Pulse Secure®

Pulse One Appliance Administration Guide

Supporting Pulse One Appliance 2.0.1904.1

Product Release	2.0.1904.1
Published	11 March 2020
Document Version	1.0

Pulse Secure, LLC
2700 Zanker Road,
Suite 200 San Jose
CA 95134

https://www.pulsesecure.net

Pulse Secure, LLC assumes no responsibility for any inaccuracies in this document. Pulse Secure, LLC reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Pulse One Appliance Administration Guide

The information in this document is current as of the date on the title page.

END USER LICENSE AGREEMENT

The Pulse Secure product that is the subject of this technical documentation consists of (or is intended for use with) Pulse Secure software. Use of such software is subject to the terms and conditions of the End User License Agreement (“EULA”) posted at http://www.pulsesecure.net/support/eula/. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Contents

Preface

Document Conventions

The document conventions describe text formatting conventions, command syntax conventions, and important notice formats used in Pulse Secure technical documentation.

Text Formatting Conventions

Text formatting conventions such as boldface, italic, or Courier font may be used in the flow of the text to highlight specific words or phrases.

Format	Description
bold text	Identifies command names
	Identifies keywords and operands
	Identifies the names of user-manipulated GUI elements
	Identifies text to enter at the GUI
italic text	Identifies emphasis
	Identifies variables
	Identifies document titles
`Courier Font`	Identifies command output
	Identifies command syntax examples

Command Syntax Conventions

Bold and italic text identify command syntax components. Delimiters and operators define groupings of parameters and their logical relationships.

Convention	Description
bold text	Identifies command names, keywords, and command options.
italic text	Identifies a variable.
[ ]	Syntax components displayed within square brackets are optional. Default responses to system prompts are enclosed in square brackets.

Convention	Description
{ **x** | **y** | **z** }	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.
x | **y**	A vertical bar separates mutually exclusive elements.
< >	Non-printing characters, for example, passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, member[member...].
\	Indicates a "soft" line break in command examples. If a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

Notes and Warnings

Note, Attention, and Caution statements might be used in this document.

Note: A Note provides a tip, guidance, or advice, emphasizes important information, or provides a reference to related information.

ATTENTION
An Attention statement indicates a stronger note, for example, to alert you when traffic might be interrupted or the device might reboot.

CAUTION
A Caution statement alerts you to situations that can be potentially hazardous to you or cause damage to hardware, firmware, software, or data.

Requesting Technical Support

Technical product support is available through the Pulse Secure Global Support Center (PSGSC). If you have a support contract, file a ticket with PSGSC.

- Product warranties—For product warranty information, visit **https://support.pulsesecure.net/product-service-policies/**

Self-Help Online Tools and Resources

For quick and easy problem resolution, Pulse Secure provides an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: **https://support.pulsesecure.net**
- Search for known bugs: **https://support.pulsesecure.net**
- Find product documentation: **https://www.pulsesecure.net/techpubs**
- Download the latest versions of software and review release notes: **https://support.pulsesecure.net**

- Open a case online in the CSC Case Management tool: **https://support.pulsesecure.net**
- To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: **https://support.pulsesecure.net**

For important product notices, technical articles, and to ask advice:

- Search the Pulse Secure Knowledge Center for technical bulletins and security advisories: **https://kb.pulsesecure.net**
- Ask questions and find solutions at the Pulse Community online forum: **https://community.pulsesecure.net**

Opening a Case with PSGSC

You can open a case with PSGSC on the Web or by telephone.

- Use the Case Management tool in the PSGSC at **https://support.pulsesecure.net**.
- Call 1-844 751 7629 (Toll Free, US).

For international or direct-dial options in countries without toll-free numbers, see **https://support.pulsesecure.net/support/support-contacts/**

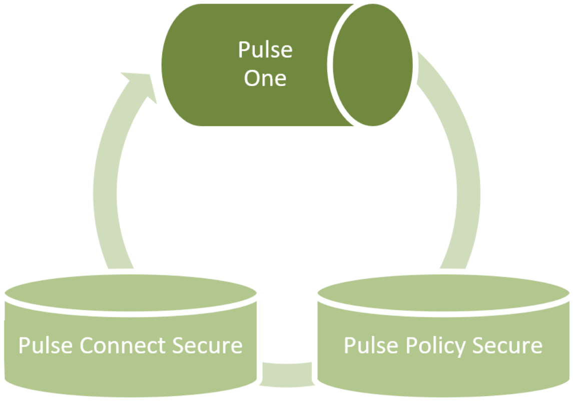
Getting Started With Pulse One

Overview of Pulse One

Pulse One provides unified management of Pulse Connect Secure and Pulse Policy Secure in a single easy-to-use console.

Pulse One, a single, comprehensive management console, offers the superior administrative end-to-end control and visibility needed to manage remote, local and mobile access to any corporate applications. Administrators use its intuitive, role-based console to monitor system health, manage security policies, troubleshoot issues, report on the appliance and device health, and publish appliance and mobile device configuration.

FIGURE 1 Pulse One Unified Management



It controls enterprise access to data center and cloud from a single console.

- **Role-based access** - Grants console access and privileges based on IT role and credentials.
- **Group-based management** - Publish software updates, policy changes and configuration provisioning by custom-defined groups. ESAP updates to appliances are also supported.
- **Centralized administration** - Collectively administers multiple appliances without logging into them on a box-by-box basis.

- **Built-in Mobility Management** - Provides basic EMM functionality for iOS and Android devices and management of BYOD and corporate-owned workspaces.
- **System Dashboard** - Assesses the collective health of all appliances and provides security alerts and appliance alarms.
- **Appliance Dashboard** - Provides appliance status with analytics for connectivity, capacity, utilization, and uptime.
- **Administrator Audit Logging** - Tracks administrator changes to appliance configuration.
- **Monitor and Reporting** - Monitors system activity and provides historical reporting.
- **Deployment** - Introduces new features and scales without data center logistics and planning.

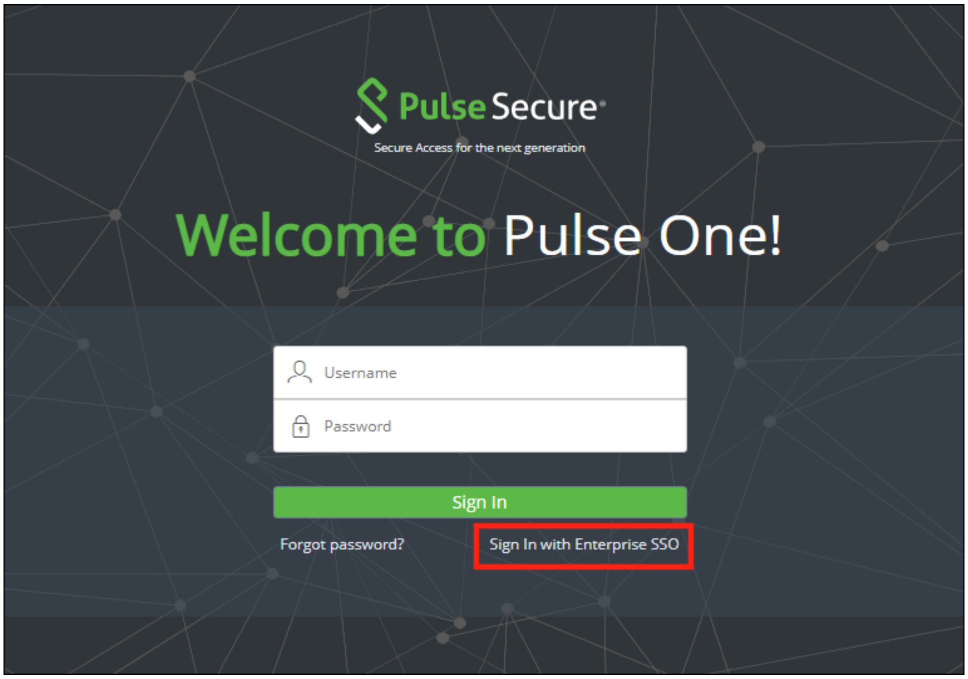
Logging Into Pulse One

This section details the steps to log in to Pulse One as an administrator.

Use the Pulse One admin URL to launch the Pulse One Admin Console.

- If you are an existing user, enter the user name and password. Click **Sign In** to log in to Pulse One.
- If Enterprise SSO is configured for your user ID, then click **Sign In with Enterprise SSO**. For details about the Enterprise SSO configuration, see **"Enterprise Connection Properties" on page 142**.

FIGURE 2 Pulse One Login Page



If you are a new user, you will have received a welcome mail from Pulse One to your registered mail ID. Click the **Set your password** link in the welcome mail. In the Pulse One login page that appears, provide a strong password and confirm the password. On successful login, the **End User License Agreement (EULA)** page appears.

If you have forgotten your Pulse One password, click the **Forgot password?** link. In the page that appears, enter your user id and click **Request reset**.

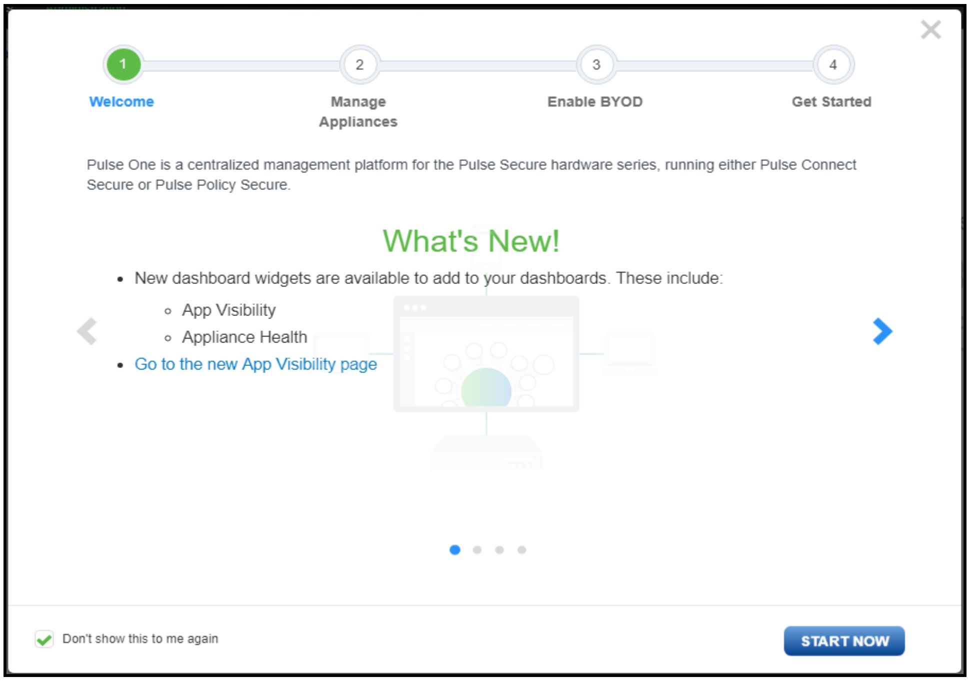
An email that contains a **Reset your password** link will be sent to your registered mail id. Use this link to launch Pulse One and provide your new password and confirm the new password.

Note: The **Reset your password** link has an expiration time of 1 hour. Beyond this time, you should make a new request for reset.

If you are a new user logging into Pulse One for the first time, then in the EULA page use the scroll bar to read through the terms of the agreement and then click **Agree**.

The Welcome wizard appears. This provides you a brief overview of Pulse One, appliance management and Bring Your Own Devices (BYODs).

FIGURE 3 Pulse One Welcome Wizard



Pulse One is a centralized management platform for the Pulse Secure hardware series, running either Pulse Connect Secure or Pulse Policy Secure.

What's New!

- New dashboard widgets are available to add to your dashboards. These include:
  - App Visibility
  - Appliance Health
- Go to the new App Visibility page

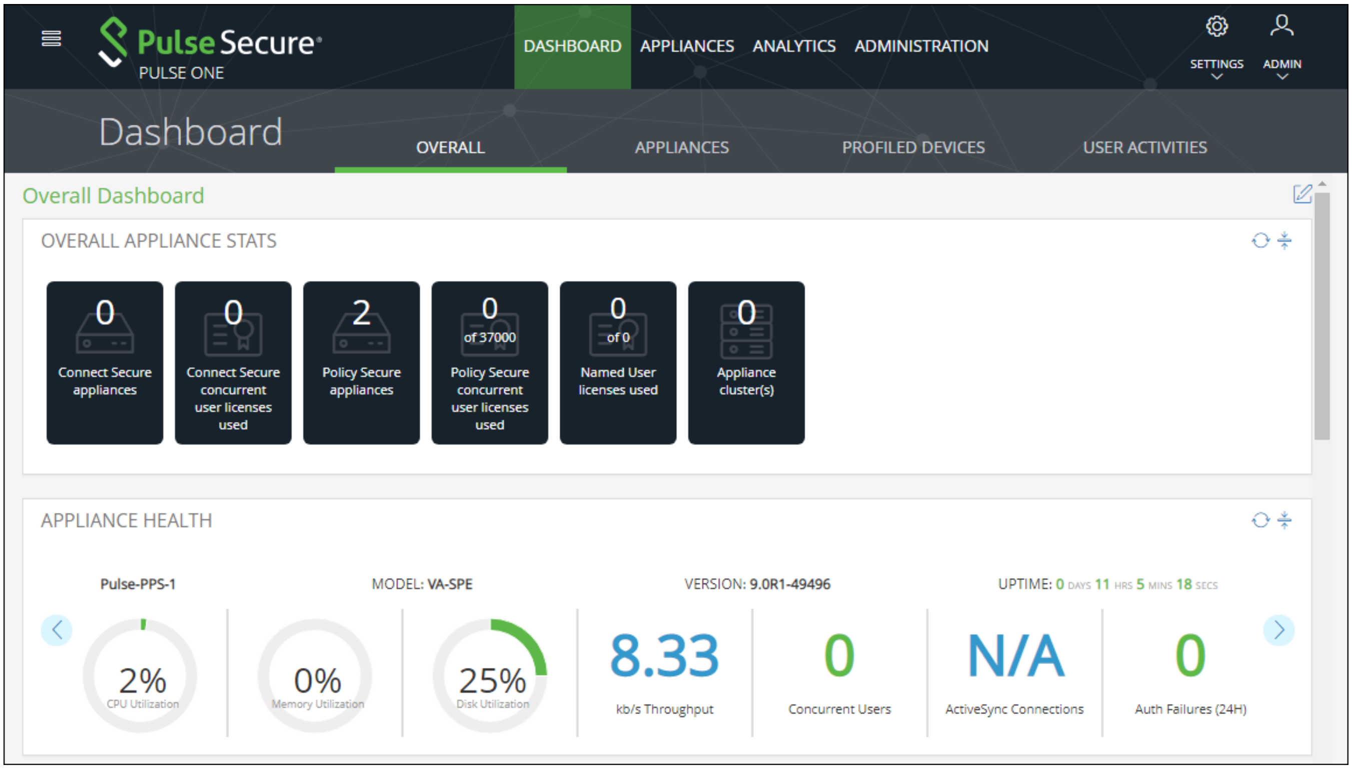
☑ Don't show this to me again

In the Welcome wizard, click the right-arrow button until the **Get Started** option appears. If required, select the **Don't show this to me again** check box and then click **Start Now**.

Note: You can view the Welcome wizard any time by clicking the **Settings** icon on the top right corner of the page and selecting **Show Welcome Wizard**.

The Pulse One **Home** page appears:

FIGURE 4 Pulse One Home Page



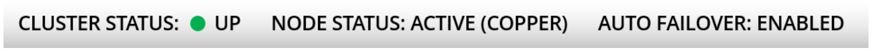
Select the appropriate tab, settings icon or user icon, and get started with the administration.

Note: A summary of cluster/node statuses appears in the bottom right corner of the **Home** screen. See "Understanding Cluster/Node Status Summary" on page 9 for details.

Understanding Cluster/Node Status Summary

On all Pulse One screens, a summary of cluster-related statuses appears at the bottom right of the screen. This summary reflects the current state of the cluster, as viewed from the current node. For example:

FIGURE 5 Cluster Status Summary



CLUSTER STATUS: ● UP NODE STATUS: ACTIVE (COPPER) AUTO FAILOVER: ENABLED

The summary statuses are included:

- **Cluster Status**: The status of the Pulse One cluster, as reported by the cluster. This status can be:
  - *Disabled*. There is no Active/Passive cluster configured.
  - *Up*. An Active/Passive cluster is configured, and both nodes are available.
  - *Down*. An Active/Passive cluster is configured, but only one node is available.

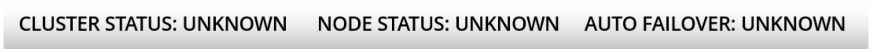
    This state indicates that some intervention is required to return the cluster status to *Up*.
  - *Changing*. This is a transitional state that only appears when a standalone node is changing to be the first (Active) node in a cluster.
- **Node Status**: The status of the current node, as reported by the node. This status can be:
  - *Active*. The current node is available, and part of an Active/Passive cluster.
  - *Standalone*. The current node is available, but is not part of an Active/Passive cluster.

  Note: After a clustered pair has been formed, the name of the Active node is displayed in brackets.
- **Auto Failover**: The current setting of the automatic failover switch. The switch state is set by the **cluster config** CLI command. This status can be:
  - *Enabled*. Auto-failover of a correctly-configured Active/Passive pair will be attempted if the current Active node fails.
  - *Disabled*. Auto-failover is off. Manual failover of a correctly-configured Active/Passive pair is still supported.

  Note: The automatic failover switch setting is independent of the cluster status and node status.

An *Unknown* status is also supported for all three summary statuses. For example:

FIGURE 6 Cluster Status Summary: Unknown



CLUSTER STATUS: UNKNOWN NODE STATUS: UNKNOWN AUTO FAILOVER: UNKNOWN

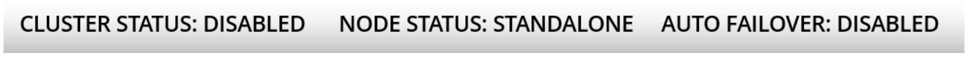
This indicates that either an internal issue has occurred with the cluster, or that the GUI is unable to retrieve the cluster status from the server.

All Active/Passive cluster configuration is performed from the Pulse One Command-Line Interface. See the *Pulse One Getting Started Guide* for details of all configuration and failover processes.

Example: Typical Node Lifecycle

When you log into a new standalone node, such as one that has just been created, the following summary status appears:

FIGURE 7 Cluster Status Summary: New Node



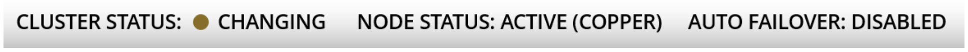
CLUSTER STATUS: DISABLED NODE STATUS: STANDALONE AUTO FAILOVER: DISABLED

You can then use the **cluster** commands in the Pulse One CLI to change the standalone node to be the Active Node in an Active/Passive pair with (optionally) auto-failover enabled. To do this:

1. Using the CLI on the standalone node, promote the node to be the Active node in a planned Active/ Passive cluster. The name of the node (in this example, *Copper*) is now included in brackets.

   The following summary status appears:

   FIGURE 8 Cluster Status Summary: Single Standalone Node Transitions to Active

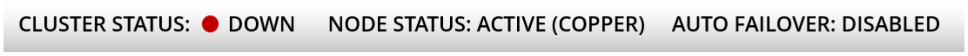
   CLUSTER STATUS: ● CHANGING NODE STATUS: ACTIVE (COPPER) AUTO FAILOVER: DISABLED

   This summary indicates that the node is no longer standalone, but that the transition is still in progress.

2. Using the CLI of the Active node, you can add a Passive node to the intended cluster. Once completed, this creates the required join token.

   After this process completes on the Active node, the summary statuses update so that the **Cluster Status** is *Down*. This indicates that only a single node is available.

   FIGURE 9 Cluster Status Summary: Single Node Now Active

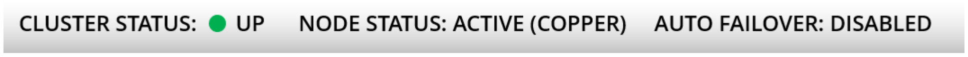
   

   CLUSTER STATUS: ● DOWN NODE STATUS: ACTIVE (COPPER) AUTO FAILOVER: DISABLED

3. Using the CLI of the Passive node, you can then use the join token to finalize the join.

   After this process completes on the Passive node, the following summary statuses appear:

   FIGURE 10 Cluster Status Summary: Active/Passive Cluster Formed

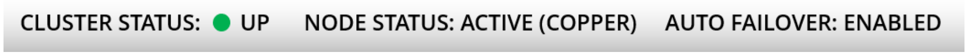
   

   CLUSTER STATUS: ● UP NODE STATUS: ACTIVE (COPPER) AUTO FAILOVER: DISABLED

4. (Optional) Enable automatic failover from the CLI on the Active node.

   After this process completes, the following summary statuses appear:

   FIGURE 11 Cluster Status Summary: Auto Failover Enabled for Active/Passive Cluster

   CLUSTER STATUS: ● UP NODE STATUS: ACTIVE (COPPER) AUTO FAILOVER: ENABLED

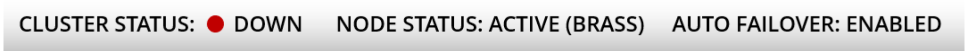
Configuration of the Active/Passive cluster is now complete, and reported correctly in the Pulse One GUI.

If either node in an Active/Passive cluster fails:

1. Perform either an automatic or manual failover. After this process completes, the new Active node is a standalone Active node.

   The following summary statuses appear:

   FIGURE 12 Cluster Status Summary: After Auto Failover

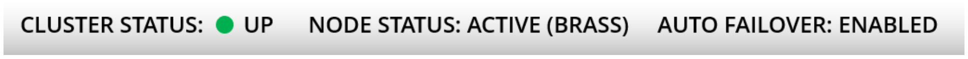
   CLUSTER STATUS: ● DOWN NODE STATUS: ACTIVE (BRASS) AUTO FAILOVER: ENABLED

   Note: In this example, the Active node is now the previous Passive node, *Brass*.

2. Repair the failed node and re-form the Active/Passive cluster.

   After this process completes, the summary statuses of the cluster returns to an operational state:

   FIGURE 13 Cluster Status Summary: Re-Formed Cluster

   CLUSTER STATUS: ● UP NODE STATUS: ACTIVE (BRASS) AUTO FAILOVER: ENABLED

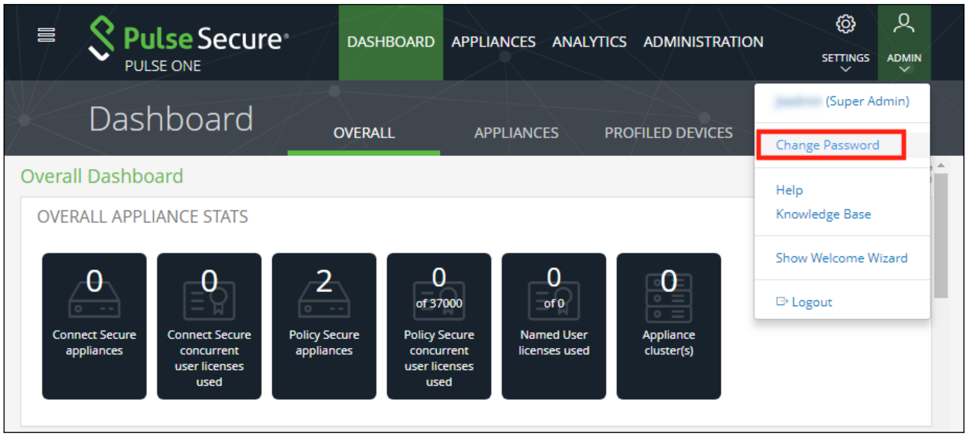
Changing the User Password

To change the user password:

1. Click the **User** icon on the top-right corner of the page.

2. From the menu, click **Change Password** to change your login password.

   FIGURE 14 Change Password

   An email that contains **Set new password** link will be sent to your registered mail id. Use this link to launch Pulse One and provide your new password.

