Normal
nimbleGroupAttrSyncComplete	.1.3.6.1.4.1.37447.2.1.2.10245	Normal
nimbleGlCtrlrAttrSyncDelayDeprecated	.1.3.6.1.4.1.37447.2.1.2.10246	Normal
nimbleGlCtrlrAttrSyncCompleteDeprecated	.1.3.6.1.4.1.37447.2.1.2.10247	Normal
nimbleGlCtrlrAttrSyncDelay	.1.3.6.1.4.1.37447.2.1.2.10248	Normal
nimbleGlCtrlrAttrSyncComplete	.1.3.6.1.4.1.37447.2.1.2.10249	Normal
nimbleVolMoveComplete	.1.3.6.1.4.1.37447.2.1.2.10250	Normal
nimbleVolMoveAbortComplete	.1.3.6.1.4.1.37447.2.1.2.10251	Normal

Name	OID	Severity
nimbleGmPoolArrUnassgnCompleteDeprecated	.1.3.6.1.4.1.37447.2.1.2.10252	Normal
nimbleGmPoolArrUnassgnComplete	.1.3.6.1.4.1.37447.2.1.2.10253	Normal
nimbleGmPoolArrAssgn	.1.3.6.1.4.1.37447.2.1.2.10256	Normal
nimbleGmPoolArrUnassgn	.1.3.6.1.4.1.37447.2.1.2.10257	Normal
nimbleGmPoolMrg	.1.3.6.1.4.1.37447.2.1.2.10260	Normal
nimbleGmVolSpcCurCritUpNonWritable	.1.3.6.1.4.1.37447.2.1.2.10261	Normal
nimbleGmVolSpcCurQuotaNonWritable	.1.3.6.1.4.1.37447.2.1.2.10262	Normal
nimbleGmSnapSpcCurCritUpNonWritable	.1.3.6.1.4.1.37447.2.1.2.10263	Normal
nimbleGmVolSpcSnapQuotaNonWritable	.1.3.6.1.4.1.37447.2.1.2.10264	Normal
nimbleGmVolSpcCurReserveNonWritable	.1.3.6.1.4.1.37447.2.1.2.10265	Normal
nimbleGmVolSpcSnapReserveNonWritable	.1.3.6.1.4.1.37447.2.1.2.10266	Normal
nimbleSchedSnapSucceededDeprecated	.1.3.6.1.4.1.37447.2.1.2.10300	Normal
nimbleSchedSnapFailed	.1.3.6.1.4.1.37447.2.1.2.10301	Normal
nimbleSchedSnapSkippedExists	.1.3.6.1.4.1.37447.2.1.2.10302	Normal
nimbleSchedSnapSkippedHandover	.1.3.6.1.4.1.37447.2.1.2.10303	Normal
nimbleSchedSnapSucceededLagInfoDeprecated	.1.3.6.1.4.1.37447.2.1.2.10304	Normal
nimbleSchedSnapFailedVmwareCredentialDeprecated	.1.3.6.1.4.1.37447.2.1.2.10305	Normal
nimbleSchedSnapFailedVmwareConnectionTimeoutDeprecated	.1.3.6.1.4.1.37447.2.1.2.10306	Normal
nimbleSchedSnapFailedVmwareConnectionRefusedDeprecated	.1.3.6.1.4.1.37447.2.1.2.10307	Normal
nimbleSchedSnapFailedVmwareConnectionResetDeprecated	.1.3.6.1.4.1.37447.2.1.2.10308	Normal
nimbleSchedSnapFailedVmwareConnectionNorouteDeprecated	.1.3.6.1.4.1.37447.2.1.2.10309	Normal
nimbleSchedSnapFailedVmwareConnectionSocketDeprecated	.1.3.6.1.4.1.37447.2.1.2.10310	Normal
nimbleSchedSnapFailedVmwareConnectionUnreachableDeprecated	.1.3.6.1.4.1.37447.2.1.2.10311	Normal
nimbleSchedSnapFailedVmwareDisabledDeprecated	.1.3.6.1.4.1.37447.2.1.2.10312	Normal
nimbleSchedSnapFailedVmwareObjectnfDeprecated	.1.3.6.1.4.1.37447.2.1.2.10313	Normal
nimbleSchedSnapFailedVmwarePermissionDeprecated	.1.3.6.1.4.1.37447.2.1.2.10314	Normal
nimbleSchedSnapFailedVmwareUkhostDeprecated	.1.3.6.1.4.1.37447.2.1.2.10315	Normal
nimbleSchedSnapFailedVmwareEncodingPlainDeprecated	.1.3.6.1.4.1.37447.2.1.2.10316	Normal
nimbleSchedSnapFailedVmwareNullDeprecated	.1.3.6.1.4.1.37447.2.1.2.10317	Normal
nimbleSchedSnapFailedVmwareDcnotfoundDeprecated	.1.3.6.1.4.1.37447.2.1.2.10318	Normal
nimbleSchedSnapFailedVmwareVolsnemptyDeprecated	.1.3.6.1.4.1.37447.2.1.2.10319	Normal
nimbleSchedSnapFailedVmwareUnknownDeprecated	.1.3.6.1.4.1.37447.2.1.2.10320	Normal
nimbleSchedSnapFailedVmwareBsizeDeprecated	.1.3.6.1.4.1.37447.2.1.2.10321	Normal
nimbleSchedSnapSucceeded	.1.3.6.1.4.1.37447.2.1.2.10322	Normal
nimbleSchedSnapSucceededLagInfo	.1.3.6.1.4.1.37447.2.1.2.10323	Normal
nimbleSchedSnapFailedVmwareDisabledDeprecatedTwo	.1.3.6.1.4.1.37447.2.1.2.10324	Normal
nimbleSchedSnapFailedVmwareTimeoutDeprecated	.1.3.6.1.4.1.37447.2.1.2.10325	Normal
nimbleSchedSnapFailedVmwareSnapNameMaxLengthExceededDeprecated	.1.3.6.1.4.1.37447.2.1.2.10326	Normal

Name	OID	Severity
nimbleSchedSnapFallback	.1.3.6.1.4.1.37447.2.1.2.10327	Normal
nimbleSchedSnapFailedVmwarePermissionPerVm	.1.3.6.1.4.1.37447.2.1.2.10340	Normal
nimbleSchedSnapFailedVmwareObjectnfPerVm	.1.3.6.1.4.1.37447.2.1.2.10341	Normal
nimbleSchedSnapFailedVmwareEncodingPlainPerVm	.1.3.6.1.4.1.37447.2.1.2.10342	Normal
nimbleSchedSnapFailedVmwareNullPerVm	.1.3.6.1.4.1.37447.2.1.2.10343	Normal
nimbleSchedSnapFailedVmwareDcnotfoundPerVm	.1.3.6.1.4.1.37447.2.1.2.10344	Normal
nimbleSchedSnapFailedVmwareVolsnemptyPerVm	.1.3.6.1.4.1.37447.2.1.2.10345	Normal
nimbleSchedSnapFailedVmwareUnknownPerVmDeprecated	.1.3.6.1.4.1.37447.2.1.2.10346	Normal
nimbleSchedSnapFailedVmwareBsizePerVm	.1.3.6.1.4.1.37447.2.1.2.10347	Normal
nimbleSchedSnapFailedVmwareDisabledPerVm	.1.3.6.1.4.1.37447.2.1.2.10348	Normal
nimbleSchedSnapFailedVmwareTimeoutPerVm	.1.3.6.1.4.1.37447.2.1.2.10349	Normal
nimbleSchedSnapFailedVmwareSnapNameMaxLengthExceededPerVm	.1.3.6.1.4.1.37447.2.1.2.10350	Normal
nimbleSchedSnapFailedVmwareGuestToolsNotRunningPerVm	.1.3.6.1.4.1.37447.2.1.2.10351	Normal
nimbleSchedSnapFailedVmwareInvalidVcenter	.1.3.6.1.4.1.37447.2.1.2.10352	Normal
nimbleSchedSnapFailedVmwareBusy	.1.3.6.1.4.1.37447.2.1.2.10353	Normal
nimbleSchedSnapFailedVssIncompatible	.1.3.6.1.4.1.37447.2.1.2.10354	Normal
nimbleSchedSnapFailedVmwareCredentialNw	.1.3.6.1.4.1.37447.2.1.2.10355	Normal
nimbleSchedSnapFailedVmwareConnectionTimeoutNw	.1.3.6.1.4.1.37447.2.1.2.10356	Normal
nimbleSchedSnapFailedVmwareConnectionRefusedNw	.1.3.6.1.4.1.37447.2.1.2.10357	Normal
nimbleSchedSnapFailedVmwareConnectionResetNw	.1.3.6.1.4.1.37447.2.1.2.10358	Normal
nimbleSchedSnapFailedVmwareConnectionNorouteNw	.1.3.6.1.4.1.37447.2.1.2.10359	Normal
nimbleSchedSnapFailedVmwareConnectionSocketNw	.1.3.6.1.4.1.37447.2.1.2.10360	Normal
nimbleSchedSnapFailedVmwareConnectionUnreachableNw	.1.3.6.1.4.1.37447.2.1.2.10361	Normal
nimbleSchedSnapFailedVmwareUkhostNw	.1.3.6.1.4.1.37447.2.1.2.10362	Normal
nimbleSchedSnapFailedVmwareConnectionUnknownNw	.1.3.6.1.4.1.37447.2.1.2.10363	Normal
nimbleSchedSnapFailedVmwareTimeoutNw	.1.3.6.1.4.1.37447.2.1.2.10364	Normal
nimbleSchedSnapFailedVmwareUnknownNw	.1.3.6.1.4.1.37447.2.1.2.10365	Normal
nimbleSchedSnapFailedVmwareUnknownPerVm	.1.3.6.1.4.1.37447.2.1.2.10366	Normal
nimbleSchedSnapFailedVmwareQuiescingVmFailed	.1.3.6.1.4.1.37447.2.1.2.10367	Normal
nimbleGmSpaceReserveWarnUp	.1.3.6.1.4.1.37447.2.1.2.10401	Normal
nimbleGmSpaceReserveWarnDown	.1.3.6.1.4.1.37447.2.1.2.10402	Normal
nimbleGmSpaceReserveCritUp	.1.3.6.1.4.1.37447.2.1.2.10403	Normal
nimbleGmSpaceReserveCritDown	.1.3.6.1.4.1.37447.2.1.2.10404	Normal
nimbleGmSpaceUtilizationOk	.1.3.6.1.4.1.37447.2.1.2.10405	Normal
nimbleGmSpaceUtilizationInfo	.1.3.6.1.4.1.37447.2.1.2.10406	Normal
nimbleGmSpaceUtilizationHigh	.1.3.6.1.4.1.37447.2.1.2.10407	Normal
nimbleGmSpaceUtilizationCrit	.1.3.6.1.4.1.37447.2.1.2.10408	Normal
nimbleGmPoolSpaceReserveWarnUpDeprecated	.1.3.6.1.4.1.37447.2.1.2.10409	Normal

Name	OID	Severity
nimbleGmPoolSpaceReserveWarnDownDeprecated	.1.3.6.1.4.1.37447.2.1.2.10410	Normal
nimbleGmPoolSpaceReserveCritUpDeprecated	.1.3.6.1.4.1.37447.2.1.2.10411	Normal
nimbleGmPoolSpaceReserveCritDownDeprecated	.1.3.6.1.4.1.37447.2.1.2.10412	Normal
nimbleGmPoolSpaceUtilizationOkDeprecated	.1.3.6.1.4.1.37447.2.1.2.10413	Normal
nimbleGmPoolSpaceUtilizationInfoDeprecated	.1.3.6.1.4.1.37447.2.1.2.10414	Normal
nimbleGmPoolSpaceUtilizationHighDeprecated	.1.3.6.1.4.1.37447.2.1.2.10415	Normal
nimbleGmPoolSpaceUtilizationCritDeprecated	.1.3.6.1.4.1.37447.2.1.2.10416	Normal
nimbleGmPoolSpaceReserveWarnUp	.1.3.6.1.4.1.37447.2.1.2.10417	Normal
nimbleGmPoolSpaceReserveWarnDown	.1.3.6.1.4.1.37447.2.1.2.10418	Normal
nimbleGmPoolSpaceReserveCritUp	.1.3.6.1.4.1.37447.2.1.2.10419	Normal
nimbleGmPoolSpaceReserveCritDown	.1.3.6.1.4.1.37447.2.1.2.10420	Normal
nimbleGmPoolSpaceUtilizationOk	.1.3.6.1.4.1.37447.2.1.2.10421	Normal
nimbleGmPoolSpaceUtilizationInfo	.1.3.6.1.4.1.37447.2.1.2.10422	Normal
nimbleGmPoolSpaceUtilizationHigh	.1.3.6.1.4.1.37447.2.1.2.10423	Normal
nimbleGmPoolSpaceUtilizationCrit	.1.3.6.1.4.1.37447.2.1.2.10424	Normal
nimbleLimitMaxOver	.1.3.6.1.4.1.37447.2.1.2.10500	Normal
nimbleLimitMaxUnder	.1.3.6.1.4.1.37447.2.1.2.10501	Normal
nimbleLimitWarnOver	.1.3.6.1.4.1.37447.2.1.2.10502	Normal
nimbleLimitWarnUnder	.1.3.6.1.4.1.37447.2.1.2.10503	Normal
nimbleReplSnapcollSucceeded	.1.3.6.1.4.1.37447.2.1.2.11000	Normal
nimbleReplSnapcollDelayedInfo	.1.3.6.1.4.1.37447.2.1.2.11001	Normal
nimbleReplSnapcollDelayedWarn	.1.3.6.1.4.1.37447.2.1.2.11002	Normal
nimbleReplPartnerSyncFail	.1.3.6.1.4.1.37447.2.1.2.11003	Normal
nimbleReplBranchPinned	.1.3.6.1.4.1.37447.2.1.2.11004	Normal
nimbleReplHandoverCompleted	.1.3.6.1.4.1.37447.2.1.2.11005	Normal
nimbleReplMultiArrayGroup	.1.3.6.1.4.1.37447.2.1.2.11006	Normal
nimbleReplPartnerMisconfiguration	.1.3.6.1.4.1.37447.2.1.2.11007	Normal
nimbleReplSnapshotCorrectedDeprecated	.1.3.6.1.4.1.37447.2.1.2.11008	Normal
nimbleReplCbrRequestedDeprecated	.1.3.6.1.4.1.37447.2.1.2.11009	Normal
nimbleReplCbrNeeded	.1.3.6.1.4.1.37447.2.1.2.11010	Normal
nimbleReplSnapshotCorrectedDeprecated2	.1.3.6.1.4.1.37447.2.1.2.11011	Normal
nimbleReplCbrRequestedDeprecated2	.1.3.6.1.4.1.37447.2.1.2.11012	Normal
nimbleReplPartnerAuthFailDeprecated	.1.3.6.1.4.1.37447.2.1.2.11013	Normal
nimbleReplSnapshotCorrected	.1.3.6.1.4.1.37447.2.1.2.11014	Normal
nimbleReplCbrRequested	.1.3.6.1.4.1.37447.2.1.2.11015	Normal
nimbleReplPartnerAuthFail	.1.3.6.1.4.1.37447.2.1.2.11016	Normal
nimbleOvertempShutdownDeprecated	.1.3.6.1.4.1.37447.2.1.2.12000	Normal
nimbleCtrlrOvertempDeprecated	.1.3.6.1.4.1.37447.2.1.2.12001	Normal
nimbleBackplaneOvertempDeprecated	.1.3.6.1.4.1.37447.2.1.2.12002	Normal
nimbleDiskFailedCritDeprecated	.1.3.6.1.4.1.37447.2.1.2.12100	Normal
nimbleDiskFailedDeprecated	.1.3.6.1.4.1.37447.2.1.2.12101	Normal
nimbleDiskAbsentDeprecated	.1.3.6.1.4.1.37447.2.1.2.12102	Normal
nimbleDiskAddedDeprecated	.1.3.6.1.4.1.37447.2.1.2.12103	Normal
nimbleDiskRemovedDeprecated	.1.3.6.1.4.1.37447.2.1.2.12104	Normal
nimbleSsdFailedDeprecated	.1.3.6.1.4.1.37447.2.1.2.12105	Normal
nimbleSsdAbsentDeprecated	.1.3.6.1.4.1.37447.2.1.2.12106	Normal
nimbleSsdAddedDeprecated	.1.3.6.1.4.1.37447.2.1.2.12107	Normal
nimbleSsdRemovedDeprecated	.1.3.6.1.4.1.37447.2.1.2.12108	Normal
nimbleDiskInvalidLabel	.1.3.6.1.4.1.37447.2.1.2.12109	Normal
nimbleSsdInvalidLabel	.1.3.6.1.4.1.37447.2.1.2.12110	Normal

Name	OID	Severity
nimbleDiskSizeMismatchDeprecated	.1.3.6.1.4.1.37447.2.1.2.12111	Normal
nimbleHddFailedV2	.1.3.6.1.4.1.37447.2.1.2.12112	Critical
nimbleHddAbsentV2	.1.3.6.1.4.1.37447.2.1.2.12113	Normal
nimbleHddAddedV2	.1.3.6.1.4.1.37447.2.1.2.12114	Normal
nimbleHddRemovedV2	.1.3.6.1.4.1.37447.2.1.2.12115	Minor
nimbleSsdFailedV2	.1.3.6.1.4.1.37447.2.1.2.12116	Critical
nimbleSsdAbsentV2	.1.3.6.1.4.1.37447.2.1.2.12117	Normal
nimbleSsdAddedV2	.1.3.6.1.4.1.37447.2.1.2.12118	Normal
nimbleSsdRemovedV2	.1.3.6.1.4.1.37447.2.1.2.12119	Minor
nimbleSsdLastOne	.1.3.6.1.4.1.37447.2.1.2.12120	Normal
nimbleHddFailedV3	.1.3.6.1.4.1.37447.2.1.2.12121	Critical
nimbleHddAddedV3	.1.3.6.1.4.1.37447.2.1.2.12122	Normal
nimbleHddRemovedV3	.1.3.6.1.4.1.37447.2.1.2.12123	Minor
nimbleSsdFailedV3	.1.3.6.1.4.1.37447.2.1.2.12124	Critical
nimbleSsdAddedV3	.1.3.6.1.4.1.37447.2.1.2.12125	Normal
nimbleSsdRemovedV3	.1.3.6.1.4.1.37447.2.1.2.12126	Minor
nimbleDiskSizeMismatchV2	.1.3.6.1.4.1.37447.2.1.2.12127	Normal
nimbleSsdSizeMismatchV2	.1.3.6.1.4.1.37447.2.1.2.12128	Normal
nimbleHddFailedAfsDeprecated	.1.3.6.1.4.1.37447.2.1.2.12129	Normal
nimbleHddFailedAfs	.1.3.6.1.4.1.37447.2.1.2.12130	Normal
nimbleIpIfDown	.1.3.6.1.4.1.37447.2.1.2.12200	Critical
nimbleIpIfUp	.1.3.6.1.4.1.37447.2.1.2.12201	Informational
nimbleIpIfGroupUnavailDeprecated	.1.3.6.1.4.1.37447.2.1.2.12202	Normal
nimbleIpIfDataUnavailDeprecated	.1.3.6.1.4.1.37447.2.1.2.12203	Normal
nimbleIpIfCantFailoverDeprecated	.1.3.6.1.4.1.37447.2.1.2.12204	Normal
nimbleSubnetNicMigrationDeprecated	.1.3.6.1.4.1.37447.2.1.2.12205	Normal
nimbleSubnetNicMissingDeprecated	.1.3.6.1.4.1.37447.2.1.2.12206	Normal
nimbleIpNicMigrationDeprecated	.1.3.6.1.4.1.37447.2.1.2.12207	Normal
nimbleIpNicMissingDeprecated	.1.3.6.1.4.1.37447.2.1.2.12208	Normal
nimbleRouteNicMigrationDeprecated	.1.3.6.1.4.1.37447.2.1.2.12209	Normal
nimbleRouteNicMissingDeprecated	.1.3.6.1.4.1.37447.2.1.2.12210	Normal
nimbleIpIfFailover	.1.3.6.1.4.1.37447.2.1.2.12211	Minor
nimbleIpDupFound	.1.3.6.1.4.1.37447.2.1.2.12212	Normal
nimbleIpIfDiscoveryUnavailDeprecated	.1.3.6.1.4.1.37447.2.1.2.12213	Normal
nimbleIpIfTargetUnavailDeprecated	.1.3.6.1.4.1.37447.2.1.2.12214	Normal
nimbleIpIfGroupUnavail	.1.3.6.1.4.1.37447.2.1.2.12215	Normal
nimbleIpIfDiscoveryUnavail	.1.3.6.1.4.1.37447.2.1.2.12216	Normal
nimbleIpIfTargetUnavail	.1.3.6.1.4.1.37447.2.1.2.12217	Normal
nimbleIpIfDataUnavail	.1.3.6.1.4.1.37447.2.1.2.12218	Normal
nimbleIpIfIscsiDataUnavail	.1.3.6.1.4.1.37447.2.1.2.12219	Normal
nimbleIpIfClusterDataUnavail	.1.3.6.1.4.1.37447.2.1.2.12220	Normal
nimbleUnresponsiveNicDetected	.1.3.6.1.4.1.37447.2.1.2.12221	Normal
nimbleIpIfCantFailoverDeprecated2	.1.3.6.1.4.1.37447.2.1.2.12222	Normal
nimbleIpIfCantFailover	.1.3.6.1.4.1.37447.2.1.2.12223	Normal
nimbleSensorLinearWarn	.1.3.6.1.4.1.37447.2.1.2.12301	Normal
nimbleSensorLinearClear	.1.3.6.1.4.1.37447.2.1.2.12302	Normal
nimbleSensorBoolWarn	.1.3.6.1.4.1.37447.2.1.2.12303	Normal
nimbleSensorBoolClear	.1.3.6.1.4.1.37447.2.1.2.12304	Normal
nimbleSensorDoesNotExist	.1.3.6.1.4.1.37447.2.1.2.12305	Normal

Name	OID	Severity
nimbleNvramBattDisabled	.1.3.6.1.4.1.37447.2.1.2.12306	Normal
nimbleNvramBattDisabledCrit	.1.3.6.1.4.1.37447.2.1.2.12307	Normal
nimbleNvramBattOk	.1.3.6.1.4.1.37447.2.1.2.12308	Normal
nimbleTempSensorHighDep	.1.3.6.1.4.1.37447.2.1.2.12310	Normal
nimbleTempSensorLowDep	.1.3.6.1.4.1.37447.2.1.2.12311	Normal
nimbleTempSensorOkDep	.1.3.6.1.4.1.37447.2.1.2.12312	Normal
nimbleTempSensorMissingDep	.1.3.6.1.4.1.37447.2.1.2.12313	Normal
nimbleTempSensorOperationalDep	.1.3.6.1.4.1.37447.2.1.2.12314	Normal
nimbleFanSensorHighDep	.1.3.6.1.4.1.37447.2.1.2.12315	Normal
nimbleFanSensorLowDep	.1.3.6.1.4.1.37447.2.1.2.12316	Normal
nimbleFanSensorOkDep	.1.3.6.1.4.1.37447.2.1.2.12317	Normal
nimbleFanSensorStoppedDep	.1.3.6.1.4.1.37447.2.1.2.12318	Normal
nimbleFanSensorMissingDep	.1.3.6.1.4.1.37447.2.1.2.12319	Normal
nimblePwrSupplySensorFailDep	.1.3.6.1.4.1.37447.2.1.2.12320	Normal
nimblePwrSupplySensorMissingDep	.1.3.6.1.4.1.37447.2.1.2.12321	Normal
nimblePwrSupplySensorOkDep	.1.3.6.1.4.1.37447.2.1.2.12322	Normal
nimbleTempSensorHighDep2	.1.3.6.1.4.1.37447.2.1.2.12323	Normal
nimbleTempSensorLowDep2	.1.3.6.1.4.1.37447.2.1.2.12324	Normal
nimbleTempSensorOkDep2	.1.3.6.1.4.1.37447.2.1.2.12325	Normal
nimbleTempSensorMissingDep2	.1.3.6.1.4.1.37447.2.1.2.12326	Normal
nimbleTempSensorOperationalDep2	.1.3.6.1.4.1.37447.2.1.2.12327	Normal
nimbleFanSensorHighDep2	.1.3.6.1.4.1.37447.2.1.2.12328	Normal
nimbleFanSensorLowDep2	.1.3.6.1.4.1.37447.2.1.2.12329	Normal
nimbleFanSensorOkDep2	.1.3.6.1.4.1.37447.2.1.2.12330	Normal
nimbleFanSensorStoppedDep2	.1.3.6.1.4.1.37447.2.1.2.12331	Normal
nimbleFanSensorMissingDep2	.1.3.6.1.4.1.37447.2.1.2.12332	Normal
nimblePwrSupplySensorFailDep2	.1.3.6.1.4.1.37447.2.1.2.12333	Normal
nimblePwrSupplySensorMissingDep2	.1.3.6.1.4.1.37447.2.1.2.12334	Normal
nimblePwrSupplySensorOkDep2	.1.3.6.1.4.1.37447.2.1.2.12335	Normal
nimbleTempSensorHighDeprecatedDep2	.1.3.6.1.4.1.37447.2.1.2.12336	Normal
nimbleTempSensorLow	.1.3.6.1.4.1.37447.2.1.2.12337	Normal
nimbleTempSensorOk	.1.3.6.1.4.1.37447.2.1.2.12338	Normal
nimbleTempSensorMissing	.1.3.6.1.4.1.37447.2.1.2.12339	Normal
nimbleTempSensorOperational	.1.3.6.1.4.1.37447.2.1.2.12340	Normal
nimbleFanSensorHigh	.1.3.6.1.4.1.37447.2.1.2.12341	Normal
nimbleFanSensorLow	.1.3.6.1.4.1.37447.2.1.2.12342	Normal
nimbleFanSensorOk	.1.3.6.1.4.1.37447.2.1.2.12343	Normal
nimbleFanSensorStopped	.1.3.6.1.4.1.37447.2.1.2.12344	Normal
nimbleFanSensorMissing	.1.3.6.1.4.1.37447.2.1.2.12345	Normal
nimblePwrSupplySensorFail	.1.3.6.1.4.1.37447.2.1.2.12346	Critical
nimblePwrSupplySensorMissing	.1.3.6.1.4.1.37447.2.1.2.12347	Normal
nimblePwrSupplySensorOk	.1.3.6.1.4.1.37447.2.1.2.12348	Normal
nimbleRaidDegraded	.1.3.6.1.4.1.37447.2.1.2.12400	Normal
nimbleRaidRebuildStart	.1.3.6.1.4.1.37447.2.1.2.12401	Normal
nimbleRaidRebuildDone	.1.3.6.1.4.1.37447.2.1.2.12402	Normal
nimbleRaidRebuildFailRead	.1.3.6.1.4.1.37447.2.1.2.12403	Normal
nimbleRaidRebuildFail	.1.3.6.1.4.1.37447.2.1.2.12404	Normal
nimbleRaidDisksMissing	.1.3.6.1.4.1.37447.2.1.2.12405	Normal
nimbleRaidSpare	.1.3.6.1.4.1.37447.2.1.2.12406	Normal
nimbleRaidAssemblyFailed	.1.3.6.1.4.1.37447.2.1.2.12407	Normal

Name	OID	Severity
nimbleRaidDegradedV2	.1.3.6.1.4.1.37447.2.1.2.12408	Normal
nimbleRaidRebuildStartV2	.1.3.6.1.4.1.37447.2.1.2.12409	Normal
nimbleRaidRebuildDoneV2	.1.3.6.1.4.1.37447.2.1.2.12410	Normal
nimbleRaidRebuildFailReadV2	.1.3.6.1.4.1.37447.2.1.2.12411	Normal
nimbleRaidRebuildFailV2	.1.3.6.1.4.1.37447.2.1.2.12412	Normal
nimbleRaidDisksMissingV2	.1.3.6.1.4.1.37447.2.1.2.12413	Normal
nimbleRaidSpareV2	.1.3.6.1.4.1.37447.2.1.2.12414	Normal
nimbleRaidAssemblyFailedV2	.1.3.6.1.4.1.37447.2.1.2.12415	Normal
nimbleRaidRebuildScheduledV2	.1.3.6.1.4.1.37447.2.1.2.12416	Normal
nimbleRaidRebuildStopV2	.1.3.6.1.4.1.37447.2.1.2.12417	Normal
nimbleIscsiMultiInitiatorDeprecated	.1.3.6.1.4.1.37447.2.1.2.12500	Normal
nimbleIscsiConnHardLimitDeprecated1	.1.3.6.1.4.1.37447.2.1.2.12501	Normal
nimbleIscsiUnalignedOpsDeprecated	.1.3.6.1.4.1.37447.2.1.2.12502	Normal
nimbleIscsiMultiInitiator	.1.3.6.1.4.1.37447.2.1.2.12503	Normal
nimbleIscsiConnHardLimitDeprecated2	.1.3.6.1.4.1.37447.2.1.2.12504	Normal
nimbleIscsiUnalignedOps	.1.3.6.1.4.1.37447.2.1.2.12505	Normal
nimbleIscsiConnHardLimit	.1.3.6.1.4.1.37447.2.1.2.12506	Normal
nimbleIscsiErroneousItorConns	.1.3.6.1.4.1.37447.2.1.2.12057	Normal
nimbleNvramBattCharging	.1.3.6.1.4.1.37447.2.1.2.12601	Normal
nimbleNvramBattCharged	.1.3.6.1.4.1.37447.2.1.2.12602	Normal
nimbleNvramFpgaVersion	.1.3.6.1.4.1.37447.2.1.2.12603	Normal
nimbleNvramMbeDeprecated	.1.3.6.1.4.1.37447.2.1.2.12604	Normal
nimbleNvramSbeDeprecated	.1.3.6.1.4.1.37447.2.1.2.12605	Normal
nimbleNvramMbe	.1.3.6.1.4.1.37447.2.1.2.12606	Normal
nimbleNvramSbe	.1.3.6.1.4.1.37447.2.1.2.12607	Normal
nimbleNvdimmReservedBlocksWarn	.1.3.6.1.4.1.37447.2.1.2.12608	Normal
nimbleNvdimmReservedBlocksCrit	.1.3.6.1.4.1.37447.2.1.2.12609	Normal
nimbleNvdimmUltracapDischargedDeprecated	.1.3.6.1.4.1.37447.2.1.2.12610	Normal
nimbleNtbBadLink	.1.3.6.1.4.1.37447.2.1.2.12611	Normal
nimbleNvdimmUltracapDischarged	.1.3.6.1.4.1.37447.2.1.2.12612	Normal
nimbleNvramMissing	.1.3.6.1.4.1.37447.2.1.2.12613	Normal
nimbleShelfCtrlrSide	.1.3.6.1.4.1.37447.2.1.2.12701	Normal
nimbleShelfSesErr	.1.3.6.1.4.1.37447.2.1.2.12702	Normal
nimbleShelfDiskSasLink	.1.3.6.1.4.1.37447.2.1.2.12703	Critical
nimbleShelfDiskCount	.1.3.6.1.4.1.37447.2.1.2.12704	Normal
nimbleShelfInvalidEeprom	.1.3.6.1.4.1.37447.2.1.2.12705	Normal
nimbleShelfWrongSasPortDeprecated	.1.3.6.1.4.1.37447.2.1.2.12706	Normal
nimbleShelfSasLink	.1.3.6.1.4.1.37447.2.1.2.12707	Critical
nimbleShelfSasExpErr	.1.3.6.1.4.1.37447.2.1.2.12708	Major
nimbleShelfCtrlrLoop	.1.3.6.1.4.1.37447.2.1.2.12709	Normal
nimbleShelfMissing	.1.3.6.1.4.1.37447.2.1.2.12710	Normal
nimbleShelfOrder	.1.3.6.1.4.1.37447.2.1.2.12711	Normal
nimbleShelfSesMshipErrDeprecated	.1.3.6.1.4.1.37447.2.1.2.12712	Normal
nimbleShelfFailover	.1.3.6.1.4.1.37447.2.1.2.12713	Normal
nimbleShelfNewShelf	.1.3.6.1.4.1.37447.2.1.2.12714	Normal
nimbleShelfDisconnect	.1.3.6.1.4.1.37447.2.1.2.12715	Critical
nimbleShelfChassisSwap	.1.3.6.1.4.1.37447.2.1.2.12716	Normal
nimbleShelfLocIdOverLimit	.1.3.6.1.4.1.37447.2.1.2.12717	Normal
nimbleShelfActivatedDeprecated	.1.3.6.1.4.1.37447.2.1.2.12718	Normal
nimbleShelfReconnect	.1.3.6.1.4.1.37447.2.1.2.12719	Normal

Name	OID	Severity
nimbleShelfSasLinkDisabledDeprecated	.1.3.6.1.4.1.37447.2.1.2.12720	Normal
nimbleShelfDiskSasLinkErrDeprecated	.1.3.6.1.4.1.37447.2.1.2.12721	Normal
nimbleShelfWrongSasPortDeprecated2	.1.3.6.1.4.1.37447.2.1.2.12730	Normal
nimbleShelfSesMshipErrDeprecated2	.1.3.6.1.4.1.37447.2.1.2.12731	Normal
nimbleShelfSasLinkDisabled	.1.3.6.1.4.1.37447.2.1.2.12732	Normal
nimbleShelfDiskSasLinkErr	.1.3.6.1.4.1.37447.2.1.2.12733	Major
nimbleShelfWrongSasPort	.1.3.6.1.4.1.37447.2.1.2.12734	Normal
nimbleShelfSesMshipErrDeprecated3	.1.3.6.1.4.1.37447.2.1.2.12735	Normal
nimbleShelfSesMshipErrDeprecated4	.1.3.6.1.4.1.37447.2.1.2.12736	Normal
nimbleShelfActivatedV2Deprecated	.1.3.6.1.4.1.37447.2.1.2.12737	Normal
nimbleShelfSesMshipErr	.1.3.6.1.4.1.37447.2.1.2.12738	Critical
nimbleShelfActivatedV2	.1.3.6.1.4.1.37447.2.1.2.12739	Normal
nimblePhysMemMismatch	.1.3.6.1.4.1.37447.2.1.2.12901	Normal
nimbleVolSysLimitWarnEnter	.1.3.6.1.4.1.37447.2.1.2.13101	Normal
nimbleVolSysLimitWarnExit	.1.3.6.1.4.1.37447.2.1.2.13102	Normal
nimbleGmTakeoverSuccessDeprecatedDeprecated	.1.3.6.1.4.1.37447.2.1.2.13501	Normal
nimbleGmTakeoverSuccessDeprecated	.1.3.6.1.4.1.37447.2.1.2.13504	Normal
nimbleGmTakeoverSuccess	.1.3.6.1.4.1.37447.2.1.2.13505	Normal
nimbleGmMigrateFailure	.1.3.6.1.4.1.37447.2.1.2.13506	Normal
nimbleGmTakeoverRejectByArrayDeprecated	.1.3.6.1.4.1.37447.2.1.2.13502	Normal
nimbleGmTakeoverRejectByArray	.1.3.6.1.4.1.37447.2.1.2.13503	Normal
nimbleGmGrpMrgDone	.1.3.6.1.4.1.37447.2.1.2.13601	Normal
nimbleGmGrpQscFail	.1.3.6.1.4.1.37447.2.1.2.13602	Normal
nimbleGmGrpMrgRollbackDone	.1.3.6.1.4.1.37447.2.1.2.13603	Normal
nimbleGmGrpMrgReassFail	.1.3.6.1.4.1.37447.2.1.2.13604	Normal
nimbleGmGrpMrgDbFail	.1.3.6.1.4.1.37447.2.1.2.13605	Normal
nimbleGmBinMigContAbortDeprecated	.1.3.6.1.4.1.37447.2.1.2.13701	Normal
nimbleGmBinMigContAbort	.1.3.6.1.4.1.37447.2.1.2.13702	Normal
nimbleCsmodelChanged	.1.3.6.1.4.1.37447.2.1.2.14000	Normal
nimbleCsmodelUnknown	.1.3.6.1.4.1.37447.2.1.2.14001	Normal
nimbleTempSensorHighDeprecated	.1.3.6.1.4.1.37447.2.1.2.14002	Normal
nimbleOvertempShutdownDeprecated2	.1.3.6.1.4.1.37447.2.1.2.14003	Critical
nimbleCtrlrOvertemp	.1.3.6.1.4.1.37447.2.1.2.14004	Normal
nimbleBackplaneOvertemp	.1.3.6.1.4.1.37447.2.1.2.14005	Normal
nimbleTempSensorHighDeprecated2	.1.3.6.1.4.1.37447.2.1.2.14006	Normal
nimbleTempSensorCrithighDeprecated	.1.3.6.1.4.1.37447.2.1.2.14007	Normal
nimblePwrSupplySensorCallsupportDeprecated	.1.3.6.1.4.1.37447.2.1.2.14008	Normal
nimbleOvertempShutdown	.1.3.6.1.4.1.37447.2.1.2.14009	Normal
nimblePwrSupplySensorCallsupport	.1.3.6.1.4.1.37447.2.1.2.14010	Normal
nimbleTempSensorHigh	.1.3.6.1.4.1.37447.2.1.2.14011	Major
nimbleTempSensorCrithigh	.1.3.6.1.4.1.37447.2.1.2.14012	Critical
nimbleUpdateUnknownFirmware	.1.3.6.1.4.1.37447.2.1.2.14200	Normal
nimbleFcLinkUp	.1.3.6.1.4.1.37447.2.1.2.14400	Normal
nimbleFcLinkDown	.1.3.6.1.4.1.37447.2.1.2.14401	Critical
nimbleFcLinkNotConnected	.1.3.6.1.4.1.37447.2.1.2.14402	Normal
nimbleEventPurging	.1.3.6.1.4.1.37447.2.1.2.14700	Normal
nimbleEventWarnOver	.1.3.6.1.4.1.37447.2.1.2.14701	Normal

EMC VNXe3200:

Name	OID	Severity
vnxeGenericTrapEmergency	.1.3.6.1.4.1.1139.18.1.18.2.0	Critical
vnxeGenericTrapAlert	.1.3.6.1.4.1.1139.18.1.18.2.1	Critical
vnxeGenericTrapCritical	.1.3.6.1.4.1.1139.18.1.18.2.2	Critical
vnxeGenericTrapError	.1.3.6.1.4.1.1139.18.1.18.2.3	Critical
vnxeGenericTrapWarning	.1.3.6.1.4.1.1139.18.1.18.2.4	Major
vnxeGenericTrapNotice	.1.3.6.1.4.1.1139.18.1.18.2.5	Informational
vnxeGenericTrapInformational	.1.3.6.1.4.1.1139.18.1.18.2.6	Informational
vnxeGenericTrapDebug	.1.3.6.1.4.1.1139.18.1.18.2.7	Normal

VSP Switches:

Name	OID	Severity
authenticationFailure	.1.3.6.1.6.3.1.1.5.5	Normal
bgpBackwardTransition	.1.3.6.1.2.1.15.7.2	Normal
bgpEstablished	.1.3.6.1.2.1.15.7.1	Normal
bgpEstablishedNotification	.1.3.6.1.2.1.15.0.1	Normal
bnLogMsgBufferFull	.1.3.6.1.4.1.45.1.6.16.1.2.0.1	Normal
bsAdacPortConfigNotification	.1.3.6.1.4.1.45.5.9.0.1	Normal
bsAdacPortOperDisabledNotification	.1.3.6.1.4.1.45.5.9.0.2	Normal
bsaiArpPacketDroppedOnUntrustedPort	.1.3.6.1.4.1.45.5.18.0.1	Normal
bsaiArpPacketDroppedOnUntrustedPortMoreInfo	.1.3.6.1.4.1.45.5.18.0.2	Normal
bsDdiSfpBiasAlarm	.1.3.6.1.4.1.45.5.29.0.7	Normal
bsDdiSfpBiasNormal	.1.3.6.1.4.1.45.5.29.0.9	Normal
bsDdiSfpBiasWarn	.1.3.6.1.4.1.45.5.29.0.8	Normal
bsDdiSfpRxAlarm	.1.3.6.1.4.1.45.5.29.0.13	Normal
bsDdiSfpRxNormal	.1.3.6.1.4.1.45.5.29.0.15	Normal
bsDdiSfpRxWarn	.1.3.6.1.4.1.45.5.29.0.14	Normal
bsDdiSfpTempAlarm	.1.3.6.1.4.1.45.5.29.0.1	Normal
bsDdiSfpTempNormal	.1.3.6.1.4.1.45.5.29.0.3	Normal
bsDdiSfpTempWarn	.1.3.6.1.4.1.45.5.29.0.2	Normal
bsDdiSfpTxAlarm	.1.3.6.1.4.1.45.5.29.0.10	Normal
bsDdiSfpTxNormal	.1.3.6.1.4.1.45.5.29.0.12	Normal
bsDdiSfpTxWarn	.1.3.6.1.4.1.45.5.29.0.11	Normal
bsDdiSfpVoltageAlarm	.1.3.6.1.4.1.45.5.29.0.4	Normal
bsDdiSfpVoltageNormal	.1.3.6.1.4.1.45.5.29.0.6	Normal
bsDdiSfpVoltageWarn	.1.3.6.1.4.1.45.5.29.0.5	Normal
bsDhcpOption82MaxLengthExceeded	.1.3.6.1.4.1.45.5.17.0.3	Normal
bsDhcpSnoopingBindingTableFull	.1.3.6.1.4.1.45.5.17.0.1	Normal
bsDhcpSnoopingExtSaveEntryIfTrustedConflict	.1.3.6.1.4.1.45.5.17.0.22	Normal
bsDhcpSnoopingExtSaveEntryInvalidInterface	.1.3.6.1.4.1.45.5.17.0.5	Normal
bsDhcpSnoopingExtSaveEntryInvalidVlan	.1.3.6.1.4.1.45.5.17.0.17	Normal
bsDhcpSnoopingExtSaveEntryLeaseExpired	.1.3.6.1.4.1.45.5.17.0.6	Normal
bsDhcpSnoopingExtSaveEntryMACConflict	.1.3.6.1.4.1.45.5.17.0.4	Normal
bsDhcpSnoopingExtSaveEntryParsingFailure	.1.3.6.1.4.1.45.5.17.0.7	Normal
bsDhcpSnoopingExtSaveNTP	.1.3.6.1.4.1.45.5.17.0.8	Normal
bsDhcpSnoopingExtSaveSFTPRestoreFailure	.1.3.6.1.4.1.45.5.17.0.21	Normal
bsDhcpSnoopingExtSaveSFTPRestoreSuccess	.1.3.6.1.4.1.45.5.17.0.20	Normal
bsDhcpSnoopingExtSaveSFTPSyncFailure	.1.3.6.1.4.1.45.5.17.0.19	Normal

Name	OID	Severity
bsDhcpSnoopingExtSaveSFTPSyncSuccess	.1.3.6.1.4.1.45.5.17.0.18	Normal
bsDhcpSnoopingExtSaveTFTPRestoreFailure	.1.3.6.1.4.1.45.5.17.0.16	Normal
bsDhcpSnoopingExtSaveTFTPRestoreSuccess	.1.3.6.1.4.1.45.5.17.0.14	Normal
bsDhcpSnoopingExtSaveTFTPSyncFailure	.1.3.6.1.4.1.45.5.17.0.12	Normal
bsDhcpSnoopingExtSaveTFTPSyncSuccess	.1.3.6.1.4.1.45.5.17.0.10	Normal
bsDhcpSnoopingExtSaveUSBRestoreFailure	.1.3.6.1.4.1.45.5.17.0.15	Normal
bsDhcpSnoopingExtSaveUSBRestoreSuccess	.1.3.6.1.4.1.45.5.17.0.13	Normal
bsDhcpSnoopingExtSaveUSBSyncFailure	.1.3.6.1.4.1.45.5.17.0.11	Normal
bsDhcpSnoopingExtSaveUSBSyncSuccess	.1.3.6.1.4.1.45.5.17.0.9	Normal
bsDhcpSnoopingStaticEntryMACConflict	.1.3.6.1.4.1.45.5.17.0.23	Normal
bsDhcpSnoopingTrap	.1.3.6.1.4.1.45.5.17.0.2	Normal
bsdsDhcpv4ServerDuplicateAddress	.1.3.6.1.4.1.45.5.38.0.5	Normal
bsdsDhcpv4ServerFreeAddressHigh	.1.3.6.1.4.1.45.5.38.0.2	Normal
bsdsDhcpv4ServerFreeAddressLow	.1.3.6.1.4.1.45.5.38.0.1	Normal
bsdsDhcpv4ServerStartTime	.1.3.6.1.4.1.45.5.38.0.3	Normal
bsdsDhcpv4ServerStopTime	.1.3.6.1.4.1.45.5.38.0.4	Normal
bsifnInstallationFailure	.1.3.6.1.4.1.45.5.35.0.1	Normal
bsIpv6NDNotificationsUntrustedPort	.1.3.6.1.4.1.45.5.45.0.2	Normal
bsIpv6NDSBTTableFull	.1.3.6.1.4.1.45.5.45.0.1	Normal
bsLstGroupOperStateChanged	.1.3.6.1.4.1.45.5.43.0.2	Normal
bsLstInterfaceStatusChanged	.1.3.6.1.4.1.45.5.43.0.1	Normal
bsnAaaAlreadyConnected	.1.3.6.1.4.1.45.5.2.2.0.30	Normal
bsnAaaIncorrectLogOnThresholdExceeded	.1.3.6.1.4.1.45.5.2.2.0.31	Normal
bsnAaaMaxNoOfSessionsExceeded	.1.3.6.1.4.1.45.5.2.2.0.32	Normal
bsnAaaUserAccountNotUsed	.1.3.6.1.4.1.45.5.2.2.0.29	Normal
bsnAaaUserPasswordExpired	.1.3.6.1.4.1.45.5.2.2.0.37	Normal
bsnAuditRecordEventsFailure	.1.3.6.1.4.1.45.5.2.2.0.34	Normal
bsnAuditShutDownTrap	.1.3.6.1.4.1.45.5.2.2.0.36	Normal
bsnAuditStartUpTrap	.1.3.6.1.4.1.45.5.2.2.0.35	Normal
bsnAuditUnsentMessages	.1.3.6.1.4.1.45.5.2.2.0.33	Normal
bsnConfigurationSavedToNvram	.1.3.6.1.4.1.45.5.2.2.0.1	Normal
bsnConfigurationSavedToNvramV1	.1.3.6.1.4.1.45.5.2.2.1	Normal
bsnEapAccessViolation	.1.3.6.1.4.1.45.5.2.2.0.2	Normal
bsnEapAccessViolationV1	.1.3.6.1.4.1.45.5.2.2.2	Normal
bsnEapRateLimitExceeded	.1.3.6.1.4.1.45.5.2.2.0.19	Normal
bsnEapRAVError	.1.3.6.1.4.1.45.5.2.2.0.18	Normal
bsnEapUbpFailure	.1.3.6.1.4.1.45.5.2.2.0.14	Normal
bsnEnteredForcedStackMode	.1.3.6.1.4.1.45.5.2.2.0.16	Normal
bsnesActivated	.1.3.6.1.4.1.45.5.34.0.7	Normal
bsnesDeactivated	.1.3.6.1.4.1.45.5.34.0.8	Normal
bsnesGloballyDisabled	.1.3.6.1.4.1.45.5.34.0.2	Normal
bsnesGloballyEnabled	.1.3.6.1.4.1.45.5.34.0.1	Normal
bsnesManuallyActivated	.1.3.6.1.4.1.45.5.34.0.3	Normal
bsnesManuallyDeactivated	.1.3.6.1.4.1.45.5.34.0.4	Normal
bsnesScheduleApplied	.1.3.6.1.4.1.45.5.34.0.6	Normal
bsnesScheduleNotApplied	.1.3.6.1.4.1.45.5.34.0.5	Normal
bsnLacPortDisabledDueToLossOfVLACPDU	.1.3.6.1.4.1.45.5.2.2.0.11	Normal
bsnLacPortDisabledDueToLossOfVLACPDUV1	.1.3.6.1.4.1.45.5.2.2.11	Normal
bsnLacPortDisabledToPreventBroadcastStorm	.1.3.6.1.4.1.45.5.2.2.0.9	Normal
bsnLacPortDisabledToPreventBroadcastStormV1	.1.3.6.1.4.1.45.5.2.2.9	Normal

Name	OID	Severity
bsnLacPortEnabledDueToReceiptOfVLACPDU	.1.3.6.1.4.1.45.5.2.2.0.12	Normal
bsnLacPortEnabledDueToReceiptOfVLACPDUV1	.1.3.6.1.4.1.45.5.2.2.12	Normal
bsnLacTrunkUnavailable	.1.3.6.1.4.1.45.5.2.2.0.5	Normal
bsnLacTrunkUnavailableV1	.1.3.6.1.4.1.45.5.2.2.5	Normal
bsnLoginFailure	.1.3.6.1.4.1.45.5.2.2.0.6	Normal
bsnLoginFailureV1	.1.3.6.1.4.1.45.5.2.2.6	Normal
bsnMLTHealthFailure	.1.3.6.1.4.1.45.5.2.2.0.7	Normal
bsnMLTHealthFailureV1	.1.3.6.1.4.1.45.5.2.2.7	Normal
bsnPortSpeedDuplexMismatch	.1.3.6.1.4.1.45.5.2.2.0.3	Normal
bsnPortSpeedDuplexMismatchV1	.1.3.6.1.4.1.45.5.2.2.3	Normal
bsnROPasswordExpired	.1.3.6.1.4.1.45.5.2.2.0.25	Normal
bsnRunScripts	.1.3.6.1.4.1.45.5.2.2.0.28	Normal
bsnRWPasswordExpired	.1.3.6.1.4.1.45.5.2.2.0.26	Normal
bsnSFPInsertion	.1.3.6.1.4.1.45.5.2.2.0.23	Normal
bsnSFPRemoval	.1.3.6.1.4.1.45.5.2.2.0.24	Normal
bsnStackConfigurationError	.1.3.6.1.4.1.45.5.2.2.0.13	Normal
bsnStackConfigurationErrorV1	.1.3.6.1.4.1.45.5.2.2.13	Normal
bsnStackManagerReconfiguration	.1.3.6.1.4.1.45.5.2.2.0.4	Normal
bsnStackManagerReconfigurationV1	.1.3.6.1.4.1.45.5.2.2.4	Normal
bsnStackProtection	.1.3.6.1.4.1.45.5.2.2.0.27	Normal
bsnSystemUp365Days	.1.3.6.1.4.1.45.5.2.2.0.20	Normal
bsnTemperatureExceeded	.1.3.6.1.4.1.45.5.2.2.0.17	Normal
bsnTrialLicenseExpiration	.1.3.6.1.4.1.45.5.2.2.0.15	Normal
bsnTrunkPortDisabledToPreventBroadcastStorm	.1.3.6.1.4.1.45.5.2.2.0.8	Normal
bsnTrunkPortDisabledToPreventBroadcastStormV1	.1.3.6.1.4.1.45.5.2.2.8	Normal
bsnTrunkPortEnabledToPreventBroadcastStorm	.1.3.6.1.4.1.45.5.2.2.0.10	Normal
bsnTrunkPortEnabledToPreventBroadcastStormV1	.1.3.6.1.4.1.45.5.2.2.10	Normal
bsnUSBInsertion	.1.3.6.1.4.1.45.5.2.2.0.21	Normal
bsnUSBRemoval	.1.3.6.1.4.1.45.5.2.2.0.22	Normal
bspeIpPhonePowerLimitNotification	.1.3.6.1.4.1.45.5.8.0.2	Normal
bspeIpPhonePowerPriorityNotification	.1.3.6.1.4.1.45.5.8.0.3	Normal
bspePethPsePortCurrentStatusNotification	.1.3.6.1.4.1.45.5.8.0.1	Normal
bspimeNeighborStateChanged	.1.3.6.1.4.1.45.5.27.0.1	Normal
bsRadiusReachabilityServerDown	.1.3.6.1.4.1.45.5.21.0.1	Normal
bsRadiusReachabilityServerUp	.1.3.6.1.4.1.45.5.21.0.2	Normal
bsSourceGuardCannotEnablePort	.1.3.6.1.4.1.45.5.20.0.2	Normal
bsSourceGuardReachedMaxIpEntries	.1.3.6.1.4.1.45.5.20.0.1	Normal
bsStormControlAboveHighWatermark	.1.3.6.1.4.1.45.5.42.0.2	Normal
bsStormControlBelowLowWatermark	.1.3.6.1.4.1.45.5.42.0.1	Normal
bsUnicastStormControlAboveHighWatermark	.1.3.6.1.4.1.45.5.22.0.2	Normal
bsUnicastStormControlBelowLowWatermark	.1.3.6.1.4.1.45.5.22.0.1	Normal
bsveVrrpTrapStateTransition	.1.3.6.1.4.1.45.5.11.0.1	Normal
coldStart	.1.3.6.1.6.3.1.1.5.1	Normal
dvmrpNeighborLoss	.1.3.6.1.3.62.1.1.7.1	Normal
dvmrpNeighborNotPruning	.1.3.6.1.3.62.1.1.7.2	Normal
entConfigChange	.1.3.6.1.2.1.47.2.0.1	Normal
fallingAlarm	.1.3.6.1.2.1.16.0.2	Normal
ipv6IfStateChange	.1.3.6.1.2.1.55.2.0.1	Normal
isisAdjacencyChange	.1.3.6.1.2.1.138.0.17	Normal
isisAreaMismatch	.1.3.6.1.2.1.138.0.12	Normal

Name	OID	Severity
isisAttemptToExceedMaxSequence	.1.3.6.1.2.1.138.0.4	Normal
isisAuthenticationFailure	.1.3.6.1.2.1.138.0.10	Normal
isisAuthenticationTypeFailure	.1.3.6.1.2.1.138.0.9	Normal
isisCorruptedLSPDetected	.1.3.6.1.2.1.138.0.3	Normal
isisDatabaseOverload	.1.3.6.1.2.1.138.0.1	Normal
isisIDLenMismatch	.1.3.6.1.2.1.138.0.5	Normal
isisLSPErrorDetected	.1.3.6.1.2.1.138.0.18	Normal
isisLSPTooLargeToPropagate	.1.3.6.1.2.1.138.0.14	Normal
isisManualAddressDrops	.1.3.6.1.2.1.138.0.2	Normal
isisMaxAreaAddressesMismatch	.1.3.6.1.2.1.138.0.6	Normal
isisOrigLSPBuffSizeMismatch	.1.3.6.1.2.1.138.0.15	Normal
isisOwnLSPPurge	.1.3.6.1.2.1.138.0.7	Normal
isisProtocolsSupportedMismatch	.1.3.6.1.2.1.138.0.16	Normal
isisRejectedAdjacency	.1.3.6.1.2.1.138.0.13	Normal
isisSequenceNumberSkip	.1.3.6.1.2.1.138.0.8	Normal
isisVersionSkew	.1.3.6.1.2.1.138.0.11	Normal
linkDown	.1.3.6.1.6.3.1.1.5.3	Normal
linkUp	.1.3.6.1.6.3.1.1.5.4	Normal
lldpRemTablesChange	.1.0.8802.1.1.2.0.0.1	Normal
lldpXMedTopologyChangeDetected	.1.0.8802.1.1.2.1.5.4795.0.1	Normal
mplsLdpInitSessionThresholdExceeded	.1.3.6.1.2.1.10.166.4.0.1	Normal
mplsLdpPathVectorLimitMismatch	.1.3.6.1.2.1.10.166.4.0.2	Normal
mplsLdpSessionDown	.1.3.6.1.2.1.10.166.4.0.4	Normal
mplsLdpSessionUp	.1.3.6.1.2.1.10.166.4.0.3	Normal
mplsTunnelDown	.1.3.6.1.2.1.10.166.3.0.2	Normal
mplsTunnelReoptimized	.1.3.6.1.2.1.10.166.3.0.4	Normal
mplsTunnelRerouted	.1.3.6.1.2.1.10.166.3.0.3	Normal
mplsTunnelUp	.1.3.6.1.2.1.10.166.3.0.1	Normal
mplsXCDown	.1.3.6.1.2.1.10.166.2.0.2	Normal
mplsXCUp	.1.3.6.1.2.1.10.166.2.0.1	Normal
msdpBackwardTransition	.1.3.6.1.3.92.1.1.0.2	Normal
msdpEstablished	.1.3.6.1.3.92.1.1.0.1	Normal
newRoot	.1.3.6.1.2.1.17.0.1	Normal
nnMstErrorEvent	.1.3.6.1.4.1.45.5.5.0.2	Normal
nnMstGeneralEvent	.1.3.6.1.4.1.45.5.5.0.1	Normal
nnMstNewRoot	.1.3.6.1.4.1.45.5.5.0.3	Normal
nnMstProtocolMigration	.1.3.6.1.4.1.45.5.5.0.5	Normal
nnMstRegionConfigChange	.1.3.6.1.4.1.45.5.5.0.6	Normal
nnMstTopologyChange	.1.3.6.1.4.1.45.5.5.0.4	Normal
nnRstErrorEvent	.1.3.6.1.4.1.45.5.4.0.2	Normal
nnRstGeneralEvent	.1.3.6.1.4.1.45.5.4.0.1	Normal
nnRstNewRoot	.1.3.6.1.4.1.45.5.4.0.3	Normal
nnRstProtocolMigration	.1.3.6.1.4.1.45.5.4.0.5	Normal
nnRstTopologyChange	.1.3.6.1.4.1.45.5.4.0.4	Normal
nsnaClosedConnectionToSnas	.1.3.6.1.4.1.45.5.10.0.1	Normal
nsnaInvalidMessageFromSnas	.1.3.6.1.4.1.45.5.10.0.3	Normal
nsnaStatusQuoIntervalExpired	.1.3.6.1.4.1.45.5.10.0.2	Normal
ntwsAPBootTrap	.1.3.6.1.4.1.45.6.1.5.0.5	Normal
ntwsApManagerChangeTrap	.1.3.6.1.4.1.45.6.1.5.0.63	Normal
ntwsApNonOperStatusTrap	.1.3.6.1.4.1.45.6.1.5.0.37	Normal