   Note: The **Set new password** link that you received in the email has an expiration time of 1 hour.

3. To log out of the admin console, click **Logout**.

Adding Pulse One Licenses

To view and install a license on Pulse One OnPrem, access the Command-Line Interface (CLI) and use the following commands:

```
licenses show
licenses add <license key>
```

Refer to the *Pulse One Command Reference* for full details of CLI commands.

Whitelisting IP Addresses for Admin Login

When Pulse One is installed, admins can log into the Pulse One console from any IP address.

Note: You can also whitelist countries, see **"Whitelisting Countries for Admin Login" on page 14**.

If you want to restrict the IP addresses from which admins can log into Pulse One, you can *whitelist* one or more IP addresses and ranges. All IP addresses outside the whitelist are then blocked from accessing Pulse One.

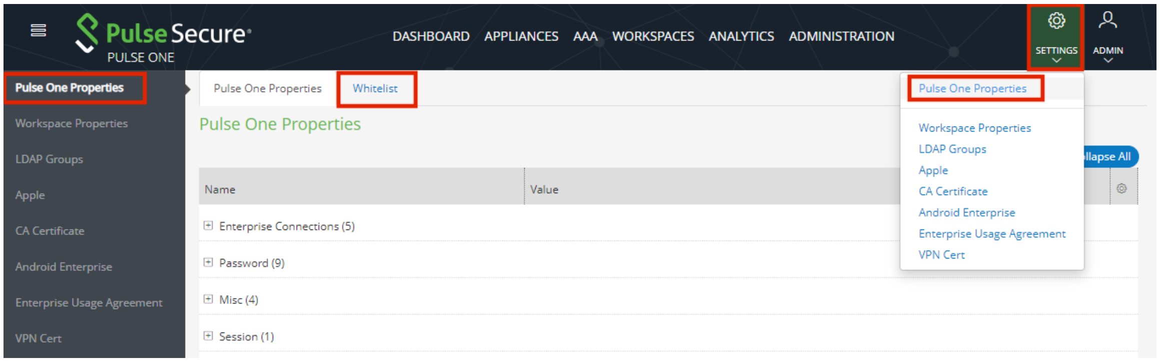
Whitelisting IP addresses/ranges is disabled by default. It is enabled when you add your first IP address/range to the whitelist, *which must include your current IP address*. After you have added your first whitelist item, all other IP addresses/ranges are automatically blacklisted. You can then continue to add all other required IP addresses/ranges until you have added all IP addresses/ranges from which admins can log in.

To whitelist IP addresses/ranges:

1. Log into Pulse One as an administrator.
2. Click the **Settings** icon on top-right-corner of the page.
3. Select **Pulse One Properties**.

   The **Pulse One Properties** page appears.

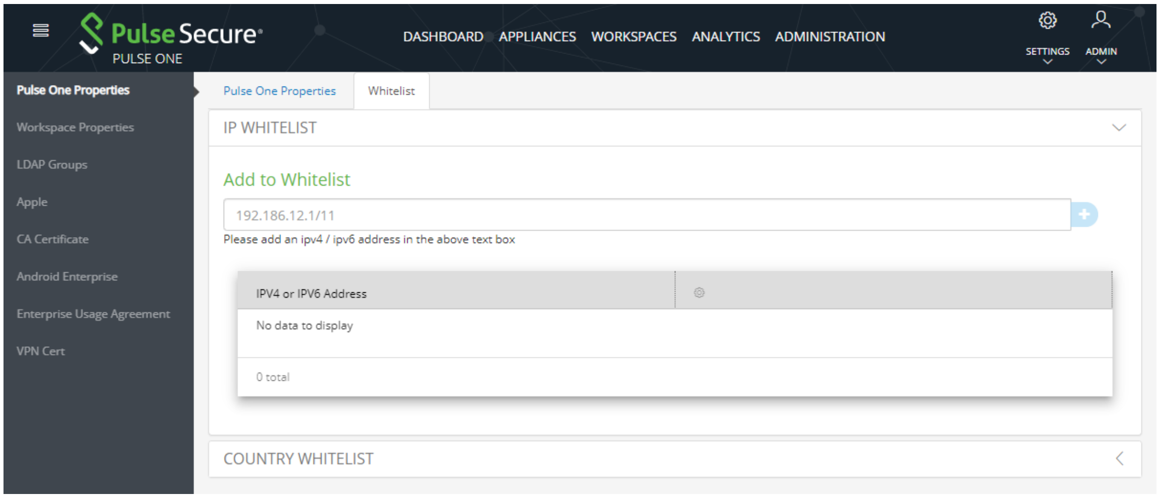
FIGURE 15 Pulse One Properties



Name	Value
⊟ Enterprise Connections (5)	
⊟ Password (9)	
⊟ Misc (4)	
⊟ Session (1)	

4. Click the **Whitelist** tab to view the **Add to Whitelist** page.

FIGURE 16 Add to Whitelist Page



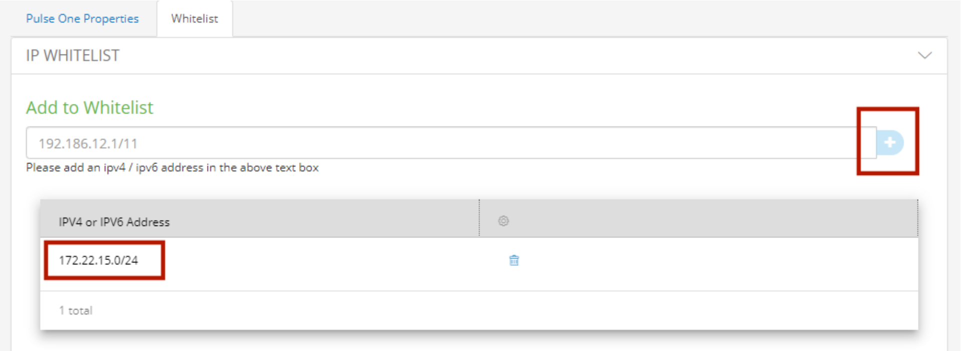
5. Click **IP Whitelist**.

6. Under **Add to Whitelist**, add your first whitelist item:

   - Enter an IP address/range (with CIDR netmask suffix) that includes the IP address from which you are currently logged in.
   - Click the plus icon.

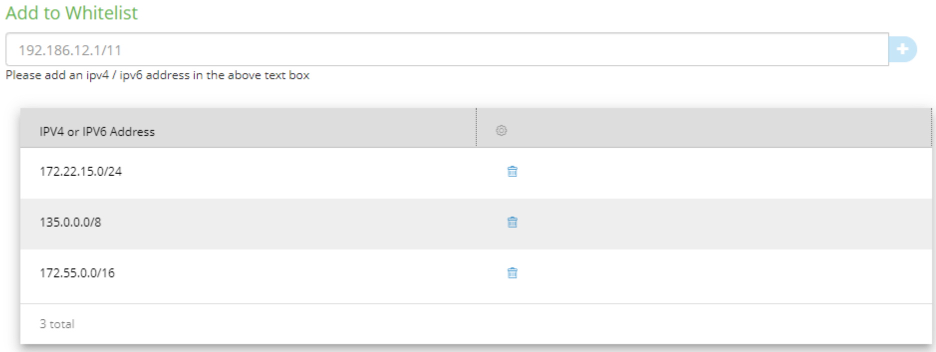
   The IP address/range is added to the whitelist. For example:

FIGURE 17 First Whitelist Entry



7. Repeat step 6 to add additional IP addresses/ranges to the whitelist. For example:

FIGURE 18 Additional Whitelist Entries



Add to Whitelist

192.186.12.1/11

Please add an ipv4 / ipv6 address in the above text box

IPV4 or IPV6 Address	⚙
172.22.15.0/24	🗑
135.0.0.0/8	🗑
172.55.0.0/16	🗑

3 total

8. (Optional) Delete a whitelist entry by clicking its **Delete** icon.

   Note: You cannot delete the whitelist item that includes your current login IP address. You can only delete this after all other whitelisted items are deleted. When you do this, whitelisting is then disabled, and admins will be able to login from any IP address.

Note: If your IP address changes, it is possible for you to be locked out of Pulse One. In this case, log into the Command-Line Interface (CLI) and perform the **p1 domain whitelist reset** command. This clears all items from the whitelist, and disables the whitelisting feature so that all incoming IP addresses are valid. You can then log into Pulse One again and create a new whitelist.

Whitelisting Countries for Admin Login

When Pulse One is installed, admins can log into the Pulse One console from any country.

Note: You can also whitelist IP addresses and ranges, see **"Whitelisting IP Addresses for Admin Login" on page 12**.

If you want to restrict the countries from which admins can log into Pulse One, you can *whitelist* one or more countries. All outside outside the whitelist are then blocked from accessing Pulse One.

Whitelisting counties is disabled by default. It is enabled when you add your first country to the whitelist, *which must be your current country*. After you have added your first whitelist item, all other countires are automatically blacklisted. You can then continue to add all other required countries until you have added all countries from which admins can log in.

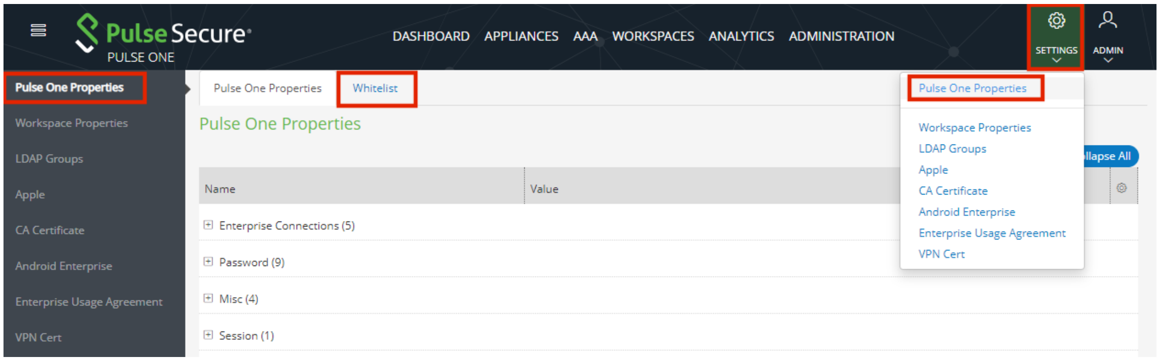
To whitelist countries:

1. Log into Pulse One as an administrator.
2. Click the **Settings** icon on top-right-corner of the page.

3. Select **Pulse One Properties**.

   The **Pulse One Properties** page appears.

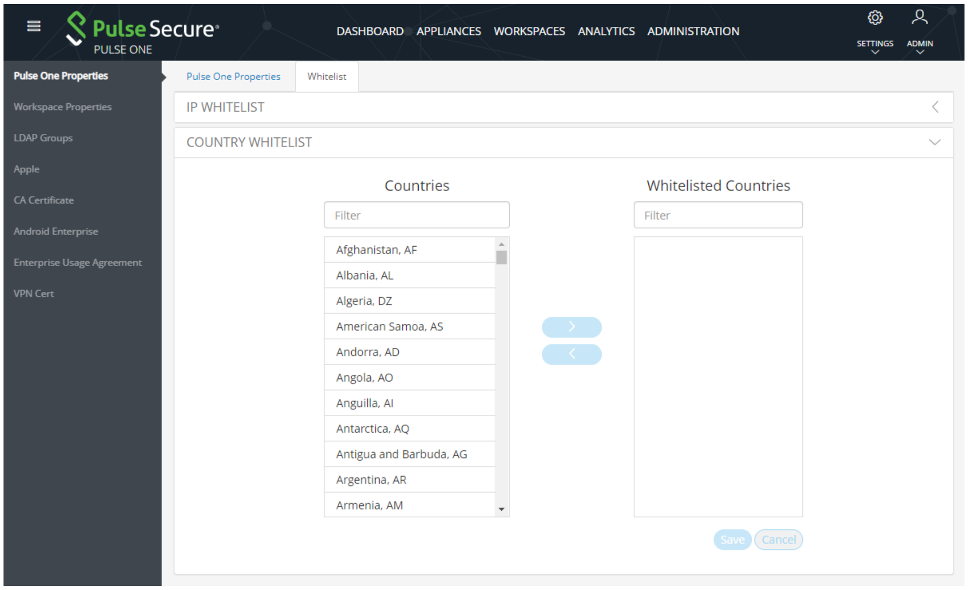
   FIGURE 19 Pulse One Properties



4. Click the **Whitelist** tab to view the **Add to Whitelist** page.

5. Click **Country Whitelist**.

   FIGURE 20 Add to Whitelist Page

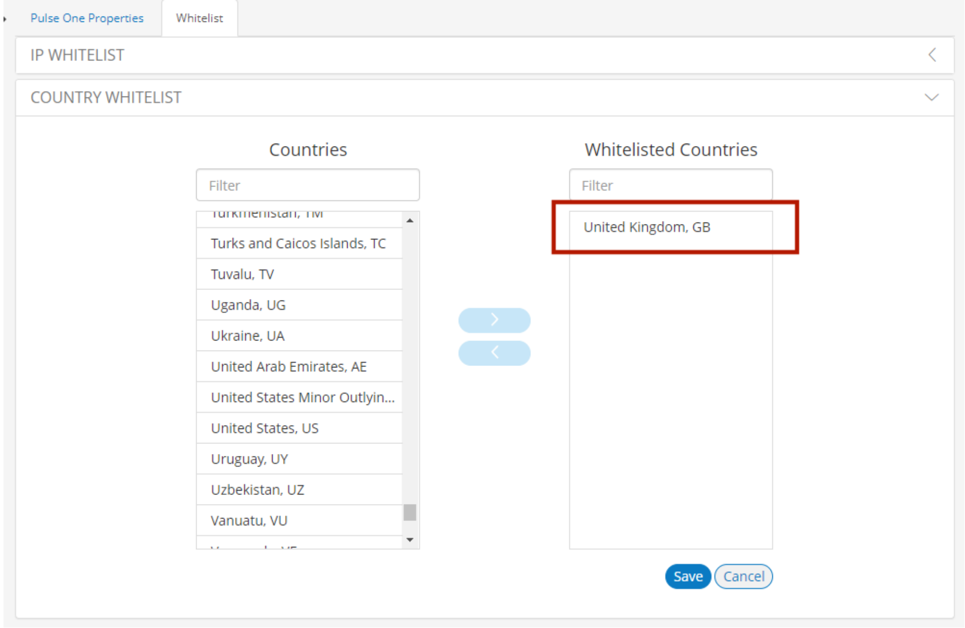


6. Add your first whitelist item:

   - Under **Countries**, locate and select the country from which you are currently logged in. You can do this by scrolling down the list, or by using a filter string. For example, the "ind" string matches to *India*, *British Indian Ocean Territory* and *Indonesia*.
   - Click the **>** icon.

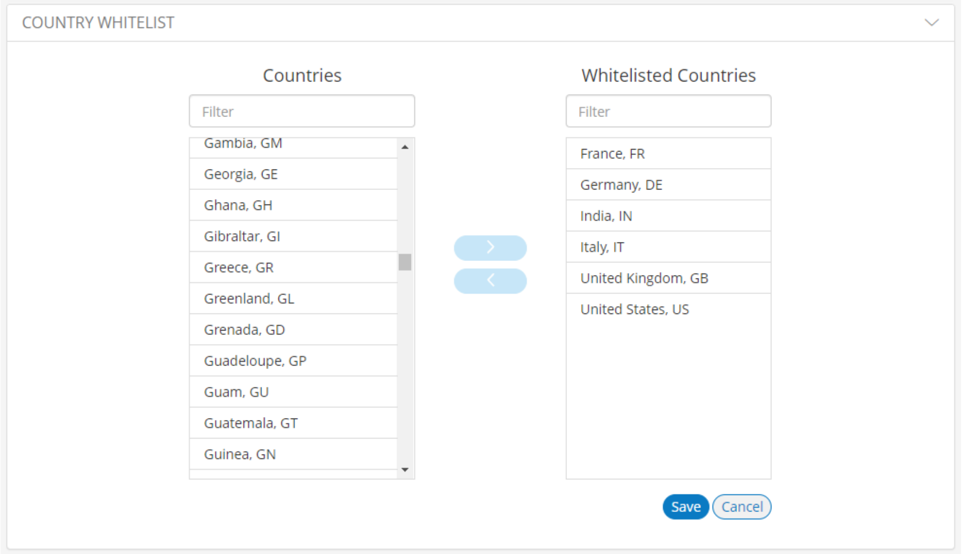
The country is added to the **Whitelisted Countries** list. For example:

FIGURE 21 First Whitelist Entry



7. Repeat step 6 to add additional countries to the whitelist. For example:

FIGURE 22 Additional Whitelist Entries



8. (Optional) Delete a whitelist entry by clicking its **Delete** icon.

Note: You cannot delete the whitelist item that includes your current country. You can only delete this after all other whitelisted items are deleted. When you do this, country whitelisting is then disabled, and admins will be able to login from any country.

Note: If your country changes, it is possible for you to be locked out of Pulse One. In this case, log into the Command-Line Interface (CLI) and perform the **p1 domain whitelist reset** command. This clears all items from the whitelist, and disables the whitelisting feature so that all incoming countries are valid. You can then log into Pulse One again and create a new whitelist.

Setting a Session Timeout Threshold

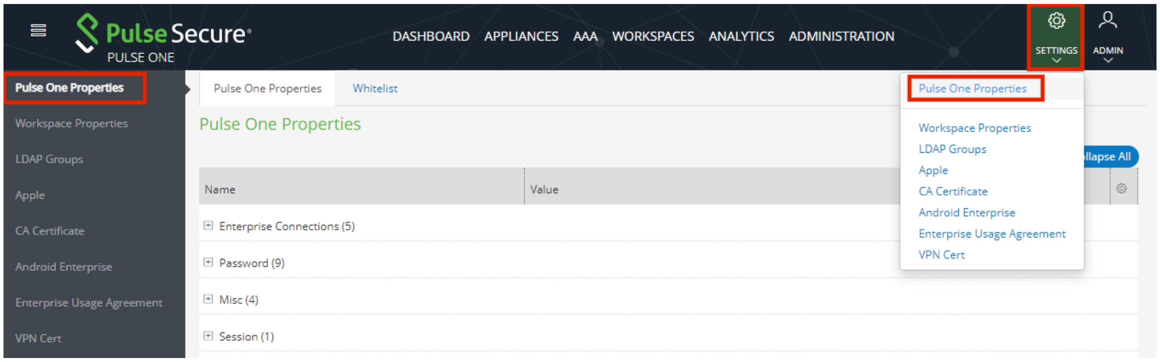
You can set a session timeout threshold. After a period of activity reaches this threshold, the user is logged out, and must log in again to continue.

To set a session timeout threshold:

1. Log into Pulse One as an administrator.
2. Click the **Settings** icon on top-right-corner of the page.
3. Select **Pulse One Properties**.

   The **Pulse One Properties** page appears.

   FIGURE 23 Pulse One Properties

4. Expand the *Session* category.
5. Edit the **Session idle timeout (minutes)** property and specify a new setting.

   Note: The default setting is *20*.

6. **Save** the new setting.

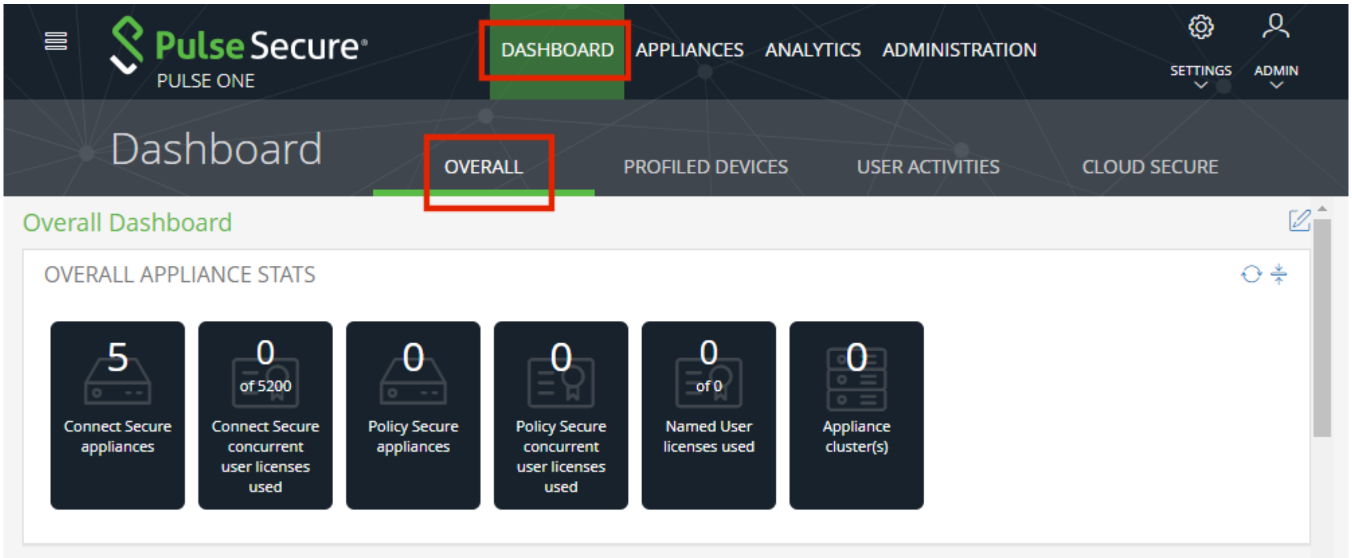
The new session timeout threshold is applied to your current session and all subsequent sessions.

Working with the Pulse One Dashboard

Viewing Overall System Health

To view metrics for system health, select the **Dashboard** tab, and then select the **Overall** tab. For example:

FIGURE 24 Overall System Health Dashboard



This dashboard includes the following widgets by default:

- Overall appliance statistics.
- Appliance health for individual appliances.
- VPN realm usage.
- Role usage.
- Frequent user logins.
- Logins in the past 24 hours.
- Critical appliance events with timestamps.