Name	OID	Severity
ntwsApNonOperStatusTrap2	.1.3.6.1.4.1.45.6.1.5.0.59	Normal
ntwsApOperRadioStatusTrap	.1.3.6.1.4.1.45.6.1.5.0.38	Normal
ntwsApOperRadioStatusTrap2	.1.3.6.1.4.1.45.6.1.5.0.60	Normal
ntwsApOperRadioStatusTrap3	.1.3.6.1.4.1.45.6.1.5.0.66	Normal
ntwsApRejectLicenseExceededTrap	.1.3.6.1.4.1.45.6.1.5.0.46	Normal
ntwsApTimeoutTrap	.1.3.6.1.4.1.45.6.1.5.0.4	Normal
ntwsAutoTuneRadioChannelChangeTrap	.1.3.6.1.4.1.45.6.1.5.0.19	Normal
ntwsAutoTuneRadioPowerChangeTrap	.1.3.6.1.4.1.45.6.1.5.0.18	Normal
ntwsClientAssociationFailureTrap	.1.3.6.1.4.1.45.6.1.5.0.14	Normal
ntwsClientAssociationSuccessTrap	.1.3.6.1.4.1.45.6.1.5.0.40	Normal
ntwsClientAuthenticationFailureTrap	.1.3.6.1.4.1.45.6.1.5.0.12	Normal
ntwsClientAuthenticationSuccessTrap	.1.3.6.1.4.1.45.6.1.5.0.41	Normal
ntwsClientAuthorizationFailureTrap	.1.3.6.1.4.1.45.6.1.5.0.13	Normal
ntwsClientAuthorizationSuccessTrap	.1.3.6.1.4.1.45.6.1.5.0.15	Normal
ntwsClientAuthorizationSuccessTrap2	.1.3.6.1.4.1.45.6.1.5.0.24	Normal
ntwsClientAuthorizationSuccessTrap3	.1.3.6.1.4.1.45.6.1.5.0.62	Normal
ntwsClientAuthorizationSuccessTrap4	.1.3.6.1.4.1.45.6.1.5.0.67	Normal
ntwsClientClearedTrap	.1.3.6.1.4.1.45.6.1.5.0.23	Normal
ntwsClientClearedTrap2	.1.3.6.1.4.1.45.6.1.5.0.64	Normal
ntwsClientDeAssociationTrap	.1.3.6.1.4.1.45.6.1.5.0.16	Normal
ntwsClientDeAuthenticationTrap	.1.3.6.1.4.1.45.6.1.5.0.42	Normal
ntwsClientDisconnectTrap	.1.3.6.1.4.1.45.6.1.5.0.49	Normal
ntwsClientDot1xFailureTrap	.1.3.6.1.4.1.45.6.1.5.0.22	Normal
ntwsClientDynAuthorChangeFailureTrap	.1.3.6.1.4.1.45.6.1.5.0.48	Normal
ntwsClientDynAuthorChangeSuccessTrap	.1.3.6.1.4.1.45.6.1.5.0.47	Normal
ntwsClientIpAddrChangeTrap	.1.3.6.1.4.1.45.6.1.5.0.39	Normal
ntwsClientRoamingTrap	.1.3.6.1.4.1.45.6.1.5.0.17	Normal
ntwsClusterFailureTrap	.1.3.6.1.4.1.45.6.1.5.0.70	Normal
ntwsConfigurationSavedTrap	.1.3.6.1.4.1.45.6.1.5.0.58	Normal
ntwsCounterMeasureStartTrap	.1.3.6.1.4.1.45.6.1.5.0.20	Normal
ntwsCounterMeasureStopTrap	.1.3.6.1.4.1.45.6.1.5.0.21	Normal
ntwsDAPConnectWarningTrap	.1.3.6.1.4.1.45.6.1.5.0.34	Normal
ntwsDeviceFailTrap	.1.3.6.1.4.1.45.6.1.5.0.1	Normal
ntwsDeviceOkayTrap	.1.3.6.1.4.1.45.6.1.5.0.2	Normal
ntwsMichaelMICFailure	.1.3.6.1.4.1.45.6.1.5.0.61	Normal
ntwsMobilityDomainFailBackTrap	.1.3.6.1.4.1.45.6.1.5.0.51	Normal
ntwsMobilityDomainFailOverTrap	.1.3.6.1.4.1.45.6.1.5.0.50	Normal
ntwsMobilityDomainJoinTrap	.1.3.6.1.4.1.45.6.1.5.0.6	Normal
ntwsMobilityDomainResiliencyStatusTrap	.1.3.6.1.4.1.45.6.1.5.0.65	Normal
ntwsMobilityDomainTimeoutTrap	.1.3.6.1.4.1.45.6.1.5.0.7	Normal
ntwsMpMichaelMICFailure	.1.3.6.1.4.1.45.6.1.5.0.8	Normal
ntwsMpMichaelMICFailure2	.1.3.6.1.4.1.45.6.1.5.0.36	Normal
ntwsPoEFailTrap	.1.3.6.1.4.1.45.6.1.5.0.3	Normal
ntwsRFDetectAdhocUserDisappearTrap	.1.3.6.1.4.1.45.6.1.5.0.45	Normal
ntwsRFDetectAdhocUserTrap	.1.3.6.1.4.1.45.6.1.5.0.10	Normal
ntwsRFDetectBlacklistedTrap	.1.3.6.1.4.1.45.6.1.5.0.43	Normal
ntwsRFDetectClassificationChangeTrap	.1.3.6.1.4.1.45.6.1.5.0.57	Normal
ntwsRFDetectClientViaRogueWiredAPTrap	.1.3.6.1.4.1.45.6.1.5.0.28	Normal
ntwsRFDetectClientViaRogueWiredAPTrap2	.1.3.6.1.4.1.45.6.1.5.0.44	Normal
ntwsRFDetectClientViaRogueWiredAPTrap3	.1.3.6.1.4.1.45.6.1.5.0.56	Normal

Name	OID	Severity
ntwsRFDetectDoSPortTrap	.1.3.6.1.4.1.45.6.1.5.0.35	Normal
ntwsRFDetectDoSTrap	.1.3.6.1.4.1.45.6.1.5.0.27	Normal
ntwsRFDetectInterferingRogueAPTrap	.1.3.6.1.4.1.45.6.1.5.0.29	Normal
ntwsRFDetectInterferingRogueDisappearTrap	.1.3.6.1.4.1.45.6.1.5.0.30	Normal
ntwsRFDetectRogueAPTrap	.1.3.6.1.4.1.45.6.1.5.0.9	Normal
ntwsRFDetectRogueDeviceDisappearTrap	.1.3.6.1.4.1.45.6.1.5.0.53	Normal
ntwsRFDetectRogueDeviceTrap	.1.3.6.1.4.1.45.6.1.5.0.52	Normal
ntwsRFDetectRogueDeviceTrap2	.1.3.6.1.4.1.45.6.1.5.0.68	Normal
ntwsRFDetectRogueDisappearTrap	.1.3.6.1.4.1.45.6.1.5.0.11	Normal
ntwsRFDetectSpoofedMacAPTrap	.1.3.6.1.4.1.45.6.1.5.0.25	Normal
ntwsRFDetectSpoofedSsidAPTrap	.1.3.6.1.4.1.45.6.1.5.0.26	Normal
ntwsRFDetectSuspectDeviceDisappearTrap	.1.3.6.1.4.1.45.6.1.5.0.55	Normal
ntwsRFDetectSuspectDeviceTrap	.1.3.6.1.4.1.45.6.1.5.0.54	Normal
ntwsRFDetectSuspectDeviceTrap2	.1.3.6.1.4.1.45.6.1.5.0.69	Normal
ntwsRFDetectUnAuthorizedAPTrap	.1.3.6.1.4.1.45.6.1.5.0.33	Normal
ntwsRFDetectUnAuthorizedOuiTrap	.1.3.6.1.4.1.45.6.1.5.0.32	Normal
ntwsRFDetectUnAuthorizedSsidTrap	.1.3.6.1.4.1.45.6.1.5.0.31	Normal
ospfIfAuthFailure	.1.3.6.1.2.1.14.16.2.6	Normal
ospfIfConfigError	.1.3.6.1.2.1.14.16.2.4	Normal
ospfIfStateChange	.1.3.6.1.2.1.14.16.2.16	Normal
ospfNbrStateChange	.1.3.6.1.2.1.14.16.2.2	Normal
ospfVirtIfAuthFailure	.1.3.6.1.2.1.14.16.2.7	Normal
ospfVirtIfConfigError	.1.3.6.1.2.1.14.16.2.5	Normal
ospfVirtIfStateChange	.1.3.6.1.2.1.14.16.2.1	Normal
ospfVirtNbrStateChange	.1.3.6.1.2.1.14.16.2.3	Normal
pethMainPowerUsageOffNotification	.1.3.6.1.2.1.10.7.20.2.5	Normal
pethMainPowerUsageOnNotification	.1.3.6.1.2.1.10.7.20.2.4	Normal
pethMainPseBackUpActivatedNotification	.1.3.6.1.2.1.10.7.20.2.3	Normal
pethPsePortOnOffNotification	.1.3.6.1.2.1.10.7.20.2.1	Normal
pethPsePortPowerMaintenanceStatusNotification	.1.3.6.1.2.1.10.7.20.2.2	Normal
pingProbeFailed	.1.3.6.1.2.1.80.0.1	Normal
pingTestCompleted	.1.3.6.1.2.1.80.0.3	Normal
pingTestFailed	.1.3.6.1.2.1.80.0.2	Normal
rc2kAtmPvcLinkStateChange	.1.3.6.1.4.1.2272.1.21.15	Normal
rc2kCardDown	.1.3.6.1.4.1.2272.1.21.11	Normal
rc2kCardUp	.1.3.6.1.4.1.2272.1.21.12	Normal
rc2kTemperature	.1.3.6.1.4.1.2272.1.21.13	Normal
rcAggLinkDown	.1.3.6.1.4.1.2272.1.21.42	Normal
rcAggLinkUp	.1.3.6.1.4.1.2272.1.21.41	Normal
rcBfdTmpSessDown	.1.3.6.1.4.1.2272.1.81.1.0.2	Normal
rcBfdTmpSessUp	.1.3.6.1.4.1.2272.1.81.1.0.1	Normal
rcbgpBackwardTransition	.1.3.6.1.4.1.2272.1.21.40	Normal
rcbgpEstablished	.1.3.6.1.4.1.2272.1.21.39	Normal
rcCardCpldNotUpDate	.1.3.6.1.4.1.2272.1.21.27	Normal
rcCardDown	.1.3.6.1.4.1.2272.1.21.1	Normal
rcCardUp	.1.3.6.1.4.1.2272.1.21.2	Normal
rcChasFanDown	.1.3.6.1.4.1.2272.1.21.7	Normal
rcChasFanUp	.1.3.6.1.4.1.2272.1.21.21	Normal
rcChasPowerSupplyDown	.1.3.6.1.4.1.2272.1.21.6	Normal
rcChasPowerSupplyUp	.1.3.6.1.4.1.2272.1.21.14	Normal

Name	OID	Severity
rcCpLimitShutDown	.1.3.6.1.4.1.2272.1.21.29	Normal
rcDuplexMismatch	.1.3.6.1.4.1.2272.1.21.123	Normal
rcDvmrpIfStateChange	.1.3.6.1.4.1.2272.1.21.47	Normal
rcDvmrpNbrLossChange	.1.3.6.1.4.1.2272.1.21.49	Normal
rcDvmrpNewNbrChange	.1.3.6.1.4.1.2272.1.21.48	Normal
rcEmError	.1.3.6.1.4.1.2272.1.21.23	Normal
rcErrorNotification	.1.3.6.1.4.1.2272.1.21.3	Normal
rcHaCpuState	.1.3.6.1.4.1.2272.1.21.35	Normal
rcIgapLogFileFull	.1.3.6.1.4.1.2272.1.21.28	Normal
rcIgmpLossGroupMember	.1.3.6.1.4.1.2272.1.21.44	Normal
rcIgmpNewGroupMember	.1.3.6.1.4.1.2272.1.21.43	Normal
rcIgmpNewQuerier	.1.3.6.1.4.1.2272.1.21.45	Normal
rcIgmpNewQuerierOnIf	.1.3.6.1.4.1.2272.1.21.121	Normal
rcIgmpQuerierChange	.1.3.6.1.4.1.2272.1.21.46	Normal
rcIgmpQuerierChanged	.1.3.6.1.4.1.2272.1.21.122	Normal
rcInsufficientMemory	.1.3.6.1.4.1.2272.1.21.36	Normal
rcInvalidEsuModIdTrap	.1.3.6.1.4.1.2272.1.21.0.109	Normal
rcIpBgpTmpAfBackwardTransitionNotification	.1.3.6.1.4.1.2272.1.8.101.17.0.4	Normal
rcIpBgpTmpAfEstablishedNotification	.1.3.6.1.4.1.2272.1.8.101.17.0.3	Normal
rcIpBgpTmpBackwardTransNotification	.1.3.6.1.4.1.2272.1.8.101.17.0.2	Normal
rcIpBgpTmpEstablishedNotification	.1.3.6.1.4.1.2272.1.8.101.17.0.1	Normal
rcLinkOscillation	.1.3.6.1.4.1.2272.1.21.8	Normal
rcLoopDetectOnPort	.1.3.6.1.4.1.2272.1.21.38	Normal
rcMacViolation	.1.3.6.1.4.1.2272.1.21.9	Normal
rcMainPowerUsageOff	.1.3.6.1.4.1.2272.1.21.54	Normal
rcMainPowerUsageOn	.1.3.6.1.4.1.2272.1.21.53	Normal
rcMainPseBackupActivate	.1.3.6.1.4.1.2272.1.21.52	Normal
rcMltConfigError	.1.3.6.1.4.1.2272.40.1.21.0.1	Normal
rcn2kAtmPvcLinkStateChange	.1.3.6.1.4.1.2272.1.21.0.15	Normal
rcn2kCardDown	.1.3.6.1.4.1.2272.1.21.0.11	Critical
rcn2kCardDownExpandedTrap	.1.3.6.1.4.1.2272.1.21.0.145	Critical
rcn2kCardNormalTemp	.1.3.6.1.4.1.2272.1.21.0.303	Normal
rcn2kCardOverheat	.1.3.6.1.4.1.2272.1.21.0.300	Minor
rcn2kCardOverheatShutDown	.1.3.6.1.4.1.2272.1.21.0.304	Critical
rcn2kCardShutDownTrap	.1.3.6.1.4.1.2272.1.21.0.298	Critical
rcn2kCardUp	.1.3.6.1.4.1.2272.1.21.0.12	Normal
rcn2kCardUpExpandedTrap	.1.3.6.1.4.1.2272.1.21.0.146	Normal
rcn2kCardZoneNormalTemp	.1.3.6.1.4.1.2272.1.21.0.302	Normal
rcn2kCardZoneOverheat	.1.3.6.1.4.1.2272.1.21.0.301	Minor
rcn2kGbicInsertedTrap	.1.3.6.1.4.1.2272.1.21.0.144	Normal
rcn2kGbicRemovedTrap	.1.3.6.1.4.1.2272.1.21.0.143	Normal
rcn2kLinkDownTrap	.1.3.6.1.4.1.2272.1.21.0.125	Normal
rcn2kLinkUpTrap	.1.3.6.1.4.1.2272.1.21.0.126	Normal
rcn2kQosDropClearTrap	.1.3.6.1.4.1.2272.1.21.0.133	Normal
rcn2kQosDropTrap	.1.3.6.1.4.1.2272.1.21.0.132	Normal
rcn2kTemperature	.1.3.6.1.4.1.2272.1.21.0.13	Critical
rcnaAuthenticationSuccess	.1.3.6.1.4.1.2272.1.21.0.287	Normal
rcnAggLinkDown	.1.3.6.1.4.1.2272.1.21.0.42	Critical
rcnAggLinkStateChange	.1.3.6.1.4.1.2272.1.21.0.182	Normal
rcnAggLinkUp	.1.3.6.1.4.1.2272.1.21.0.41	Normal

Name	OID	Severity
rcnaSshSessionLogin	.1.3.6.1.4.1.2272.1.21.0.288	Normal
rcnaSshSessionLogout	.1.3.6.1.4.1.2272.1.21.0.285	Normal
rcnaSshUnauthorizedAccess	.1.3.6.1.4.1.2272.1.21.0.286	Normal
rcnAuthenticationSuccess	.1.3.6.1.4.1.2272.1.21.0.268	Normal
rcnAutoRecoverLoopDetectedPort	.1.3.6.1.4.1.2272.1.21.0.69	Normal
rcnAutoRecoverPort	.1.3.6.1.4.1.2272.1.21.0.68	Normal
rcnAutoSaveFailed	.1.3.6.1.4.1.2272.1.21.0.258	Normal
rcnBanRingStateChangeTrap	.1.3.6.1.4.1.2272.1.21.0.88	Normal
rcnBfdNewStatusChange	.1.3.6.1.4.1.2272.1.21.0.293	Normal
rcnBfdSessExceedThreshold	.1.3.6.1.4.1.2272.1.21.0.183	Normal
rcnBfdStatusChange	.1.3.6.1.4.1.2272.1.21.0.184	Normal
rcnbgpBackwardTransition	.1.3.6.1.4.1.2272.1.21.0.40	Normal
rcnbgpEstablished	.1.3.6.1.4.1.2272.1.21.0.39	Normal
rcnBpduGuardPortShutdown	.1.3.6.1.4.1.2272.1.21.0.319	Normal
rcnBpduGuardPortShutdownTimerExpired	.1.3.6.1.4.1.2272.1.21.0.320	Normal
rcnBpduReceived	.1.3.6.1.4.1.2272.1.21.0.79	Normal
rcnCardCpldNotUpDate	.1.3.6.1.4.1.2272.1.21.0.27	Normal
rcnCardCpuUtilizationHigh	.1.3.6.1.4.1.2272.1.21.0.276	Critical
rcnCardCpuUtilizationNormal	.1.3.6.1.4.1.2272.1.21.0.277	Normal
rcnCardDown	.1.3.6.1.4.1.2272.1.21.0.1	Critical
rcnCardInsert	.1.3.6.1.4.1.2272.1.21.0.269	Normal
rcnCardNormalTemp	.1.3.6.1.4.1.2272.1.21.0.274	Normal
rcnCardOverheat	.1.3.6.1.4.1.2272.1.21.0.273	Normal
rcnCardOverheatShutDown	.1.3.6.1.4.1.2272.1.21.0.275	Normal
rcnCardRemove	.1.3.6.1.4.1.2272.1.21.0.270	Minor
rcnCardUp	.1.3.6.1.4.1.2272.1.21.0.2	Normal
rcnCfmDHRingEndptClientMepCcmTrap	.1.3.6.1.4.1.2272.1.21.0.166	Normal
rcnCfmDHUniEntptClientMepIftlvTrap	.1.3.6.1.4.1.2272.1.21.0.249	Normal
rcnCfmDualHomeUniClientMepCcmTrap	.1.3.6.1.4.1.2272.1.21.0.211	Normal
rcnCfmEndPointCcmTrap	.1.3.6.1.4.1.2272.1.21.0.87	Normal
rcnCfmEndptClientFdTrap	.1.3.6.1.4.1.2272.1.21.0.138	Normal
rcnCfmEndptClientFdvTrap	.1.3.6.1.4.1.2272.1.21.0.139	Normal
rcnCfmEndptClientFlrFarEndTrap	.1.3.6.1.4.1.2272.1.21.0.187	Normal
rcnCfmEndptClientFlrNearEndTrap	.1.3.6.1.4.1.2272.1.21.0.186	Normal
rcnCfmEndptClientMepCcmExpandedTrap	.1.3.6.1.4.1.2272.1.21.0.129	Normal
rcnCfmEndptClientMepCcmTrap	.1.3.6.1.4.1.2272.1.21.0.101	Normal
rcnCfmEndptClientMepIftlvTrap	.1.3.6.1.4.1.2272.1.21.0.245	Normal
rcnCfmEndptClientMltFdTrap	.1.3.6.1.4.1.2272.1.21.0.222	Normal
rcnCfmEndptClientMltFdvTrap	.1.3.6.1.4.1.2272.1.21.0.223	Normal
rcnCfmEndptClientMltFlrFarEndTrap	.1.3.6.1.4.1.2272.1.21.0.225	Normal
rcnCfmEndptClientMltFlrNearEndTrap	.1.3.6.1.4.1.2272.1.21.0.224	Normal
rcnCfmEndptClientRingFdTrap	.1.3.6.1.4.1.2272.1.21.0.250	Normal
rcnCfmEndptClientRingFdvTrap	.1.3.6.1.4.1.2272.1.21.0.251	Normal
rcnCfmEndptClientRingFlrFarEndTrap	.1.3.6.1.4.1.2272.1.21.0.253	Normal
rcnCfmEndptClientRingFlrNearEndTrap	.1.3.6.1.4.1.2272.1.21.0.252	Normal
rcnCfmEndptClientStandAloneFdTrap	.1.3.6.1.4.1.2272.1.21.0.254	Normal
rcnCfmEndptClientStandAloneFdvTrap	.1.3.6.1.4.1.2272.1.21.0.255	Normal
rcnCfmEndptClientStandAloneFlrFarEndTrap	.1.3.6.1.4.1.2272.1.21.0.257	Normal
rcnCfmEndptClientStandAloneFlrNearEndTrap	.1.3.6.1.4.1.2272.1.21.0.256	Normal
rcnCfmEndptCvidClientMepCcmTrap	.1.3.6.1.4.1.2272.1.21.0.102	Normal

Name	OID	Severity
rcnCfmEndptMepCcmTrap	.1.3.6.1.4.1.2272.1.21.0.100	Normal
rcnCfmFaultAlarm	.1.3.6.1.4.1.2272.1.21.0.212	Normal
rcnCfmMltEndptClientMepCcmTrap	.1.3.6.1.4.1.2272.1.21.0.140	Normal
rcnCfmMltEndptClientMepIftlvTrap	.1.3.6.1.4.1.2272.1.21.0.246	Normal
rcnCfmPortMepCcmExpandedTrap	.1.3.6.1.4.1.2272.1.21.0.127	Normal
rcnCfmPortMepCcmTrap	.1.3.6.1.4.1.2272.1.21.0.98	Normal
rcnCfmRingEndptClientMepCcmTrap	.1.3.6.1.4.1.2272.1.21.0.142	Normal
rcnCfmRingEndptClientMepIftlvTrap	.1.3.6.1.4.1.2272.1.21.0.247	Normal
rcnCfmServiceGroupCcmTrap	.1.3.6.1.4.1.2272.1.21.0.86	Normal
rcnCfmStandEndptClientMepCcmTrap	.1.3.6.1.4.1.2272.1.21.0.159	Normal
rcnCfmStandEndptClientMepIftlvTrap	.1.3.6.1.4.1.2272.1.21.0.248	Normal
rcnCfmTrunkCcmTrap	.1.3.6.1.4.1.2272.1.21.0.85	Normal
rcnCfmTrunkFdTrap	.1.3.6.1.4.1.2272.1.21.0.136	Normal
rcnCfmTrunkFdvTrap	.1.3.6.1.4.1.2272.1.21.0.137	Normal
rcnCfmTrunkFlrFarEndTrap	.1.3.6.1.4.1.2272.1.21.0.135	Normal
rcnCfmTrunkFlrNearEndTrap	.1.3.6.1.4.1.2272.1.21.0.134	Normal
rcnCfmTrunkGroupDownExpandedTrap	.1.3.6.1.4.1.2272.1.21.0.156	Normal
rcnCfmTrunkGroupDownTrap	.1.3.6.1.4.1.2272.1.21.0.96	Normal
rcnCfmTrunkGroupLostProtectionExpandedTrap	.1.3.6.1.4.1.2272.1.21.0.153	Normal
rcnCfmTrunkGroupLostProtectionTrap	.1.3.6.1.4.1.2272.1.21.0.97	Normal
rcnCfmTrunkGroupNewActiveTrunkExpandedTrap	.1.3.6.1.4.1.2272.1.21.0.155	Normal
rcnCfmTrunkGroupNewActiveTrunkTrap	.1.3.6.1.4.1.2272.1.21.0.103	Normal
rcnCfmTrunkGroupRecoverProtectionExpandedTrap	.1.3.6.1.4.1.2272.1.21.0.154	Normal
rcnCfmTrunkGroupRecoverProtectionTrap	.1.3.6.1.4.1.2272.1.21.0.108	Normal
rcnCfmTrunkGroupTrap	.1.3.6.1.4.1.2272.1.21.0.107	Normal
rcnCfmTrunkGroupUpExpandedTrap	.1.3.6.1.4.1.2272.1.21.0.157	Normal
rcnCfmTrunkMepCcmExpandedTrap	.1.3.6.1.4.1.2272.1.21.0.158	Normal
rcnCfmTrunkMepCcmTrap	.1.3.6.1.4.1.2272.1.21.0.106	Normal
rcnCfmVlanMltMepCcmTrap	.1.3.6.1.4.1.2272.1.21.0.141	Normal
rcnCfmVlanNodalMepCcmTrap	.1.3.6.1.4.1.2272.1.21.0.242	Normal
rcnCfmVlanPortMepCcmExpandedTrap	.1.3.6.1.4.1.2272.1.21.0.128	Normal
rcnCfmVlanPortMepCcmTrap	.1.3.6.1.4.1.2272.1.21.0.99	Normal
rcnChasCoolingInsufficientTrap	.1.3.6.1.4.1.2272.1.21.0.190	Normal
rcnChasCoolingSufficientTrap	.1.3.6.1.4.1.2272.1.21.0.191	Normal
rcnChasFanCoolingLow	.1.3.6.1.4.1.2272.1.21.0.196	Critical
rcnChasFanDown	.1.3.6.1.4.1.2272.1.21.0.7	Critical
rcnChasFanFail	.1.3.6.1.4.1.2272.1.21.0.271	Normal
rcnChasFanOk	.1.3.6.1.4.1.2272.1.21.0.272	Normal
rcnChasFanUp	.1.3.6.1.4.1.2272.1.21.0.21	Normal
rcnChasPowerSupplyDown	.1.3.6.1.4.1.2272.1.21.0.6	Critical
rcnChasPowerSupplyNoRedundancy	.1.3.6.1.4.1.2272.1.21.0.167	Critical
rcnChasPowerSupplyOppositeAirflowClearTrap	.1.3.6.1.4.1.2272.1.21.0.354	Normal
rcnChasPowerSupplyOppositeAirflowDetectedTrap	.1.3.6.1.4.1.2272.1.21.0.353	Normal
rcnChasPowerSupplyRedundancy	.1.3.6.1.4.1.2272.1.21.0.168	Normal
rcnChasPowerSupplyRunningLow	.1.3.6.1.4.1.2272.1.21.0.185	Critical
rcnChasPowerSupplyRunningNormal	.1.3.6.1.4.1.2272.1.21.0.340	Normal
rcnChasPowerSupplyUp	.1.3.6.1.4.1.2272.1.21.0.14	Normal
rcnCpLimitShutDown	.1.3.6.1.4.1.2272.1.21.0.29	Normal
rcnCSUCardResetEndTrap	.1.3.6.1.4.1.2272.1.21.0.150	Normal
rcnCSUCardResetStartTrap	.1.3.6.1.4.1.2272.1.21.0.149	Normal

Name	OID	Severity
rcnCSUEndTrap	.1.3.6.1.4.1.2272.1.21.0.148	Normal
rcnCSUInProgressTrap	.1.3.6.1.4.1.2272.1.21.0.151	Normal
rcnCSUStartTrap	.1.3.6.1.4.1.2272.1.21.0.147	Normal
rcnCtrlPktRateLimitDropClearTrap	.1.3.6.1.4.1.2272.1.21.0.234	Normal
rcnCtrlPktRateLimitDropTrap	.1.3.6.1.4.1.2272.1.21.0.233	Normal
rcnCtrlPktRateLimitShutdownClearTrap	.1.3.6.1.4.1.2272.1.21.0.236	Normal
rcnCtrlPktRateLimitShutdownTrap	.1.3.6.1.4.1.2272.1.21.0.235	Normal
rcnDigitalCertStatusTrap	.1.3.6.1.4.1.2272.1.21.0.336	Normal
rcnDNSRequestResponse	.1.3.6.1.4.1.2272.1.21.0.62	Normal
rcnDNSv6RequestResponseTrap	.1.3.6.1.4.1.2272.1.21.0.307	Normal
rcnDuplexMismatch	.1.3.6.1.4.1.2272.1.21.0.123	Normal
rcnDuplicateIpAddress	.1.3.6.1.4.1.2272.1.21.0.63	Normal
rcnDvmrpIfStateChange	.1.3.6.1.4.1.2272.1.21.0.47	Normal
rcnDvmrpNbrLossChange	.1.3.6.1.4.1.2272.1.21.0.49	Normal
rcnDvmrpNewNbrChange	.1.3.6.1.4.1.2272.1.21.0.48	Normal
rcnDvrVistPeerDomainMismatchErrorClearTrap	.1.3.6.1.4.1.2272.1.21.0.342	Normal
rcnDvrVistPeerDomainMismatchErrorTrap	.1.3.6.1.4.1.2272.1.21.0.341	Normal
rcnEapMacIntrusion	.1.3.6.1.4.1.2272.1.21.0.83	Normal
rcnEgrAggregateCirRateLimitDropClearTrap	.1.3.6.1.4.1.2272.1.21.0.260	Normal
rcnEgrAggregateCirRateLimitDropTrap	.1.3.6.1.4.1.2272.1.21.0.259	Normal
rcnEgrAggregatePirRateLimitDropClearTrap	.1.3.6.1.4.1.2272.1.21.0.262	Normal
rcnEgrAggregatePirRateLimitDropTrap	.1.3.6.1.4.1.2272.1.21.0.261	Normal
rcnEmError	.1.3.6.1.4.1.2272.1.21.0.23	Critical
rcnErrorNotification	.1.3.6.1.4.1.2272.1.21.0.3	Critical
rcnExtCpLimitShutDown	.1.3.6.1.4.1.2272.1.21.0.70	Normal
rcnExtCpLimitShutDownNormal	.1.3.6.1.4.1.2272.1.21.0.82	Normal
rcnExtCpLimitSopCongestion	.1.3.6.1.4.1.2272.1.21.0.71	Normal
rcnFabricDropTrap	.1.3.6.1.4.1.2272.1.21.0.198	Normal
rcnFdbProtectViolation	.1.3.6.1.4.1.2272.1.21.0.59	Normal
rcnFOQDropTrap	.1.3.6.1.4.1.2272.1.21.0.197	Normal
rcnHaCpuState	.1.3.6.1.4.1.2272.1.21.0.35	Normal
rcnHighCopUtil	.1.3.6.1.4.1.2272.1.21.0.210	Normal
rcnIgapLogFileFull	.1.3.6.1.4.1.2272.1.21.0.28	Normal
rcnIgmpLossGroupMember	.1.3.6.1.4.1.2272.1.21.0.44	Normal
rcnIgmpNewGroupMember	.1.3.6.1.4.1.2272.1.21.0.43	Normal
rcnIgmpNewQuerier	.1.3.6.1.4.1.2272.1.21.0.45	Normal
rcnIgmpNewQuerierOnIf	.1.3.6.1.4.1.2272.1.21.0.121	Normal
rcnIgmpQuerierChange	.1.3.6.1.4.1.2272.1.21.0.46	Normal
rcnIgmpQuerierChanged	.1.3.6.1.4.1.2272.1.21.0.122	Normal
rcnIngAggregateCirRateLimitDropClearTrap	.1.3.6.1.4.1.2272.1.21.0.238	Normal
rcnIngAggregateCirRateLimitDropTrap	.1.3.6.1.4.1.2272.1.21.0.237	Normal
rcnIngAggregatePirRateLimitDropClearTrap	.1.3.6.1.4.1.2272.1.21.0.240	Normal
rcnIngAggregatePirRateLimitDropTrap	.1.3.6.1.4.1.2272.1.21.0.239	Normal
rcnInsufficientMemory	.1.3.6.1.4.1.2272.1.21.0.36	Normal
rcnInterCpuCommStatus	.1.3.6.1.4.1.2272.1.21.0.84	Normal
rcnIpv6FhsSnoopTableFullTrap	.1.3.6.1.4.1.2272.1.21.0.321	Normal
rcnIpv6MaxRouteDropClear	.1.3.6.1.4.1.2272.1.21.0.349	Normal
rcnIpv6MaxRouteDropSet	.1.3.6.1.4.1.2272.1.21.0.350	Normal
rcnIpv6MaxRouteWarnClear	.1.3.6.1.4.1.2272.1.21.0.347	Normal
rcnIpv6MaxRouteWarnSet	.1.3.6.1.4.1.2272.1.21.0.348	Normal

Name	OID	Severity
rcnIsisPlsbAdjStateTrap	.1.3.6.1.4.1.2272.1.21.0.281	Normal
rcnIsisPlsbBvidMismatchTrap	.1.3.6.1.4.1.2272.1.21.0.278	Normal
rcnIsisPlsbDuplicateNicknameTrap	.1.3.6.1.4.1.2272.1.21.0.195	Normal
rcnIsisPlsbDuplicateNnameTrap	.1.3.6.1.4.1.2272.1.21.0.282	Normal
rcnIsisPlsbDuplicateSysidTrap	.1.3.6.1.4.1.2272.1.21.0.193	Normal
rcnIsisPlsbGlobalDuplicateNnameTrap	.1.3.6.1.4.1.2272.1.21.0.316	Normal
rcnIsisPlsbGlobalDuplicateSysidTrap	.1.3.6.1.4.1.2272.1.21.0.312	Normal
rcnIsisPlsbIsisEnabledWithZeroNicknameTrap	.1.3.6.1.4.1.2272.1.21.0.351	Normal
rcnIsisPlsbLocalDuplicateNnameTrap	.1.3.6.1.4.1.2272.1.21.0.315	Normal
rcnIsisPlsbLsdbUpdateTrap	.1.3.6.1.4.1.2272.1.21.0.194	Normal
rcnIsisPlsbMetricMismatchTrap	.1.3.6.1.4.1.2272.1.21.0.192	Normal
rcnIsisPlsbMultiLinkAdjTrap	.1.3.6.1.4.1.2272.1.21.0.284	Normal
rcnIsisPlsbSmltPeerBmacMismatchTrap	.1.3.6.1.4.1.2272.1.21.0.280	Normal
rcnIsisPlsbSmltSplitBebMismatchTrap	.1.3.6.1.4.1.2272.1.21.0.283	Normal
rcnIsisPlsbSmltVirtBmacMismatchTrap	.1.3.6.1.4.1.2272.1.21.0.279	Normal
rcnIsisSpbmSmltVirtBmacMisconfigTrap	.1.3.6.1.4.1.2272.1.21.0.305	Normal
rcnLacpMisconfigTrap	.1.3.6.1.4.1.2272.1.21.0.294	Normal
rcnLacpNegotiated	.1.3.6.1.4.1.2272.1.21.0.231	Normal
rcnLacpNotNegotiated	.1.3.6.1.4.1.2272.1.21.0.232	Normal
rcnLegacyCardDetected	.1.3.6.1.4.1.2272.1.21.0.265	Normal
rcnLicenseDowngraded	.1.3.6.1.4.1.2272.1.21.0.339	Normal
rcnLicenseExpired	.1.3.6.1.4.1.2272.1.21.0.324	Normal
rcnLicenseNotGranted	.1.3.6.1.4.1.2272.1.21.0.337	Normal
rcnLicenseNotLoaded	.1.3.6.1.4.1.2272.1.21.0.338	Normal
rcnLicenseTrialPeriodExpired	.1.3.6.1.4.1.2272.1.21.0.171	Normal
rcnLicenseTrialPeriodExpiry	.1.3.6.1.4.1.2272.1.21.0.172	Normal
rcnLicenseWillExpire	.1.3.6.1.4.1.2272.1.21.0.323	Normal
rcnLinkBadConnection	.1.3.6.1.4.1.2272.1.21.0.162	Normal
rcnLinkOamRemoteCriticalEventTrap	.1.3.6.1.4.1.2272.1.21.0.216	Normal
rcnLinkOamRemoteDiscoveryFailureTrap	.1.3.6.1.4.1.2272.1.21.0.219	Normal
rcnLinkOamRemoteDiscoveryTrap	.1.3.6.1.4.1.2272.1.21.0.243	Normal
rcnLinkOamRemoteDyingGaspTrap	.1.3.6.1.4.1.2272.1.21.0.263	Normal
rcnLinkOamRemoteLinkFaultTrap	.1.3.6.1.4.1.2272.1.21.0.264	Normal
rcnLinkOamRemoteLinkHeartbeatFailureTrap	.1.3.6.1.4.1.2272.1.21.0.221	Normal
rcnLinkOamRemoteLoopbackActiveTrap	.1.3.6.1.4.1.2272.1.21.0.217	Normal
rcnLinkOamRemoteLoopbackFailureTrap	.1.3.6.1.4.1.2272.1.21.0.218	Normal
rcnLinkOamRemoteLoopbackTerminateFailureTrap	.1.3.6.1.4.1.2272.1.21.0.227	Normal
rcnLinkOamRemoteLoopbackTerminateSucceedTrap	.1.3.6.1.4.1.2272.1.21.0.226	Normal
rcnLinkOscillation	.1.3.6.1.4.1.2272.1.21.0.8	Normal
rcnLockupDetected	.1.3.6.1.4.1.2272.1.21.0.201	Normal
rcnLogMsgControl	.1.3.6.1.4.1.2272.1.21.0.60	Normal
rcnLoopDetectMacDiscard	.1.3.6.1.4.1.2272.1.21.0.67	Normal
rcnLoopDetectOnPort	.1.3.6.1.4.1.2272.1.21.0.38	Normal
rcnLoopDetectPortDown	.1.3.6.1.4.1.2272.1.21.0.64	Normal
rcnMacResetForLockup	.1.3.6.1.4.1.2272.1.21.0.202	Normal
rcnMacViolation	.1.3.6.1.4.1.2272.1.21.0.9	Normal
rcnMainPowerUsageOff	.1.3.6.1.4.1.2272.1.21.0.54	Normal
rcnMainPowerUsageOn	.1.3.6.1.4.1.2272.1.21.0.53	Normal
rcnMainPseBackupActivate	.1.3.6.1.4.1.2272.1.21.0.52	Normal
rcnMaxMrouteDropClear	.1.3.6.1.4.1.2272.1.21.0.181	Normal

Name	OID	Severity
rcnMaxMrouteDropSet	.1.3.6.1.4.1.2272.1.21.0.179	Normal
rcnMaxMrouteWarnClear	.1.3.6.1.4.1.2272.1.21.0.180	Normal
rcnMaxMrouteWarnSet	.1.3.6.1.4.1.2272.1.21.0.178	Normal
rcnMaxRouteDropClear	.1.3.6.1.4.1.2272.1.21.0.112	Normal
rcnMaxRouteDropSet	.1.3.6.1.4.1.2272.1.21.0.113	Normal
rcnMaxRouteWarnClear	.1.3.6.1.4.1.2272.1.21.0.110	Normal
rcnMaxRouteWarnSet	.1.3.6.1.4.1.2272.1.21.0.111	Normal
rcnMcEgRecMoreThanThreshold	.1.3.6.1.4.1.2272.1.21.0.164	Normal
rcnMcInRecMoreThanThreshold	.1.3.6.1.4.1.2272.1.21.0.163	Normal
rcnMldLossGroupMemberTrap	.1.3.6.1.4.1.2272.1.21.0.309	Normal
rcnMldNewGroupMemberTrap	.1.3.6.1.4.1.2272.1.21.0.308	Normal
rcnMldNewQuerierTrap	.1.3.6.1.4.1.2272.1.21.0.310	Normal
rcnMldQuerierChangeTrap	.1.3.6.1.4.1.2272.1.21.0.311	Normal
rcnMltLinkDown	.1.3.6.1.4.1.2272.1.21.0.161	Normal
rcnMltLinkUp	.1.3.6.1.4.1.2272.1.21.0.160	Normal
rcnModuleFatalError	.1.3.6.1.4.1.2272.1.21.0.204	Normal
rcnModuleResetForLockup	.1.3.6.1.4.1.2272.1.21.0.203	Normal
rcnMrouteEgressThresholdExceeded	.1.3.6.1.4.1.2272.1.21.0.176	Normal
rcnMrouteIngressThresholdExceeded	.1.3.6.1.4.1.2272.1.21.0.175	Normal
rcnMRouteIpv6EgressThresholdExceeded	.1.3.6.1.4.1.2272.1.21.0.314	Normal
rcnMRouteIpv6IngressThresholdExceeded	.1.3.6.1.4.1.2272.1.21.0.313	Normal
rcnMsdpBackwardTransition	.1.3.6.1.4.1.2272.1.80.1.0.10	Normal
rcnMsdpBackwardTransitionTrap	.1.3.6.1.4.1.2272.1.21.0.334	Normal
rcnMsdpEstablished	.1.3.6.1.4.1.2272.1.80.1.0.9	Normal
rcnMsdpEstablishedTrap	.1.3.6.1.4.1.2272.1.21.0.333	Normal
rcnMsdpMaxPeerSACacheErrorClear	.1.3.6.1.4.1.2272.1.80.1.0.8	Normal
rcnMsdpMaxPeerSACacheErrorClearTrap	.1.3.6.1.4.1.2272.1.21.0.332	Normal
rcnMsdpMaxPeerSACacheErrorSet	.1.3.6.1.4.1.2272.1.80.1.0.7	Normal
rcnMsdpMaxPeerSACacheErrorSetTrap	.1.3.6.1.4.1.2272.1.21.0.331	Normal
rcnMsdpMaxPeerSACacheWarnClear	.1.3.6.1.4.1.2272.1.80.1.0.6	Normal
rcnMsdpMaxPeerSACacheWarnClearTrap	.1.3.6.1.4.1.2272.1.21.0.330	Normal
rcnMsdpMaxPeerSACacheWarnSet	.1.3.6.1.4.1.2272.1.80.1.0.5	Normal
rcnMsdpMaxPeerSACacheWarnSetTrap	.1.3.6.1.4.1.2272.1.21.0.329	Normal
rcnMsdpMaxSACacheErrorClear	.1.3.6.1.4.1.2272.1.80.1.0.4	Normal
rcnMsdpMaxSACacheErrorClearTrap	.1.3.6.1.4.1.2272.1.21.0.328	Normal
rcnMsdpMaxSACacheErrorSet	.1.3.6.1.4.1.2272.1.80.1.0.3	Normal
rcnMsdpMaxSACacheErrorSetTrap	.1.3.6.1.4.1.2272.1.21.0.327	Normal
rcnMsdpMaxSACacheWarnClear	.1.3.6.1.4.1.2272.1.80.1.0.2	Normal
rcnMsdpMaxSACacheWarnClearTrap	.1.3.6.1.4.1.2272.1.21.0.326	Normal
rcnMsdpMaxSACacheWarnSet	.1.3.6.1.4.1.2272.1.80.1.0.1	Normal
rcnMsdpMaxSACacheWarnSetTrap	.1.3.6.1.4.1.2272.1.21.0.325	Normal
rcnMstpNewCistRegionalRoot	.1.3.6.1.4.1.2272.1.21.0.119	Normal
rcnMstpNewCistRoot	.1.3.6.1.4.1.2272.1.21.0.117	Normal
rcnMstpNewMstiRoot	.1.3.6.1.4.1.2272.1.21.0.118	Normal
rcnNonEapIntrusion	.1.3.6.1.4.1.2272.1.21.0.72	Normal
rcnPasswordChange	.1.3.6.1.4.1.2272.1.21.0.22	Normal
rcnPbtUnknownDiscardClearTrap	.1.3.6.1.4.1.2272.1.21.0.131	Normal
rcnPbtUnknownDiscardTrap	.1.3.6.1.4.1.2272.1.21.0.130	Normal
rcnPcmciaCardRemoved	.1.3.6.1.4.1.2272.1.21.0.25	Critical
rcnPimMaxInterfaceWarnSet	.1.3.6.1.4.1.2272.1.21.0.213	Normal

Name	OID	Severity
rcnPimMaxNeighborsWarnSet	.1.3.6.1.4.1.2272.1.21.0.214	Normal
rcnPimMaxPassiveInterfaceWarnSet	.1.3.6.1.4.1.2272.1.21.0.215	Normal
rcnPlugModInsertedInNotRecommendedPortTrap	.1.3.6.1.4.1.2272.1.21.0.317	Normal
rcnPlugModRemovedFromNotRecommendedPortTrap	.1.3.6.1.4.1.2272.1.21.0.318	Normal
rcnPortAdminStatusChangeTrap	.1.3.6.1.4.1.2272.1.21.0.169	Normal
rcnPortChannelizedStateChangeTrap	.1.3.6.1.4.1.2272.1.21.0.306	Normal
rcnPrFilterRspMemoryFull	.1.3.6.1.4.1.2272.1.21.0.266	Normal
rcnPrFilterStatsCntExst	.1.3.6.1.4.1.2272.1.21.0.267	Normal
rcnPseCardOnOff	.1.3.6.1.4.1.2272.1.21.0.55	Normal
rcnPsePortOnOff	.1.3.6.1.4.1.2272.1.21.0.50	Normal
rcnPsePortPowerMaintenanceStatus	.1.3.6.1.4.1.2272.1.21.0.51	Normal
rcnRadiusEapRAVError	.1.3.6.1.4.1.2272.1.21.0.344	Normal
rcnRadiusEapServersDown	.1.3.6.1.4.1.2272.1.21.0.345	Normal
rcnRadiusEapServerUp	.1.3.6.1.4.1.2272.1.21.0.346	Normal
rcnRemoteMirroringStatus	.1.3.6.1.4.1.2272.1.21.0.177	Normal
rcnRestConfServerOperationStatusTrap	.1.3.6.1.4.1.2272.1.21.0.352	Normal
rcnRSlotFabricActiveTrap	.1.3.6.1.4.1.2272.1.21.0.199	Normal
rcnRSlotFabricInactiveTrap	.1.3.6.1.4.1.2272.1.21.0.200	Normal
rcnRsmltEdgePeerModified	.1.3.6.1.4.1.2272.1.21.0.124	Normal
rcnRstpNewRoot	.1.3.6.1.4.1.2272.1.21.0.120	Normal
rcnSaveConfigAction	.1.3.6.1.4.1.2272.1.21.0.37	Normal
rcnSaveConfigFailTrap	.1.3.6.1.4.1.2272.1.21.0.170	Normal
rcnSaveConfigFile	.1.3.6.1.4.1.2272.1.21.0.61	Normal
rcnSlotPowerAvailableTrap	.1.3.6.1.4.1.2272.1.21.0.295	Normal
rcnSlppGuardHoldDownExpired	.1.3.6.1.4.1.2272.1.64.1.0.4	Normal
rcnSlppGuardPacketReceived	.1.3.6.1.4.1.2272.1.64.1.0.5	Normal
rcnSlppLoopOnDiffVlan	.1.3.6.1.4.1.2272.1.64.1.0.3	Normal
rcnSlppPortDownEvent	.1.3.6.1.4.1.2272.1.64.1.0.1	Normal
rcnSlppPortDownEventNew	.1.3.6.1.4.1.2272.1.64.1.0.2	Normal
rcnSmartCpldTimerFired	.1.3.6.1.4.1.2272.1.21.0.26	Normal
rcnSmltIstLinkDown	.1.3.6.1.4.1.2272.1.21.0.18	Critical
rcnSmltIstLinkUp	.1.3.6.1.4.1.2272.1.21.0.17	Normal
rcnSmltLinkDown	.1.3.6.1.4.1.2272.1.21.0.20	Critical
rcnSmltLinkUp	.1.3.6.1.4.1.2272.1.21.0.19	Normal
rcnSmpFtpFail	.1.3.6.1.4.1.2272.1.21.0.205	Normal
rcnSmpLogFileDeleted	.1.3.6.1.4.1.2272.1.21.0.206	Normal
rcnSonetTrap	.1.3.6.1.4.1.2272.1.21.0.10	Normal
rcnSshServerDisabled	.1.3.6.1.4.1.2272.1.21.0.31	Normal
rcnSshServerEnabled	.1.3.6.1.4.1.2272.1.21.0.30	Normal
rcnSshSessionLogin	.1.3.6.1.4.1.2272.1.21.0.32	Normal
rcnSshSessionLogout	.1.3.6.1.4.1.2272.1.21.0.33	Normal
rcnSshUnauthorizedAccess	.1.3.6.1.4.1.2272.1.21.0.34	Normal
rcnStpNewRoot	.1.3.6.1.4.1.2272.1.21.0.4	Normal
rcnStpTCN	.1.3.6.1.4.1.2272.1.21.0.16	Normal
rcnStpTopologyChange	.1.3.6.1.4.1.2272.1.21.0.5	Normal
rcnSystemUsbInternalAccessErrorTrap	.1.3.6.1.4.1.2272.1.21.0.335	Normal
rcnTacacsAuthFailure	.1.3.6.1.4.1.2272.1.21.0.74	Normal
rcnTacacsClientFailure	.1.3.6.1.4.1.2272.1.21.0.78	Normal
rcnTacacsExceededMaxLogins	.1.3.6.1.4.1.2272.1.21.0.77	Normal
rcnTacacsNoServers	.1.3.6.1.4.1.2272.1.21.0.75	Normal

Name	OID	Severity
rcnTacacsRxUnsupportedFrame	.1.3.6.1.4.1.2272.1.21.0.76	Normal
rcnTdcTestResultTrap	.1.3.6.1.4.1.2272.1.21.0.57	Normal
rcnTdcTestRttExceedTrap	.1.3.6.1.4.1.2272.1.21.0.58	Normal
rcnTlsIpServiceWatermarkTrap	.1.3.6.1.4.1.2272.1.21.0.152	Normal
rcnTlsPortWatermarkTrap	.1.3.6.1.4.1.2272.1.21.0.66	Normal
rcnTlsUniIpServiceWatermarkTrap	.1.3.6.1.4.1.2272.1.21.0.73	Normal
rcnTlsWatermarkTrap	.1.3.6.1.4.1.2272.1.21.0.56	Normal
rcnTmuxParityError	.1.3.6.1.4.1.2272.1.21.0.165	Normal
rcnTosBufferClearTrap	.1.3.6.1.4.1.2272.1.21.0.189	Normal
rcnTosBufferLimitTrap	.1.3.6.1.4.1.2272.1.21.0.188	Normal
rcnTrialPeriodExpired	.1.3.6.1.4.1.2272.1.21.0.114	Normal
rcnUnauthorizedAccessToStandByCPU	.1.3.6.1.4.1.2272.1.21.0.65	Normal
rcnUpgradeFailure	.1.3.6.1.4.1.2272.1.21.0.208	Normal
rcnUpgradeSuccessful	.1.3.6.1.4.1.2272.1.21.0.207	Normal
rcnUpgradeSuccessfulAckRequired	.1.3.6.1.4.1.2272.1.21.0.228	Normal
rcnVersionMisMatch	.1.3.6.1.4.1.2272.1.21.0.209	Normal
rcnVLacpFlapDetectShutDown	.1.3.6.1.4.1.2272.1.21.0.289	Normal
rcnVlacpPortDown	.1.3.6.1.4.1.2272.1.21.0.80	Normal
rcnVlacpPortUp	.1.3.6.1.4.1.2272.1.21.0.81	Normal
rcnVpnTrap	.1.3.6.1.4.1.2272.1.21.0.24	Normal
rcnVrfDown	.1.3.6.1.4.1.2272.1.21.0.174	Normal
rcnVrfForwardingDisabled	.1.3.6.1.4.1.2272.1.21.0.116	Normal
rcnVrfForwardingEnabled	.1.3.6.1.4.1.2272.1.21.0.115	Normal
rcnVrfUp	.1.3.6.1.4.1.2272.1.21.0.173	Normal
rcnWlanTrap	.1.3.6.1.4.1.2272.1.21.0.290	Normal
rcPasswordChange	.1.3.6.1.4.1.2272.1.21.22	Normal
rcPcmciaCardRemoved	.1.3.6.1.4.1.2272.1.21.25	Normal
rcPlugOptModAux1StatusTrap	.1.3.6.1.4.1.2272.1.21.0.94	Normal
rcPlugOptModAux2StatusTrap	.1.3.6.1.4.1.2272.1.21.0.95	Normal
rcPlugOptModBiasStatusTrap	.1.3.6.1.4.1.2272.1.21.0.91	Normal
rcPlugOptModRxPowerStatusTrap	.1.3.6.1.4.1.2272.1.21.0.93	Normal
rcPlugOptModTemperatureStatusTrap	.1.3.6.1.4.1.2272.1.21.0.89	Normal
rcPlugOptModTxPowerStatusTrap	.1.3.6.1.4.1.2272.1.21.0.92	Normal
rcPlugOptModVoltageStatusTrap	.1.3.6.1.4.1.2272.1.21.0.90	Normal
rcPseCardOnOff	.1.3.6.1.4.1.2272.1.21.55	Normal
rcPsePortOnOff	.1.3.6.1.4.1.2272.1.21.50	Normal
rcPsePortPowerMaintenanceStatus	.1.3.6.1.4.1.2272.1.21.51	Normal
rcSaveConfigAction	.1.3.6.1.4.1.2272.1.21.37	Normal
rcSmartCpldTimerFired	.1.3.6.1.4.1.2272.1.21.26	Normal
rcSmltIstLinkDown	.1.3.6.1.4.1.2272.1.21.18	Normal
rcSmltIstLinkUp	.1.3.6.1.4.1.2272.1.21.17	Normal
rcSmltLinkDown	.1.3.6.1.4.1.2272.1.21.20	Normal
rcSmltLinkUp	.1.3.6.1.4.1.2272.1.21.19	Normal
rcSonetTrap	.1.3.6.1.4.1.2272.1.21.10	Normal
rcSshServerDisabled	.1.3.6.1.4.1.2272.1.21.31	Normal
rcSshServerEnabled	.1.3.6.1.4.1.2272.1.21.30	Normal
rcSshSessionLogin	.1.3.6.1.4.1.2272.1.21.32	Normal
rcSshSessionLogout	.1.3.6.1.4.1.2272.1.21.33	Normal
rcSshUnauthorizedAccess	.1.3.6.1.4.1.2272.1.21.34	Normal
rcStpNewRoot	.1.3.6.1.4.1.2272.1.21.4	Normal

Name	OID	Severity
rcStpTCN	.1.3.6.1.4.1.2272.1.21.16	Normal
rcStpTopologyChange	.1.3.6.1.4.1.2272.1.21.5	Normal
rcTdcTestResultTrap	.1.3.6.1.4.1.2272.1.21.57	Normal
rcTdcTestRttExceedTrap	.1.3.6.1.4.1.2272.1.21.58	Normal
rcTlsBackupTunnelSelectedTrap	.1.3.6.1.4.1.2272.1.200.1.2	Normal
rcTlsIsidWatermarkTrap	.1.3.6.1.4.1.2272.1.21.0.105	Normal
rcTlsTdiWatermarkTrap	.1.3.6.1.4.1.2272.1.21.0.104	Normal
rcTlsTunnelChangeTrap	.1.3.6.1.4.1.2272.1.200.1.1	Normal
rcTlsWatermarkTrap	.1.3.6.1.4.1.2272.1.21.56	Normal
rcVpnTrap	.1.3.6.1.4.1.2272.1.21.24	Normal
rcVrrpExtTrapStateTransition	.1.3.6.1.4.1.2272.1.206.2.2.1	Normal
rcVrrpTmpTrapNewMaster	.1.3.6.1.4.1.2272.1.206.1.0.1	Normal
rcVrrpTmpTrapProtoError	.1.3.6.1.4.1.2272.1.206.1.0.3	Normal
rcVrrpTrapStateTransition	.1.3.6.1.4.1.2272.1.73.1.2.1	Normal
risingAlarm	.1.3.6.1.2.1.16.0.1	Normal
s5CtrFanDirectionError	.1.3.6.1.4.1.45.1.6.2.4.0.6	Normal
s5CtrFanRotationError	.1.3.6.1.4.1.45.1.6.2.4.0.5	Normal
s5CtrHighTemperatureError	.1.3.6.1.4.1.45.1.6.2.4.0.7	Normal
s5CtrHotSwap	.1.3.6.1.4.1.45.1.6.2.4.1	Normal
s5CtrNewHotSwap	.1.3.6.1.4.1.45.1.6.2.4.0.1	Normal
s5CtrNewProblem	.1.3.6.1.4.1.45.1.6.2.4.0.2	Normal
s5CtrNewUnitDown	.1.3.6.1.4.1.45.1.6.2.4.0.4	Normal
s5CtrNewUnitUp	.1.3.6.1.4.1.45.1.6.2.4.0.3	Normal
s5CtrProblem	.1.3.6.1.4.1.45.1.6.2.4.2	Normal
s5CtrUnitDown	.1.3.6.1.4.1.45.1.6.2.4.4	Normal
s5CtrUnitUp	.1.3.6.1.4.1.45.1.6.2.4.3	Normal
s5EtrMacAddressTablesThresholdReached	.1.3.6.1.4.1.45.1.6.2.1.0.12	Normal
s5EtrMgmAccessViolation	.1.3.6.1.4.1.45.1.6.2.1.6	Normal
s5EtrNewMgmAccessViolation	.1.3.6.1.4.1.45.1.6.2.1.0.6	Normal
s5EtrNewPortAutoPart	.1.3.6.1.4.1.45.1.6.2.1.0.8	Normal
s5EtrNewPortDteJabbering	.1.3.6.1.4.1.45.1.6.2.1.0.9	Normal
s5EtrNewPortManualPart	.1.3.6.1.4.1.45.1.6.2.1.0.7	Normal
s5EtrNewRedBadRemCfgDetected	.1.3.6.1.4.1.45.1.6.2.1.0.11	Normal
s5EtrNewRedPortFailure	.1.3.6.1.4.1.45.1.6.2.1.0.10	Normal
s5EtrNewSbsMacAccessViolation	.1.3.6.1.4.1.45.1.6.2.1.0.5	Normal
s5EtrPortAutoPart	.1.3.6.1.4.1.45.1.6.2.1.1	Normal
s5EtrPortDteJabbering	.1.3.6.1.4.1.45.1.6.2.1.2	Normal
s5EtrPortManualPart	.1.3.6.1.4.1.45.1.6.2.1.7	Normal
s5EtrRedBadRemCfgDetected	.1.3.6.1.4.1.45.1.6.2.1.4	Normal
s5EtrRedPortFailure	.1.3.6.1.4.1.45.1.6.2.1.3	Normal
s5EtrSbsMacAccessViolation	.1.3.6.1.4.1.45.1.6.2.1.5	Normal
s5EtrSbsMacRemoved	.1.3.6.1.4.1.45.1.6.2.1.0.4	Normal
s5EtrSbsMacTableCleared	.1.3.6.1.4.1.45.1.6.2.1.0.3	Normal
s5EtrSbsMacTableClearedForPort	.1.3.6.1.4.1.45.1.6.2.1.0.2	Normal
s5EtrSbsMacTableFull	.1.3.6.1.4.1.45.1.6.2.1.0.1	Normal
slaMonitorAgentExceptionDetected	.1.3.6.1.4.1.45.4.8.0.1	Normal
topologyChange	.1.3.6.1.2.1.17.0.2	Normal
traceRoutePathChange	.1.3.6.1.2.1.81.0.1	Normal
traceRouteTestCompleted	.1.3.6.1.2.1.81.0.3	Normal
traceRouteTestFailed	.1.3.6.1.2.1.81.0.2	Normal

Name	OID	Severity
vrrpTrapAuthFailure	.1.3.6.1.2.1.46.1.3.0.0.2	Normal
vrrpTrapNewMaster	.1.3.6.1.2.1.46.1.3.0.0.1	Normal
warmStart	.1.3.6.1.6.3.1.1.5.2	Normal

G450:

Name	OID	Severity
avSurvEnabled	.1.3.6.1.4.1.6889.2.6.4.0.1	Normal
avSurvDisabled	.1.3.6.1.4.1.6889.2.6.4.0.2	Normal
avSurvActive	.1.3.6.1.4.1.6889.2.6.4.0.3	Normal
avSurvInactive	.1.3.6.1.4.1.6889.2.6.4.0.4	Normal
avstrTrackerOperStateChangeNotification	.1.3.6.1.4.1.6889.2.6.2.2.0.1	Normal
cmgMultipleFanFault	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.2	Normal
cmgMultipleFanClear	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.3	Normal
cmgPsuFanBriefFault	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.4	Normal
cmgPsuFanBriefClear	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.5	Normal
cmgPsuFanProlongedFault	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.6	Normal
cmgPsuFanProlongedClear	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.7	Normal
cmgCpuTempWarningFault	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.10	Normal
cmgCpuTempWarningClear	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.11	Normal
cmgDspTempWarningFault	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.12	Normal
cmgDspTempWarningClear	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.13	Normal
cmgTempShutdownFault	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.14	Normal
cmgMgpPowerFault	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.16	Normal
cmgMgpPowerClear	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.17	Normal
cmgMediaModulePowerFault	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.18	Normal
cmgMediaModulePowerClear	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.19	Normal
cmgVoipPowerFault	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.20	Normal
cmgVoipPowerClear	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.21	Normal
cmgDspPowerFault	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.22	Normal
cmgDspPowerClear	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.23	Normal
cmg8260PowerFault	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.24	Normal
cmg8260PowerClear	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.25	Normal
cmgAuxPowerFault	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.26	Normal
cmgAuxPowerClear	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.27	Normal
cmgFanPowerFault	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.28	Normal
cmgFanPowerClear	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.29	Normal
cmgSyncSignalFault	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.30	Normal
cmgSyncSignalClear	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.31	Normal
cmgVoipHardwareFault	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.32	Normal
cmgVoipHardwareClear	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.33	Normal
cmgSyncSignalWarn	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.34	Normal
cmgSyncWarnClear	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.35	Normal
cmgSyncSignalExcess	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.36	Normal
cmgSyncExcessClear	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.37	Normal
cmgVoipCoreFault	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.38	Normal
cmgVoipCoreClear	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.39	Normal
cmgModuleRemove	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.50	Normal
cmgModuleInsertFault	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.52	Normal
cmgModuleInsertSuccess	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.53	Normal