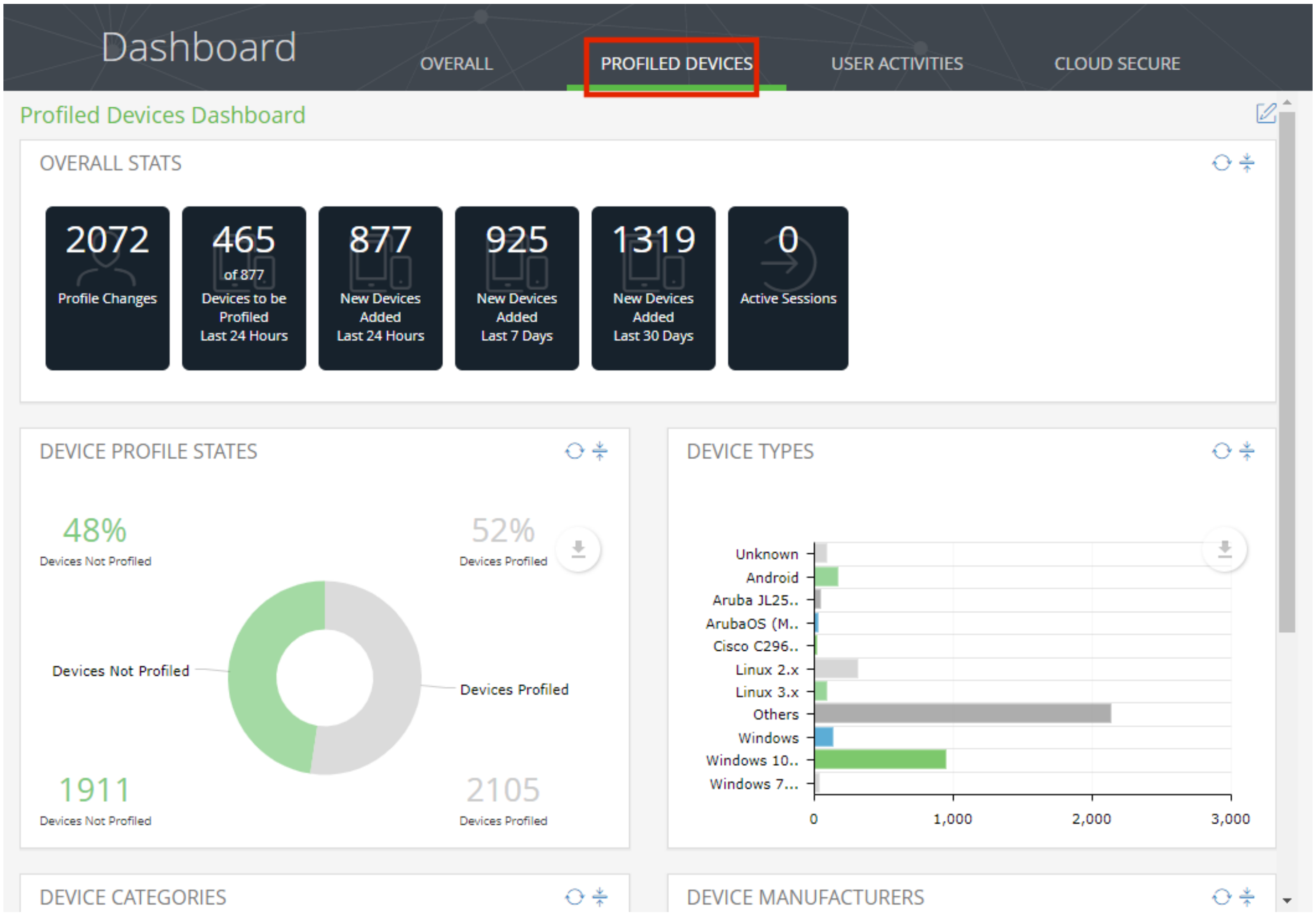
- Resource dial.
- Pulse Connect Secure versions.
- Pulse Policy Secure versions.

Each widget that can be refreshed by clicking **Reload Widget Content** (⟳) and collapsed by clicking **Collapse/ Expand Widget** (⇳).

Viewing Profiled Devices

To view metrics for profiled devices, select the **Dashboard** tab, and then select the **Profiled Devices** tab. For example:

FIGURE 25 Profiled Devices Dashboard



2072 Profile Changes

465 of 877 Devices to be Profiled Last 24 Hours

877 New Devices Added Last 24 Hours

925 New Devices Added Last 7 Days

1319 New Devices Added Last 30 Days

0 Active Sessions

This dashboard includes the following widgets by default:

- Overall profiled device statistics.
- Device profile states.
- Device types.
- Device categories.
- Device manufacturers.

Note: Each widget that can be refreshed by clicking **Reload Widget Content** and collapsed by clicking **Collapse/Expand Widget**.

Note: The **Profiled Devices** dashboard tab requires that a Reports license is installed on Pulse One, see **"Adding Pulse One Licenses" on page 12**.

For more information on profiled devices, see **"Viewing the Profiled Devices Report" on page 126**.

Viewing User Activities

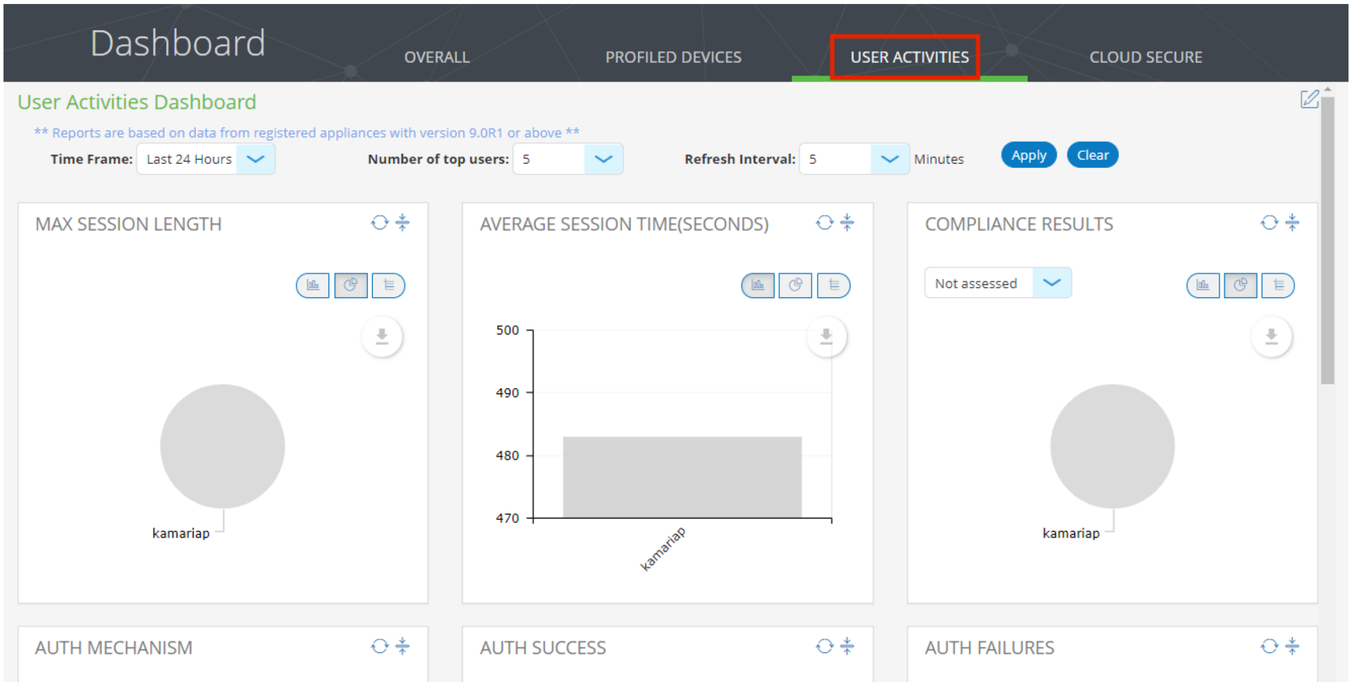
To view metrics for user activities, select the **Dashboard** tab, and then select the **User Activities** tab.

Note: Displayed reports are the **User Activities** tab are based on data from registered appliances with version 9.0R1 or above.

This dashboard includes the following widgets by default:

- Maximum session length.
- Average session time (in seconds).
- Compliance results.
- Authorization mechanism.
- Authorization successes.
- Authorization failures.
- Top roles.
- Operating system type.

FIGURE 26 User Activities Dashboard



Note: Each widget that can be refreshed by clicking **Reload Widget Content** and collapsed by clicking **Collapse/Expand Widget**.

Note: The **User Activities** dashboard tab requires that a Reports license is installed on Pulse One, see **“Adding Pulse One Licenses” on page 12**.

For more information on user activities, see **“Viewing the User Activities Report” on page 128**.

Viewing UEBA Metrics

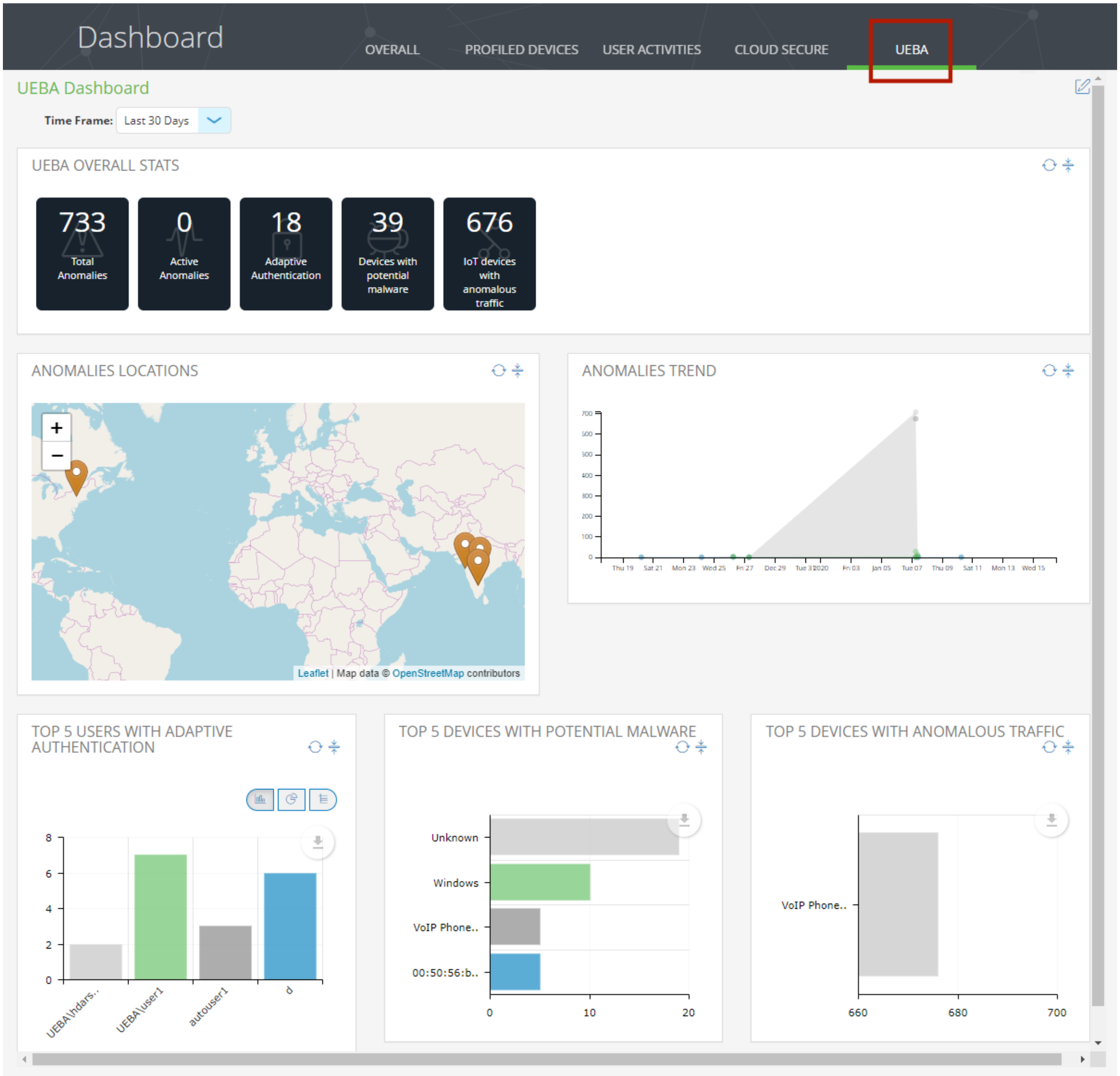
User and Entity Behavior Analytics (UEBA) software analyzes user activity data from logs, network traffic and endpoints. It correlates this data with threat intelligence to identify activities/behaviours that might indicate a malicious presence in your environment.

Pulse One supports the collection and display of UEBA metrics.

Note: To view UEBA metrics, you must install an analytics-enabled license.

To view metrics, select the **Dashboard** tab, and then select the **UEBA** tab. For example:

FIGURE 27 UEBA Dashboard



Time Frame: Last 30 Days

In this example, there are no active (current) anomalies, but there are many reported anomalies across two geographical areas.

The administrator can view the following information:

- The map location from which the anomaly occurred.
- A graph of anomaly numbers across time.
- The top five users with adaptive authentication.
- The top five devices with potential malware.
- The top five devices with anomalous traffic.

Note: You can also view a pair of analytics reports for UEBA, see **"Viewing the UEBA Analytics Reports" on page 129**.

Viewing Cloud Secure Statistics

The **Cloud Secure** dashboard tab displays the collected statistics from all Cloud Secure appliances that are registered on Pulse One. If there are no registered Cloud Secure appliances, the tab is empty.

Note: The **Cloud Secure** dashboard tab requires that a Reports license is installed on Pulse One, see **"Adding Pulse One Licenses" on page 12**.

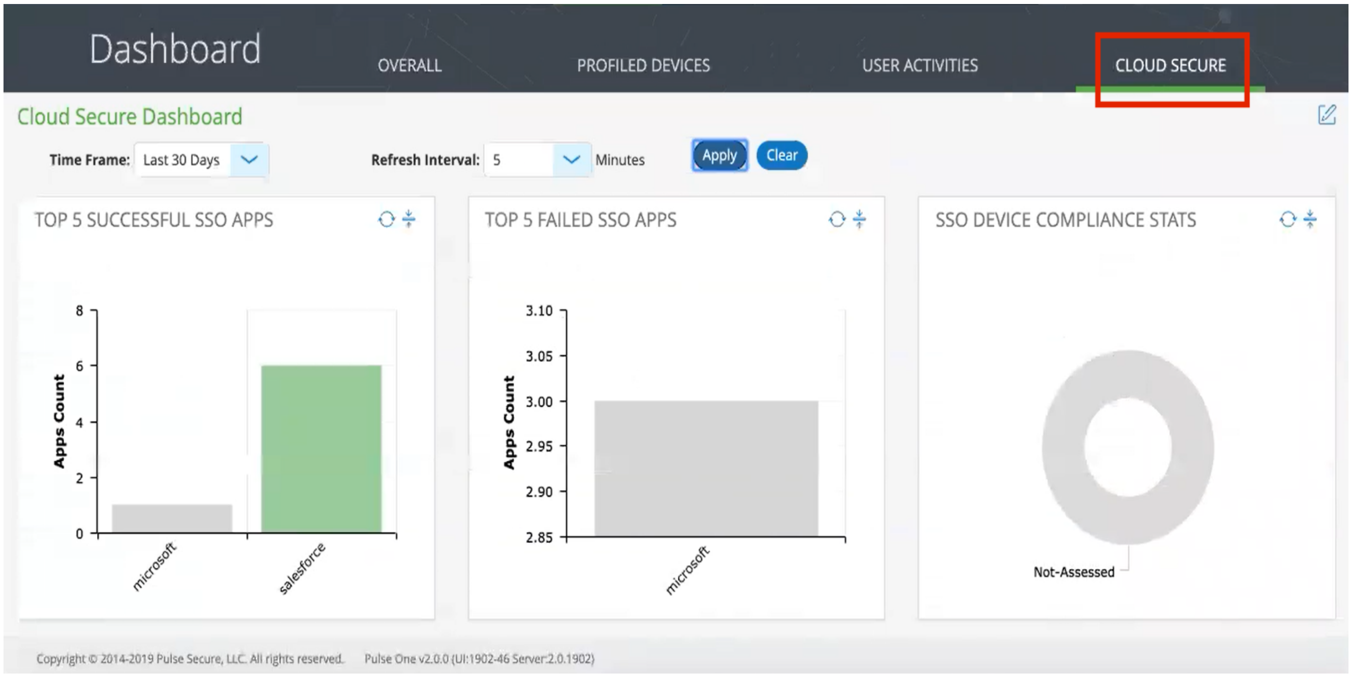
This dashboard includes the following widgets by default:

- Top five apps with successful single sign-on (SSO) attempts.
- Top five apps with failed single sign-on (SSO) attempts.
- SSO device compliance statistics.
- SSO device details.
- SSO application trends.
- Top five SSO user roles.

To view metrics for all Cloud Secure appliances:

1. Select the **Dashboard** tab, and then select the **Cloud Secure** tab.
2. Select the required **Time Frame** for the dashboard. For example, *Last 24 Hours*, *Last 30 Days*.
3. Select the required **Refresh Interval** for the dashboard. For example, *5 Mins*, *10 Mins*, *15 Mins*.
4. Click **Apply** to view the filtered statistics. For example:

FIGURE 28 Cloud Secure Dashboard



Cloud Secure Dashboard

Time Frame: Last 30 Days

Refresh Interval: 5 Minutes

Copyright © 2014-2019 Pulse Secure, LLC. All rights reserved. Pulse One v2.0.0 (UI:1902-46 Server:2.0.1902)

Note: Each widget that can be refreshed by clicking **Reload Widget Content** and collapsed by clicking **Collapse/Expand Widget**.

For more information on Cloud Secure appliances and statistics, see the *Pulse Policy Secure* product documentation.

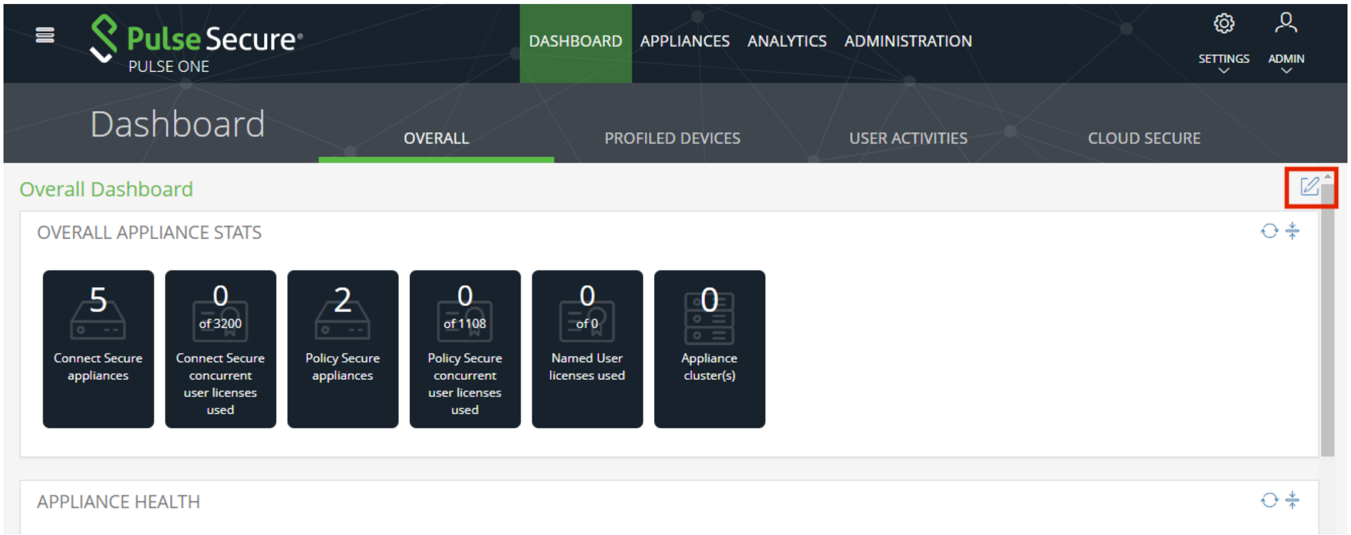
Customizing Dashboards and Widgets

The dashboard views are customizable. You can change the dashboard layout, add/remove widgets, and rearrange the widgets.

To customize the widgets on a **Dashboard** tab:

1. Display the required dashboard tab. For example, the **Overall** tab.

FIGURE 29 Customizing the Dashboard

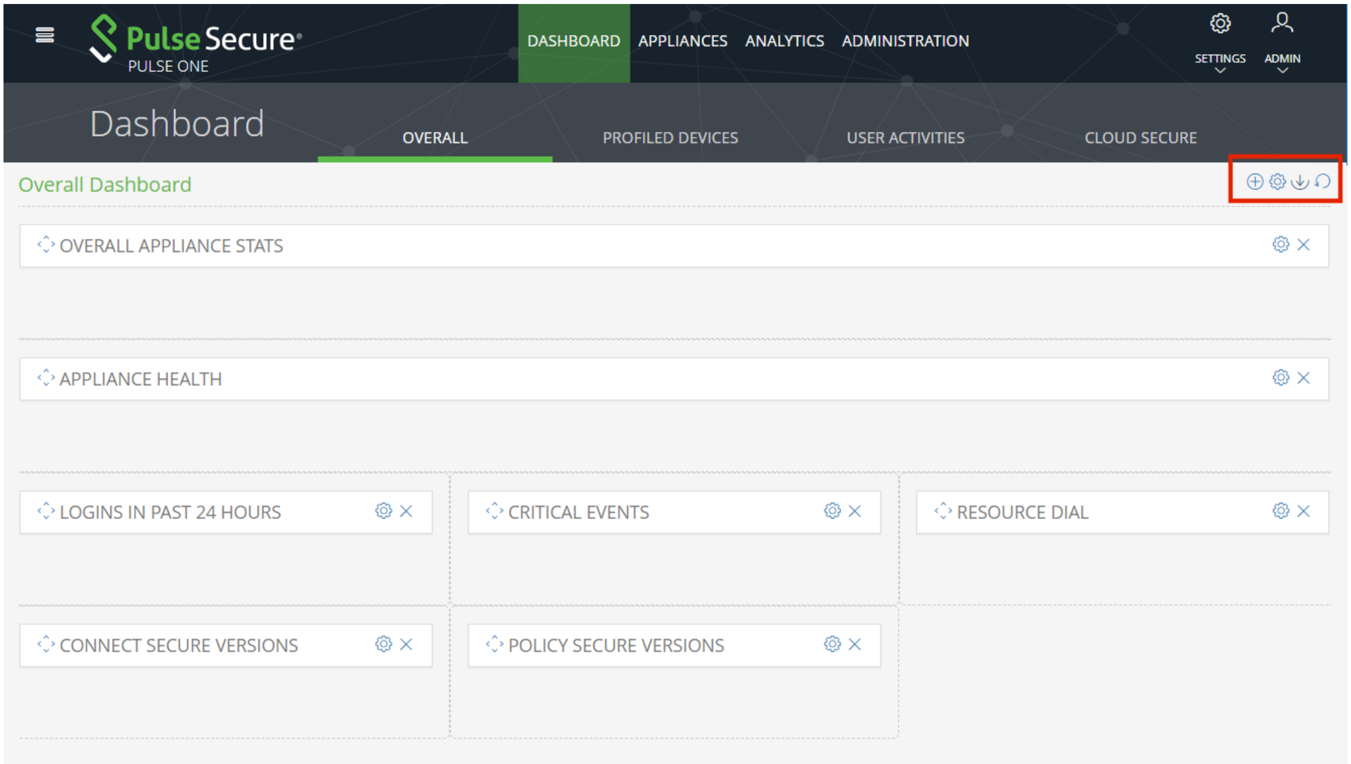


Note: The inclusion of individual menus and tabs will reflect all loaded licenses. Your view may differ from that shown above.