Name	OID	Severity
cmgMgBusyout	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.54	Normal
cmgMgRelease	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.55	Normal
cmgUnsupportedMmEnrolement	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.56	Normal
cmgDataModuleAwohConflict	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.57	Normal
cmgFirmwareDownloadBegun	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.70	Normal
cmgFirmwareDownloadSuccess	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.71	Normal
cmgRegistrationSuccess	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.73	Normal
cmgMgManualReset	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.74	Normal
cmgModuleManualReset	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.75	Normal
cmgVoipManualReset	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.76	Normal
cmgDsuManualReset	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.77	Normal
cmgConfigUploadBegun	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.78	Normal
cmgConfigUploadSuccess	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.79	Normal
cmgMemoryFault	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.90	Normal
cmgMemoryClear	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.91	Normal
cmgDhcpRequestFault	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.92	Normal
cmgDhcpRequestClear	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.93	Normal
cmgFirmwareDownloadFault	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.94	Normal
cmgFirmwareDownloadWarning	.1.3.6.1.4.1.6889.2.9.1.5.2.2.95	Normal
cmgProcessRestart	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.96	Normal
cmgProcessRestartClear	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.97	Normal
cmgIccMissingFault	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.98	Normal
cmgIccMissingClear	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.99	Normal
cmgIccAutoReset	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.100	Normal
cmgIccAutoResetClear	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.101	Normal
cmgPrimaryControllerFault	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.102	Normal
cmgPrimaryControllerClear	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.103	Normal
cmgNoControllerFault	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.104	Normal
cmgNoControllerClear	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.105	Normal
cmgRegistrationFault	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.106	Normal
cmgH248LinkDown	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.108	Normal
cmgH248LinkUp	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.109	Normal
cmgTestFault	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.110	Normal
cmgTestClear	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.111	Normal
cmgTestThresholdFault	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.112	Normal
cmgTestThresholdClear	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.113	Normal
cmgMgAutoReset	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.114	Normal
cmgModuleAutoReset	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.116	Normal
cmgModuleAutoResetClear	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.117	Normal
cmgModulePostFault	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.118	Normal
cmgModulePostClear	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.119	Normal
cmgModuleParameterFault	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.120	Normal
cmgModuleParameterClear	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.121	Normal
cmgConfigUploadFault	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.122	Normal
cmgVoipOccFault	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.124	Normal
cmgVoipOccClear	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.125	Normal
cmgVoipAvgOccFault	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.126	Normal
cmgVoipAvgOccClear	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.127	Normal
cmgVoipAutoReset	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.128	Normal
cmgVoipAutoResetClear	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.129	Normal

Name	OID	Severity
cmgDsuFpgaConfigureFault	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.130	Normal
cmgDsuFpgaConfigureClear	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.131	Normal
cmgDsuAutoReset	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.132	Normal
cmgDsuAutoResetClear	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.133	Normal
cmgDsuDteDtrFault	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.134	Normal
cmgDsuDteDtrClear	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.135	Normal
cmgDsuDteRtsFault	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.136	Normal
cmgDsuDteRtsClear	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.137	Normal
cmgDsuTxDFault	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.138	Normal
cmgDsuTxDClear	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.139	Normal
cmgDsuRxDFailure	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.140	Normal
cmgDsuRxDClear	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.141	Normal
cmgVoipIpConfigFault	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.142	Normal
cmgVoipIpConfigClear	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.143	Normal
cmgConfigDownloadFault	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.144	Normal
cmgConfigDownloadBegun	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.145	Normal
cmgConfigDownloadSuccess	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.146	Normal
cmgTimeslotOccupancyFault	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.147	Normal
cmgTimeslotOccupancyClear	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.148	Normal
cmgTimeslotAvailabilityFault	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.149	Normal
cmgTimeslotAvailabilityClear	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.150	Normal
cmgRegistrationSuccessInetAddress	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.151	Normal
cmgRegistrationFaultInetAddress	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.152	Normal
cmgDs1Layer2Down	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.153	Normal
cmgDs1Layer2Up	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.154	Normal
cmgFipsErrorMode	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.155	Normal
cmgCertErrorCertRevoked	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.156	Normal
cmgCrlAccessDenied	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.157	Normal
cmgCrlFileSize	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.158	Normal
cmgCertErrorCertExpired	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.159	Normal
cmgCertErrorNearExpiry	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.160	Normal
cmgCertErrorIdAuthentication	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.161	Normal
cmgOcspAccessDenied	.1.3.6.1.4.1.6889.2.9.1.5.2.2.0.162	Normal
avEntFanFlt	.1.3.6.1.4.1.6889.2.1.99.2.0.1	Normal
avEntFanOk	.1.3.6.1.4.1.6889.2.1.99.2.0.2	Normal
avEnt48vPwrFlt	.1.3.6.1.4.1.6889.2.1.99.2.0.4	Normal
avEnt48vPwrFltOk	.1.3.6.1.4.1.6889.2.1.99.2.0.5	Normal
avEnt5vPwrFlt	.1.3.6.1.4.1.6889.2.1.99.2.0.7	Normal
avEnt5vPwrFltOk	.1.3.6.1.4.1.6889.2.1.99.2.0.8	Normal
avEnt3300mvPwrFlt	.1.3.6.1.4.1.6889.2.1.99.2.0.10	Normal
avEnt3300mvPwrFltOk	.1.3.6.1.4.1.6889.2.1.99.2.0.11	Normal
avEnt2500mvPwrFlt	.1.3.6.1.4.1.6889.2.1.99.2.0.13	Normal
avEnt2500mvPwrFltOk	.1.3.6.1.4.1.6889.2.1.99.2.0.14	Normal
avEnt1800mvPwrFlt	.1.3.6.1.4.1.6889.2.1.99.2.0.16	Normal
avEnt1800mvPwrFltOk	.1.3.6.1.4.1.6889.2.1.99.2.0.17	Normal
avEnt1600mvPwrFlt	.1.3.6.1.4.1.6889.2.1.99.2.0.19	Normal
avEnt1600mvPwrFltOk	.1.3.6.1.4.1.6889.2.1.99.2.0.20	Normal
avEntAmbientHiTempFlt	.1.3.6.1.4.1.6889.2.1.99.2.0.22	Normal
avEntAmbientHiTempFltOk	.1.3.6.1.4.1.6889.2.1.99.2.0.23	Normal
avEntAmbientLoTempFlt	.1.3.6.1.4.1.6889.2.1.99.2.0.24	Normal

Name	OID	Severity
avEntAmbientLoTempFltOk	.1.3.6.1.4.1.6889.2.1.99.2.0.25	Normal
avEntPhyUSBDeviceRemovalOnBackupRestoreOperation	.1.3.6.1.4.1.6889.2.1.99.3.0.1	Normal
avEntPhyUSBDeviceInsecureRemoval	.1.3.6.1.4.1.6889.2.1.99.3.0.2	Normal
avEntPhyUSBDevicePowerFailure	.1.3.6.1.4.1.6889.2.1.99.3.0.3	Normal
avEntPhyUSBDeviceNotSupported	.1.3.6.1.4.1.6889.2.1.99.3.0.4	Normal
avEntPhyUSBDeviceExceedMaxNumber	.1.3.6.1.4.1.6889.2.1.99.3.0.5	Normal
avEntPhyUSBFileSystemNotSupported	.1.3.6.1.4.1.6889.2.1.99.3.0.6	Normal
avEntPhyChFruRemoval	.1.3.6.1.4.1.6889.2.1.99.5.0.1	Normal
avEntPhyChFruInsertion	.1.3.6.1.4.1.6889.2.1.99.5.0.2	Normal
avEntPhyChFruPsuFlt	.1.3.6.1.4.1.6889.2.1.99.5.0.3	Normal
avEntPhyChFruPsuFltOk	.1.3.6.1.4.1.6889.2.1.99.5.0.4	Normal
avEntPhyChFruExpansionTestFailure	.1.3.6.1.4.1.6889.2.1.99.5.0.5	Normal
avEntPhyChFruExpansionTestClear	.1.3.6.1.4.1.6889.2.1.99.5.0.6	Normal
lntConfigChangeEvent	.1.3.6.1.4.1.81.38.1.0.1	Normal
lntStackMasterReelection	.1.3.6.1.4.1.81.38.1.0.82	Normal
lntSoftRedDelEvent	.1.3.6.1.4.1.81.38.2.0.12	Normal
lntSoftRedNewEvent	.1.3.6.1.4.1.81.38.2.0.13	Normal
lntTemprature Warning	.1.3.6.1.4.1.81.38.3.0.14	Normal
lntTemprature Ok	.1.3.6.1.4.1.81.38.3.0.23	Normal
lntPortCAMLastChange	.1.3.6.1.4.1.81.38.4.0.22	Normal
lntMainPSUFlt	.1.3.6.1.4.1.81.38.5.0.2303	Normal
lntMainPSUOk	.1.3.6.1.4.1.81.38.5.0.2304	Normal
lntBackupPSUFlt	.1.3.6.1.4.1.81.38.5.0.2305	Normal
lntBackupPSUOk	.1.3.6.1.4.1.81.38.5.0.2306	Normal
lntDuplicateIPFlt	.1.3.6.1.4.1.81.38.6.0.27	Normal
lntVLANViolationEvent	.1.3.6.1.4.1.81.38.6.0.28	Normal
lntARPViolationEvent	.1.3.6.1.4.1.81.38.6.0.70	Normal
lntPortLinkDownEvent	.1.3.6.1.4.1.81.38.7.0.3039	Normal
lntPortLinkUpEvent	.1.3.6.1.4.1.81.38.7.0.3040	Normal
lntVPortLinkDownEvent	.1.3.6.1.4.1.81.38.7.0.3041	Normal
lntVPortLinkUpEvent	.1.3.6.1.4.1.81.38.7.0.3042	Normal
lntLAGConnLostFlt	.1.3.6.1.4.1.81.38.8.0.44	Normal
lntLAGConnLostOk	.1.3.6.1.4.1.81.38.8.0.46	Normal
lntLAGPartialConnLostFlt	.1.3.6.1.4.1.81.38.8.0.48	Normal
lntLAGPartialConnLostOk	.1.3.6.1.4.1.81.38.8.0.50	Normal
lntLAGAutoNegFlt	.1.3.6.1.4.1.81.38.8.0.52	Normal
lntLAGAutoNegOk	.1.3.6.1.4.1.81.38.8.0.54	Normal
lntLAGDeleteEvent	.1.3.6.1.4.1.81.38.8.0.56	Normal
lntLAGCreateEvent	.1.3.6.1.4.1.81.38.8.0.58	Normal
lntMainFansFlt	.1.3.6.1.4.1.81.38.9.0.2307	Normal
lntMainFansOK	.1.3.6.1.4.1.81.38.9.0.2308	Normal
lntBackupFansFlt	.1.3.6.1.4.1.81.38.9.0.2309	Normal
lntBackupFansOK	.1.3.6.1.4.1.81.38.9.0.2310	Normal
lntCascadUpConnFlt	.1.3.6.1.4.1.81.38.10.0.2315	Normal
lntCascadUpConnOk	.1.3.6.1.4.1.81.38.10.0.2316	Normal
lntCascadDownConnFlt	.1.3.6.1.4.1.81.38.10.0.2317	Normal
lntCascadDownConnOk	.1.3.6.1.4.1.81.38.10.0.2318	Normal
lntPolicyChangeEvent	.1.3.6.1.4.1.81.38.11.0.60	Normal
lntPolicyAccessControlListLvlRuleTrap	.1.3.6.1.4.1.81.38.11.0.62	Normal

Name	OID	Severity
IntPolicyAccessControlViolationFlt	.1.3.6.1.4.1.81.38.11.0.64	Normal
IntEthPortAutoNegotiationFlt	.1.3.6.1.4.1.81.38.12.0.3001	Normal
IntEthPortAutoNegotiationOK	.1.3.6.1.4.1.81.38.12.0.3002	Normal
IntPortFEFlt	.1.3.6.1.4.1.81.38.12.0.3005	Normal
IntPortFEOk	.1.3.6.1.4.1.81.38.12.0.3006	Normal
IntVPortFEFlt	.1.3.6.1.4.1.81.38.12.0.3015	Normal
IntVPortFEOk	.1.3.6.1.4.1.81.38.12.0.3016	Normal
IntPortAutoPartFlt	.1.3.6.1.4.1.81.38.12.0.3023	Normal
IntPortAutoPartOk	.1.3.6.1.4.1.81.38.12.0.3024	Normal
IntVPortAutoPartFlt	.1.3.6.1.4.1.81.38.12.0.3025	Normal
IntVPortAutoPartOK	.1.3.6.1.4.1.81.38.12.0.3026	Normal
IntEthVPortAutoNegotiationFlt	.1.3.6.1.4.1.81.38.12.0.3031	Normal
IntEthVPortAutoNegotiationOK	.1.3.6.1.4.1.81.38.12.0.3032	Normal
IntPortInlinePowerFlt	.1.3.6.1.4.1.81.38.12.0.3933	Normal
IntPortInlinePowerOK	.1.3.6.1.4.1.81.38.12.0.3934	Normal
IntUnAuthAccessEvent	.1.3.6.1.4.1.81.38.13.0.68	Normal
IntMACSecurityEvent	.1.3.6.1.4.1.81.38.13.0.104	Normal
IntUnknownHostCopyEvent	.1.3.6.1.4.1.81.38.13.0.1002	Normal
IntAccountLockoutEvent	.1.3.6.1.4.1.81.38.13.0.1003	Normal
IntLicenseStartupValidationFlt	.1.3.6.1.4.1.81.38.13.0.1004	Normal
IntLicenseDownloadValidationFlt	.1.3.6.1.4.1.81.38.13.0.1005	Normal
IntDot1xMaxAuthRateReachedEvent	.1.3.6.1.4.1.81.38.13.0.1006	Normal
IntDot1xAuthFailureEvent	.1.3.6.1.4.1.81.38.13.0.1007	Normal
IntDot1xMaxAuthModuleNumReachedEvent	.1.3.6.1.4.1.81.38.13.0.1008	Normal
IntDot1xMaxAuthPortNumReachedEvent	.1.3.6.1.4.1.81.38.13.0.1009	Normal
IntWanPhysicalAlarmOn	.1.3.6.1.4.1.81.38.15.0.30	Normal
IntWanPhysicalAlarmOff	.1.3.6.1.4.1.81.38.15.0.31	Normal
IntWanLocalAlarmOn	.1.3.6.1.4.1.81.38.15.0.32	Normal
IntWanLocalAlarmOff	.1.3.6.1.4.1.81.38.15.0.33	Normal
IntWanRemoteAlarmOn	.1.3.6.1.4.1.81.38.15.0.34	Normal
IntWanRemoteAlarmOff	.1.3.6.1.4.1.81.38.15.0.35	Normal
IntWanMinorAlarmOn	.1.3.6.1.4.1.81.38.15.0.36	Normal
IntWanMinorAlarmOff	.1.3.6.1.4.1.81.38.15.0.37	Normal
avipsIskampEstablished	.1.3.6.1.4.1.6889.2.6.1.2.0.1	Normal
avipsIskampClosed	.1.3.6.1.4.1.6889.2.6.1.2.0.2	Normal
avipsIskampFailed	.1.3.6.1.4.1.6889.2.6.1.2.0.3	Normal
avipsIpsecTunnelEstablished	.1.3.6.1.4.1.6889.2.6.1.2.0.4	Normal
avipsIpsecTunnelClosed	.1.3.6.1.4.1.6889.2.6.1.2.0.5	Normal
avipsIpsecTunnelFailed	.1.3.6.1.4.1.6889.2.6.1.2.0.6	Normal
cigDhcpClientsConflictDetectionTrap	.1.3.6.1.4.1.6889.2.1.17.1.0.1	Normal
avDownloadBegun	.1.3.6.1.4.1.6889.2.6.5.0.1	Normal
avDownloadSuccess	.1.3.6.1.4.1.6889.2.6.5.0.2	Normal
avDownloadFault	.1.3.6.1.4.1.6889.2.6.5.0.3	Normal
avUploadBegun	.1.3.6.1.4.1.6889.2.6.5.0.4	Normal
avUploadSuccess	.1.3.6.1.4.1.6889.2.6.5.0.5	Normal
avUploadFault	.1.3.6.1.4.1.6889.2.6.5.0.6	Normal
avRtpQoSTrap	.1.3.6.1.4.1.6889.2.7.0.1	Normal
avRtpQoSFault	.1.3.6.1.4.1.6889.2.7.0.2	Normal
avRtpQoSClear	.1.3.6.1.4.1.6889.2.7.0.3	Normal
avRtpQoSInetTrap	.1.3.6.1.4.1.6889.2.7.0.4	Normal

Name	OID	Severity
avMSSDenialOfService	.1.3.6.1.4.1.6889.2.1.14.1.7.0.1	Normal
avConfigurationEncKeyMismatchFault	.1.3.6.1.4.1.6889.2.1.14.1.10.0.1	Normal
avConfigurationMasterKeyChange	.1.3.6.1.4.1.6889.2.1.14.1.10.0.2	Normal
avPasswordToExpireAlert	.1.3.6.1.4.1.6889.2.1.14.1.10.0.3	Normal
avUnAuthAccessEvent	.1.3.6.1.4.1.6889.2.1.14.1.10.0.200	Normal
avAccountLockoutEvent	.1.3.6.1.4.1.6889.2.1.14.1.10.0.201	Normal
avIPv6AddressDuplicationEvent	.1.3.6.1.4.1.6889.2.1.14.1.10.0.202	Normal
avASGAFDownloadSuccess	.1.3.6.1.4.1.6889.2.1.14.1.12.3.5.0.1	Normal
avASGAFDownloadFailure	.1.3.6.1.4.1.6889.2.1.14.1.12.3.5.0.2	Normal
cigTftpServersDownloadFailureTrap	.1.3.6.1.4.1.6889.2.1.16.1.0.1	Normal
cigTftpServersUploadFailureTrap	.1.3.6.1.4.1.6889.2.1.16.1.0.2	Normal
cigDhcpServersClientConflictDetectionTrap	.1.3.6.1.4.1.6889.2.1.16.2.0.1	Normal
cigDhcpServersServerNacksTrap	.1.3.6.1.4.1.6889.2.1.16.2.0.2	Normal
cigDhcpServersNoIpAddressLeft	.1.3.6.1.4.1.6889.2.1.16.2.0.3	Normal

VMware ESXi:

Name	OID	Severity
vmwEnvIpmiSelFull	.1.3.6.1.4.1.6876.4.1.0.390	Normal
vmwEnvIpmiSelMemoryRaised	.1.3.6.1.4.1.6876.4.1.0.400	Normal
vmwEnvIpmiSelMemoryCleared	.1.3.6.1.4.1.6876.4.1.0.401	Normal
vmwEnvIpmiSelPowerSupplyRaised	.1.3.6.1.4.1.6876.4.1.0.410	Normal
vmwEnvIpmiSelPowerSupplyCleared	.1.3.6.1.4.1.6876.4.1.0.411	Normal
vmwEnvIpmiSelFanRaised	.1.3.6.1.4.1.6876.4.1.0.420	Normal
vmwEnvIpmiSelFanCleared	.1.3.6.1.4.1.6876.4.1.0.421	Normal
vmwEnvIpmiSelCpuRaised	.1.3.6.1.4.1.6876.4.1.0.430	Normal
vmwEnvIpmiSelCpuCleared	.1.3.6.1.4.1.6876.4.1.0.431	Normal
vmwEnvHardwareEvent	.1.3.6.1.4.1.6876.0.301	Normal
vmwESXEnvHardwareEvent	.1.3.6.1.4.1.6876.4.1.0.301	Normal
vmwESXEnvHardwareAlert	.1.3.6.1.4.1.6876.4.1.0.302	Normal
vmwESXEnvBatteryAlert	.1.3.6.1.4.1.6876.4.1.0.303	Normal
vmwESXEnvChassisAlert	.1.3.6.1.4.1.6876.4.1.0.304	Normal
vmwESXEnvThermalAlert	.1.3.6.1.4.1.6876.4.1.0.305	Normal
vmwESXEnvDiskAlert	.1.3.6.1.4.1.6876.4.1.0.306	Normal
vmwESXEnvPowerAlert	.1.3.6.1.4.1.6876.4.1.0.307	Normal
vmwESXEnvProcessorAlert	.1.3.6.1.4.1.6876.4.1.0.308	Normal
vmwESXEnvMemoryAlert	.1.3.6.1.4.1.6876.4.1.0.309	Normal
vmwESXEnvBIOSAlert	.1.3.6.1.4.1.6876.4.1.0.310	Normal
vmwSnmpTrapsAreConfigured	.1.3.6.1.4.1.6876.100.1.0.101	Normal
vmwSnmpTrapsAreDisabled	.1.3.6.1.4.1.6876.100.1.0.102	Normal
vmwTestTrap	.1.3.6.1.4.1.6876.100.1.0.103	Normal
vmwEntityDiscoveryChangeEvent	.1.3.6.1.4.1.6876.100.1.0.20001	Normal
vmwEntityPropertiesChangeEvent	.1.3.6.1.4.1.6876.100.1.0.20002	Normal
vmwFirewallNotInstalledOnHostEvent	.1.3.6.1.4.1.6876.100.1.0.20003	Normal
vmwHostWithStaleFirewallRulesEvent	.1.3.6.1.4.1.6876.100.1.0.20004	Normal
vmwIpAddressChangeEvent	.1.3.6.1.4.1.6876.100.1.0.20005	Normal
vmwL2GatewayAnomalyEvent	.1.3.6.1.4.1.6876.100.1.0.20006	Normal
vmwL2NetworkAddressAnomalyEvent	.1.3.6.1.4.1.6876.100.1.0.20007	Normal
vmwL2NetworkDiameterExceededEvent	.1.3.6.1.4.1.6876.100.1.0.20008	Normal
vmwL2NetworkUplinkMissingEvent	.1.3.6.1.4.1.6876.100.1.0.20009	Normal

Name	OID	Severity
vmwL2NetworkWithNoVMsEvent	.1.3.6.1.4.1.6876.100.1.0.20010	Normal
vmwLayer2NetworkDiameterChangedEvent	.1.3.6.1.4.1.6876.100.1.0.20011	Normal
vmwMTUMismatchEvent	.1.3.6.1.4.1.6876.100.1.0.20012	Normal
vmwNetworkIsolationEvent	.1.3.6.1.4.1.6876.100.1.0.20013	Normal
vmwNoPathEvent	.1.3.6.1.4.1.6876.100.1.0.20014	Normal
vmwSpoofguardDisabledEvent	.1.3.6.1.4.1.6876.100.1.0.20015	Normal
vmwVMotionEvent	.1.3.6.1.4.1.6876.100.1.0.20018	Normal
vmwVMWithDisconnectedVnicsEvent	.1.3.6.1.4.1.6876.100.1.0.20019	Normal
vmwVMWithMulipleVnicsOnDifferentVxlansEvent	.1.3.6.1.4.1.6876.100.1.0.20020	Normal
vmwVMWithMulipleVnicsOnSameL2Event	.1.3.6.1.4.1.6876.100.1.0.20021	Normal
vmwVMWithNoIpAddressEvent	.1.3.6.1.4.1.6876.100.1.0.20022	Normal
vmwVTEPMissingEvent	.1.3.6.1.4.1.6876.100.1.0.20023	Normal
vmwL2Event	.1.3.6.1.4.1.6876.100.1.0.20024	Normal
vmwMembershipChangeEvent	.1.3.6.1.4.1.6876.100.1.0.20025	Normal
vmwSecurityGroupMembershipChangeEvent	.1.3.6.1.4.1.6876.100.1.0.20026	Normal
vmwFirewallRuleMembershipChangeEvent	.1.3.6.1.4.1.6876.100.1.0.20027	Normal
vmwVlanMembershipChangeEvent	.1.3.6.1.4.1.6876.100.1.0.20028	Normal
vmwVxlanMembershipChangeEvent	.1.3.6.1.4.1.6876.100.1.0.20029	Normal
vmwDeleteChangeEvent	.1.3.6.1.4.1.6876.100.1.0.20030	Normal
vmwVtepFailedPingEvent	.1.3.6.1.4.1.6876.100.1.0.20031	Normal
vmwEmptySearchStreamChangeEvent	.1.3.6.1.4.1.6876.100.1.0.20034	Normal
vmwSearchStreamMembershipChangeEvent	.1.3.6.1.4.1.6876.100.1.0.20035	Normal
vmwEmptySearchStreamProblemEvent	.1.3.6.1.4.1.6876.100.1.0.20036	Normal
vmwSearchStreamMembershipProblemEvent	.1.3.6.1.4.1.6876.100.1.0.20037	Normal
vmwOspfConfigurationMismatchEvent	.1.3.6.1.4.1.6876.100.1.0.20038	Normal
vmwServiceVMNotHealthyEvent	.1.3.6.1.4.1.6876.100.1.0.20039	Normal
vmwServiceVMNotPoweredOnEvent	.1.3.6.1.4.1.6876.100.1.0.20040	Normal
vmwServiceVMHighCPUUsageEvent	.1.3.6.1.4.1.6876.100.1.0.20041	Normal
vmwServiceVMHighMemoryUsageEvent	.1.3.6.1.4.1.6876.100.1.0.20042	Normal
vmwServiceVMHighDiskUsageEvent	.1.3.6.1.4.1.6876.100.1.0.20043	Normal
vmwIPSetPropertiesChangeEvent	.1.3.6.1.4.1.6876.100.1.0.20050	Normal
vmwFirewallRulePropertiesChangeEvent	.1.3.6.1.4.1.6876.100.1.0.20051	Normal
vmwSecurityGroupPropertiesChangeEvent	.1.3.6.1.4.1.6876.100.1.0.20052	Normal
vmwIPSetMembershipChangeEvent	.1.3.6.1.4.1.6876.100.1.0.20053	Normal
vmwFirewallRuleMaskEvent	.1.3.6.1.4.1.6876.100.1.0.20054	Normal
vmwSecurityMembershipChangeEvent	.1.3.6.1.4.1.6876.100.1.0.20056	Normal
vmwSecurityTagPropertiesChangeEvent	.1.3.6.1.4.1.6876.100.1.0.20057	Normal
vmwSecurityTagMembershipChangeEvent	.1.3.6.1.4.1.6876.100.1.0.20058	Normal
vmwHostDatastoreChangeEvent	.1.3.6.1.4.1.6876.100.1.0.20059	Normal
vmwVMDatastoreChangeEvent	.1.3.6.1.4.1.6876.100.1.0.20060	Normal
vmwVMSnapshotChangeEvent	.1.3.6.1.4.1.6876.100.1.0.20061	Normal
vmwVMVirtualDiskChangeEvent	.1.3.6.1.4.1.6876.100.1.0.20062	Normal
vmwIPSetDefinitionMismatchEvent	.1.3.6.1.4.1.6876.100.1.0.20063	Normal
vmwSegmentMismatchEvent	.1.3.6.1.4.1.6876.100.1.0.20064	Normal
vmwVtepEvent	.1.3.6.1.4.1.6876.100.1.0.20065	Normal
vmwVtepConfigurationFaultEvent	.1.3.6.1.4.1.6876.100.1.0.20066	Normal
vmwVtepSubnetMismatchEvent	.1.3.6.1.4.1.6876.100.1.0.20068	Normal
vmwVtepCountMismatchEvent	.1.3.6.1.4.1.6876.100.1.0.20069	Normal
vmwDLRNetworksNotReachableEvent	.1.3.6.1.4.1.6876.100.1.0.20067	Normal

Name	OID	Severity
vmwEdgeNetworksNotReachableEvent	.1.3.6.1.4.1.6876.100.1.0.20070	Normal
vmwThresholdExceededEventCpuReady	.1.3.6.1.4.1.6876.100.1.0.30001	Normal
vmwThresholdExceededEventCpuCoStop	.1.3.6.1.4.1.6876.100.1.0.30002	Normal
vmwThresholdExceededEventDiskCommandAbortRule	.1.3.6.1.4.1.6876.100.1.0.30003	Normal
vmwThresholdExceededEventIODeviceLatencyRule	.1.3.6.1.4.1.6876.100.1.0.30004	Normal
vmwThresholdExceededEventIOKernelLatencyRule	.1.3.6.1.4.1.6876.100.1.0.30005	Normal
vmwThresholdExceededEventMemorySwapInRule	.1.3.6.1.4.1.6876.100.1.0.30006	Normal
vmwThresholdExceededEventMemorySwapOutRule	.1.3.6.1.4.1.6876.100.1.0.30007	Normal
vmwThresholdExceededEventNetworkRxDropRule	.1.3.6.1.4.1.6876.100.1.0.30008	Normal
vmwThresholdExceededEventNetworkTxDropRule	.1.3.6.1.4.1.6876.100.1.0.30009	Normal
vmwPacketDropEvent	.1.3.6.1.4.1.6876.100.1.0.30100	Normal
vmwSwitchPortPacketDropEvent	.1.3.6.1.4.1.6876.100.1.0.30101	Normal
vmwRouterInterfacePacketDropEvent	.1.3.6.1.4.1.6876.100.1.0.30102	Normal
vmwVnicPacketDropEvent	.1.3.6.1.4.1.6876.100.1.0.30103	Normal
vmwVTEPUnderlayPacketDropEvent	.1.3.6.1.4.1.6876.100.1.0.30104	Normal
vmwPnicUnderlyingSwitchPortPacketDropEvent	.1.3.6.1.4.1.6876.100.1.0.30105	Normal
vmwDevicePacketDropEvent	.1.3.6.1.4.1.6876.100.1.0.30106	Normal
vmwThresholdExceededEventDatastoreFreeSpaceWarning	.1.3.6.1.4.1.6876.100.1.0.30203	Normal
vmwThresholdExceededEventDatastoreFreeSpaceCritical	.1.3.6.1.4.1.6876.100.1.0.30204	Normal
vmwThresholdExceededEventDatastoreReadLatency	.1.3.6.1.4.1.6876.100.1.0.30205	Normal
vmwThresholdExceededEventDatastoreWriteLatency	.1.3.6.1.4.1.6876.100.1.0.30206	Normal
vmwDistributedFirewallApplyHostEvent	.1.3.6.1.4.1.6876.100.1.0.35001	Normal
vmwDistributedFirewallApplyVMEvent	.1.3.6.1.4.1.6876.100.1.0.35002	Normal
vmwNsxEvent	.1.3.6.1.4.1.6876.100.1.0.35003	Normal
vmwFeatureImpactedEvent	.1.3.6.1.4.1.6876.100.1.0.35004	Normal
vmwClusterFeatureVersionMismatchEvent	.1.3.6.1.4.1.6876.100.1.0.36022	Normal
vmwHostFeatureVersionMismatchEvent	.1.3.6.1.4.1.6876.100.1.0.36023	Normal
vmwFeatureVersionMismatchEvent	.1.3.6.1.4.1.6876.100.1.0.36024	Normal
vmwHostFeatureEnabledMismatchEvent	.1.3.6.1.4.1.6876.100.1.0.36025	Normal
vmwHostFeatureInstalledMismatchEvent	.1.3.6.1.4.1.6876.100.1.0.36026	Normal
vmwHostVtepNotFoundEvent	.1.3.6.1.4.1.6876.100.1.0.36027	Normal
vmwHostVtepDisconnectedEvent	.1.3.6.1.4.1.6876.100.1.0.36028	Normal
vmwHostVtepEvent	.1.3.6.1.4.1.6876.100.1.0.36029	Normal
vmwClusterHostsVtepMTUMismatchEvent	.1.3.6.1.4.1.6876.100.1.0.36030	Normal
vmwFeatureUnhealthyEvent	.1.3.6.1.4.1.6876.100.1.0.36031	Normal
vmwEdgeHANotConfiguredEvent	.1.3.6.1.4.1.6876.100.1.0.36032	Normal
vmwEdgeInterfacesDownEvent	.1.3.6.1.4.1.6876.100.1.0.36033	Normal
vmwModuleUnhealthyEvent	.1.3.6.1.4.1.6876.100.1.0.36041	Normal
vmwModuleNotLoadedEvent	.1.3.6.1.4.1.6876.100.1.0.36042	Normal

Name	OID	Severity
vmwModuleNetworkConnectionFailureEvent	.1.3.6.1.4.1.6876.100.1.0.36043	Normal
vmwHostNetworkControlPlaneMismatchEvent	.1.3.6.1.4.1.6876.100.1.0.36044	Normal
vmwHostNetworkControlPlaneConnectionFailureEvent	.1.3.6.1.4.1.6876.100.1.0.36045	Normal
vmwHostNetworkControlPlaneNotSyncedEvent	.1.3.6.1.4.1.6876.100.1.0.36046	Normal
vmwNSXControllerClusterMajorityEvent	.1.3.6.1.4.1.6876.100.1.0.36047	Normal
vmwNSXControllersVMOnSameHostEvent	.1.3.6.1.4.1.6876.100.1.0.36048	Normal
vmwVxLanRangeExhaustEvent	.1.3.6.1.4.1.6876.100.1.0.36049	Normal
vmwNSXFirewallDefaultAllowAllRulesEvent	.1.3.6.1.4.1.6876.100.1.0.36050	Normal
vmwLogicalRouterNoUplinkEvent	.1.3.6.1.4.1.6876.100.1.0.36051	Normal
vmwEdgeNotHAEvent	.1.3.6.1.4.1.6876.100.1.0.36052	Normal
vmwEdgeNotDeployedEvent	.1.3.6.1.4.1.6876.100.1.0.36053	Normal
vmwEcmpIsEnabledAndStatefulServicesAreUpEvent	.1.3.6.1.4.1.6876.100.1.0.36054	Normal
vmwLogicalRouterDeployedOnEcmpEdgeHostEvent	.1.3.6.1.4.1.6876.100.1.0.36055	Normal
vmwEdgeMissingInterfaceOSPFAreaMappingEvent	.1.3.6.1.4.1.6876.100.1.0.36056	Normal
vmwOspfInsecureAuthRouterEvent	.1.3.6.1.4.1.6876.100.1.0.36057	Normal
vmwNSXControllersDeployedCountEvent	.1.3.6.1.4.1.6876.100.1.0.36058	Normal
vmwNSXControllerNotActiveCountEvent	.1.3.6.1.4.1.6876.100.1.0.36059	Normal
vmwNSXControllerEvent	.1.3.6.1.4.1.6876.100.1.0.36060	Normal
vmwNSXEcmpEdgeDownEvent	.1.3.6.1.4.1.6876.100.1.0.36061	Normal
vmwNSXMajorityEcmpEdgesDownEvent	.1.3.6.1.4.1.6876.100.1.0.36062	Normal
vmwNSXAllEcmpEdgesDownEvent	.1.3.6.1.4.1.6876.100.1.0.36063	Normal
vmwNSXEdgeMtuMismatchEvent	.1.3.6.1.4.1.6876.100.1.0.36064	Normal
vmwNSXEdgeSplitBrainEvent	.1.3.6.1.4.1.6876.100.1.0.36065	Normal
vmwNSXComponentEvent	.1.3.6.1.4.1.6876.100.1.0.35221	Normal
vmwNSXBackupEvent	.1.3.6.1.4.1.6876.100.1.0.35222	Normal
vmwNSXBackupAuditLogExcludedEvent	.1.3.6.1.4.1.6876.100.1.0.35223	Normal
vmwNSXUnsecureBackupEvent	.1.3.6.1.4.1.6876.100.1.0.35224	Normal
vmwNSXBackupSystemEventsExcludedEvent	.1.3.6.1.4.1.6876.100.1.0.35225	Normal
vmwNSXBackupNotScheduledEvent	.1.3.6.1.4.1.6876.100.1.0.35226	Normal
vmwNSXBackupNotRecordedEvent	.1.3.6.1.4.1.6876.100.1.0.35227	Normal
vmwNSXNtpServerEvent	.1.3.6.1.4.1.6876.100.1.0.35228	Normal
vmwNSXSysLogServerEvent	.1.3.6.1.4.1.6876.100.1.0.35229	Normal
vmwControllerSysLogServerEvent	.1.3.6.1.4.1.6876.100.1.0.35230	Normal
vmwNSXIpV6EnabledEvent	.1.3.6.1.4.1.6876.100.1.0.35231	Normal
vmwNSXOspfNeighborDownEvent	.1.3.6.1.4.1.6876.100.1.0.35232	Normal
vmwGenericNSXSystemEvent	.1.3.6.1.4.1.6876.100.1.0.70000	Normal
vmwOtherCriticalNSXEvent	.1.3.6.1.4.1.6876.100.1.0.71000	Normal
vmwFilterConfigApplyOnHostFailedEvent	.1.3.6.1.4.1.6876.100.1.0.70001	Normal
vmwRulesetLoadOnHostFailedEvent	.1.3.6.1.4.1.6876.100.1.0.70002	Normal
vmwConfigUpdateOnHostFailedEvent	.1.3.6.1.4.1.6876.100.1.0.70003	Normal
vmwSpoofguardConfigUpdateOnHostFailedEvent	.1.3.6.1.4.1.6876.100.1.0.70004	Normal
vmwApplyRuleToVnicFailedEvent	.1.3.6.1.4.1.6876.100.1.0.70005	Normal
vmwContainerConfigUpdateOnVnicFailedEvent	.1.3.6.1.4.1.6876.100.1.0.70006	Normal
vmwSpoofguardApplyToVnicFailedEvent	.1.3.6.1.4.1.6876.100.1.0.70007	Normal

Name	OID	Severity
vmwHostMessagingConfigurationFailedEvent	.1.3.6.1.4.1.6876.100.1.0.70008	Normal
vmwHostMessagingConnectionReconfigurationFailedEvent	.1.3.6.1.4.1.6876.100.1.0.70009	Normal
vmwHostMessagingConfigurationFailedNotificationSkippedEvent	.1.3.6.1.4.1.6876.100.1.0.70010	Normal
vmwHostMessagingInfrastructureDownEvent	.1.3.6.1.4.1.6876.100.1.0.70011	Normal
vmwEdgeVMNotRespondingEvent	.1.3.6.1.4.1.6876.100.1.0.70012	Normal
vmwEdgeUnhealthyEvent	.1.3.6.1.4.1.6876.100.1.0.70013	Normal
vmwEdgeVMCommunicationFailureEvent	.1.3.6.1.4.1.6876.100.1.0.70014	Normal
vmwNSXEdgeEvent	.1.3.6.1.4.1.6876.100.1.0.70015	Normal
vmwPanEvent	.1.3.6.1.4.1.6876.100.1.0.80000	Normal
vmwPanNsxNotInRegisteredStateEvent	.1.3.6.1.4.1.6876.100.1.0.80001	Normal
vmwPanNsxDynamicUpdateDelayedEvent	.1.3.6.1.4.1.6876.100.1.0.80002	Normal
vmwPanDeviceInDisconnectedStateEvent	.1.3.6.1.4.1.6876.100.1.0.80003	Normal
vmwPanNsxServiceApplianceViewMismatchEvent	.1.3.6.1.4.1.6876.100.1.0.80004	Normal
vmwPanNsxFabricAgentNotFoundOnHostEvent	.1.3.6.1.4.1.6876.100.1.0.80005	Normal
vmwPanNsxServiceVMNotFoundOnHostEvent	.1.3.6.1.4.1.6876.100.1.0.80006	Normal
vmwCheckpointEvent	.1.3.6.1.4.1.6876.100.1.0.80100	Normal
vmwCheckpointNsxFabricAgentNotFoundOnHostEvent	.1.3.6.1.4.1.6876.100.1.0.80102	Normal
vmwCheckpointNsxServiceVMNotFoundOnHostEvent	.1.3.6.1.4.1.6876.100.1.0.80103	Normal
vmwCheckpointGatewaySicStatusNotCommunicatingEvent	.1.3.6.1.4.1.6876.100.1.0.80104	Normal
vmwCheckpointNsxServiceApplianceViewMismatchEvent	.1.3.6.1.4.1.6876.100.1.0.80105	Normal
vmwCriticalHostNotAccessibleEvent	.1.3.6.1.4.1.6876.100.1.0.40001	Normal
vmwVchaNodeJoined	.1.3.6.1.4.1.6876.53.0.100	Normal
vmwVchaNodeLeft	.1.3.6.1.4.1.6876.53.0.105	Normal
vmwVchaNodeIsolated	.1.3.6.1.4.1.6876.53.0.110	Normal
vmwVchaClusterStateChanged	.1.3.6.1.4.1.6876.53.0.130	Normal
vmwVchaClusterModeChanged	.1.3.6.1.4.1.6876.53.0.150	Normal
vmwVchaPublicIpUp	.1.3.6.1.4.1.6876.53.0.205	Normal
vmwVchaPublicIpDown	.1.3.6.1.4.1.6876.53.0.206	Normal
vmwVchaFailoverTriggered	.1.3.6.1.4.1.6876.53.0.210	Normal
vmwVchaFailoverSucceeded	.1.3.6.1.4.1.6876.53.0.220	Normal
vmwVchaFailoverFailedDisabledMode	.1.3.6.1.4.1.6876.53.0.225	Normal
vmwVchaFailoverFailedNodeLost	.1.3.6.1.4.1.6876.53.0.226	Normal
vmwVchaFailoverFailedPassiveNotReady	.1.3.6.1.4.1.6876.53.0.227	Normal
vmwVchaContinueAsActive	.1.3.6.1.4.1.6876.53.0.230	Normal
vmwVchaDbReplicationStateChanged	.1.3.6.1.4.1.6876.53.0.300	Normal
vmwVchaFileReplicationStateChanged	.1.3.6.1.4.1.6876.53.0.350	Normal
vmwHbHeartbeat	.1.3.6.1.4.1.6876.4.190.0.401	Normal
vmwCimOmHeartbeat	.1.3.6.1.4.1.6876.4.90.0.401	Normal
vmwareTrapKPIBreachActive	.1.3.6.1.4.1.6876.4.5.1.0.1	Normal
vmwareTrapKPIBreachClear	.1.3.6.1.4.1.6876.4.5.1.0.2	Normal
vmwareTrapKPIBreachChange	.1.3.6.1.4.1.6876.4.5.1.0.3	Normal
vmwareTrapKPIPredictionActive	.1.3.6.1.4.1.6876.4.5.1.0.4	Normal
vmwareTrapKPIPredictionClear	.1.3.6.1.4.1.6876.4.5.1.0.5	Normal

Name	OID	Severity
vmwareTrapKPIPredictionChange	.1.3.6.1.4.1.6876.4.5.1.0.6	Normal
vmwareTrapAggregateAnomalyActive	.1.3.6.1.4.1.6876.4.5.1.0.7	Normal
vmwareTrapAggregateAnomalyClear	.1.3.6.1.4.1.6876.4.5.1.0.8	Normal
vmwareTrapKPIHTBreachActive	.1.3.6.1.4.1.6876.4.5.1.0.10	Normal
vmwareTrapKPIHTBreachClear	.1.3.6.1.4.1.6876.4.5.1.0.11	Normal
vmwareTrapKPIHTBreachChange	.1.3.6.1.4.1.6876.4.5.1.0.12	Normal
vmwareTrapNotificationActive	.1.3.6.1.4.1.6876.4.5.1.0.13	Normal
vmwareTrapNotificationClear	.1.3.6.1.4.1.6876.4.5.1.0.14	Normal
vmwareTrapNotificationChange	.1.3.6.1.4.1.6876.4.5.1.0.15	Normal
vmwareTrapAbnormalityActive	.1.3.6.1.4.1.6876.4.5.1.0.16	Normal
vmwareTrapAbnormalityClear	.1.3.6.1.4.1.6876.4.5.1.0.17	Normal
vmwareTrapAbnormalityChange	.1.3.6.1.4.1.6876.4.5.1.0.18	Normal
vmwareTrapWorkloadActive	.1.3.6.1.4.1.6876.4.5.1.0.19	Normal
vmwareTrapWorkloadClear	.1.3.6.1.4.1.6876.4.5.1.0.20	Normal
vmwareTrapWorkloadChange	.1.3.6.1.4.1.6876.4.5.1.0.21	Normal
vmwareTrapAnomalyActive	.1.3.6.1.4.1.6876.4.5.1.0.22	Normal
vmwareTrapAnomalyClear	.1.3.6.1.4.1.6876.4.5.1.0.23	Normal
vmwareTrapAnomalyChange	.1.3.6.1.4.1.6876.4.5.1.0.24	Normal
vmwareTrapFaultActive	.1.3.6.1.4.1.6876.4.5.1.0.25	Normal
vmwareTrapFaultClear	.1.3.6.1.4.1.6876.4.5.1.0.26	Normal
vmwareTrapFaultChange	.1.3.6.1.4.1.6876.4.5.1.0.27	Normal
vmwareTrapTimeRemainingActive	.1.3.6.1.4.1.6876.4.5.1.0.28	Normal
vmwareTrapTimeRemainingClear	.1.3.6.1.4.1.6876.4.5.1.0.29	Normal
vmwareTrapTimeRemainingChange	.1.3.6.1.4.1.6876.4.5.1.0.30	Normal
vmwareTrapCapacityRemainingActive	.1.3.6.1.4.1.6876.4.5.1.0.31	Normal
vmwareTrapCapacityRemainingClear	.1.3.6.1.4.1.6876.4.5.1.0.32	Normal
vmwareTrapCapacityRemainingChange	.1.3.6.1.4.1.6876.4.5.1.0.33	Normal
vmwareTrapStressActive	.1.3.6.1.4.1.6876.4.5.1.0.34	Normal
vmwareTrapStressClear	.1.3.6.1.4.1.6876.4.5.1.0.35	Normal
vmwareTrapStressChange	.1.3.6.1.4.1.6876.4.5.1.0.36	Normal
vmwareTrapWasteActive	.1.3.6.1.4.1.6876.4.5.1.0.37	Normal
vmwareTrapWasteClear	.1.3.6.1.4.1.6876.4.5.1.0.38	Normal
vmwareTrapWasteChange	.1.3.6.1.4.1.6876.4.5.1.0.39	Normal
vmwareTrapDensityActive	.1.3.6.1.4.1.6876.4.5.1.0.40	Normal
vmwareTrapDensityClear	.1.3.6.1.4.1.6876.4.5.1.0.41	Normal
vmwareTrapDensityChange	.1.3.6.1.4.1.6876.4.5.1.0.42	Normal
vmwareTrapComplianceActive	.1.3.6.1.4.1.6876.4.5.1.0.43	Normal
vmwareTrapComplianceClear	.1.3.6.1.4.1.6876.4.5.1.0.44	Normal
vmwareTrapComplianceChange	.1.3.6.1.4.1.6876.4.5.1.0.45	Normal
vmwareTrapProblemActive	.1.3.6.1.4.1.6876.4.5.1.0.46	Normal
vmwareTrapProblemClear	.1.3.6.1.4.1.6876.4.5.1.0.47	Normal
vmwareTrapProblemChange	.1.3.6.1.4.1.6876.4.5.1.0.48	Normal
vmwareTrapAliveComponentFailureActive	.1.3.6.1.4.1.6876.4.5.1.0.101	Normal
vmwareTrapAliveComponentFailureClear	.1.3.6.1.4.1.6876.4.5.1.0.102	Normal
vmwareTrapResourceDisconnectedActive	.1.3.6.1.4.1.6876.4.5.1.0.103	Normal
vmwareTrapResourceDisconnectedClear	.1.3.6.1.4.1.6876.4.5.1.0.104	Normal
vmwareTrapConsolidatedAlertActive	.1.3.6.1.4.1.6876.4.5.1.0.60	Normal
vmwareTrapConsolidatedAlertClear	.1.3.6.1.4.1.6876.4.5.1.0.61	Normal
vmwareTrapConsolidatedAlertChange	.1.3.6.1.4.1.6876.4.5.1.0.62	Normal
vmwareTrapTest	.1.3.6.1.4.1.6876.4.5.1.0.200	Normal

Name	OID	Severity
vmwNsxMConfigGroup	.1.3.6.1.4.1.6876.90.1.2.0.1.0.1	Normal
vmwNsxMSnmpDisabled	.1.3.6.1.4.1.6876.90.1.2.1.0.1	Normal
vmwNsxMSnmpManagerConfigUpdated	.1.3.6.1.4.1.6876.90.1.2.1.0.2	Normal
vmwNsxMIpAddedBlackList	.1.3.6.1.4.1.6876.90.1.2.2.0.1	Normal
vmwNsxMIpRemovedBlackList	.1.3.6.1.4.1.6876.90.1.2.2.0.2	Normal
vmwNsxMSsoConfigFailure	.1.3.6.1.4.1.6876.90.1.2.2.0.3	Normal
vmwNsxMSsoUnconfigured	.1.3.6.1.4.1.6876.90.1.2.2.0.4	Normal
vmwNsxMUserRoleAssigned	.1.3.6.1.4.1.6876.90.1.2.2.0.5	Normal
vmwNsxMUserRoleUnassigned	.1.3.6.1.4.1.6876.90.1.2.2.0.6	Normal
vmwNsxMGroupRoleAssigned	.1.3.6.1.4.1.6876.90.1.2.2.0.7	Normal
vmwNsxMGroupRoleUnassigned	.1.3.6.1.4.1.6876.90.1.2.2.0.8	Normal
vmwNsxMVcLoginFailed	.1.3.6.1.4.1.6876.90.1.2.2.0.9	Normal
vmwNsxMVcDisconnected	.1.3.6.1.4.1.6876.90.1.2.2.0.10	Normal
vmwNsxMLostVcConnectivity	.1.3.6.1.4.1.6876.90.1.2.2.0.11	Normal
vmwNsxMSsoDisconnected	.1.3.6.1.4.1.6876.90.1.2.2.0.12	Normal
vmwNsxMSsoTimeout	.1.3.6.1.4.1.6876.90.1.2.2.0.13	Normal
vmwNsxMFltrCnfgUpdateFailed	.1.3.6.1.4.1.6876.90.1.2.3.0.1	Normal
vmwNsxMFltrCnfgNotAppliedToVnic	.1.3.6.1.4.1.6876.90.1.2.3.0.2	Normal
vmwNsxMFltrCnfgAppliedToVnic	.1.3.6.1.4.1.6876.90.1.2.3.0.3	Normal
vmwNsxMFltrCreatedForVnic	.1.3.6.1.4.1.6876.90.1.2.3.0.4	Normal
vmwNsxMFltrDeletedForVnic	.1.3.6.1.4.1.6876.90.1.2.3.0.5	Normal
vmwNsxMFirewallConfigUpdateFailed	.1.3.6.1.4.1.6876.90.1.2.3.0.6	Normal
vmwNsxMFirewallRuleFailedVnic	.1.3.6.1.4.1.6876.90.1.2.3.0.7	Normal
vmwNsxMFirewallRuleAppliedVnic	.1.3.6.1.4.1.6876.90.1.2.3.0.8	Normal
vmwNsxMCntnrCnfgUpdateFailed	.1.3.6.1.4.1.6876.90.1.2.3.0.9	Normal
vmwNsxMFlowMissed	.1.3.6.1.4.1.6876.90.1.2.3.0.10	Normal
vmwNsxMSpoofGuardCnfgUpdateFailed	.1.3.6.1.4.1.6876.90.1.2.3.0.11	Normal
vmwNsxMSpoofGuardFailed	.1.3.6.1.4.1.6876.90.1.2.3.0.12	Normal
vmwNsxMSpoofGuardApplied	.1.3.6.1.4.1.6876.90.1.2.3.0.13	Normal
vmwNsxMSpoofGuardDisableFail	.1.3.6.1.4.1.6876.90.1.2.3.0.14	Normal
vmwNsxMSpoofGuardDisabled	.1.3.6.1.4.1.6876.90.1.2.3.0.15	Normal
vmwNsxMLegacyAppServiceDeletionFailed	.1.3.6.1.4.1.6876.90.1.2.3.0.16	Normal
vmwNsxMFirewallCpuThresholdCrossed	.1.3.6.1.4.1.6876.90.1.2.3.0.17	Normal
vmwNsxMFirewallMemThresholdCrossed	.1.3.6.1.4.1.6876.90.1.2.3.0.18	Normal
vmwNsxMConnPerSecThrshldCrossed	.1.3.6.1.4.1.6876.90.1.2.3.0.19	Normal
vmwNsxMFirewallCnfgUpdateTimedOut	.1.3.6.1.4.1.6876.90.1.2.3.0.20	Normal
vmwNsxMSpoofGuardCnfgUpdateTmOut	.1.3.6.1.4.1.6876.90.1.2.3.0.21	Normal
vmwNsxMFirewallPublishFailed	.1.3.6.1.4.1.6876.90.1.2.3.0.22	Normal
vmwNsxMCntnrUpdatePublishFailed	.1.3.6.1.4.1.6876.90.1.2.3.0.23	Normal
vmwNsxMSpoofGuardUpdatePublishFailed	.1.3.6.1.4.1.6876.90.1.2.3.0.24	Normal
vmwNsxMExcludeListPublishFailed	.1.3.6.1.4.1.6876.90.1.2.3.0.25	Normal
vmwNsxMFirewallCnfgUpdateOnDltCntnr	.1.3.6.1.4.1.6876.90.1.2.3.0.26	Normal
vmwNsxMHostSyncFailed	.1.3.6.1.4.1.6876.90.1.2.3.0.27	Normal
vmwNsxMHostSynced	.1.3.6.1.4.1.6876.90.1.2.3.0.28	Normal
vmwNsxMFirewallInstalled	.1.3.6.1.4.1.6876.90.1.2.3.0.29	Normal
vmwNsxMFirewallInstallFailed	.1.3.6.1.4.1.6876.90.1.2.3.0.30	Normal
vmwNsxMFirewallClusterInstalled	.1.3.6.1.4.1.6876.90.1.2.3.0.31	Normal
vmwNsxMFirewallClusterUninstalled	.1.3.6.1.4.1.6876.90.1.2.3.0.32	Normal
vmwNsxMFirewallClusterDisabled	.1.3.6.1.4.1.6876.90.1.2.3.0.33	Normal
vmwNsxMFirewallForceSyncClusterFailed	.1.3.6.1.4.1.6876.90.1.2.3.0.34	Normal

Name	OID	Severity
vmwNsxMFirewallForceSyncClusterSuccess	.1.3.6.1.4.1.6876.90.1.2.3.0.35	Normal
vmwNsxMFirewallVsfwdProcessStarted	.1.3.6.1.4.1.6876.90.1.2.3.0.36	Normal
vmwNsxMFirewallRulesetApplyAllFailed	.1.3.6.1.4.1.6876.90.1.2.3.0.37	Normal
vmwNsxMFirewallRulesetAppliedAll	.1.3.6.1.4.1.6876.90.1.2.3.0.38	Normal
vmwNsxMCntnrCnfgApplyFailedToVnic	.1.3.6.1.4.1.6876.90.1.2.3.0.39	Normal
vmwNsxMCntnrCnfgApplyAllFailedToVnic	.1.3.6.1.4.1.6876.90.1.2.3.0.40	Normal
vmwNsxMCntnrCnfgAppliedAllToVnic	.1.3.6.1.4.1.6876.90.1.2.3.0.41	Normal
vmwNsxMSpoofGuardApplyAllFailed	.1.3.6.1.4.1.6876.90.1.2.3.0.42	Normal
vmwNsxMSpoofGuardAppliedAll	.1.3.6.1.4.1.6876.90.1.2.3.0.43	Normal
vmwNsxMFirewallTimeoutUpdateFailed	.1.3.6.1.4.1.6876.90.1.2.3.0.44	Normal
vmwNsxMFirewallTimeoutApplyFailed	.1.3.6.1.4.1.6876.90.1.2.3.0.45	Normal
vmwNsxMFirewallTimeoutApplied	.1.3.6.1.4.1.6876.90.1.2.3.0.46	Normal
vmwNsxMFirewallTimeoutApplyAllFailed	.1.3.6.1.4.1.6876.90.1.2.3.0.47	Normal
vmwNsxMFirewallTimeoutAppliedAll	.1.3.6.1.4.1.6876.90.1.2.3.0.48	Normal
vmwNsxMCntnrCnfgAppliedToVnic	.1.3.6.1.4.1.6876.90.1.2.3.0.49	Normal
vmwNsxMFirewallMaxConcurrentConnectionsThresholdCrossed	.1.3.6.1.4.1.6876.90.1.2.3.0.50	Normal
vmwNsxMFirewallProcessMemoryThresholdCrossed	.1.3.6.1.4.1.6876.90.1.2.3.0.51	Normal
vmwNsxMFirewallCpuThresholdCrossCleared	.1.3.6.1.4.1.6876.90.1.2.3.0.52	Normal
vmwNsxMFirewallMemThresholdCrossCleared	.1.3.6.1.4.1.6876.90.1.2.3.0.53	Normal
vmwNsxMConnPerSecThrshldCrossCleared	.1.3.6.1.4.1.6876.90.1.2.3.0.54	Normal
vmwNsxMFirewallMaxConcurrentConnectionsThresholdCrossCleared	.1.3.6.1.4.1.6876.90.1.2.3.0.55	Normal
vmwNsxMFirewallProcessMemoryThresholdCrossCleared	.1.3.6.1.4.1.6876.90.1.2.3.0.56	Normal
vmwNsxMFirewallThresholdConfigApplied	.1.3.6.1.4.1.6876.90.1.2.3.0.57	Normal
vmwNsxMFirewallThresholdConfigApplyFailed	.1.3.6.1.4.1.6876.90.1.2.3.0.58	Normal
vmwNsxMUnsupportedIPsetConfigured	.1.3.6.1.4.1.6876.90.1.2.3.0.59	Normal
vmwNsxMEdgeNoVmServing	.1.3.6.1.4.1.6876.90.1.2.4.0.1	Normal
vmwNsxMEdgeGatewayCreated	.1.3.6.1.4.1.6876.90.1.2.4.0.2	Normal
vmwNsxMEdgeVmBadState	.1.3.6.1.4.1.6876.90.1.2.4.0.3	Normal
vmwNsxMEdgeVmCommFailed	.1.3.6.1.4.1.6876.90.1.2.4.0.4	Normal
vmwNsxMEdgeVmCnfgChanged	.1.3.6.1.4.1.6876.90.1.2.4.0.5	Normal
vmwNsxMEdgeGatewayDeleted	.1.3.6.1.4.1.6876.90.1.2.4.0.6	Normal
vmwNsxMEdgeGatewayReDeployed	.1.3.6.1.4.1.6876.90.1.2.4.0.7	Normal
vmwNsxMEdgeVmPowerOff	.1.3.6.1.4.1.6876.90.1.2.4.0.8	Normal
vmwNsxMEdgeApplianceSizeChanged	.1.3.6.1.4.1.6876.90.1.2.4.0.9	Normal
vmwNsxMEdgeUpgrade51x	.1.3.6.1.4.1.6876.90.1.2.4.0.10	Normal
vmwNsxMEdgeLicenseChanged	.1.3.6.1.4.1.6876.90.1.2.4.0.11	Normal
vmwNsxMEdgeApplianceMoved	.1.3.6.1.4.1.6876.90.1.2.4.0.12	Normal
vmwNsxMEdgeApplianceNotFound	.1.3.6.1.4.1.6876.90.1.2.4.0.13	Normal
vmwNsxMEdgeVMHealthCheckMiss	.1.3.6.1.4.1.6876.90.1.2.4.0.14	Normal
vmwNsxMEdgeHealthCheckMiss	.1.3.6.1.4.1.6876.90.1.2.4.0.15	Normal
vmwNsxMEdgeCommAgentNotConnected	.1.3.6.1.4.1.6876.90.1.2.4.0.16	Normal
vmwNsxMApplianceWithDifferentId	.1.3.6.1.4.1.6876.90.1.2.4.0.17	Normal
vmwNsxMFirewallRuleModified	.1.3.6.1.4.1.6876.90.1.2.4.0.18	Normal
vmwNsxMEdgeAntiAffinityRuleViolated	.1.3.6.1.4.1.6876.90.1.2.4.0.19	Normal
vmwNsxMEdgeHaEnabled	.1.3.6.1.4.1.6876.90.1.2.4.0.20	Normal
vmwNsxMEdgeHaDisabled	.1.3.6.1.4.1.6876.90.1.2.4.0.21	Normal
vmwNsxMEdgeGatewayRecovered	.1.3.6.1.4.1.6876.90.1.2.4.0.22	Normal