2. Click the **Enable Edit mode** icon (✎) on the top-right of the tab.

A widget layout summary for the dashboard appears. For example, for the **Overall** tab:

FIGURE 30 Dashboard Widget Layout



3. (Optional) Click **Add New Widget** (⊕) to add a widget to the current layout, see **"Adding a New Widget" on page 28**.

4. (Optional) Click **Edit Dashboard** (⚙) to select a new layout, see **"Editing the Dashboard Layout" on page 29**.

5. (Optional) Rearrange the current widgets by dragging a widget using its **Change Widget Location** (✥) handle.

6. (Optional) Change the settings for a widget by clicking its **Edit Widget Configuration** (⚙), see **"Editing Widget Configuration" on page 31**.

7. (Optional) Remove a widget by clicking its **Remove Widget** control.

8. (Optional) Click **Undo Changes** (↺) to reset all unsaved changes and close the layout summary.

9. Click **Save Changes** (⤓) to save all changes and close the layout summary.

Adding a New Widget

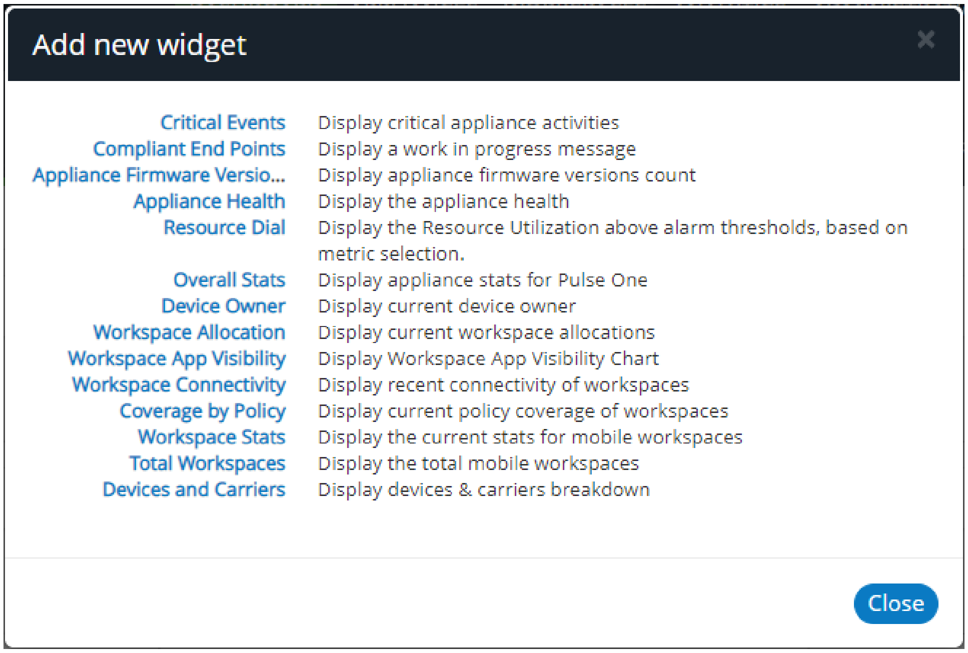
To add a new widget to a dashboard tab:

1. Display the required dashboard tab. For example, the **Overall** tab.
2. Click the **Enable Edit mode** icon (✎) on the top-right of the tab.

   A widget layout summary for the dashboard appears.
3. Click the **Add New Widget** (⊕) control.

   A list of widgets appears.

   FIGURE 31 Add New Widget

Critical Events	Display critical appliance activities
Compliant End Points	Display a work in progress message
Appliance Firmware Versio...	Display appliance firmware versions count
Appliance Health	Display the appliance health
Resource Dial	Display the Resource Utilization above alarm thresholds, based on metric selection.
Overall Stats	Display appliance stats for Pulse One
Device Owner	Display current device owner
Workspace Allocation	Display current workspace allocations
Workspace App Visibility	Display Workspace App Visibility Chart
Workspace Connectivity	Display recent connectivity of workspaces
Coverage by Policy	Display current policy coverage of workspaces
Workspace Stats	Display the current stats for mobile workspaces
Total Workspaces	Display the total mobile workspaces
Devices and Carriers	Display devices & carriers breakdown

4. Select the required widget.

   The selected new widget is added to the top of the layout summary.
5. (Optional) On the widget layout, change the settings for the widget by clicking its **Edit Widget Configuration** (⚙) control, see **"Editing Widget Configuration" on page 31**.
6. (Optional) Click **Undo Changes** (↺) to reset all unsaved changes and close the layout summary.
7. Click **Save Changes** (⤓) to save all changes and close the layout summary.

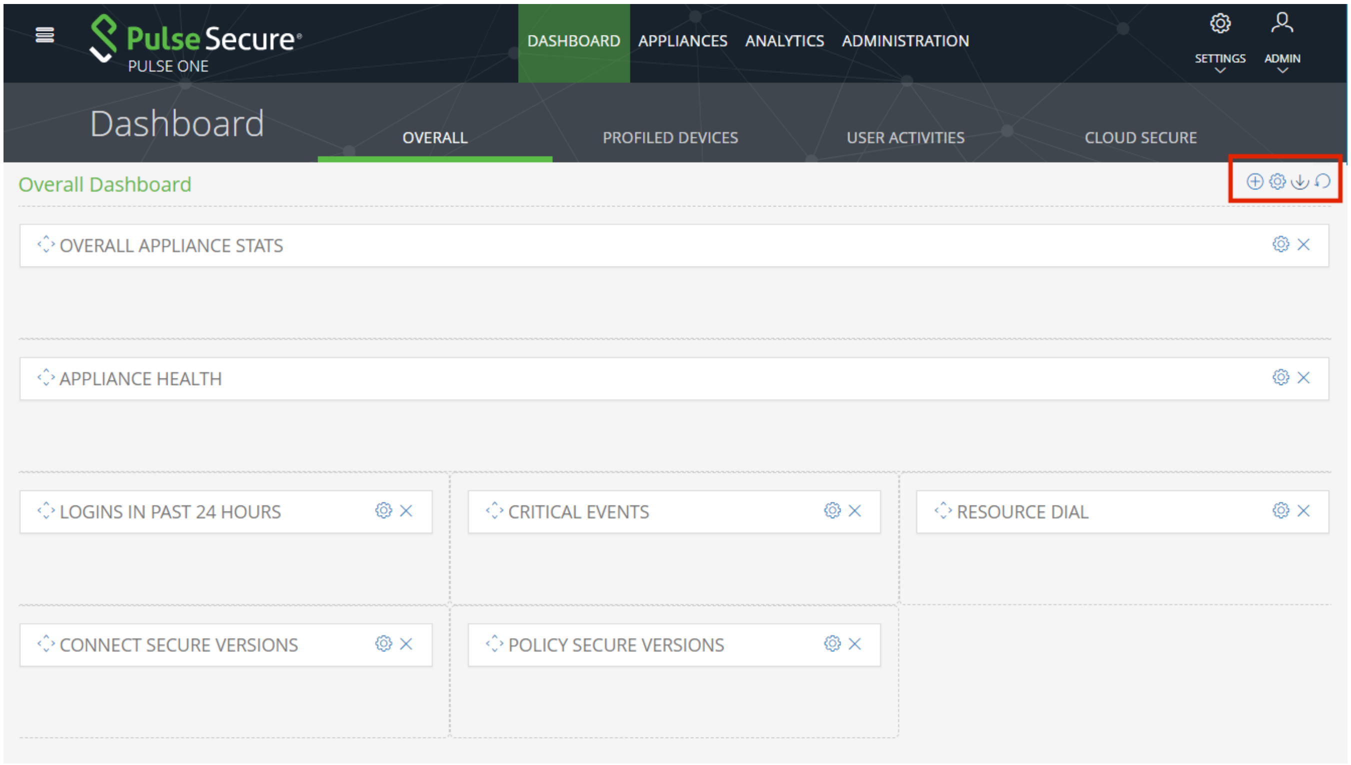
Editing the Dashboard Layout

To change the layout of a dashboard tab:

1. Display the required dashboard tab. For example, the **Overall** tab.
2. Click the **Enable Edit mode** icon (✎) on the top-right of the tab.

   A widget layout summary for the dashboard appears. For example, for the **Overall** tab:

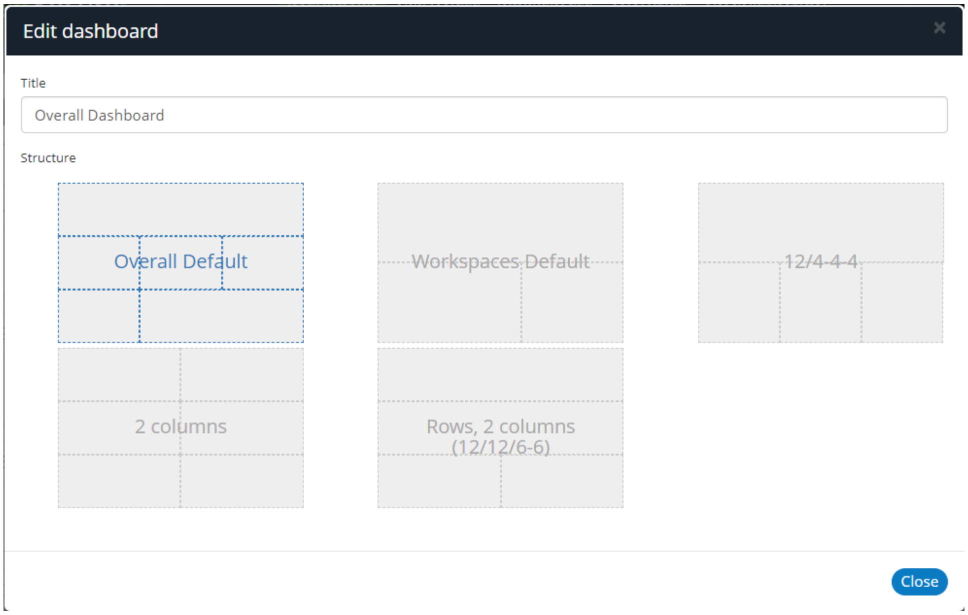
   FIGURE 32 Dashboard Widget Layout



Note: The inclusion of individual menus and tabs will reflect all loaded licenses. Your view may differ from that shown above.

3. Click the **Edit Dashboard** (⚙) icon. A display of available layouts appears.

FIGURE 33 Edit Dashboard Layout



Edit dashboard ×

Title

Overall Dashboard

Structure

Overall Default

Workspaces Default

12/4-4-4

2 columns

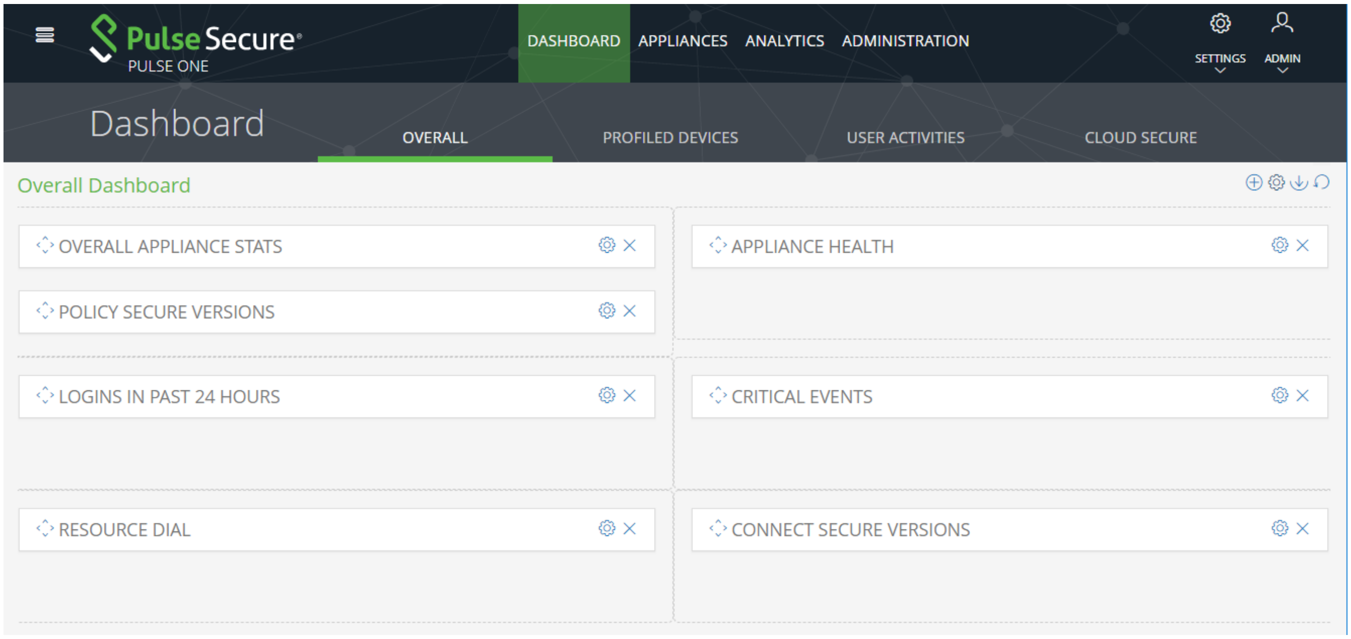
Rows, 2 columns (12/12/6-6)

Close

4. Select the required layout from the displayed list and click **Close**.

   The widget layout is rearranged to reflect the new layout. For example, to a two-column layout.

FIGURE 34 Updated Dashboard Widget Layout



Overall Dashboard

OVERALL APPLIANCE STATS

APPLIANCE HEALTH

POLICY SECURE VERSIONS

LOGINS IN PAST 24 HOURS

CRITICAL EVENTS

RESOURCE DIAL

CONNECT SECURE VERSIONS

5. (Optional) Click **Undo Changes** (↺) to reset all unsaved changes and close the layout summary.
6. Click **Save Changes** (⤓) to save all changes and close the layout summary.

The dashboard layout updates to reflect the selected layout.

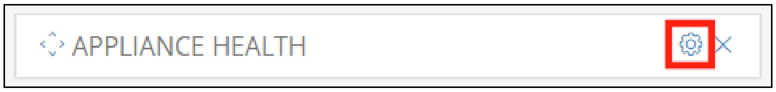
Editing Widget Configuration

To change the configuration of a widget:

1. Display the required dashboard tab. For example, the **Overall** tab.
2. Click the **Enable Edit mode** icon (✎) on the top-right of the tab.

   A widget layout summary for the dashboard appears.
3. Locate the widget you want to configure.
4. Click the **Configure Widget** (⚙) control for the widget. For example:

   FIGURE 35 Appliance Health Widget

   APPLIANCE HEALTH

   A dialog appears which displays all configurable options for the widget.
5. Make the required changes and click **Apply**.
6. (Optional) Click **Undo Changes** (↺) to reset all unsaved changes and close the layout summary.
7. Click **Save Changes** (⤓) to save all changes and close the layout summary.

Appliance Management

Registering an Existing PCS/PPS Appliance

After Pulse One is installed and configured, the next step is to register one or more PCS/PPS appliances.

Note: This process requires sufficient appliance licensing capacity.

Note: You can also create and register a virtual PCS appliance for either AWS (see **“Creating and Registering a PCS Appliance VM on AWS” on page 56**) or vSphere (see **“Creating and Registering a PCS Appliance VM on vSphere” on page 42**).

To register an existing appliance:

1. Log into Pulse One as an administrator.

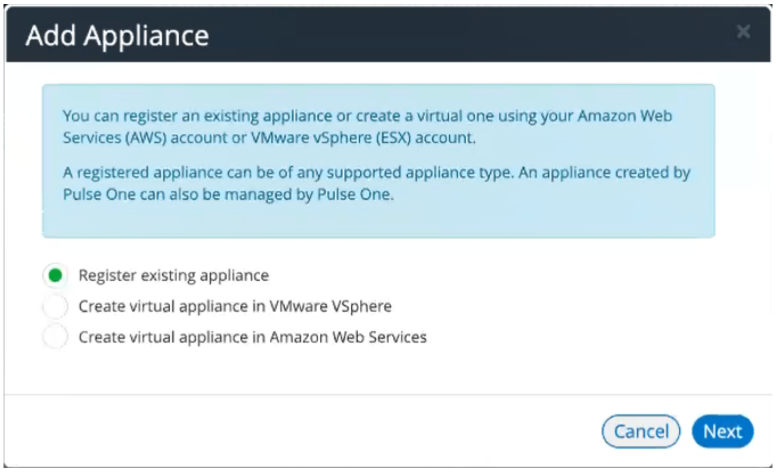
2. Click the **Appliances** menu and then the **Appliances** tab.

   The **Appliances** tab displays all current appliances.

3. Click **Add Appliance**.

   The **Add Appliance** dialog box appears.

   FIGURE 36 Add Appliance



Add Appliance

You can register an existing appliance or create a virtual one using your Amazon Web Services (AWS) account or VMware vSphere (ESX) account.

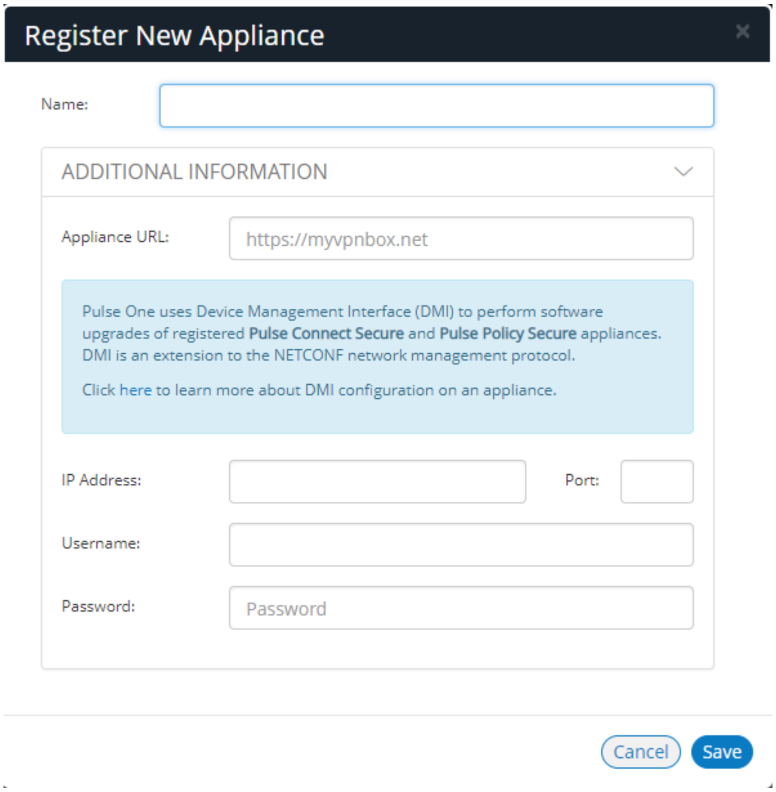
A registered appliance can be of any supported appliance type. An appliance created by Pulse One can also be managed by Pulse One.

● Register existing appliance
○ Create virtual appliance in VMware VSphere
○ Create virtual appliance in Amazon Web Services

4. Select **Register existing appliance** and click **Next**.

   The **Register Appliance** dialog appears.

   FIGURE 37 Register New Appliance



Register New Appliance

Name:

ADDITIONAL INFORMATION

Appliance URL: https://myvpnbox.net

Pulse One uses Device Management Interface (DMI) to perform software upgrades of registered **Pulse Connect Secure** and **Pulse Policy Secure** appliances. DMI is an extension to the NETCONF network management protocol.

Click here to learn more about DMI configuration on an appliance.

IP Address: Port:

Username:

Password: Password

5. Enter the required **Name** for the appliance. For example: *appliance.pcs*.

6. Enter the management interface address of the appliance as the **Appliance URL**. Typically, this URL will end with "/admin".

7. (Optional) If you want the appliance to support Device Management Interface (DMI) software upgrades directly from Pulse One:

    - For **IP Address**, specify the IP Address on which the appliance is configured to receive DMI requests. This is either the internal interface or the management interface.
    - For **Port**, specify the port on which the appliance is configured to receive DMI requests. Typically, this is 830.
    - Specify the required admin **Username** and **Password** for the appliance. This will be used to receive DMI requests.

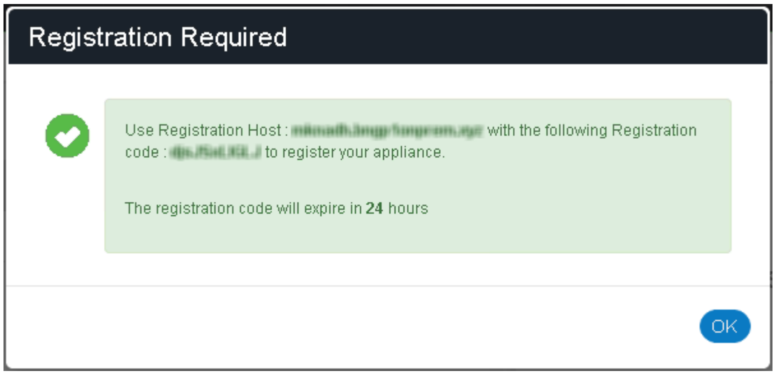
    Note: You must record this information for when you configure software upgrades. For full details of software upgrades on registered appliances, see **"Upgrading Managed Appliances" on page 89**.

    Note: DMI does not need to be configured for ESAP package uploads to appliances.

8. Click **Save**.

    A dialog displays the required **Registration Host** and a **Registration Code**. For example:

    FIGURE 38 Registration Required



Registration Required

Use Registration Host : [redacted] with the following Registration code : [redacted] to register your appliance.

The registration code will expire in **24** hours

9. Record the **Registration Host** and **Registration Code** and close the dialog.

10. Switch to the appliance application (for example, PCS) and enter the **Registration Host** and a **Registration Code** in the appliance's panel, see **"Configuring an Appliance to Connect to Pulse One" on page 38**.

When the auto-registration process is complete, the appliance is added to Pulse One. The Pulse One console displays the appliance status as *Connected* in the **Appliances** list.

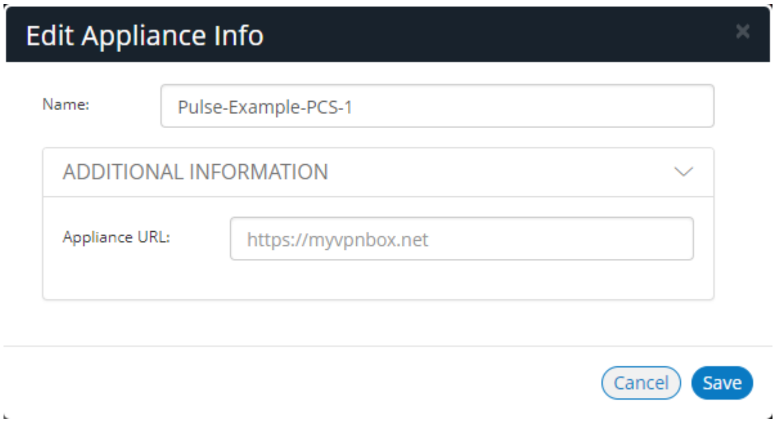
Editing Appliance Information

To edit appliance information:

1. Log into Pulse One as an administrator.
2. Click the **Appliances** menu and then the **Appliances** tab.

   The **Appliances** tab displays all current appliances.
3. Select the required appliance from the list and click its **Actions** icon (⋮).
4. From the menu options, select **Edit Appliance Info**.
5. In the **Edit Appliance Info** dialog, make the required changes.

   FIGURE 39 Edit Appliance Information

   Edit Appliance Info

   Name: Pulse-Example-PCS-1

   ADDITIONAL INFORMATION

   Appliance URL: https://myvpnbox.net

   Note: If you want the Launch Appliance UI option to be available on the **Actions** menu for the appliance, specify the **Appliance URL**. This URL typically ends with "/admin".
6. Click **Save** to update the appliance.

Launching the User Interface for an Appliance

You can launch the administration user interface for a registered appliance directly from the **Appliances** tab.

To support this, ensure that you have specified an **Appliance URL** property for the appliance. Where no **Appliance URL** is specified for an appliance, you can manually edit the appliance properties to specify one, see **"Editing Appliance Information" on page 36**.

To launch the admin UI for an appliance.

1. Log into Pulse One as an administrator.
2. Click the **Appliances** menu and then the **Appliances** tab.

   The **Appliances** tab displays all current appliances.

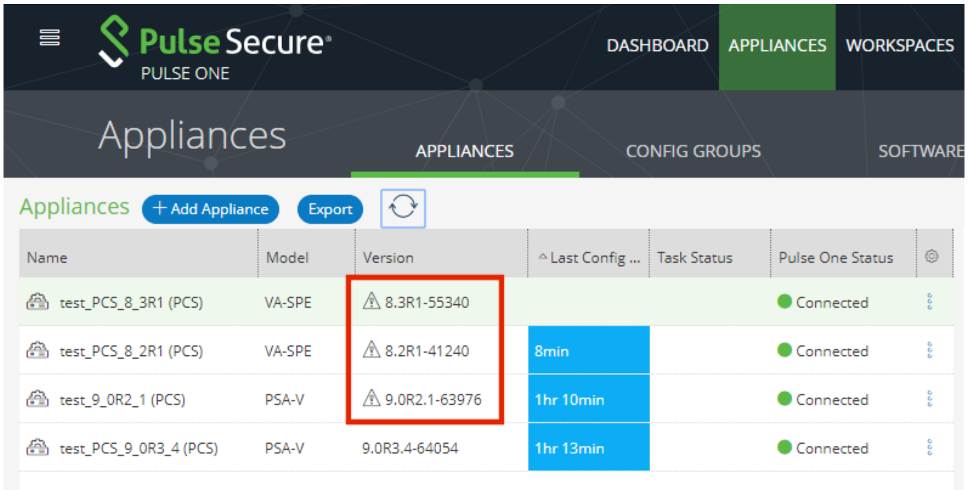
3. Select the required appliance from the list and click its **Actions** icon (⋮).
4. From the menu options, select **Launch Appliance UI**.

   The graphical user interface for the appliance starts in a new tab of your browser.

Recognizing Critical Vulnerabilities

On Pulse One, the Appliances list displays all registered appliances. Summary information for each appliance includes a **Version** number for the appliance. A warning flag appears beside the version number if the version has known critical vulnerabilities. For example:

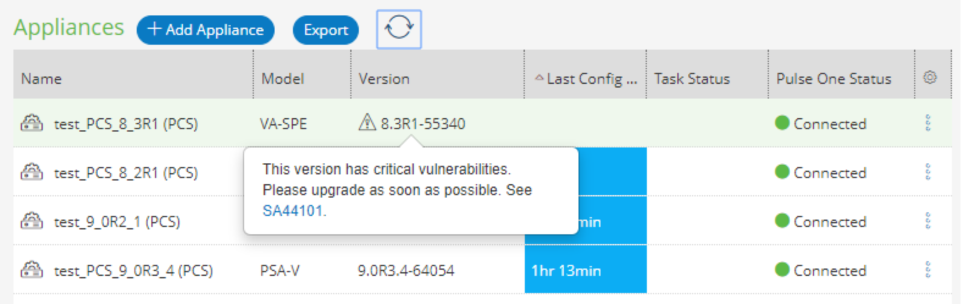
FIGURE 40 Critical Vulnerability



Name	Model	Version	Last Config ...	Task Status	Pulse One Status
test_PCS_8_3R1 (PCS)	VA-SPE	⚠ 8.3R1-55340			● Connected
test_PCS_8_2R1 (PCS)	VA-SPE	⚠ 8.2R1-41240	8min		● Connected
test_9_0R2_1 (PCS)	PSA-V	⚠ 9.0R2.1-63976	1hr 10min		● Connected
test_PCS_9_0R3_4 (PCS)	PSA-V	9.0R3.4-64054	1hr 13min		● Connected

Hover over the **Version** number to see additional information.

FIGURE 41 Details of a Critical Vulnerability



Name	Model	Version	Last Config ...	Task Status	Pulse One Status
test_PCS_8_3R1 (PCS)	VA-SPE	⚠ 8.3R1-55340			● Connected
test_PCS_8_2R1 (PCS)					● Connected
test_9_0R2_1 (PCS)			min		● Connected
test_PCS_9_0R3_4 (PCS)	PSA-V	9.0R3.4-64054	1hr 13min		● Connected

This version has critical vulnerabilities. Please upgrade as soon as possible. See SA44101.

To upgrade the software on the appliance, see **"Upgrading Software on an Appliance" on page 94**.

Configuring an Appliance to Connect to Pulse One

After you have added an appliance record into Pulse One:

- Complete the Pulse One registration from the appliance, see "Completing Registration of an Appliance" on page 38.
- Configure the appliance to send logs to Pulse One, see "Configuring Log Settings on the Appliance" on page 39.
- Configure the ActiveSync handler on the appliance as required, see "Configuring ActiveSync Handler" on page 41.

Completing Registration of an Appliance

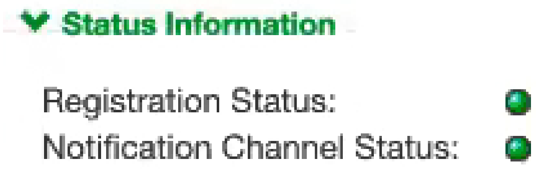
To complete registration of an appliance in Pulse Connect Secure:

1. Log into the PCS/PPS appliance.
2. Select the **System > Configuration > Pulse One > Settings** tab.
3. Enter the **Registration Host** and **Registration Code**.

   Note: These were displayed during "Registering an Existing PCS/PPS Appliance" on page 33.
4. Click **Save Changes**.

   The **Status Information** displays the **Registration Status** in green.

   FIGURE 42 Pulse Connect Secure: Pulse One Settings



Status Information

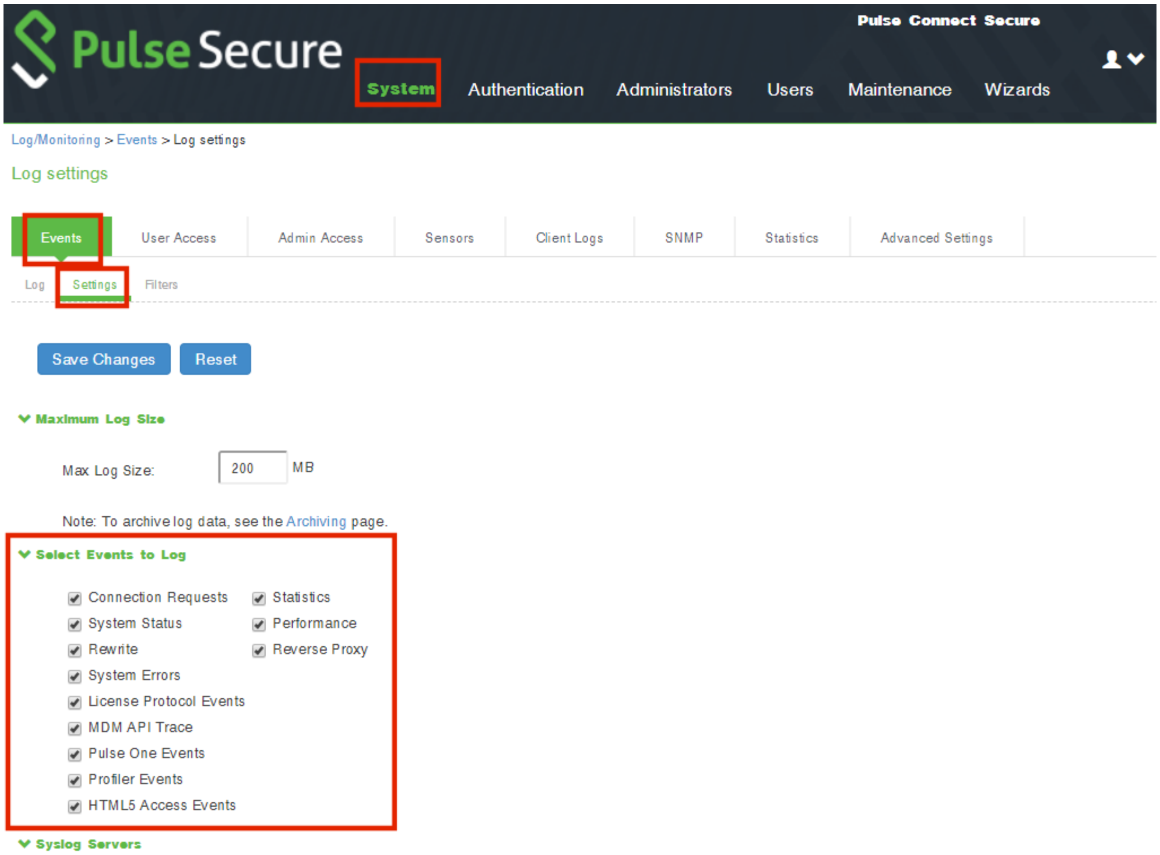
Registration Status: ●
Notification Channel Status: ●

Configuring Log Settings on the Appliance

You must then perform the following steps on each PCS/PPS appliance that will use the syslog server:

1. Log into the PCS/PPS appliance.
2. Navigate to **System** > **Log/Monitoring** > **Events** > **Settings**.
3. Under **Select Events to Log**, select all options that need tracking. For example:

FIGURE 43 Log Events Settings



Log settings

Maximum Log Size

Max Log Size: 200 MB

Note: To archive log data, see the Archiving page.

Select Events to Log

☑ Connection Requests
☑ System Status
☑ Rewrite
☑ System Errors
☑ License Protocol Events
☑ MDM API Trace
☑ Pulse One Events
☑ Profiler Events
☑ HTML5 Access Events
☑ Statistics
☑ Performance
☑ Reverse Proxy

Syslog Servers

4. Under **Syslog Servers**:
   - **Server name/IP**: Enter the FQDN or IP address of the Pulse One appliance.
   - **Facility**: Select an option from the list. This will identify this log type.

     Note: To distinguish between different log types (Events, User Access, Admin Access), you must select a different **Facility** for each type.
   - **Type**: Select *TCP*.
   - **Client Certificate**: Select *Select Client Cert*.
   - **Filter**: Select *WELF: WELF*.

5. Click the **Add** button to add this external syslog server.
6. Click **Save Changes** to save the configuration.
7. Navigate to **System > Log/Monitoring > User Access > Settings**.
8. Under **Syslog Servers**:
    - **Server name/IP**: Enter the FQDN or IP address of the Pulse One appliance.
    - **Facility**: Select an option from the list. This will identify this log type.

      Note: To distinguish between different log types (Events, User Access, Admin Access), you must select a different **Facility** for each type.
    - **Type**: Select *TCP*.
    - **Client Certificate**: Select *Select Client Cert*.
    - **Filter**: Select *WELF: WELF*.
9. Navigate to **System > Log/Monitoring > Admin Access > Settings**.
10. Under **Syslog Servers**:
    - **Server name/IP**: Enter the FQDN or IP address of the Pulse One appliance.
    - **Facility**: Select an option from the list. This will identify this log type.

      Note: To distinguish between different log types (Events, User Access, Admin Access), you must select a different **Facility** for each type.
    - **Type**: Select *TCP*.
    - **Client Certificate**: Select *Select Client Cert*.
    - **Filter**: Select *WELF: WELF*.
11. Select the **Advanced Settings** tab and enable **Fault Tolerance** for the Pulse One syslog server.

After you have completed this procedure, the appliance will send all configured logs to the Pulse One syslog server.

Configuring ActiveSync Handler

The Pulse Connect Secure gateway can act as an ActiveSync proxy for Mobile devices that are onboarded through Pulse Workspace Server. Pulse Connect Secure gateway will:

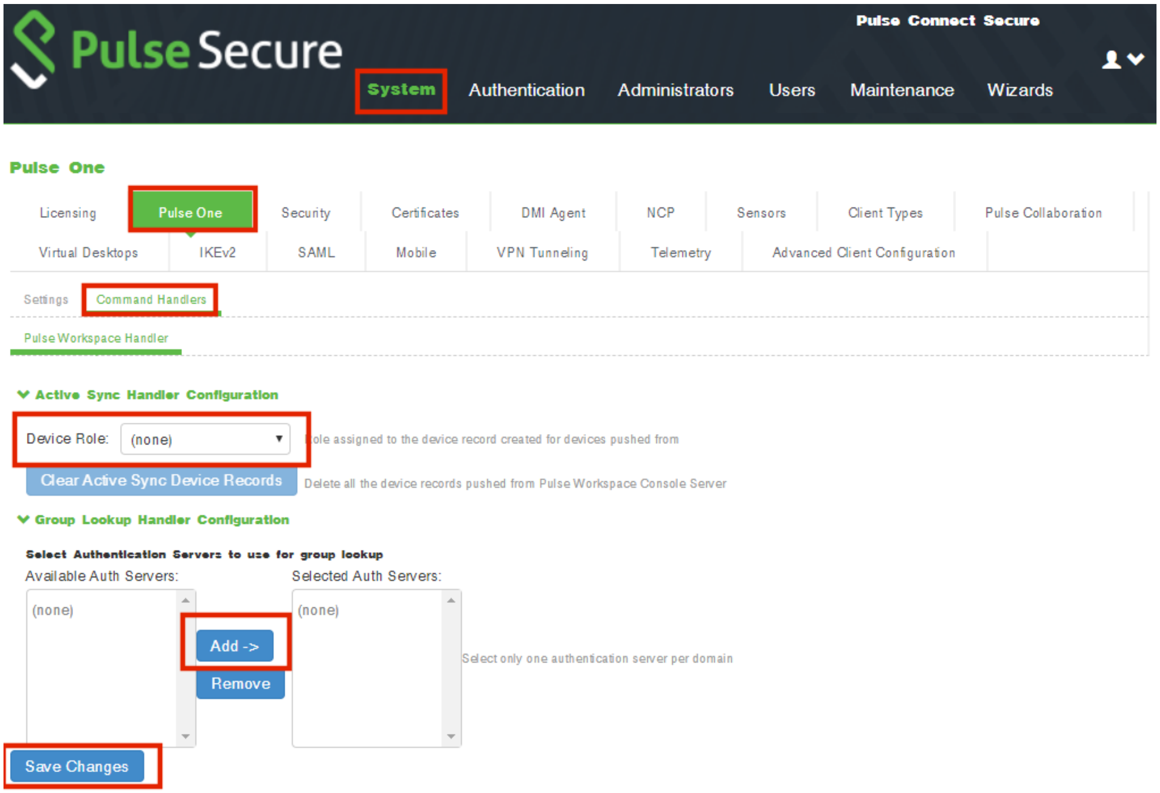
- Filter out and reject ActiveSync connection requests coming from unauthorized Mobile devices.
- Allow only those devices that have been successfully provisioned on Pulse Workspace Server.

To configure ActiveSync handler, in the Connect Secure Device screen:

1. Start the appliance user interface.
2. Select the **System > Configuration > Pulse One > Command Handlers** tab.

   The **Pulse Workspace Handler** screen appears.

   FIGURE 44 Pulse Connect Secure: Command Handlers



Device Role: (none)

Role assigned to the device record created for devices pushed from

Delete all the device records pushed from Pulse Workspace Console Server

Available Auth Servers: (none)

Selected Auth Servers: (none)

Select only one authentication server per domain

3. Select a role where secure email is enabled.
4. Select authentication servers to use for group look up and click **Add**.
5. (Optional) To delete the device records set by the Pulse Workspace Console Server, click **Clear Active Sync Device Records**.
6. Click **Save Changes**.

Note: To create a user rule, refer to the Pulse Connect Secure Administration Guide available at: **https://www.pulsesecure.net/techpubs.**

After you register a PCS appliance, it regularly sends the following information to Pulse One:

- Non-Hardware-specific PCS XML configuration. (Sent to On-Prem/Appliance and SaaS/Cloud)
- Hardware-specific PCS XML configuration. (Sent to On-Prem/Appliance and SaaS/Cloud)

  Note: Hardware-specific PCS XML configuration is not shared during configuration distribution.
- General information. That is, PCS health, statistics (such as CPU, network throughput), licensing details, cluster information and so on. (Sent to On-Prem/Appliance and SaaS/Cloud)
- User sign-in history. That is, logins from both web and the Pulse client. (Sent to On-Prem/Appliance only)
- User and System binary configuration. (Sent to On-Prem/Appliance only)

Creating and Registering a PCS Appliance VM on vSphere

You can create and register a PCS appliance as a vSphere Virtual Machine from Pulse One directly. This process will create the VM appliance and perform all required registration activities on the appliance automatically.

Note: You can also create and register a virtual PCS appliance for AWS, see **"Creating and Registering a PCS Appliance VM on AWS" on page 56**.

Note: This process requires sufficient appliance licensing capacity on Pulse One.

Note: Before beginning this process, ensure that your vSphere host is synced to an NTP server. Failure to do this may result in certificate verification issues that cause auto-registration of any resulting PCS appliance to fail. Refer to the *VMware vSphere* documentation for details of this operation.

Note: During this process, you can optionally use a master appliance template. A master template encapsulates an existing deployed appliance, and enables the re-use of many configuration settings on any appliance that is deployed using the template. To create a master template, see **"Creating an Appliance Master Template on vSphere" on page 50**.

To create and register a PCS appliance as a VM on vSphere:

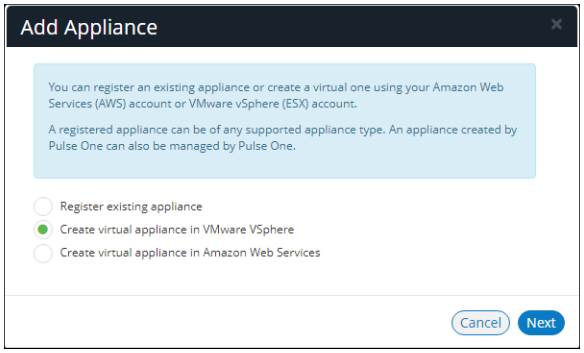
1. Log into Pulse One as an administrator.
2. Click the **Appliances** menu and then the **Appliances** tab.

   The **Appliances** tab displays all current appliances.

3. Click **Add Appliance**.

   The **Add Appliance** wizard starts.

   FIGURE 45 Add Appliance

   You can register an existing appliance or create a virtual one using your Amazon Web Services (AWS) account or VMware vSphere (ESX) account.

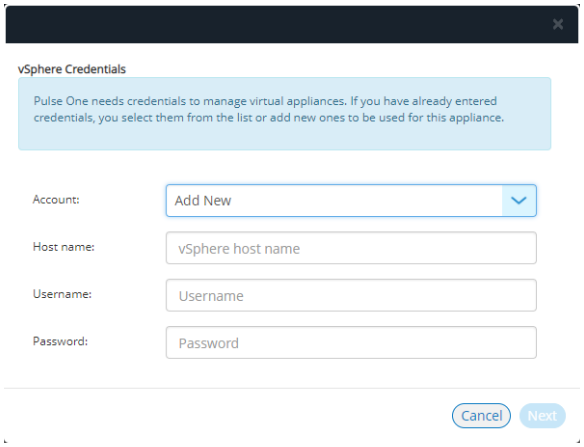
   A registered appliance can be of any supported appliance type. An appliance created by Pulse One can also be managed by Pulse One.

   ○ Register existing appliance
   ● Create virtual appliance in VMware VSphere
   ○ Create virtual appliance in Amazon Web Services

4. Select **Create virtual appliance in VMware vSphere** and click **Next**.

   The **vSphere Credentials** panel of the wizard appears.

   FIGURE 46 vSphere Credentials

   vSphere Credentials

   Pulse One needs credentials to manage virtual appliances. If you have already entered credentials, you select them from the list or add new ones to be used for this appliance.

   Account: Add New
   Host name: vSphere host name
   Username: Username
   Password: Password

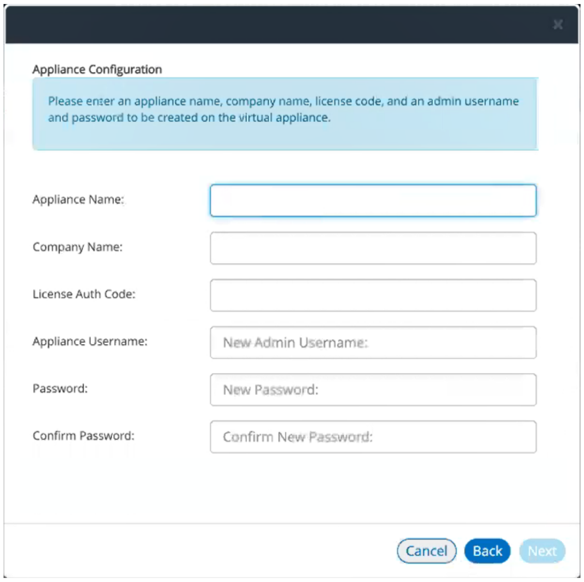
5. You must then specify vCenter credentials. Either:

   - Select *Add New* for **Account**, then:
     - For **Account**, select *Add New*.
     - For **Hostname**, enter the FQDN or IP address of your vCenter host.
     - For **Username** and **Password**, enter your vSphere credentials.
   - Select an existing vCenter **Account**.

6. Click **Next**.

   The **Appliance Configuration** panel of the wizard appears.

   FIGURE 47 Appliance Configuration



Appliance Configuration

Please enter an appliance name, company name, license code, and an admin username and password to be created on the virtual appliance.

Appliance Name:

Company Name:

License Auth Code:

Appliance Username: New Admin Username:

Password: New Password:

Confirm Password: Confirm New Password:

7. Enter the **Appliance Name**. This will be the displayed name in the list of appliances and will also be used to automatically populate the **Internal FQDN** and **External FQDN** properties on subsequent wizard panels.