Name	OID	Severity
vmwNsxMEdgeVmRecovered	.1.3.6.1.4.1.6876.90.1.2.4.0.23	Normal
vmwNsxMEdgeGatewayUpgraded	.1.3.6.1.4.1.6876.90.1.2.4.0.24	Normal
vmwNsxMEdgeVmHlthChkDisabled	.1.3.6.1.4.1.6876.90.1.2.4.0.25	Normal
vmwNsxMEdgePrePublishFailed	.1.3.6.1.4.1.6876.90.1.2.4.0.26	Normal
vmwNsxMEdgeForcedSync	.1.3.6.1.4.1.6876.90.1.2.4.0.27	Normal
vmwNsxMEdgeVmBooted	.1.3.6.1.4.1.6876.90.1.2.4.0.28	Normal
vmwNsxMEdgeVmInBadState	.1.3.6.1.4.1.6876.90.1.2.4.0.29	Normal
vmwNsxMEdgeVmCpuUsageIncreased	.1.3.6.1.4.1.6876.90.1.2.4.0.30	Normal
vmwNsxMEdgeVmMemUsageIncreased	.1.3.6.1.4.1.6876.90.1.2.4.0.31	Normal
vmwNsxMEdgeVmProcessFailure	.1.3.6.1.4.1.6876.90.1.2.4.0.32	Normal
vmwNsxMEdgeVmSysTimeBad	.1.3.6.1.4.1.6876.90.1.2.4.0.33	Normal
vmwNsxMEdgeVmSysTimeSync	.1.3.6.1.4.1.6876.90.1.2.4.0.34	Normal
vmwNsxMEdgeAesniCryptoEngineUp	.1.3.6.1.4.1.6876.90.1.2.4.0.35	Normal
vmwNsxMEdgeAesniCryptoEngineDown	.1.3.6.1.4.1.6876.90.1.2.4.0.36	Normal
vmwNsxMEdgeVmOom	.1.3.6.1.4.1.6876.90.1.2.4.0.37	Normal
vmwNsxMEdgeFileSysRo	.1.3.6.1.4.1.6876.90.1.2.4.0.38	Normal
vmwNsxMEdgeHaCommDisconnected	.1.3.6.1.4.1.6876.90.1.2.4.0.39	Normal
vmwNsxMEdgeHaSwitchOverSelf	.1.3.6.1.4.1.6876.90.1.2.4.0.40	Normal
vmwNsxMEdgeHaSwitchOverActive	.1.3.6.1.4.1.6876.90.1.2.4.0.41	Normal
vmwNsxMEdgeHaSwitchOverStandby	.1.3.6.1.4.1.6876.90.1.2.4.0.42	Normal
vmwNsxMEdgeMonitorProcessFailure	.1.3.6.1.4.1.6876.90.1.2.4.0.43	Normal
vmwNsxMLbVirtualServerPoolUp	.1.3.6.1.4.1.6876.90.1.2.4.0.44	Normal
vmwNsxMLbVirtualServerPoolDown	.1.3.6.1.4.1.6876.90.1.2.4.0.45	Normal
vmwNsxMLbVirtualServerPoolWrong	.1.3.6.1.4.1.6876.90.1.2.4.0.46	Normal
vmwNsxMLbPoolWarning	.1.3.6.1.4.1.6876.90.1.2.4.0.47	Normal
vmwNsxMIpsecChannelUp	.1.3.6.1.4.1.6876.90.1.2.4.0.48	Normal
vmwNsxMIpsecChannelDown	.1.3.6.1.4.1.6876.90.1.2.4.0.49	Normal
vmwNsxMIpsecTunnelUp	.1.3.6.1.4.1.6876.90.1.2.4.0.50	Normal
vmwNsxMIpsecTunnelDown	.1.3.6.1.4.1.6876.90.1.2.4.0.51	Normal
vmwNsxMIpsecChannelUnknown	.1.3.6.1.4.1.6876.90.1.2.4.0.52	Normal
vmwNsxMIpsecTunnelUnknown	.1.3.6.1.4.1.6876.90.1.2.4.0.53	Normal
vmwNsxMGlobalLbMemberUp	.1.3.6.1.4.1.6876.90.1.2.4.0.54	Normal
vmwNsxMGlobalLbMemberWarning	.1.3.6.1.4.1.6876.90.1.2.4.0.55	Normal
vmwNsxMGlobalLbMemberDown	.1.3.6.1.4.1.6876.90.1.2.4.0.56	Normal
vmwNsxMGlobalLbMemberUnknown	.1.3.6.1.4.1.6876.90.1.2.4.0.57	Normal
vmwNsxMGlobalLbPeerUp	.1.3.6.1.4.1.6876.90.1.2.4.0.58	Normal
vmwNsxMGlobalLbPeerDown	.1.3.6.1.4.1.6876.90.1.2.4.0.59	Normal
vmwNsxMDhcpServiceDisabled	.1.3.6.1.4.1.6876.90.1.2.4.0.60	Normal
vmwNsxMEdgeResourceReservationFailure	.1.3.6.1.4.1.6876.90.1.2.4.0.61	Normal
vmwNsxMEdgeSplitBrainDetected	.1.3.6.1.4.1.6876.90.1.2.4.0.62	Normal
vmwNsxMEdgeSplitBrainRecovered	.1.3.6.1.4.1.6876.90.1.2.4.0.63	Normal
vmwNsxMEdgeSplitBrainRecoveryAttempt	.1.3.6.1.4.1.6876.90.1.2.4.0.64	Normal
vmwNsxMEdgeResourceReservationSuccess	.1.3.6.1.4.1.6876.90.1.2.4.0.65	Normal
vmwNsxMEdgeSddcChannelUp	.1.3.6.1.4.1.6876.90.1.2.4.0.66	Normal
vmwNsxMEdgeSddcChannelDown	.1.3.6.1.4.1.6876.90.1.2.4.0.67	Normal
vmwNsxMEdgeDuplicateIpDetected	.1.3.6.1.4.1.6876.90.1.2.4.0.68	Normal
vmwNsxMEdgeDuplicateIpResolved	.1.3.6.1.4.1.6876.90.1.2.4.0.69	Normal
vmwNsxMEdgeBgpNeighborUp	.1.3.6.1.4.1.6876.90.1.2.4.0.70	Normal
vmwNsxMEdgeBgpNeighborDown	.1.3.6.1.4.1.6876.90.1.2.4.0.71	Normal
vmwNsxMEdgeBgpNeighborASMismatch	.1.3.6.1.4.1.6876.90.1.2.4.0.72	Normal

Name	OID	Severity
vmwNsxMEdgeOSPFNeighborUp	.1.3.6.1.4.1.6876.90.1.2.4.0.73	Normal
vmwNsxMEdgeOSPFNeighborDown	.1.3.6.1.4.1.6876.90.1.2.4.0.74	Normal
vmwNsxMEdgeOSPFNeighborMTUMismatch	.1.3.6.1.4.1.6876.90.1.2.4.0.75	Normal
vmwNsxMEdgeOSPFNeighborAreaIdMisMatch	.1.3.6.1.4.1.6876.90.1.2.4.0.76	Normal
vmwNsxMEdgeOSPFNeighborHelloTimerMisMatch	.1.3.6.1.4.1.6876.90.1.2.4.0.77	Normal
vmwNsxMEdgeOSPFNeighborDeadTimerMisMatch	.1.3.6.1.4.1.6876.90.1.2.4.0.78	Normal
vmwNsxMEdgeL2vpnTunnelUp	.1.3.6.1.4.1.6876.90.1.2.4.0.79	Normal
vmwNsxMEdgeL2vpnTunnelDown	.1.3.6.1.4.1.6876.90.1.2.4.0.80	Normal
vmwNsxMEdgeHAForceStandbyRemoved	.1.3.6.1.4.1.6876.90.1.2.4.0.81	Normal
vmwNsxMEdgeHAForceStandbyRemovalFailed	.1.3.6.1.4.1.6876.90.1.2.4.0.82	Normal
vmwNsxMEdgeVmBADStateRecovered	.1.3.6.1.4.1.6876.90.1.2.4.0.83	Normal
vmwNsxMEdgeVmBADStateAutoHealRecoveryDisabled	.1.3.6.1.4.1.6876.90.1.2.4.0.84	Normal
vmwNsxMEdgeHaInUseVnicChanged	.1.3.6.1.4.1.6876.90.1.2.4.0.85	Normal
vmwNsxMEdgeHaCommConnected	.1.3.6.1.4.1.6876.90.1.2.4.0.86	Normal
vmwNsxMEndpointThinAgentEnabled	.1.3.6.1.4.1.6876.90.1.2.5.0.1	Normal
vmwNsxMGuestIntrspctnEnabled	.1.3.6.1.4.1.6876.90.1.2.5.0.2	Normal
vmwNsxMGuestIntrspctnIncompatibleEsx	.1.3.6.1.4.1.6876.90.1.2.5.0.3	Normal
vmwNsxMGuestIntrspctnEsxConnFailed	.1.3.6.1.4.1.6876.90.1.2.5.0.4	Normal
vmwNsxMGuestIntrspctnStatusRcvFailed	.1.3.6.1.4.1.6876.90.1.2.5.0.5	Normal
vmwNsxMEsxModuleEnabled	.1.3.6.1.4.1.6876.90.1.2.5.0.6	Normal
vmwNsxMEsxModuleUninstalled	.1.3.6.1.4.1.6876.90.1.2.5.0.7	Normal
vmwNsxMGuestIntrspctnHstMxMssngRep	.1.3.6.1.4.1.6876.90.1.2.5.0.8	Normal
vmwNsxMEndpointUndefined	.1.3.6.1.4.1.6876.90.1.2.5.0.9	Normal
vmwNsxMEamGenericAlarm	.1.3.6.1.4.1.6876.90.1.2.6.0.1	Normal
vmwNsxMFabricDplymntStatusChanged	.1.3.6.1.4.1.6876.90.1.2.7.0.1	Normal
vmwNsxMFabricDplymntUnitCreated	.1.3.6.1.4.1.6876.90.1.2.7.0.2	Normal
vmwNsxMFabricDplymntUnitUpdated	.1.3.6.1.4.1.6876.90.1.2.7.0.3	Normal
vmwNsxMFabricDplymntUnitDestroyed	.1.3.6.1.4.1.6876.90.1.2.7.0.4	Normal
vmwNsxMDataStoreNotCnfgrdOnHost	.1.3.6.1.4.1.6876.90.1.2.7.0.5	Normal
vmwNsxMFabricDplymntInstallationFailed	.1.3.6.1.4.1.6876.90.1.2.7.0.6	Normal
vmwNsxMFabricAgentCreated	.1.3.6.1.4.1.6876.90.1.2.7.0.7	Normal
vmwNsxMFabricAgentDestroyed	.1.3.6.1.4.1.6876.90.1.2.7.0.8	Normal
vmwNsxMFabricSrvceNeedsRedplymnt	.1.3.6.1.4.1.6876.90.1.2.7.0.9	Normal
vmwNsxMUpgradeOfDplymntFailed	.1.3.6.1.4.1.6876.90.1.2.7.0.10	Normal
vmwNsxMFabricDependenciesNotInstalled	.1.3.6.1.4.1.6876.90.1.2.7.0.11	Normal
vmwNsxMFabricErrorNotifSecBfrUpgrade	.1.3.6.1.4.1.6876.90.1.2.7.0.12	Normal
vmwNsxMFabricErrCallbackNtRcvdUpgrade	.1.3.6.1.4.1.6876.90.1.2.7.0.13	Normal
vmwNsxMFabricErrCallbackNtRcvdUninstall	.1.3.6.1.4.1.6876.90.1.2.7.0.14	Normal
vmwNsxMFabricUninstallServiceFailed	.1.3.6.1.4.1.6876.90.1.2.7.0.15	Normal
vmwNsxMFabricErrorNotifSecBfrUninstall	.1.3.6.1.4.1.6876.90.1.2.7.0.16	Normal
vmwNsxMFabricServerRebootUninstall	.1.3.6.1.4.1.6876.90.1.2.7.0.17	Normal
vmwNsxMFabricServerRebootUpgrade	.1.3.6.1.4.1.6876.90.1.2.7.0.18	Normal
vmwNsxMFabricConnEamFailed	.1.3.6.1.4.1.6876.90.1.2.7.0.19	Normal
vmwNsxMFabricConnEamRestored	.1.3.6.1.4.1.6876.90.1.2.7.0.20	Normal
vmwNsxMFabricPreUninstallCleanUpFailed	.1.3.6.1.4.1.6876.90.1.2.7.0.21	Normal
vmwNsxMFabricBackingEamNotFound	.1.3.6.1.4.1.6876.90.1.2.7.0.22	Normal
vmwNsxMFabricVibManualInstallationRequired	.1.3.6.1.4.1.6876.90.1.2.7.0.23	Normal

Name	OID	Severity
vmwNsxMFabricUninstallDeploymentUnit	.1.3.6.1.4.1.6876.90.1.2.7.0.24	Normal
vmwNsxMDepPluginIpPoolExhausted	.1.3.6.1.4.1.6876.90.1.2.8.0.1	Normal
vmwNsxMDepPluginGenericAlarm	.1.3.6.1.4.1.6876.90.1.2.8.0.2	Normal
vmwNsxMDepPluginGenericException	.1.3.6.1.4.1.6876.90.1.2.8.0.3	Normal
vmwNsxMDepPluginVmReboot	.1.3.6.1.4.1.6876.90.1.2.8.0.4	Normal
vmwNsxMMessagingConfigFailed	.1.3.6.1.4.1.6876.90.1.2.9.0.1	Normal
vmwNsxMMessagingReconfigFailed	.1.3.6.1.4.1.6876.90.1.2.9.0.2	Normal
vmwNsxMMessagingConfigFailedNotifSkip	.1.3.6.1.4.1.6876.90.1.2.9.0.3	Normal
vmwNsxMMessagingInfraUp	.1.3.6.1.4.1.6876.90.1.2.9.0.4	Normal
vmwNsxMMessagingInfraDown	.1.3.6.1.4.1.6876.90.1.2.9.0.5	Normal
vmwNsxMMessagingDisabled	.1.3.6.1.4.1.6876.90.1.2.9.0.6	Normal
vmwNsxMServiceComposerPolicyOutOfSync	.1.3.6.1.4.1.6876.90.1.2.10.0.1	Normal
vmwNsxMServiceComposerPolicyDeleted	.1.3.6.1.4.1.6876.90.1.2.10.0.2	Normal
vmwNsxMServiceComposerFirewallPolicyOutOfSync	.1.3.6.1.4.1.6876.90.1.2.10.0.3	Normal
vmwNsxMServiceComposerNetworkPolicyOutOfSync	.1.3.6.1.4.1.6876.90.1.2.10.0.4	Normal
vmwNsxMServiceComposerGuestPolicyOutOfSync	.1.3.6.1.4.1.6876.90.1.2.10.0.5	Normal
vmwNsxMServiceComposerOutOfSync	.1.3.6.1.4.1.6876.90.1.2.10.0.6	Normal
vmwNsxMServiceComposerOutOfSyncRebootFailure	.1.3.6.1.4.1.6876.90.1.2.10.0.7	Normal
vmwNsxMServiceComposerOutOfSyncDraftRollback	.1.3.6.1.4.1.6876.90.1.2.10.0.8	Normal
vmwNsxMServiceComposerOutOfSyncSectionDeletionFailure	.1.3.6.1.4.1.6876.90.1.2.10.0.9	Normal
vmwNsxMServiceComposerOutOfSyncPrecedenceChangeFailure	.1.3.6.1.4.1.6876.90.1.2.10.0.10	Normal
vmwNsxMServiceComposerOutOfSyncDraftSettingFailure	.1.3.6.1.4.1.6876.90.1.2.10.0.11	Normal
vmwNsxMInconsistentSvmAlarm	.1.3.6.1.4.1.6876.90.1.2.11.0.1	Normal
vmwNsxMSvmRestartAlarm	.1.3.6.1.4.1.6876.90.1.2.11.0.2	Normal
vmwNsxMSvmAgentUnavailable	.1.3.6.1.4.1.6876.90.1.2.11.0.3	Normal
vmwNsxMVmAddedToSg	.1.3.6.1.4.1.6876.90.1.2.12.0.1	Normal
vmwNsxMVmRemovedFromSg	.1.3.6.1.4.1.6876.90.1.2.12.0.2	Normal
vmwNsxMFullUniversalSyncFailed	.1.3.6.1.4.1.6876.90.1.2.13.0.1	Normal
vmwNsxMSecondaryDown	.1.3.6.1.4.1.6876.90.1.2.13.0.2	Normal
vmwNsxMUniversalSyncFailedForEntity	.1.3.6.1.4.1.6876.90.1.2.13.0.3	Normal
vmwNsxMUniversalSyncStoppedOnSecondary	.1.3.6.1.4.1.6876.90.1.2.13.0.4	Normal
vmwNsxMUniversalSyncResumedOnSecondary	.1.3.6.1.4.1.6876.90.1.2.13.0.5	Normal
vmwNsxMServerUp	.1.3.6.1.4.1.6876.90.1.2.14.0.1	Normal
vmwNsxMExtensionRegistered	.1.3.6.1.4.1.6876.90.1.2.15.0.1	Normal
vmwNsxMExtensionUpdated	.1.3.6.1.4.1.6876.90.1.2.15.0.2	Normal
vmwNsxMDataSecScanStarted	.1.3.6.1.4.1.6876.90.1.2.16.0.1	Normal
vmwNsxMDataSecScanEnded	.1.3.6.1.4.1.6876.90.1.2.16.0.2	Normal
vmwNsxMSamDataCollectionEnabled	.1.3.6.1.4.1.6876.90.1.2.17.0.1	Normal
vmwNsxMSamDataCollectionDisabled	.1.3.6.1.4.1.6876.90.1.2.17.0.2	Normal
vmwNsxMSamDataStoppedFlowing	.1.3.6.1.4.1.6876.90.1.2.17.0.3	Normal
vmwNsxMSamDataResumedFlowing	.1.3.6.1.4.1.6876.90.1.2.17.0.4	Normal
vmwNsxMUsvmHeartbeatStopped	.1.3.6.1.4.1.6876.90.1.2.18.0.1	Normal
vmwNsxMUsvmHeartbeatResumed	.1.3.6.1.4.1.6876.90.1.2.18.0.2	Normal
vmwNsxMUsvmReceivedHello	.1.3.6.1.4.1.6876.90.1.2.18.0.3	Normal

Name	OID	Severity
vmwNsxMUpgradeSuccess	.1.3.6.1.4.1.6876.90.1.2.19.0.1	Normal
vmwNsxMRestoreSuccess	.1.3.6.1.4.1.6876.90.1.2.19.0.2	Normal
vmwNsxMDuplicateIp	.1.3.6.1.4.1.6876.90.1.2.19.0.3	Normal
vmwNsxMCPUHigh	.1.3.6.1.4.1.6876.90.1.2.19.0.12	Normal
vmwNsxMCPUNormal	.1.3.6.1.4.1.6876.90.1.2.19.0.13	Normal
vmwNsxMVirtualMachineMarkedAsSystemResource	.1.3.6.1.4.1.6876.90.1.2.19.0.4	Normal
vmwNsxMScaleAboveSupportedLimits	.1.3.6.1.4.1.6876.90.1.2.19.0.5	Normal
vmwNsxMScaleAboveThreshold	.1.3.6.1.4.1.6876.90.1.2.19.0.6	Normal
vmwNsxMScaleNormalized	.1.3.6.1.4.1.6876.90.1.2.19.0.7	Normal
vmwNsxMScaleNotEqualToRecommendedValue	.1.3.6.1.4.1.6876.90.1.2.19.0.8	Normal
vmwNsxMCertificateExpired	.1.3.6.1.4.1.6876.90.1.2.19.0.10	Normal
vmwNsxMCertificateAboutToExpire	.1.3.6.1.4.1.6876.90.1.2.19.0.11	Normal
vmwNsxMVxlanLogicalSwitchImproperlyCnfg	.1.3.6.1.4.1.6876.90.1.2.20.0.1	Normal
vmwNsxMVxlanLogicalSwitchProperlyCnfg	.1.3.6.1.4.1.6876.90.1.2.20.0.2	Normal
vmwNsxMVxlanInitFailed	.1.3.6.1.4.1.6876.90.1.2.20.0.3	Normal
vmwNsxMVxlanPortInitFailed	.1.3.6.1.4.1.6876.90.1.2.20.0.4	Normal
vmwNsxMVxlanInstanceDoesNotExist	.1.3.6.1.4.1.6876.90.1.2.20.0.5	Normal
vmwNsxMVxlanLogicalSwitchWrkngImproperly	.1.3.6.1.4.1.6876.90.1.2.20.0.6	Normal
vmwNsxMVxlanTransportZoneIncorrectlyWrkng	.1.3.6.1.4.1.6876.90.1.2.20.0.7	Normal
vmwNsxMVxlanTransportZoneNotUsed	.1.3.6.1.4.1.6876.90.1.2.20.0.8	Normal
vmwNsxMVxlanOverlayClassMissingOnDvs	.1.3.6.1.4.1.6876.90.1.2.20.0.9	Normal
vmwNsxMVxlanControllerRemoved	.1.3.6.1.4.1.6876.90.1.2.20.0.10	Normal
vmwNsxMVxlanControllerConnProblem	.1.3.6.1.4.1.6876.90.1.2.20.0.11	Normal
vmwNsxMVxlanControllerInactive	.1.3.6.1.4.1.6876.90.1.2.20.0.12	Normal
vmwNsxMVxlanControllerActive	.1.3.6.1.4.1.6876.90.1.2.20.0.13	Normal
vmwNsxMVxlanVmknicMissingOrDeleted	.1.3.6.1.4.1.6876.90.1.2.20.0.14	Normal
vmwNsxMVxlanInfo	.1.3.6.1.4.1.6876.90.1.2.20.0.15	Normal
vmwNsxMVxlanVmknicPortGrpMissing	.1.3.6.1.4.1.6876.90.1.2.20.0.16	Normal
vmwNsxMVxlanVmknicPortGrpAppears	.1.3.6.1.4.1.6876.90.1.2.20.0.17	Normal
vmwNsxMVxlanConnDown	.1.3.6.1.4.1.6876.90.1.2.20.0.18	Normal
vmwNsxMBackingPortgroupMissing	.1.3.6.1.4.1.6876.90.1.2.20.0.19	Normal
vmwNsxMBackingPortgroupReappears	.1.3.6.1.4.1.6876.90.1.2.20.0.20	Normal
vmwNsxMManagedObjectIdChanged	.1.3.6.1.4.1.6876.90.1.2.20.0.21	Normal
vmwNsxMHighLatencyOnDisk	.1.3.6.1.4.1.6876.90.1.2.20.0.22	Normal
vmwNsxMHighLatencyOnDiskResolved	.1.3.6.1.4.1.6876.90.1.2.20.0.23	Normal
vmwNsxMControllerVmPoweredOff	.1.3.6.1.4.1.6876.90.1.2.20.0.24	Normal
vmwNsxMControllerVmDeleted	.1.3.6.1.4.1.6876.90.1.2.20.0.25	Normal
vmwNsxMVxlanConfigNotSet	.1.3.6.1.4.1.6876.90.1.2.20.0.26	Normal
vmwNsxMVxlanPortgroupDeleted	.1.3.6.1.4.1.6876.90.1.2.20.0.27	Normal
vmwNsxMVxlanVDSandPgMismatch	.1.3.6.1.4.1.6876.90.1.2.20.0.28	Normal
vmwNsxMVxlanControllerDisconnected	.1.3.6.1.4.1.6876.90.1.2.20.0.29	Normal
vmwNsxMVxlanControllerConnected	.1.3.6.1.4.1.6876.90.1.2.20.0.30	Normal
vmwNsxMVxlanControllerVmPoweredOn	.1.3.6.1.4.1.6876.90.1.2.20.0.31	Normal
vmwNsxMVxlanHostEvents	.1.3.6.1.4.1.6876.90.1.2.20.0.32	Normal
vmwNsxMLogserverEventGenStopped	.1.3.6.1.4.1.6876.90.1.2.21.0.1	Normal
vmwNsxMApplicationRuleManagerFlowAnalysisStart	.1.3.6.1.4.1.6876.90.1.2.22.0.1	Normal
vmwNsxMApplicationRuleManagerFlowAnalysisFailed	.1.3.6.1.4.1.6876.90.1.2.22.0.2	Normal

Name	OID	Severity
vmwNsxMApplicationRuleManagerFlowAnalysisComplete	.1.3.6.1.4.1.6876.90.1.2.22.0.3	Normal
vmwareSrmRecoveryPlanExecuteTestBeginTrap	.1.3.6.1.4.1.6876.51.0.1	Normal
vmwareSrmRecoveryPlanExecuteTestEndEvent	.1.3.6.1.4.1.6876.51.0.2	Normal
vmwareSrmRecoveryPlanExecuteBeginEvent	.1.3.6.1.4.1.6876.51.0.3	Normal
vmwareVmwSrmRecoveryPlanExecuteEndEvent	.1.3.6.1.4.1.6876.51.0.4	Normal
vmwareVmwSrmRecoveryVmBeginEvent	.1.3.6.1.4.1.6876.51.0.5	Normal
vmwareSrmRecoveryVmEndEvent	.1.3.6.1.4.1.6876.51.0.6	Normal
vmwareSrmRecoveryPlanPromptDisplay	.1.3.6.1.4.1.6876.51.0.7	Normal
vmwareSrmRecoveryPlanPromptResponse	.1.3.6.1.4.1.6876.51.0.8	Normal
vmwareVmwSrmRecoveryPlanServerCommandBegin	.1.3.6.1.4.1.6876.51.0.9	Normal
vmwareSrmRecoveryPlanServerCommandEnd	.1.3.6.1.4.1.6876.51.0.10	Normal
vmwareSrmRecoveryPlanVmCommandBegin	.1.3.6.1.4.1.6876.51.0.11	Normal
vmwareSrmRecoveryPlanVmCommandEnd	.1.3.6.1.4.1.6876.51.0.12	Normal
vmwareSrmRecoveryPlanExecuteReprotectBegin	.1.3.6.1.4.1.6876.51.0.13	Normal
vmwareSrmRecoveryPlanExecuteReprotectEnd	.1.3.6.1.4.1.6876.51.0.14	Normal
vmwareVmwSrmRecoveryPlanExecuteCleanupBegin	.1.3.6.1.4.1.6876.51.0.15	Normal
vmwSrmRecoveryPlanExecuteCleanupEnd	.1.3.6.1.4.1.6876.51.0.16	Normal
vmwVmPoweredOn	.1.3.6.1.4.1.6876.4.1.0.1	Normal
vmwVmPoweredOff	.1.3.6.1.4.1.6876.4.1.0.2	Normal
vmwVmHBLost	.1.3.6.1.4.1.6876.4.1.0.3	Normal
vmwVmHBDetected	.1.3.6.1.4.1.6876.4.1.0.4	Normal
vmwVmSuspended	.1.3.6.1.4.1.6876.4.1.0.5	Normal

HPE iLO:

Name	OID	Severity
cpqIdeDriveDegraded	.1.3.6.1.4.1.232.0.14001	Critical
cpqIdeDriveOk	.1.3.6.1.4.1.232.0.14002	Informational
cpqIdeDriveUltraAtaDegraded	.1.3.6.1.4.1.232.0.14003	Informational
cpqIdeAtaDiskStatusChange	.1.3.6.1.4.1.232.0.14004	Critical
cpqIdeLogicalDriveStatusChange	.1.3.6.1.4.1.232.0.14005	Critical
cpqIdeAtaDiskSSDWearStatusChange	.1.3.6.1.4.1.232.0.14006	Critical
cpqDaLogDrvStatusChange	.1.3.6.1.4.1.232.3.0.1	Critical
cpqDaSpareStatusChange	.1.3.6.1.4.1.232.3.0.2	Critical
cpqDaPhyDrvStatusChange	.1.3.6.1.4.1.232.3.0.3	Critical
cpqDaPhyDrvThreshPassedTrap	.1.3.6.1.4.1.232.3.0.4	Critical
cpqDaAccelStatusChange	.1.3.6.1.4.1.232.3.0.5	Critical
cpqDaAccelBadDataTrap	.1.3.6.1.4.1.232.3.0.6	Critical
cpqDaAccelBatteryFailed	.1.3.6.1.4.1.232.3.0.7	Critical
cpqDa2LogDrvStatusChange	.1.3.6.1.4.1.232.0.3001	Critical
cpqDa2SpareStatusChange	.1.3.6.1.4.1.232.0.3002	Critical
cpqDa2PhyDrvStatusChange	.1.3.6.1.4.1.232.0.3003	Critical
cpqDa2PhyDrvThreshPassedTrap	.1.3.6.1.4.1.232.0.3004	Critical
cpqDa2AccelStatusChange	.1.3.6.1.4.1.232.0.3005	Critical
cpqDa2AccelBadDataTrap	.1.3.6.1.4.1.232.0.3006	Critical
cpqDa2AccelBatteryFailed	.1.3.6.1.4.1.232.0.3007	Critical