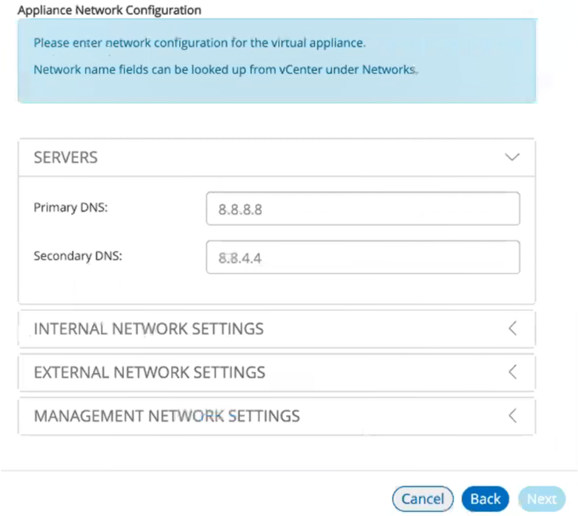
8. Specify additional information for the appliance:

   - A **Company Name**.
   - The **Appliance Username**, **Password** (and **Confirm Password**) for a required user on the appliance. This user will be created after the appliance is created.
   - (Optional) A **License Auth Code** can be entered if required.

9. Click **Next**.

   The **Appliance Network Configuration** panel of the wizard appears.

   FIGURE 48 Appliance Network Configuration: Servers



Appliance Network Configuration

Please enter network configuration for the virtual appliance.

Network name fields can be looked up from vCenter under Networks.

SERVERS

Primary DNS: 8.8.8.8

Secondary DNS: 8.8.4.4

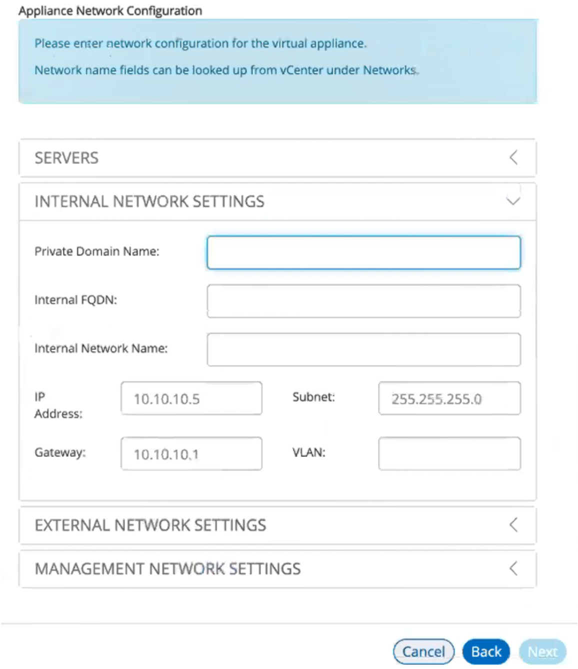
INTERNAL NETWORK SETTINGS
EXTERNAL NETWORK SETTINGS
MANAGEMENT NETWORK SETTINGS
Cancel
Back
Next

10. Specify the **Primary DNS** and the **Secondary DNS** for your network.

    Note: The displayed values are examples, and not defaults.

11. Expand the **Internal Network Settings** panel.

FIGURE 49 Appliance Network Configuration: Internal Network Settings



Appliance Network Configuration

Please enter network configuration for the virtual appliance.

Network name fields can be looked up from vCenter under Networks.

SERVERS

INTERNAL NETWORK SETTINGS

Private Domain Name:

Internal FQDN:

Internal Network Name:

IP Address: 10.10.10.5

Subnet: 255.255.255.0

Gateway: 10.10.10.1

VLAN:

EXTERNAL NETWORK SETTINGS

MANAGEMENT NETWORK SETTINGS

12. In the **Internal Network Settings**:

- For **Private Domain Name**, enter the internal domain name for your appliance.

  Note: When you shift focus away from this property, the **Private Domain Name** setting is displayed as a suffix to **Internal FQDN**.

- The **Internal FQDN** property is populated automatically using the **Appliance Name** you specified in the **Appliance Configuration** wizard panel, with the **Private Domain Name** used as a suffix. Change the **Internal FQDN** as required.

- For **Internal Network Name**, enter a name for the vSphere network. For example, VM Network.

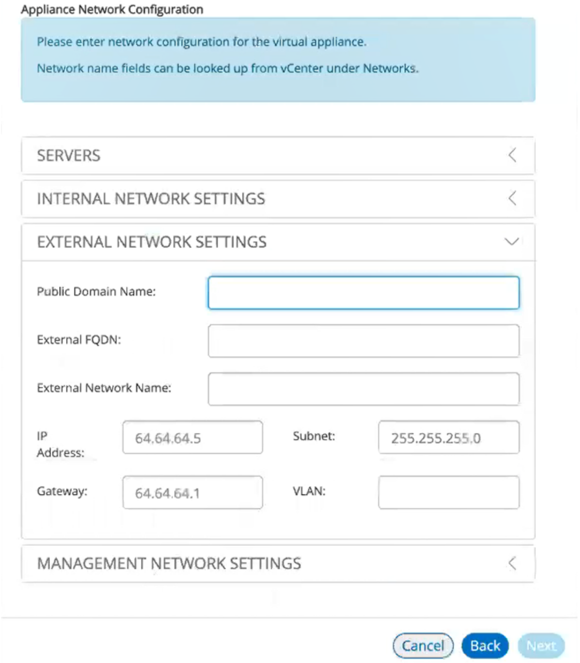
- For **IP Address**, enter the required internal IP address of the appliance.

- For **Subnet** and **Gateway**, enter the required subnet mask and gateway IP address.

- (Optional) For **VLAN**, enter your numeric VLAN identifier.

13. Expand the **External Network Settings** panel.

FIGURE 50 Appliance Network Configuration: External Network Settings



Appliance Network Configuration

Please enter network configuration for the virtual appliance.

Network name fields can be looked up from vCenter under Networks.

SERVERS
INTERNAL NETWORK SETTINGS
EXTERNAL NETWORK SETTINGS

Public Domain Name:

External FQDN:

External Network Name:

IP Address: 64.64.64.5

Subnet: 255.255.255.0

Gateway: 64.64.64.1

VLAN:

MANAGEMENT NETWORK SETTINGS
Cancel
Back
Next

14. In the **External Network Settings**:

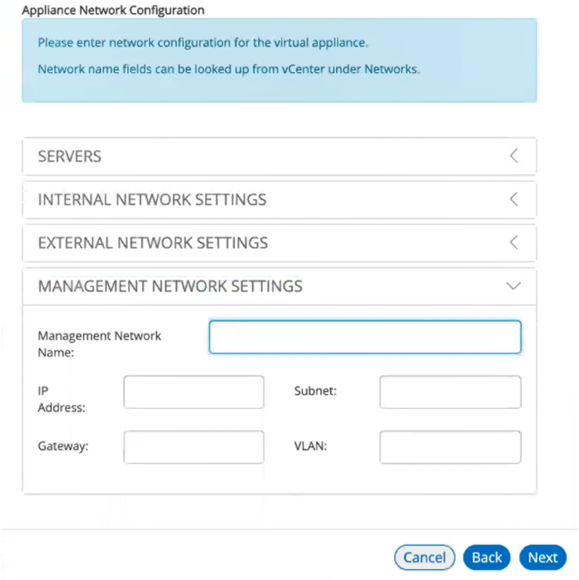
- For **Public Domain Name**, enter the external (Internet) domain name for your appliance.

  Note: When you shift focus away from this property, the **Public Domain Name** setting is displayed as a suffix to **External FQDN**.

- The **External FQDN** property is populated automatically using the **Appliance Name** you specified in the **Appliance Configuration** wizard panel, with the **Public Domain Name** used as a suffix. Change the **External FQDN** as required.
- For **External Network Name**, enter a name for the vSphere network. For example, VM Network.
- For **IP Address**, enter the required external IP address of the appliance.
- For **Subnet** and **Gateway**, enter the required subnet mask and gateway IP address.
- (Optional) For **VLAN**, enter the numeric value you used for the **Internal Network Settings** panel.

15. Expand the **Management Network Settings** panel.

FIGURE 51 Appliance Network Configuration: Management Network Settings



Appliance Network Configuration

Please enter network configuration for the virtual appliance.

Network name fields can be looked up from vCenter under Networks.

SERVERS
INTERNAL NETWORK SETTINGS
EXTERNAL NETWORK SETTINGS
MANAGEMENT NETWORK SETTINGS
Management Network Name:
IP Address:
Subnet:
Gateway:
VLAN:
Cancel
Back
Next

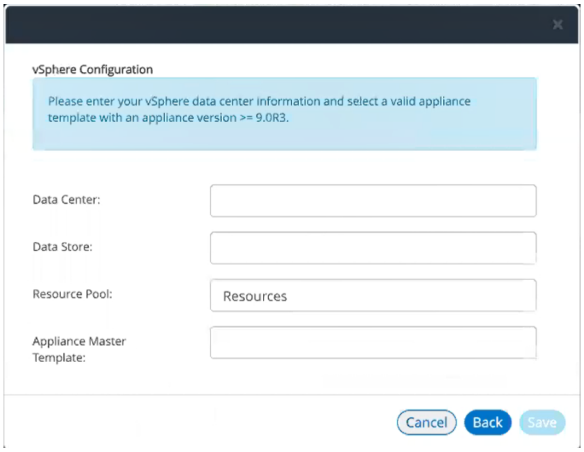
16. In the **Management Network Settings**:

    - For **Management Network Name**, enter a name for the vSphere network. For example, VM Network.
    - For **IP Address**, enter the required management IP address of the appliance.
    - For **Subnet** and **Gateway**, enter the required subnet mask and gateway IP address.
    - (Optional) For **VLAN**, enter the numeric value you used for the **External Network Settings** panel.

17. Click **Next**.

    The **vSphere Configuration** wizard panel appears.

    FIGURE 52 vSphere Configuration

    vSphere Configuration

    Please enter your vSphere data center information and select a valid appliance template with an appliance version >= 9.0R3.

    Data Center:

    Data Store:

    Resource Pool: Resources

    Appliance Master Template:

18. Complete the properties for this panel of the wizard:

    - For **Data Center**, enter your required vSphere data center. Data centers are listed on the **Storage** tab on vSphere.
    - For **Data Store**, enter the required vSphere data store from your selected data center. Data stores are listed under each data center on the **Storage** tab on vSphere.
    - For **Resource Pool**, enter the required vSphere resource pool from your selected data center. Resource pools are listed under each data center on the **Hosts and Clusters** tab on vSphere.
    - (Optional) Enter an **Appliance Master Template**. Templates are listed under the data center on the **VMs and Templates** tab on vSphere. For details of how to create an appliance master template, see **"Creating an Appliance Master Template on vSphere" on page 50**.

19. Click **Save**.

    The wizard closes, and the new *Unregistered* vSphere appliance is added to the list of appliances.

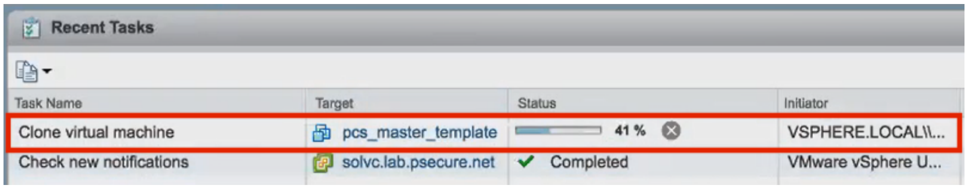
20. Click the **Actions** icon for the appliance and select **Start Appliance**.

21. The status of the new appliance goes through a series of states until it successfully running.

    - *Unregistered*
    - *Creating*
    - *Starting*
    - *Started*

22. (Optional) During the creation of the appliance, you can monitor progress from the vSphere **Recent Tasks** tab.

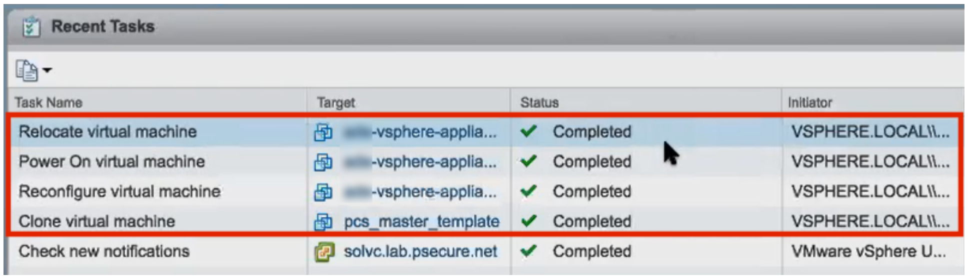
FIGURE 53 vSphere Appliance Creation In Progress



Recent Tasks

Task Name	Target	Status	Initiator
Clone virtual machine	pcs_master_template	41 %	VSPHERE.LOCAL\\...
Check new notifications	solvc.lab.psecure.net	✓ Completed	VMware vSphere U...

FIGURE 54 vSphere Appliance Creation Complete



Recent Tasks

Task Name	Target	Status	Initiator
Relocate virtual machine	[redacted]-vsphere-applia...	✓ Completed	VSPHERE.LOCAL\\...
Power On virtual machine	[redacted]-vsphere-applia...	✓ Completed	VSPHERE.LOCAL\\...
Reconfigure virtual machine	[redacted]-vsphere-applia...	✓ Completed	VSPHERE.LOCAL\\...
Clone virtual machine	pcs_master_template	✓ Completed	VSPHERE.LOCAL\\...
Check new notifications	solvc.lab.psecure.net	✓ Completed	VMware vSphere U...

23. Wait until vSphere allocates all IP addresses to the new appliance (see the vSphere **Summary** tab for a selected appliance).

    Note: The appliance is auto-registered. That is, you do not need to manually complete the registration of the appliance from the appliance GUI.

The creation and registration of the virtual PCS appliance on vSphere is now complete.

Creating an Appliance Master Template on vSphere

Pulse Connect Secure is delivered as a pair of OVF/VMDK template files for use on vSphere. You deploy these OVF template files in vSphere to create a virtual PCS appliance.

You can create a master appliance template which encapsulates the configuration for the appliance.

Appliances that are created from the master template will use the encapsulated configuration, and require less configuration after deployment.

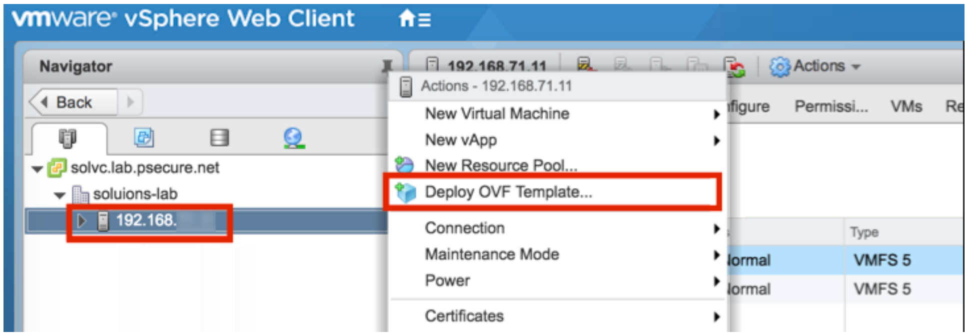
To create a master appliance template:

1. Obtain the Pulse Connect Secure template files from Pulse Secure Support and store the files in an accessible location in your network.

2. Log into the vSphere Web Client.

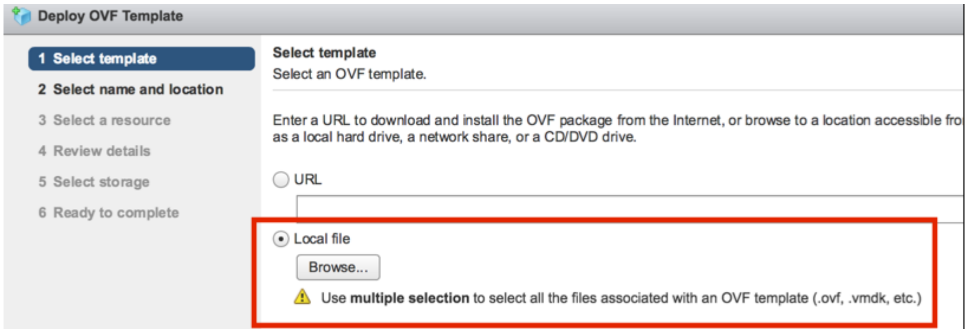
3. Right-click and an existing host and click **Deploy OVF Template**. For example:

FIGURE 55 vSphere Web Client Deploy



The **Deploy OVF Template** wizard appears.

FIGURE 56 vSphere Deploy OVF Template Wizard 1


Deploy OVF Template

1 Select template
2 Select name and location
3 Select a resource
4 Review details
5 Select storage
6 Ready to complete

Select template
Select an OVF template.

Enter a URL to download and install the OVF package from the Internet, or browse to a location accessible fro
as a local hard drive, a network share, or a CD/DVD drive.

○ URL

● Local file

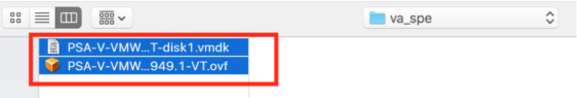
Browse...

⚠ Use **multiple selection** to select all the files associated with an OVF template (.ovf, .vmdk, etc.)

4. Select the **Local file** option and click **Browse**.

5. Locate and multi-select the OVF and VMDK template files. For example:

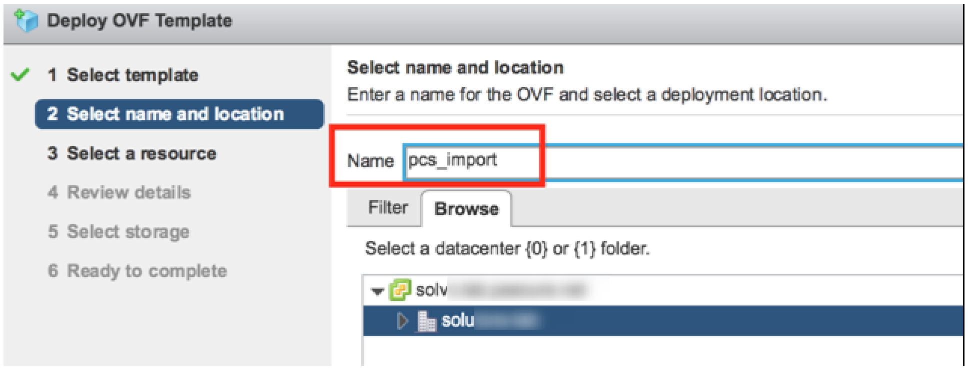
FIGURE 57 vSphere Deploy OVF Select Template Files



PSA-V-VMW...T-disk1.vmdk
PSA-V-VMW...949.1-VT.ovf

6. Click **Next** to proceed to the next panel of the wizard. For example:

FIGURE 58 vSphere Deploy OVF Template Wizard 2



Select name and location
Enter a name for the OVF and select a deployment location.

Name pcs_import

Select a datacenter {0} or {1} folder.

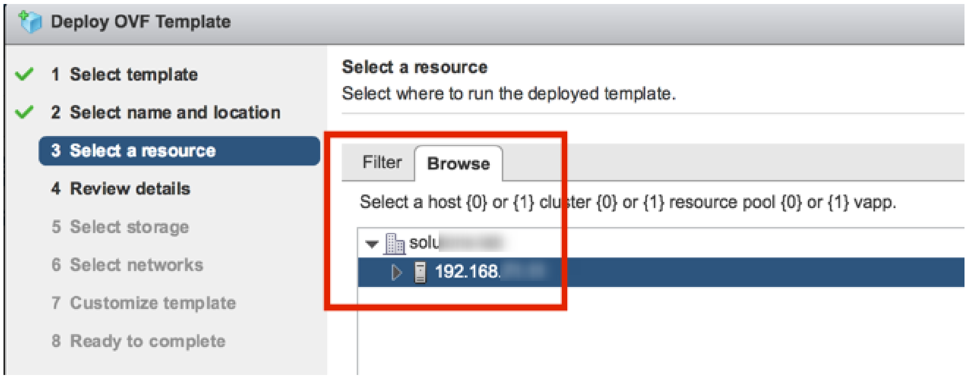
solv[redacted]
solu[redacted]

7. Enter a **Name** and select a data center for the deployment.

   In this example, the **Name** of the appliance is *pcs_import*.

8. Click **Next** to proceed to the next panel of the wizard. For example:

FIGURE 59 vSphere Deploy OVF Template Wizard 3



Select a resource
Select where to run the deployed template.

Select a host {0} or {1} cluster {0} or {1} resource pool {0} or {1} vapp.

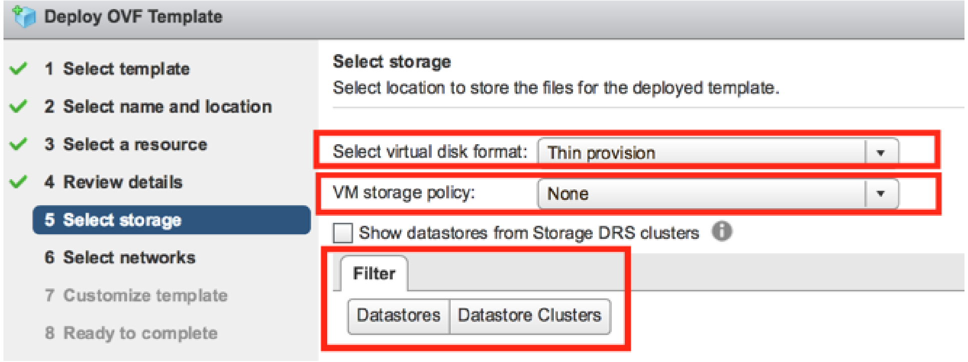
solu[redacted]
192.168.[redacted]

9. Click **Next** to proceed to the next panel of the wizard.

10. Review the displayed details and step back through the wizard to correct these if required.

11. Click **Next** to proceed to the next panel of the wizard. For example:

FIGURE 60 vSphere Deploy OVF Template Wizard 5



Deploy OVF Template

✓ 1 Select template
✓ 2 Select name and location
✓ 3 Select a resource
✓ 4 Review details
5 Select storage
6 Select networks
7 Customize template
8 Ready to complete

Select storage
Select location to store the files for the deployed template.

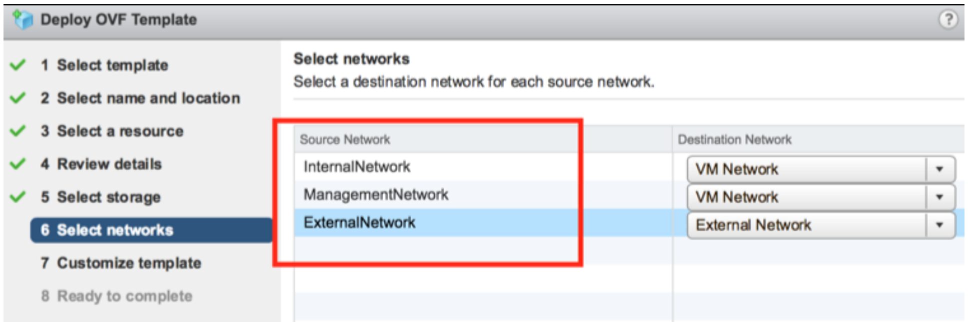
Select virtual disk format: Thin provision

VM storage policy: None

□ Show datastores from Storage DRS clusters

12. Click **Next** to proceed to the next panel of the wizard. For example:

FIGURE 61 vSphere Deploy OVF Template Wizard 6



Deploy OVF Template

✓ 1 Select template
✓ 2 Select name and location
✓ 3 Select a resource
✓ 4 Review details
✓ 5 Select storage
6 Select networks
7 Customize template
8 Ready to complete

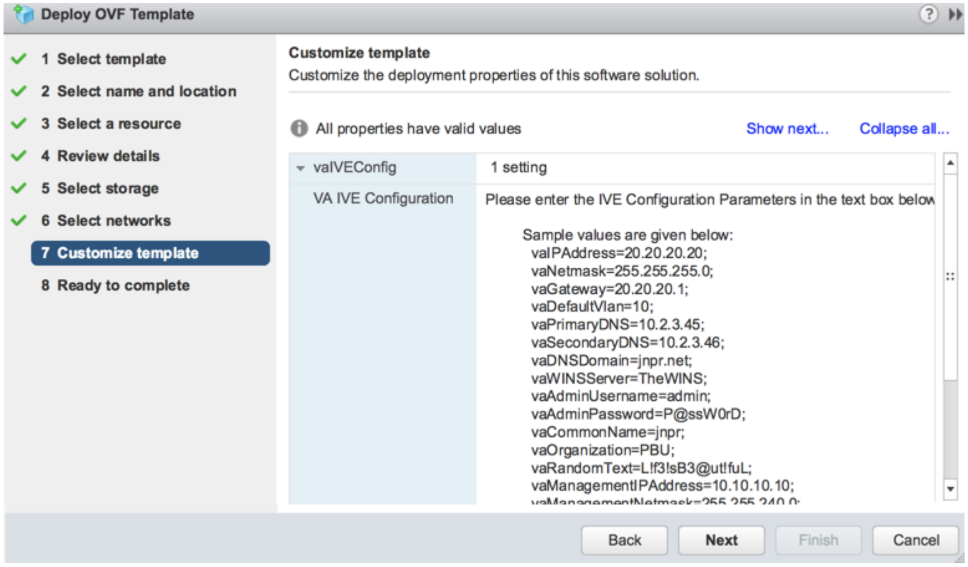
Select networks
Select a destination network for each source network.

Source Network	Destination Network
InternalNetwork	VM Network
ManagementNetwork	VM Network
ExternalNetwork	External Network

13. Select appropriate network interfaces for each of the PCS interfaces.

14. Click **Next** to proceed to the next panel of the wizard.

FIGURE 62 vSphere Deploy OVF Template Wizard 7



Customize template
Customize the deployment properties of this software solution.

All properties have valid values

valVEConfig: 1 setting

VA IVE Configuration: Please enter the IVE Configuration Parameters in the text box below

```
        Sample values are given below:
          valPAddress=20.20.20.20;
          vaNetmask=255.255.255.0;
          vaGateway=20.20.20.1;
          vaDefaultVlan=10;
          vaPrimaryDNS=10.2.3.45;
          vaSecondaryDNS=10.2.3.46;
          vaDNSDomain=jnpr.net;
          vaWINSServer=TheWINS;
          vaAdminUsername=admin;
          vaAdminPassword=P@ssW0rD;
          vaCommonName=jnpr;
          vaOrganization=PBU;
          vaRandomText=L!f3!sB3@ut!fuL;
          vaManagementIPAddress=10.10.10.10;
          vaManagementNetmask=255.255.240.0;
```

15. Make no changes to this wizard page.

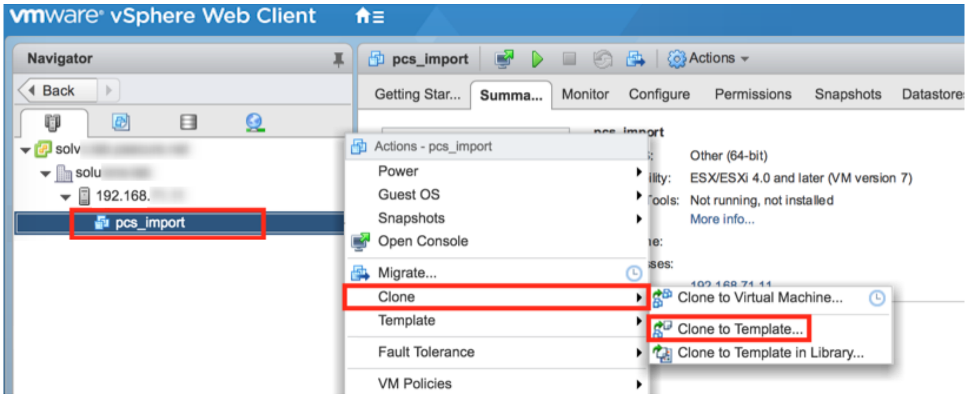
16. Click **Next** to proceed to the final panel of the wizard.

17. Review the displayed details and step back through the wizard to correct these if required.

18. Click **Finish** to complete the wizard and deploy the appliance.

    After the appliance is deployed, it appears in the main page of the vSphere Web Client. For example:

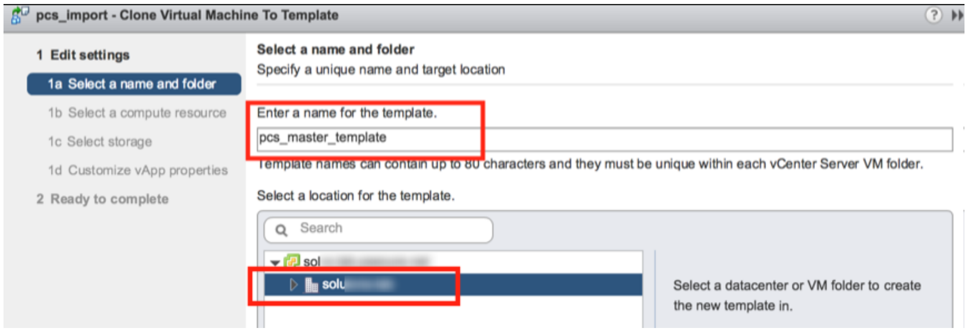
FIGURE 63 vSphere Web Client Clone



19. Right-click on the appliance and then click **Clone > Clone to Template**.

    The **Clone Virtual Machine to Template** wizard starts. For example:

FIGURE 64 vSphere Clone VM to Template Wizard


pcs_import - Clone Virtual Machine To Template
1 Edit settings
1a Select a name and folder
1b Select a compute resource
1c Select storage
1d Customize vApp properties
2 Ready to complete
Search
sol
solu

Select a name and folder

Specify a unique name and target location

Enter a name for the template.

pcs_master_template

Template names can contain up to 80 characters and they must be unique within each vCenter Server VM folder.

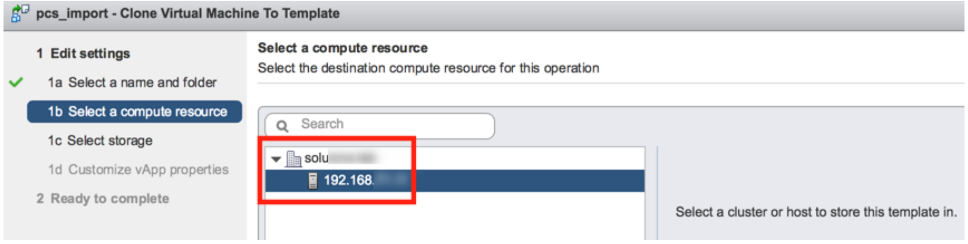
Select a location for the template.

Select a datacenter or VM folder to create the new template in.

20. Specify a name and select a location for the required template.

21. Click **Next** to proceed to the next panel of the wizard. For example:

FIGURE 65 vSphere Clone VM to Template Wizard 1b


pcs_import - Clone Virtual Machine To Template
1 Edit settings
1a Select a name and folder
1b Select a compute resource
1c Select storage
1d Customize vApp properties
2 Ready to complete
Search
solu
192.168.

Select a compute resource

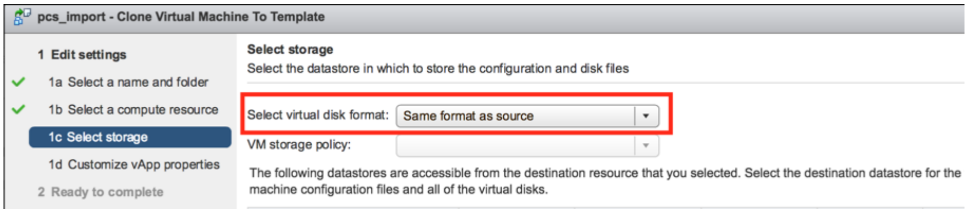
Select the destination compute resource for this operation

Select a cluster or host to store this template in.

22. Select the required compute resource.

23. Click **Next** to proceed to the next panel of the wizard. For example:

FIGURE 66 vSphere Clone VM to Template Wizard 1c



pcs_import - Clone Virtual Machine To Template

1 Edit settings
✓ 1a Select a name and folder
✓ 1b Select a compute resource
1c Select storage
1d Customize vApp properties
2 Ready to complete

Select storage

Select the datastore in which to store the configuration and disk files

Select virtual disk format: Same format as source

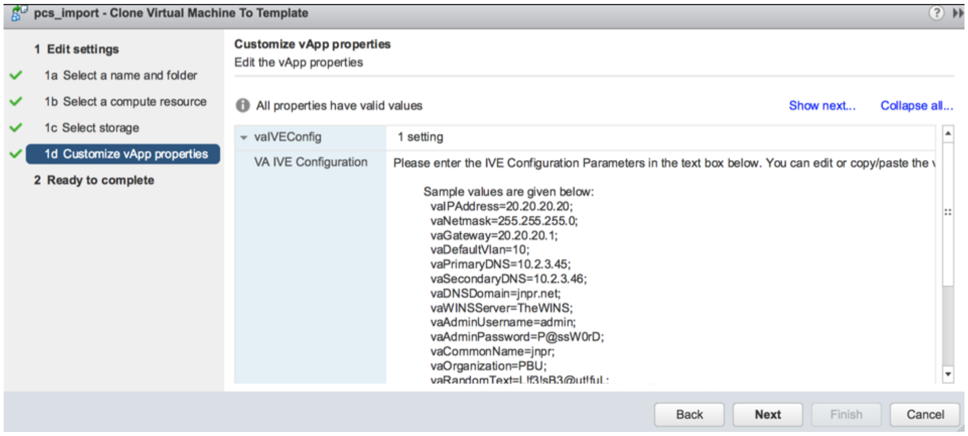
VM storage policy:

The following datastores are accessible from the destination resource that you selected. Select the destination datastore for the machine configuration files and all of the virtual disks.

24. Set **Select virtual disk format** to Same format as source.

25. Click **Next** to proceed to the next panel of the wizard. For example:

FIGURE 67 vSphere Clone VM to Template Wizard 1d



pcs_import - Clone Virtual Machine To Template

Customize vApp properties

Edit the vApp properties

All properties have valid values

valVEConfig	1 setting
VA IVE Configuration	Please enter the IVE Configuration Parameters in the text box below. You can edit or copy/paste the v

```
Sample values are given below:
  valPAddress=20.20.20.20;
  vaNetmask=255.255.255.0;
  vaGateway=20.20.20.1;
  vaDefaultVlan=10;
  vaPrimaryDNS=10.2.3.45;
  vaSecondaryDNS=10.2.3.46;
  vaDNSDomain=jnpr.net;
  vaWINSServer=TheWINS;
  vaAdminUsername=admin;
  vaAdminPassword=P@ssW0rD;
  vaCommonName=jnpr;
  vaOrganization=PBU;
  vaRandomText=L!f3!sB3@ut!fuL;
```

26. Click **Next** to proceed to the final panel of the wizard.

27. Review the displayed details and step back through the wizard to correct these if required.

28. Click **Finish** to complete the wizard and create the master appliance template.

After you have a master appliance template, you can optionally use it on the **vSphere Configuration** page of the **Add Appliance Wizard**, see **"Creating and Registering a PCS Appliance VM on vSphere" on page 42**.

Creating and Registering a PCS Appliance VM on AWS

You can create and register a PCS appliance as an AWS Virtual Machine from Pulse One directly. This process will create the VM appliance and perform all required registration activities on the appliance automatically.

Note: This process requires sufficient appliance licensing capacity on Pulse One.

Note: You can also create and register a Virtual Machine appliance for vSphere, see **"Creating and Registering a PCS Appliance VM on vSphere" on page 42**.

Perform the following tasks:

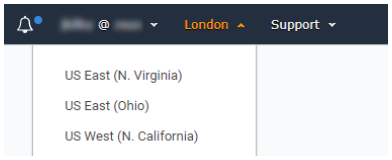
1. Before you begin, you must locate and record the following information:
    - The required Route 53 zones, see **“Identifying the Required Route 53 Zones” on page 57**.
    - The required VPC ID and Subnet IDs, see **“Identifying the Required VPC ID and Subnet IDs” on page 60**.
    - The required EC2 deployment key, see **“Identifying the EC2 Deployment Key and AMI ID” on page 62**.
2. You can then create the appliance, see **“Creating the PCS Appliance VM on AWS” on page 65**.

Identifying the Required Route 53 Zones

Both a private and a public Route 53 zone are required during the creation of a virtual machine PCS appliance. To locate this information:

1. Login to the AWS Management Console.
2. On the AWS top bar, select the required **Region**. For example, EU (London).

FIGURE 68 AWS Selecting Region

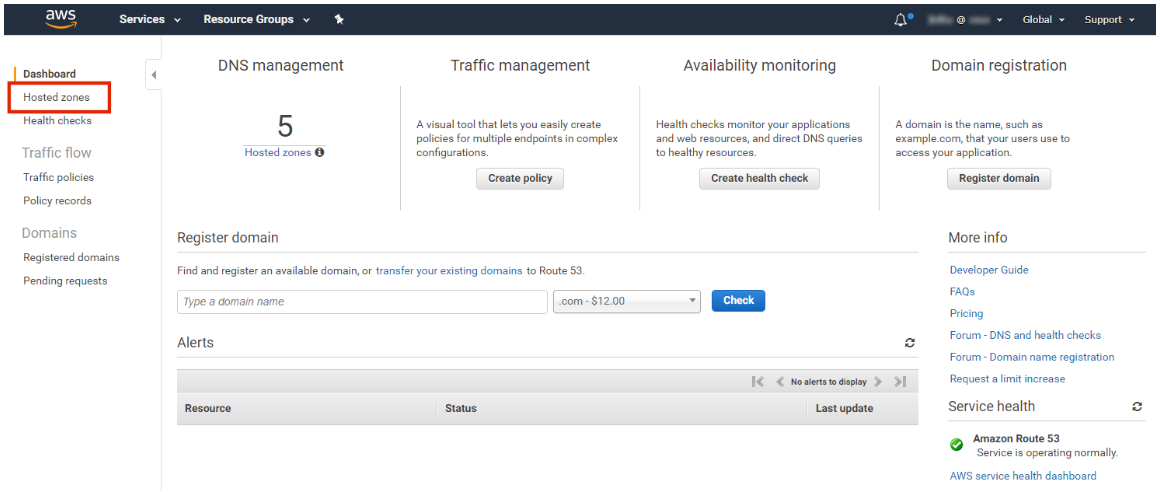


3. On the AWS top bar, click **Services** and then locate the **Network & Content Delivery** options.

4. Under **Network & Content Delivery**, select **Route 53**.

   The AWS Route 53 Management Console appears.

   FIGURE 69 AWS Route 53 Management Console



A visual tool that lets you easily create policies for multiple endpoints in complex configurations.

Health checks monitor your applications and web resources, and direct DNS queries to healthy resources.

A domain is the name, such as example.com, that your users use to access your application.

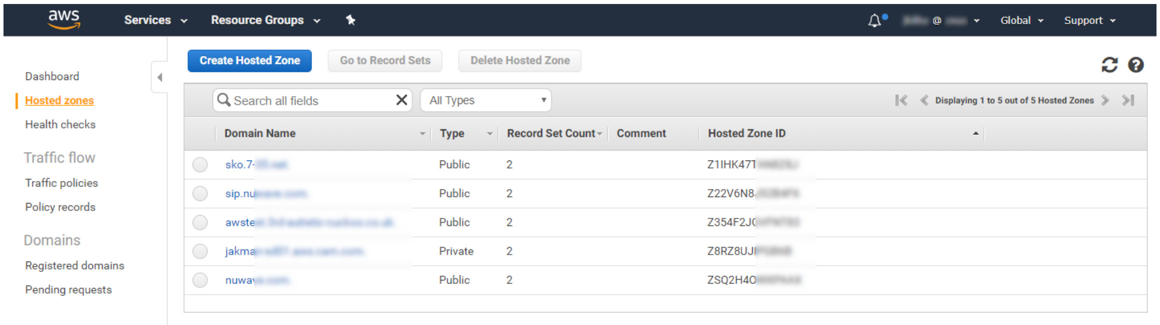
Find and register an available domain, or transfer your existing domains to Route 53.

Service is operating normally.

5. Select **Hosted Zones**.

   The hosted zones panel appears. This lists all domain names (zones) that are available to you.

   FIGURE 70 AWS Route 53 Hosted Zones



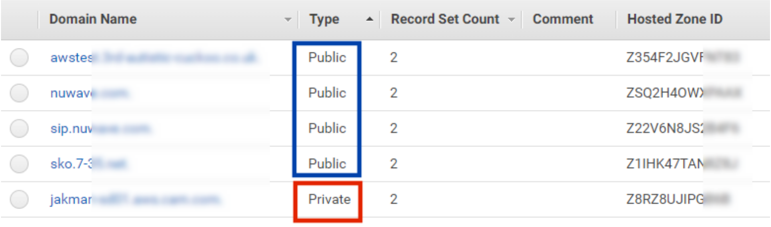
Domain Name	Type	Record Set Count	Comment	Hosted Zone ID
○ sko.7-[redacted]	Public	2		Z1IHK47T[redacted]
○ sip.nu[redacted]	Public	2		Z22V6N8[redacted]
○ awste[redacted]	Public	2		Z354F2JC[redacted]
○ jakma[redacted]	Private	2		Z8RZ8UJI[redacted]
○ nuwa[redacted]	Public	2		ZSQ2H4O[redacted]

In the domain name list:

- Zones that have a **Type** of Public have externally-facing (Internet) domain names. The external FQDN that is required when you create the PCS appliance VM will use the external domain name as a suffix.
- Zones that have a **Type** of Private have internally-facing domain names. The internal FQDN that is required when you create the PCS appliance VM will use an internal domain name as a suffix.

For example:

FIGURE 71 AWS Public and Private Zones



	Domain Name	Type	Record Set Count	Comment	Hosted Zone ID
○	awstes[redacted]	Public	2		Z354F2JGVF[redacted]
○	nuwave[redacted]	Public	2		ZSQ2H4OW[redacted]
○	sip.nu[redacted]	Public	2		Z22V6N8JS[redacted]
○	sko.7-[redacted]	Public	2		Z1IHK47TAN[redacted]
○	jakmar[redacted]	Private	2		Z8RZ8UJIPG[redacted]

6. Select the required Public zone and record its Domain Name.

7. Locate the required Private zone and record its Domain Name.

You can then perform any remaining preparations, and then continue to create and register the PCS appliance virtual machine on AWS.

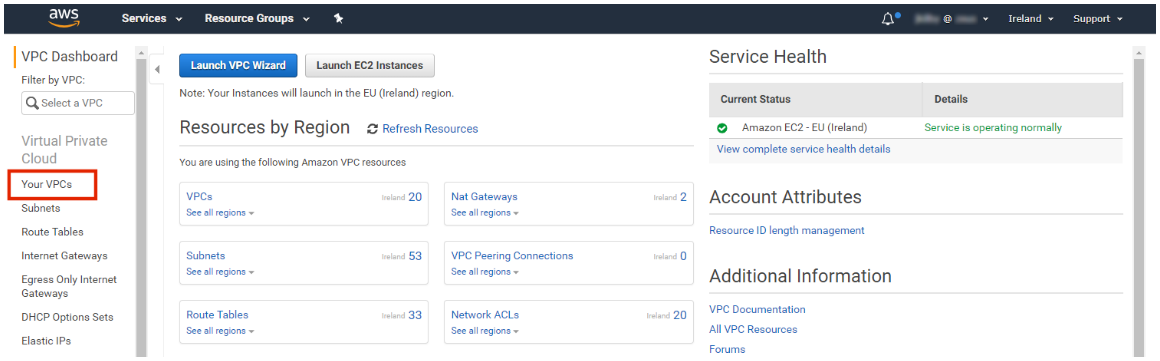
Identifying the Required VPC ID and Subnet IDs

A VPC identifier is required during the creation of a virtual machine PCS appliance. To locate this information:

1. Login to the AWS Management Console.
2. On the AWS top bar, select the required **Region**.
3. On the AWS top bar, click **Services** and then locate the **Network & Content Delivery** options.
4. Under **Network & Content Delivery**, select **VPC**.

   The **AWS VPC Dashboard** appears.

   FIGURE 72 AWS VPC Dashboard



Note: Your Instances will launch in the EU (Ireland) region.

You are using the following Amazon VPC resources

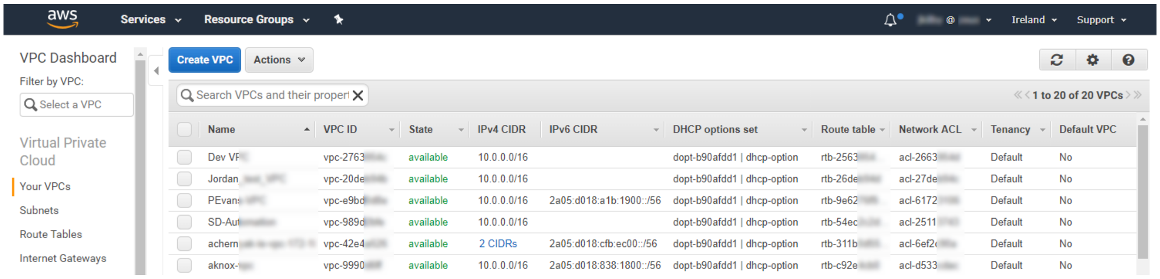
Current Status	Details
Amazon EC2 - EU (Ireland)	Service is operating normally

View complete service health details

5. Select **Your VPCs**.

A list of available VPCs appears.