Name	OID	Severity
cpqDa3LogDrvStatusChange	.1.3.6.1.4.1.232.0.3008	Critical
cpqDa3SpareStatusChange	.1.3.6.1.4.1.232.0.3009	Critical
cpqDa3PhyDrvStatusChange	.1.3.6.1.4.1.232.0.3010	Critical
cpqDa3PhyDrvThreshPassedTrap	.1.3.6.1.4.1.232.0.3011	Critical
cpqDa3AccelStatusChange	.1.3.6.1.4.1.232.0.3012	Critical
cpqDa3AccelBadDataTrap	.1.3.6.1.4.1.232.0.3013	Critical
cpqDa3AccelBatteryFailed	.1.3.6.1.4.1.232.0.3014	Critical
cpqDaCntlrStatusChange	.1.3.6.1.4.1.232.0.3015	Critical
cpqDaCntlrActive	.1.3.6.1.4.1.232.0.3016	Informational
cpqDa4SpareStatusChange	.1.3.6.1.4.1.232.0.3017	Critical
cpqDa4PhyDrvStatusChange	.1.3.6.1.4.1.232.0.3018	Critical
cpqDa4PhyDrvThreshPassedTrap	.1.3.6.1.4.1.232.0.3019	Critical
cpqDaTapeLibraryStatusChange	.1.3.6.1.4.1.232.0.3020	Critical
cpqDaTapeLibraryDoorStatusChange	.1.3.6.1.4.1.232.0.3021	Critical
cpqDaTapeDriveStatusChange	.1.3.6.1.4.1.232.0.3022	Critical
cpqDaTapeDriveCleaningRequired	.1.3.6.1.4.1.232.0.3023	Major
cpqDaTapeDriveCleanTapeReplace	.1.3.6.1.4.1.232.0.3024	Major
cpqDa5AccelStatusChange	.1.3.6.1.4.1.232.0.3025	Critical
cpqDa5AccelBadDataTrap	.1.3.6.1.4.1.232.0.3026	Critical
cpqDa5AccelBatteryFailed	.1.3.6.1.4.1.232.0.3027	Critical
cpqDa5CntlrStatusChange	.1.3.6.1.4.1.232.0.3028	Critical
cpqDa5PhyDrvStatusChange	.1.3.6.1.4.1.232.0.3029	Critical
cpqDa5PhyDrvThreshPassedTrap	.1.3.6.1.4.1.232.0.3030	Critical
cpqDa2TapeLibraryStatusChange	.1.3.6.1.4.1.232.0.3031	Critical
cpqDa2TapeDriveStatusChange	.1.3.6.1.4.1.232.0.3032	Critical
cpqDa6CntlrStatusChange	.1.3.6.1.4.1.232.0.3033	Critical
cpqDa6LogDrvStatusChange	.1.3.6.1.4.1.232.0.3034	Critical
cpqDa6SpareStatusChange	.1.3.6.1.4.1.232.0.3035	Critical
cpqDa6PhyDrvStatusChange	.1.3.6.1.4.1.232.0.3036	Critical
cpqDa6PhyDrvThreshPassedTrap	.1.3.6.1.4.1.232.0.3037	Critical
cpqDa6AccelStatusChange	.1.3.6.1.4.1.232.0.3038	Critical
cpqDa6AccelBadDataTrap	.1.3.6.1.4.1.232.0.3039	Critical
cpqDa6AccelBatteryFailed	.1.3.6.1.4.1.232.0.3040	Critical
cpqDa6TapeLibraryStatusChange	.1.3.6.1.4.1.232.0.3041	Critical
cpqDa6TapeLibraryDoorStatusChange	.1.3.6.1.4.1.232.0.3042	Critical
cpqDa6TapeDriveStatusChange	.1.3.6.1.4.1.232.0.3043	Critical
cpqDa6TapeDriveCleaningRequired	.1.3.6.1.4.1.232.0.3044	Major
cpqDa6TapeDriveCleanTapeReplace	.1.3.6.1.4.1.232.0.3045	Major
cpqDa7PhyDrvStatusChange	.1.3.6.1.4.1.232.0.3046	Critical
cpqDa7SpareStatusChange	.1.3.6.1.4.1.232.0.3047	Critical
cpqDaCntlrPartnerStatusChange	.1.3.6.1.4.1.232.0.3048	Critical
cpqDaPhyDrvSSDWearStatusChange	.1.3.6.1.4.1.232.0.3049	Critical
cpqSsFanStatusChange	.1.3.6.1.4.1.232.8.0.1	Critical
cpqSs2FanStatusChange	.1.3.6.1.4.1.232.0.8001	Critical
cpqSsTempFailed	.1.3.6.1.4.1.232.0.8002	Critical
cpqSsTempDegraded	.1.3.6.1.4.1.232.0.8003	Major
cpqSsTempOk	.1.3.6.1.4.1.232.0.8004	Informational
cpqSsSidePanelInPlace	.1.3.6.1.4.1.232.0.8005	Informational
cpqSsSidePanelRemoved	.1.3.6.1.4.1.232.0.8006	Major
cpqSsPwrSupplyDegraded	.1.3.6.1.4.1.232.0.8007	Critical

Name	OID	Severity
cpqSs3FanStatusChange	.1.3.6.1.4.1.232.0.8008	Critical
cpqSs3TempFailed	.1.3.6.1.4.1.232.0.8009	Critical
cpqSs3TempDegraded	.1.3.6.1.4.1.232.0.8010	Major
cpqSs3TempOk	.1.3.6.1.4.1.232.0.8011	Informational
cpqSs3SidePanelInPlace	.1.3.6.1.4.1.232.0.8012	Informational
cpqSs3SidePanelRemoved	.1.3.6.1.4.1.232.0.8013	Major
cpqSs3PwrSupplyDegraded	.1.3.6.1.4.1.232.0.8014	Critical
cpqSs4PwrSupplyDegraded	.1.3.6.1.4.1.232.0.8015	Critical
cpqSsExFanStatusChange	.1.3.6.1.4.1.232.0.8016	Critical
cpqSsExPowerSupplyStatusChange	.1.3.6.1.4.1.232.0.8017	Critical
cpqSsExPowerSupplyUpsStatusChange	.1.3.6.1.4.1.232.0.8018	Critical
cpqSsExTempSensorStatusChange	.1.3.6.1.4.1.232.0.8019	Critical
cpqSsEx2FanStatusChange	.1.3.6.1.4.1.232.0.8020	Critical
cpqSsEx2PowerSupplyStatusChange	.1.3.6.1.4.1.232.0.8021	Critical
cpqSsExBackplaneFanStatusChange	.1.3.6.1.4.1.232.0.8022	Critical
cpqSsExBackplaneTempStatusChange	.1.3.6.1.4.1.232.0.8023	Critical
cpqSsExBackplanePowerSupplyStatusChange	.1.3.6.1.4.1.232.0.8024	Critical
cpqSsExRecoveryServerStatusChange	.1.3.6.1.4.1.232.0.8025	Major
cpqSs5FanStatusChange	.1.3.6.1.4.1.232.0.8026	Critical
cpqSs5TempStatusChange	.1.3.6.1.4.1.232.0.8027	Critical
cpqSs5PwrSupplyStatusChange	.1.3.6.1.4.1.232.0.8028	Critical
cpqSs6FanStatusChange	.1.3.6.1.4.1.232.0.8029	Critical
cpqSs6TempStatusChange	.1.3.6.1.4.1.232.0.8030	Critical
cpqSs6PwrSupplyStatusChange	.1.3.6.1.4.1.232.0.8031	Critical
cpqSsConnectionStatusChange	.1.3.6.1.4.1.232.0.8032	Critical
cpqSsGSIStatusChange	.1.3.6.1.4.1.232.0.8033	Critical
cpqSm2ServerReset	.1.3.6.1.4.1.232.0.9001	Critical
cpqSm2ServerPowerOutage	.1.3.6.1.4.1.232.0.9002	Critical
cpqSm2UnauthorizedLoginAttempts	.1.3.6.1.4.1.232.0.9003	Informational
cpqSm2BatteryFailed	.1.3.6.1.4.1.232.0.9004	Critical
cpqSm2SelfTestError	.1.3.6.1.4.1.232.0.9005	Critical
cpqSm2InterfaceError	.1.3.6.1.4.1.232.0.9006	Major
cpqSm2BatteryDisconnected	.1.3.6.1.4.1.232.0.9007	Major
cpqSm2KeyboardCableDisconnected	.1.3.6.1.4.1.232.0.9008	Major
cpqSm2MouseCableDisconnected	.1.3.6.1.4.1.232.0.9009	Major
cpqSm2ExternalPowerCableDisconnected	.1.3.6.1.4.1.232.0.9010	Major
cpqSm2LogsFull	.1.3.6.1.4.1.232.0.9011	Minor
cpqSm2SecurityOverrideEngaged	.1.3.6.1.4.1.232.0.9012	Informational
cpqSm2SecurityOverrideDisengaged	.1.3.6.1.4.1.232.0.9013	Informational
cpqSm2ServerFatalError	.1.3.6.1.4.1.232.0.9014	Critical
cpqSm2NicLinkDown	.1.3.6.1.4.1.232.0.9015	Critical
cpqSm2NicLinkUp	.1.3.6.1.4.1.232.0.9016	Informational
cpqSm2ServerPowerOn	.1.3.6.1.4.1.232.0.9017	Informational
cpqSm2ServerPowerOff	.1.3.6.1.4.1.232.0.9018	Informational
cpqSm2ServerPowerOnFailure	.1.3.6.1.4.1.232.0.9019	Critical
cpqSm2IrsCommFailure	.1.3.6.1.4.1.232.0.9020	Major
cpqHoGenericTrap	.1.3.6.1.4.1.232.0.11001	Major
cpqHoAppErrorTrap	.1.3.6.1.4.1.232.0.11002	Major
cpqHo2GenericTrap	.1.3.6.1.4.1.232.0.11003	Major
cpqHo2AppErrorTrap	.1.3.6.1.4.1.232.0.11004	Major

Name	OID	Severity
cpqHo2NicStatusOk	.1.3.6.1.4.1.232.0.11005	Major
cpqHo2NicStatusFailed	.1.3.6.1.4.1.232.0.11006	Major
cpqHo2NicSwitchoverOccurred	.1.3.6.1.4.1.232.0.11007	Major
cpqHo2NicStatusOk2	.1.3.6.1.4.1.232.0.11008	Major
cpqHo2NicStatusFailed2	.1.3.6.1.4.1.232.0.11009	Major
cpqHo2NicSwitchoverOccurred2	.1.3.6.1.4.1.232.0.11010	Major
cpqHoProcessEventTrap	.1.3.6.1.4.1.232.0.11011	Major
cpqHoProcessCountWarning	.1.3.6.1.4.1.232.0.11012	Major
cpqHoProcessCountNormal	.1.3.6.1.4.1.232.0.11013	Informational
cpqHoCriticalSoftwareUpdateTrap	.1.3.6.1.4.1.232.0.11014	Critical
cpqHoCrashDumpNotEnabledTrap	.1.3.6.1.4.1.232.0.11015	Warning
cpqHoBootPagingFileTooSmallTrap	.1.3.6.1.4.1.232.0.11016	Warning
cpqHoSWRunningStatusChangeTrap	.1.3.6.1.4.1.232.0.11017	Warning
cpqHo2PowerThresholdTrap	.1.3.6.1.4.1.232.0.11018	Minor
cpqHoBootPagingFileOrFreeSpaceTooSmallTrap	.1.3.6.1.4.1.232.0.11019	Warning
cpqHoMibHealthStatusArrayChangeTrap	.1.3.6.1.4.1.232.0.11020	Informational
cpqNicConnectivityRestored	.1.3.6.1.4.1.232.0.18001	Informational
cpqNicConnectivityLost	.1.3.6.1.4.1.232.0.18002	Major
cpqNicRedundancyIncreased	.1.3.6.1.4.1.232.0.18003	Informational
cpqNicRedundancyReduced	.1.3.6.1.4.1.232.0.18004	Major
cpqNic2ConnectivityRestored	.1.3.6.1.4.1.232.0.18005	Informational
cpqNic2ConnectivityLost	.1.3.6.1.4.1.232.0.18006	Major
cpqNic2RedundancyIncreased	.1.3.6.1.4.1.232.0.18007	Informational
cpqNic2RedundancyReduced	.1.3.6.1.4.1.232.0.18008	Major
cpqNicVirusLikeActivityDetected	.1.3.6.1.4.1.232.0.18009	Major
cpqNicVirusLikeActivityStopped	.1.3.6.1.4.1.232.0.18010	Informational
cpqNic3ConnectivityRestored	.1.3.6.1.4.1.232.0.18011	Informational
cpqNic3ConnectivityLost	.1.3.6.1.4.1.232.0.18012	Major
cpqNic3RedundancyIncreased	.1.3.6.1.4.1.232.0.18013	Informational
cpqNic3RedundancyReduced	.1.3.6.1.4.1.232.0.18014	Major
cpqSeCpuThresholdPassed	.1.3.6.1.4.1.232.0.1001	Minor
cpqSePCCardThermalDegraded	.1.3.6.1.4.1.232.0.1002	Major
cpqSePCCardThermalFailure	.1.3.6.1.4.1.232.0.1003	Critical
cpqSePCCardThermalSafe	.1.3.6.1.4.1.232.0.1004	Informational
cpqSe2CpuThresholdPassed	.1.3.6.1.4.1.232.0.1005	Minor
cpqSeCpuStatusChange	.1.3.6.1.4.1.232.0.1006	Major
cpqSeCpuPowerPodstatusChange	.1.3.6.1.4.1.232.0.1007	Major
cpqSeUSBStorageDeviceAttached	.1.3.6.1.4.1.232.0.1008	Informational
cpqSeUSBStorageDeviceRemoved	.1.3.6.1.4.1.232.0.1009	Informational
cpqScsiCntlrStatusChange	.1.3.6.1.4.1.232.5.0.1	Critical
cpqScsiLogDrvStatusChange	.1.3.6.1.4.1.232.5.0.2	Critical
cpqScsiPhyDrvStatusChange	.1.3.6.1.4.1.232.5.0.3	Critical
cpqScsi2CntlrStatusChange	.1.3.6.1.4.1.232.0.5001	Critical
cpqScsi2LogDrvStatusChange	.1.3.6.1.4.1.232.0.5002	Critical
cpqScsi2PhyDrvStatusChange	.1.3.6.1.4.1.232.0.5003	Critical
cpqTapePhyDrvStatusChange	.1.3.6.1.4.1.232.0.5004	Critical
cpqScsi3CntlrStatusChange	.1.3.6.1.4.1.232.0.5005	Critical
cpqScsi3PhyDrvStatusChange	.1.3.6.1.4.1.232.0.5006	Critical
cpqTape3PhyDrvStatusChange	.1.3.6.1.4.1.232.0.5007	Critical
cpqTape3PhyDrvCleaningRequired	.1.3.6.1.4.1.232.0.5008	Major

Name	OID	Severity
cpqTape3PhyDrvCleanTapeReplace	.1.3.6.1.4.1.232.0.5009	Major
cpqTape3LibraryFailed	.1.3.6.1.4.1.232.0.5010	Major
cpqTape3LibraryOkay	.1.3.6.1.4.1.232.0.5011	Informational
cpqTape3LibraryDegraded	.1.3.6.1.4.1.232.0.5012	Critical
cpqTape3LibraryDoorOpen	.1.3.6.1.4.1.232.0.5013	Critical
cpqTape3LibraryDoorClosed	.1.3.6.1.4.1.232.0.5014	Informational
cpqScsiCdLibraryStatusChange	.1.3.6.1.4.1.232.0.5015	Critical
cpqTape4PhyDrvStatusChange	.1.3.6.1.4.1.232.0.5016	Critical
cpqScsi4PhyDrvStatusChange	.1.3.6.1.4.1.232.0.5017	Critical
cpqTapeLibraryStatusChange	.1.3.6.1.4.1.232.0.5018	Critical
cpqTape5PhyDrvStatusChange	.1.3.6.1.4.1.232.0.5019	Critical
cpqScsi5PhyDrvStatusChange	.1.3.6.1.4.1.232.0.5020	Critical
cpqScsi3LogDrvStatusChange	.1.3.6.1.4.1.232.0.5021	Critical
cpqSasPhyDrvStatusChange	.1.3.6.1.4.1.232.0.5022	Critical
cpqSasLogDrvStatusChange	.1.3.6.1.4.1.232.0.5023	Critical
cpqSas2TapeDrvStatusChange	.1.3.6.1.4.1.232.0.5025	Critical
cpqSasPhyDrvSSDWearStatusChange	.1.3.6.1.4.1.232.0.5026	Critical
cpqSiHoodRemoved	.1.3.6.1.4.1.232.0.2001	Major
cpqSiMonitorConditionOK	.1.3.6.1.4.1.232.0.2002	Informational
cpqSiMonitorConditionDegraded	.1.3.6.1.4.1.232.0.2003	Minor
cpqSiMonitorConditionFailed	.1.3.6.1.4.1.232.0.2004	Critical
cpqSiCorrMemErrStatusDegraded	.1.3.6.1.4.1.232.0.2005	Minor
cpqSiCorrMemErrStatusOk	.1.3.6.1.4.1.232.0.2006	Informational
cpqSiMemConfigChange	.1.3.6.1.4.1.232.0.2007	Informational
cpqSiHotPlugSlotBoardRemoved	.1.3.6.1.4.1.232.0.2008	Informational
cpqSiHotPlugSlotBoardInserted	.1.3.6.1.4.1.232.0.2009	Informational
cpqSiHotPlugSlotPowerUpFailed	.1.3.6.1.4.1.232.0.2010	Critical
cpqSiSysBatteryFailure	.1.3.6.1.4.1.232.0.2011	Major
cpqSiSysBatteryChargingDegraded	.1.3.6.1.4.1.232.0.2012	Major
cpqSiSysBatteryCalibrationError	.1.3.6.1.4.1.232.0.2013	Major
cpqHeCorrectableMemoryError	.1.3.6.1.4.1.232.6.0.1	Minor
cpqHeCorrectableMemoryLogDisabled	.1.3.6.1.4.1.232.6.0.2	Critical
cpqHe2CorrectableMemoryError	.1.3.6.1.4.1.232.0.6001	Minor
cpqHe2CorrectableMemoryLogDisabled	.1.3.6.1.4.1.232.0.6002	Critical
cpqHeThermalTempFailed	.1.3.6.1.4.1.232.0.6003	Critical
cpqHeThermalTempDegraded	.1.3.6.1.4.1.232.0.6004	Critical
cpqHeThermalTempOk	.1.3.6.1.4.1.232.0.6005	Informationalal
cpqHeThermalSystemFanFailed	.1.3.6.1.4.1.232.0.6006	Critical
cpqHeThermalSystemFanDegraded	.1.3.6.1.4.1.232.0.6007	Critical
cpqHeThermalSystemFanOk	.1.3.6.1.4.1.232.0.6008	Informationalal
cpqHeThermalCpuFanFailed	.1.3.6.1.4.1.232.0.6009	Critical
cpqHeThermalCpuFanOk	.1.3.6.1.4.1.232.0.6010	Informationalal
cpqHeAsrConfirmation	.1.3.6.1.4.1.232.0.6011	Minor
cpqHeThermalConfirmation	.1.3.6.1.4.1.232.0.6012	Minor
cpqHePostError	.1.3.6.1.4.1.232.0.6013	Minor
cpqHe3CorrectableMemoryError	.1.3.6.1.4.1.232.0.6015	Minor
cpqHe3CorrectableMemoryLogDisabled	.1.3.6.1.4.1.232.0.6016	Critical
cpqHe3ThermalTempFailed	.1.3.6.1.4.1.232.0.6017	Critical
cpqHe3ThermalTempDegraded	.1.3.6.1.4.1.232.0.6018	Critical
cpqHe3ThermalTempOk	.1.3.6.1.4.1.232.0.6019	Informational

Name	OID	Severity
cpqHe3ThermalSystemFanFailed	.1.3.6.1.4.1.232.0.6020	Critical
cpqHe3ThermalSystemFanDegraded	.1.3.6.1.4.1.232.0.6021	Critical
cpqHe3ThermalSystemFanOk	.1.3.6.1.4.1.232.0.6022	Informational
cpqHe3ThermalCpuFanFailed	.1.3.6.1.4.1.232.0.6023	Critical
cpqHe3ThermalCpuFanOk	.1.3.6.1.4.1.232.0.6024	Informational
cpqHe3AsrConfirmation	.1.3.6.1.4.1.232.0.6025	Minor
cpqHe3ThermalConfirmation	.1.3.6.1.4.1.232.0.6026	Minor
cpqHe3PostError	.1.3.6.1.4.1.232.0.6027	Minor
cpqHe3FltTolPwrSupplyDegraded	.1.3.6.1.4.1.232.0.6028	Critical
cpqHe3CorrMemReplaceMemModule	.1.3.6.1.4.1.232.0.6029	Minor
cpqHe3FltTolPowerSupplyDegraded	.1.3.6.1.4.1.232.0.6030	Critical
cpqHe3FltTolPowerSupplyFailed	.1.3.6.1.4.1.232.0.6031	Critical
cpqHe3FltTolPowerRedundancyLost	.1.3.6.1.4.1.232.0.6032	Major
cpqHe3FltTolPowerSupplyInserted	.1.3.6.1.4.1.232.0.6033	Informational
cpqHe3FltTolPowerSupplyRemoved	.1.3.6.1.4.1.232.0.6034	Major
cpqHe3FltTolFanDegraded	.1.3.6.1.4.1.232.0.6035	Critical
cpqHe3FltTolFanFailed	.1.3.6.1.4.1.232.0.6036	Critical
cpqHe3FltTolFanRedundancyLost	.1.3.6.1.4.1.232.0.6037	Major
cpqHe3FltTolFanInserted	.1.3.6.1.4.1.232.0.6038	Informational
cpqHe3FltTolFanRemoved	.1.3.6.1.4.1.232.0.6039	Major
cpqHe3TemperatureFailed	.1.3.6.1.4.1.232.0.6040	Critical
cpqHe3TemperatureDegraded	.1.3.6.1.4.1.232.0.6041	Critical
cpqHe3TemperatureOk	.1.3.6.1.4.1.232.0.6042	Informational
cpqHe3PowerConverterDegraded	.1.3.6.1.4.1.232.0.6043	Critical
cpqHe3PowerConverterFailed	.1.3.6.1.4.1.232.0.6044	Critical
cpqHe3PowerConverterRedundancyLost	.1.3.6.1.4.1.232.0.6045	Critical
cpqHe3CacheAccelParityError	.1.3.6.1.4.1.232.0.6046	Critical
cpqHeResilientMemOnlineSpareEngaged	.1.3.6.1.4.1.232.0.6047	Major
cpqHe4FltTolPowerSupplyOk	.1.3.6.1.4.1.232.0.6048	Informational
cpqHe4FltTolPowerSupplyDegraded	.1.3.6.1.4.1.232.0.6049	Critical
cpqHe4FltTolPowerSupplyFailed	.1.3.6.1.4.1.232.0.6050	Critical
cpqHeResilientMemMirroredMemoryEngaged	.1.3.6.1.4.1.232.0.6051	Major
cpqHeResilientAdvancedECCMemoryEngaged	.1.3.6.1.4.1.232.0.6052	Major
cpqHeResilientMemXorMemoryEngaged	.1.3.6.1.4.1.232.0.6053	Major
cpqHe3FltTolPowerRedundancyRestored	.1.3.6.1.4.1.232.0.6054	Informational
cpqHe3FltTolFanRedundancyRestored	.1.3.6.1.4.1.232.0.6055	Informational
cpqHe4CorrMemReplaceMemModule	.1.3.6.1.4.1.232.0.6056	Minor
cpqHeResMemBoardRemoved	.1.3.6.1.4.1.232.0.6057	Major
cpqHeResMemBoardInserted	.1.3.6.1.4.1.232.0.6058	Informational
cpqHeResMemBoardBusError	.1.3.6.1.4.1.232.0.6059	Critical
cpqHeEventOccurred	.1.3.6.1.4.1.232.0.6060	Informational
cpqHeManagementProcInReset	.1.3.6.1.4.1.232.0.6061	Minor
cpqHeManagementProcReady	.1.3.6.1.4.1.232.0.6062	Informational
cpqHeManagementProcFailedReset	.1.3.6.1.4.1.232.0.6063	Critical
cpqHe5CorrMemReplaceMemModule	.1.3.6.1.4.1.232.0.6064	Major
cpqHe5ResMemBoardRemoved	.1.3.6.1.4.1.232.0.6065	Major
cpqHe5ResMemBoardInserted	.1.3.6.1.4.1.232.0.6066	Informational
cpqHe5ResMemBoardBusError	.1.3.6.1.4.1.232.0.6067	Critical
cpqHeResilientMemLockStepMemoryEngaged	.1.3.6.1.4.1.232.0.6068	Major
cpqHe4FltTolPowerSupplyACpowerloss	.1.3.6.1.4.1.232.0.6069	Critical

Chapter 22: Resources

Documentation

The following documents are available on Avaya support site at https://support.avaya.com/:

Title	Description	Audience
Avaya Solutions Platform 4200 series		
Avaya Solutions Platform 4200 series Solution Description	Describes the key features of Avaya Solutions Platform	IT Management, sales and deployment engineers, solution architects, and support personnel.
Avaya Solutions Platform 4200 series Baseline	Describes Avaya Solutions Platform 4200 series software and hardware baseline components.	IT Management, sales and deployment engineers, solution architects, and support personnel.
Avaya Solutions Platform 4200 series Read Me First	Identifies Avaya Solutions Platform 4200 series media kit and refers to the documentation reference for all Avaya Solutions Platform 4200 series components.	IT Management, sales and deployment engineers, solution architects, and support personnel.
Documentation Reference for Avaya Solutions Platform 4200 series	Identifies Avaya Solutions Platform 4200 series customer documentation as well as the Avaya and non-Avaya products included in the Avaya Solutions Platform 4200 series solution and lists the associated customer documentation.	IT Management, sales and deployment engineers, solution architects, and support personnel.
Installing and Maintaining the Avaya Solutions Platform 4200 series	Describes how to install Avaya Solutions Platform 4200 series.	IT Management, sales and deployment engineers, solution architects, and support personnel.

Table continues…

Title	Description	Audience
Upgrading Avaya Solutions Platform 4200 series using the Management Server Console	Provides an overview of Management Server Console for Avaya Solutions Platform 4200 series. This document also provides instructions to access and use applications in the Management Console.	IT Management, sales and deployment engineers, solution architects, and support personnel.
Using Avaya Orchestrator™	Provides an overview of Avaya Orchestrator™ and instructions to access and use Avaya Orchestrator™.	IT Management, sales and deployment engineers, solution architects, and support personnel.

Finding documents on the Avaya Support website

Procedure

1. Go to https://support.avaya.com/.
2. At the top of the screen, type your username and password and click **Login**.
3. Click **Support by Product** > **Documents**.
4. In **Enter your Product Here**, type the product name and then select the product from the list.
5. In **Choose Release**, select an appropriate release number.
6. In the **Content Type** filter, click a document type, or click **Select All** to see a list of all available documents.

   For example, for user guides, click **User Guides** in the **Content Type** filter. The list displays the documents only from the selected category.
7. Click **Enter**.

Avaya Documentation Portal navigation

Customer documentation for some programs is now available on the Avaya Documentation Portal at https://documentation.avaya.com/

Important:

For documents that are not available on the Avaya Documentation Portal, click **Support** on the top menu to open https://support.avaya.com/.

Using the Avaya Documentation Portal, you can:

- Search for content in one of the following ways:

- Type a keyword in the **Search** field.
- Type a keyword in **Search**, and click **Filters** to search for content by product, release, and document type.
- Select a product or solution and then select the appropriate document from the list.

- Find a document from the Publications menu.
- Publish a PDF of the current section in a document, the section and its subsections, or the entire document.
- Add content to your collection by using **My Docs** (☆).

  Navigate to the **My Content** > **My Docs** menu, and do any of the following:

  - Create, rename, and delete a collection.
  - Add content from various documents to a collection.
  - Save a PDF of selected content in a collection and download it to your computer.
  - Share content in a collection with others through email.
  - Receive content that others have shared with you.
- Add yourself as a watcher by using the **Watch** icon (👁).

  Navigate to the **My Content** > **Watch list** menu, and do the following:

  - Set how frequently you want to be notified, starting from every day to every 60 days.
  - Unwatch selected content, all content in a document, or all content on the Watch list page.

    As a watcher, you are notified when content is updated or deleted from a document, or the document is removed from the portal.
- Share a section on social media platforms, such as Facebook, LinkedIn, Twitter, and GooglePlus.
- Send feedback on a section and rate the content.

Note:

Some functionality is only available when you log in to the portal. The available functionality depends on the role with which you are logged in.

Training

Product training is available on the Avaya Learning website. For more information or to register, see https://avaya-learning.com.

Viewing Avaya Mentor videos

Avaya Mentor videos provide technical content on how to install, configure, and troubleshoot Avaya products.

About this task

Videos are available on the Avaya Support website, listed under the video document type, and on the Avaya-run channel on YouTube.

Procedure

- To find videos on the Avaya Support website, go to https://support.avaya.com/ and do one of the following:
  - In **Search**, type `Avaya Mentor Videos` to see a list of the available videos.
  - In **Search**, type the product name. On the Search Results page, select **Video** in the **Content Type** column on the left.
- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and do one of the following:
  - Enter a key word or key words in the **Search Channel** to search for a specific product or topic.
  - Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the website.

    Note: Videos are not available for all products.

Support

Go to the Avaya Support website at https://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Using the Avaya InSite Knowledge Base

The Avaya InSite Knowledge Base is a web-based search engine that provides:

- Up-to-date troubleshooting procedures and technical tips
- Information about service packs
- Access to customer and technical documentation
- Information about training and certification programs
- Links to other pertinent information

If you are an authorized Avaya Partner or a current Avaya customer with a support contract, you can access the Knowledge Base without extra cost. You must have a login account and a valid Sold-To number.

Use the Avaya InSite Knowledge Base for any potential solutions to problems.

1. Go to https://www.avaya.com/support.
2. Log on to the Avaya website with a valid Avaya user ID and password.

   The system displays the Avaya Support page.
3. Click **Support by Product** > **Product Specific Support**.
4. In **Enter Product Name**, enter the product, and press `Enter`.
5. Select the product from the list, and select a release.
6. Click the **Technical Solutions** tab to see articles.
7. Select relevant articles.