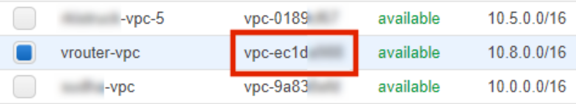
FIGURE 73 AWS Available VPCs



Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	DHCP options set	Route table	Network ACL	Tenancy	Default VPC
Dev VP[redacted]	vpc-2763[redacted]	available	10.0.0.0/16		dopt-b90afdd1 | dhcp-option	rtb-2563[redacted]	acl-2663[redacted]	Default	No
Jordan[redacted]	vpc-20de[redacted]	available	10.0.0.0/16		dopt-b90afdd1 | dhcp-option	rtb-26de[redacted]	acl-27de[redacted]	Default	No
PEvans[redacted]	vpc-e9bd[redacted]	available	10.0.0.0/16	2a05:d018:a1b:1900::/56	dopt-b90afdd1 | dhcp-option	rtb-9e62[redacted]	acl-6172[redacted]	Default	No
SD-Aut[redacted]	vpc-989d[redacted]	available	10.0.0.0/16		dopt-b90afdd1 | dhcp-option	rtb-54ec[redacted]	acl-2511[redacted]	Default	No
achern[redacted]	vpc-42e4[redacted]	available	2 CIDRs	2a05:d018:cfb:ec00::/56	dopt-b90afdd1 | dhcp-option	rtb-311b[redacted]	acl-6ef2[redacted]	Default	No
aknox-[redacted]	vpc-9990[redacted]	available	10.0.0.0/16	2a05:d018:838:1800::/56	dopt-b90afdd1 | dhcp-option	rtb-c92e[redacted]	acl-d533[redacted]	Default	No

6. Locate the required VPC and record its **VPC ID**. For example:

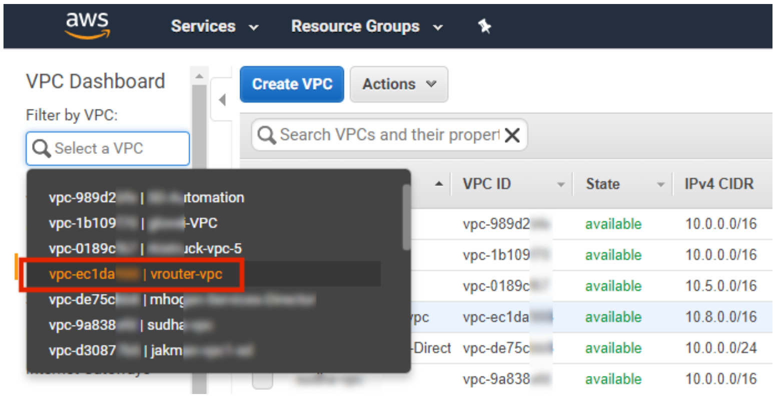
FIGURE 74 AWS VPC ID



□	[redacted]-vpc-5	vpc-0189[redacted]	available	10.5.0.0/16
■	vrouter-vpc	vpc-ec1d[redacted]	available	10.8.0.0/16
□	[redacted]-vpc	vpc-9a83[redacted]	available	10.0.0.0/16

7. In the **Filter by VPC** filter, select the required VPC. For example:

FIGURE 75 AWS Select VPC



vpc-989d2[redacted] | [redacted]tomation
vpc-1b109[redacted] | [redacted]-VPC
vpc-0189c[redacted] | [redacted]ck-vpc-5
vpc-ec1da[redacted] | vrouter-vpc
vpc-de75c[redacted] | mhog[redacted]
vpc-9a838[redacted] | sudha[redacted]
vpc-d3087[redacted] | jakm[redacted]

VPC ID	State	IPv4 CIDR
vpc-989d2[redacted]	available	10.0.0.0/16
vpc-1b109[redacted]	available	10.0.0.0/16
vpc-0189c[redacted]	available	10.5.0.0/16
vpc-ec1da[redacted]	available	10.8.0.0/16
vpc-de75c[redacted]	available	10.0.0.0/24
vpc-9a838[redacted]	available	10.0.0.0/16

8. Click **Subnets**.

A list of all subnets in the selected VPC appears.

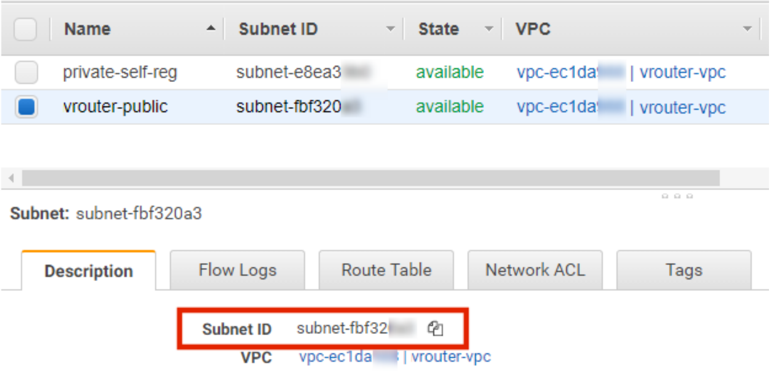
This list must include three different subnets that are in the same **Availability Zone**. Each will be used for one of the standard PCS interfaces in a later procedure (see **"Creating the PCS Appliance VM on AWS" on page 65**). The interfaces requirements are:

- Internal interface - This must be a *private* subnet.
- External Interface - This must be a *public* subnet.
- Management Interface - This can be either a *public* or *private* subnet, depending on your requirements.

Where the required subnets do not exist, you must create them before proceeding.

9. Select a public subnet and record its **Subnet ID** from the bottom panel. For example:

   FIGURE 76 AWS Select Public Subnet

☐	Name	Subnet ID	State	VPC
☐	private-self-reg	subnet-e8ea3[redacted]	available	vpc-ec1da[redacted] | vrouter-vpc
■	vrouter-public	subnet-fbf320[redacted]	available	vpc-ec1da[redacted] | vrouter-vpc

   Subnet: subnet-fbf320a3

   Subnet ID subnet-fbf32[redacted]
   VPC vpc-ec1da[redacted] | vrouter-vpc

   This subnet be used for the internal interface of the PCS appliance in a later procedure.

10. Select a private subnet (in the same **Availability Zone** as step 9) and record its **Subnet ID** from the bottom panel. This subnet be used for the external interface of the PCS appliance in a later procedure.

11. Select a third subnet (either private or public, and in the same **Availability Zone** as step 9) and record its **Subnet ID** from the bottom panel. This subnet be used for the management interface of the PCS appliance in a later procedure.

You can then perform any remaining preparations, and then continue to create and register the PCS appliance virtual machine on AWS.

Identifying the EC2 Deployment Key and AMI ID

An EC2 key pair (deployment key) and an AMI ID are required during the creation of a virtual machine PCS appliance. To locate this information:

1. Login to the AWS Management Console.

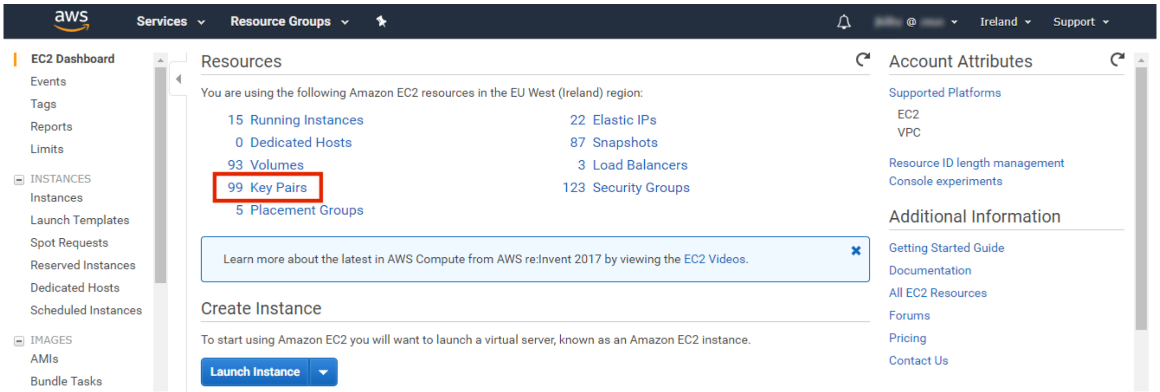
2. On the AWS top bar, select the required **Region**.

3. On the AWS top bar, click **Services** and then locate the **Compute** options.

4. Under **Compute**, select **EC2**.

The AWS EC2 Dashboard appears, showing **Key Pairs**.

FIGURE 77 AWS EC2 Dashboard



Resources

You are using the following Amazon EC2 resources in the EU West (Ireland) region:

15 Running Instances	22 Elastic IPs
0 Dedicated Hosts	87 Snapshots
93 Volumes	3 Load Balancers
99 Key Pairs	123 Security Groups
5 Placement Groups	

Learn more about the latest in AWS Compute from AWS re:Invent 2017 by viewing the EC2 Videos.

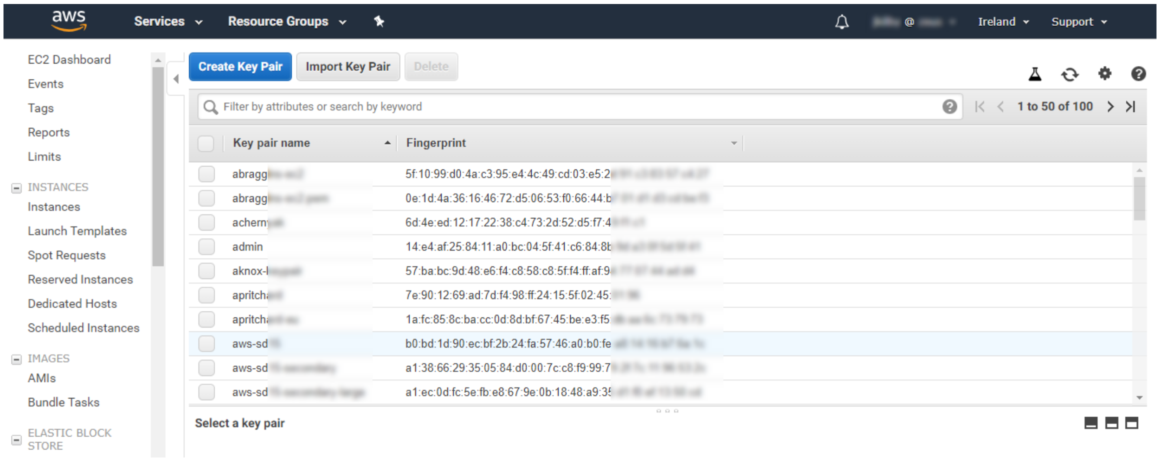
Create Instance

To start using Amazon EC2 you will want to launch a virtual server, known as an Amazon EC2 instance.

5. In the **Resources** panel, click **Key Pairs**.

   A list of defined key pairs appears.

FIGURE 78 AWS EC2 Key Pairs

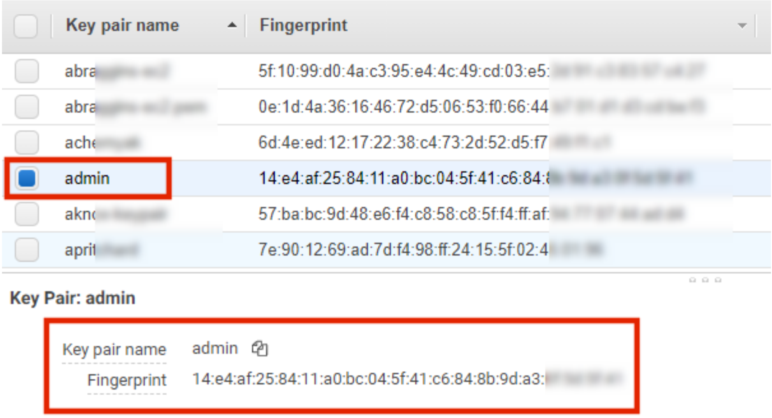


□	Key pair name	Fingerprint
□	abragg[redacted]	5f:10:99:d0:4a:c3:95:e4:4c:49:cd:03:e5:2[redacted]
□	abragg[redacted]	0e:1d:4a:36:16:46:72:d5:06:53:f0:66:44:b[redacted]
□	achern[redacted]	6d:4e:ed:12:17:22:38:c4:73:2d:52:d5:f7:4[redacted]
□	admin	14:e4:af:25:84:11:a0:bc:04:5f:41:c6:84:8b[redacted]
□	aknox-l[redacted]	57:ba:bc:9d:48:e6:f4:c8:58:c8:5f:f4:ff:af:9[redacted]
□	apritch[redacted]	7e:90:12:69:ad:7d:f4:98:ff:24:15:5f:02:45:[redacted]
□	apritch[redacted]	1a:fc:85:8c:ba:cc:0d:8d:bf:67:45:be:e3:f5[redacted]
□	aws-sd[redacted]	b0:bd:1d:90:ec:bf:2b:24:fa:57:46:a0:b0:fe[redacted]
□	aws-sd[redacted]	a1:38:66:29:35:05:84:d0:00:7c:c8:f9:99:7[redacted]
□	aws-sd[redacted]	a1:ec:0d:fc:5e:fb:e8:67:9e:0b:18:48:a9:35[redacted]

Select a key pair

6. Select the required key pair and record its **Key pair name** from the bottom panel. This name is used as the “deployment key” during installation. For example:

FIGURE 79 AWS Select EC2 Key Pair



□	Key pair name	Fingerprint
□	abra[redacted]	5f:10:99:d0:4a:c3:95:e4:4c:49:cd:03:e5:[redacted]
□	abra[redacted]	0e:1d:4a:36:16:46:72:d5:06:53:f0:66:44[redacted]
□	ache[redacted]	6d:4e:ed:12:17:22:38:c4:73:2d:52:d5:f7[redacted]
☑	admin	14:e4:af:25:84:11:a0:bc:04:5f:41:c6:84:[redacted]
□	akn[redacted]	57:ba:bc:9d:48:e6:f4:c8:58:c8:5f:f4:ff:af:[redacted]
□	aprit[redacted]	7e:90:12:69:ad:7d:f4:98:ff:24:15:5f:02:4[redacted]

Key Pair: admin

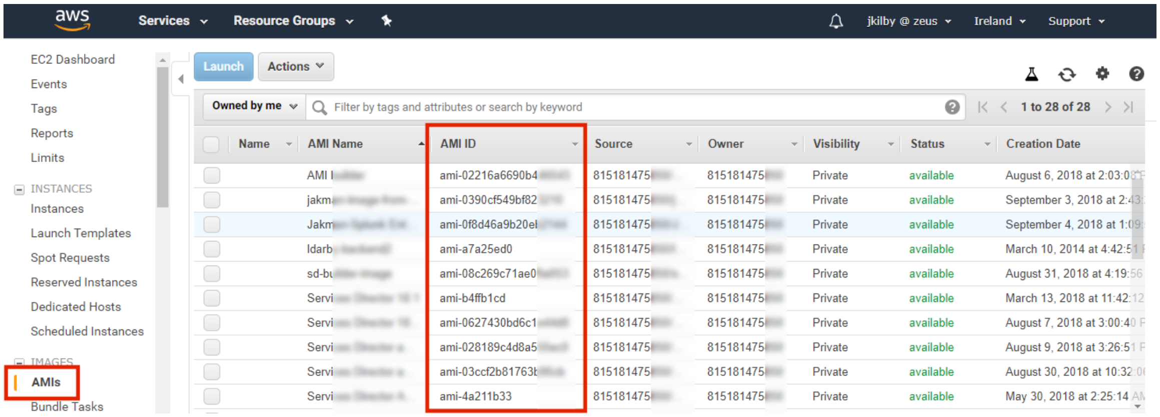
Key pair name admin

Fingerprint 14:e4:af:25:84:11:a0:bc:04:5f:41:c6:84:8b:9d:a3:[redacted]

7. On the EC2 dashboard menu, under **Images** select **AMIs**.

   A list of defined AMIs appears. For example:

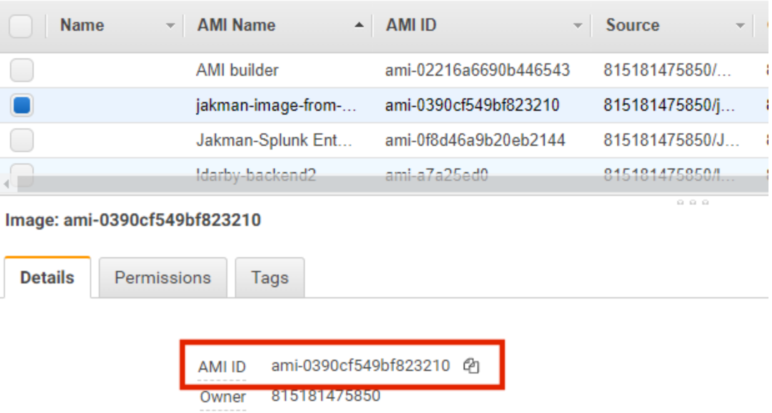
FIGURE 80 AWS EC2 AMIs



	Name	AMI Name	AMI ID	Source	Owner	Visibility	Status	Creation Date
□		AMI I[redacted]	ami-02216a6690b4[redacted]	815181475[redacted]	815181475[redacted]	Private	available	August 6, 2018 at 2:03:0
□		jakm[redacted]	ami-0390cf549bf82[redacted]	815181475[redacted]	815181475[redacted]	Private	available	September 3, 2018 at 2:4
□		Jakm[redacted]	ami-0f8d46a9b20el[redacted]	815181475[redacted]	815181475[redacted]	Private	available	September 4, 2018 at 1:0
□		Idarb[redacted]	ami-a7a25ed0	815181475[redacted]	815181475[redacted]	Private	available	March 10, 2014 at 4:42:5
□		sd-bu[redacted]	ami-08c269c71ae0[redacted]	815181475[redacted]	815181475[redacted]	Private	available	August 31, 2018 at 4:19:56
□		Servi[redacted]	ami-b4ffb1cd	815181475[redacted]	815181475[redacted]	Private	available	March 13, 2018 at 11:42:12
□		Servi[redacted]	ami-0627430bd6c1[redacted]	815181475[redacted]	815181475[redacted]	Private	available	August 7, 2018 at 3:00:40
□		Servi[redacted]	ami-028189c4d8a5[redacted]	815181475[redacted]	815181475[redacted]	Private	available	August 9, 2018 at 3:26:51
□		Servi[redacted]	ami-03ccf2b81763t[redacted]	815181475[redacted]	815181475[redacted]	Private	available	August 30, 2018 at 10:32
□		Servi[redacted]	ami-4a211b33	815181475[redacted]	815181475[redacted]	Private	available	May 30, 2018 at 2:25:14

8. Select the required AMI and record its **AMI-ID** from the bottom panel. For example:

FIGURE 81 AWS EC2 AMIs



	Name	AMI Name	AMI ID	Source
□		AMI builder	ami-02216a6690b446543	815181475850/...
■		jakman-image-from-...	ami-0390cf549bf823210	815181475850/j...
□		Jakman-Splunk Ent...	ami-0f8d46a9b20eb2144	815181475850/J...
□		Idarby-backend2	ami-a7a25ed0	815181475850/I...

Image: ami-0390cf549bf823210

AMI ID ami-0390cf549bf823210

Owner 815181475850

You can then perform any remaining preparations, and then continue to create and register the PCS appliance virtual machine on AWS.

Creating the PCS Appliance VM on AWS

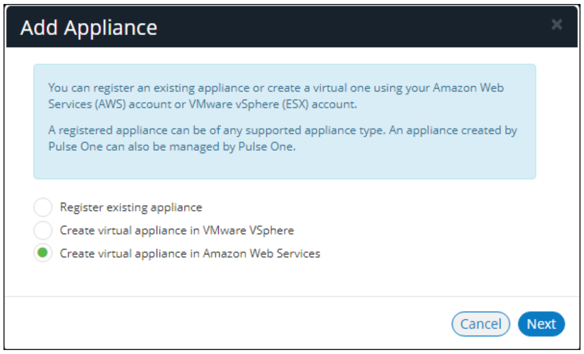
After you have identified all required information (see **"Creating and Registering a PCS Appliance VM on AWS" on page 56**), you can start the process to create and register a PCS appliance as a VM on AWS:

1. Log into Pulse One as an administrator.
2. Click the **Appliances** menu and then the **Appliances** tab.

   The **Appliances** tab displays all current appliances.
3. Click **Add Appliance**.

   The **Add Appliance** wizard starts.

   FIGURE 82 Add Appliance



Add Appliance

You can register an existing appliance or create a virtual one using your Amazon Web Services (AWS) account or VMware vSphere (ESX) account.

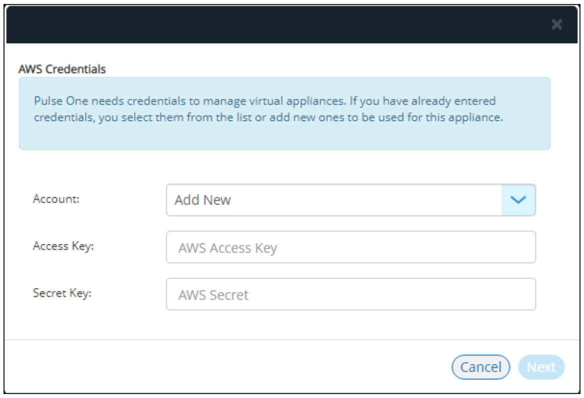
A registered appliance can be of any supported appliance type. An appliance created by Pulse One can also be managed by Pulse One.

○ Register existing appliance
○ Create virtual appliance in VMware VSphere
● Create virtual appliance in Amazon Web Services

4. Select **Create virtual appliance in Amazon Web Services** and click **Next**.

   The **AWS Credentials** panel of the wizard appears.

   FIGURE 83 AWS Credentials



AWS Credentials

Pulse One needs credentials to manage virtual appliances. If you have already entered credentials, you select them from the list or add new ones to be used for this appliance.

Account: Add New

Access Key: AWS Access Key

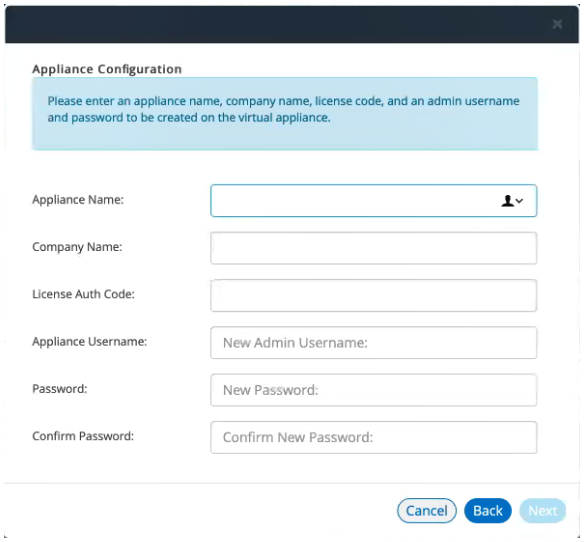
Secret Key: AWS Secret

5. You must then specify AWS credentials. Either:
   - Select *Add New* for **Account**, then enter your AWS **Access Key** and **Secret Key**, OR
   - Select an existing AWS **Account**.

6. Click **Next**.

   The **Appliance Configuration** panel of the wizard appears.

   FIGURE 84 Appliance Configuration

   Appliance Configuration

   Please enter an appliance name, company name, license code, and an admin username and password to be created on the virtual appliance.

   Appliance Name:

   Company Name:

   License Auth Code:

   Appliance Username: New Admin Username:

   Password: New Password:

   Confirm Password: Confirm New Password:

7. Enter the **Appliance Name**. This will be the displayed name in the list of appliances and will also be used to automatically populate the **Internal FQDN** and **External FQDN** properties on subsequent wizard panels.

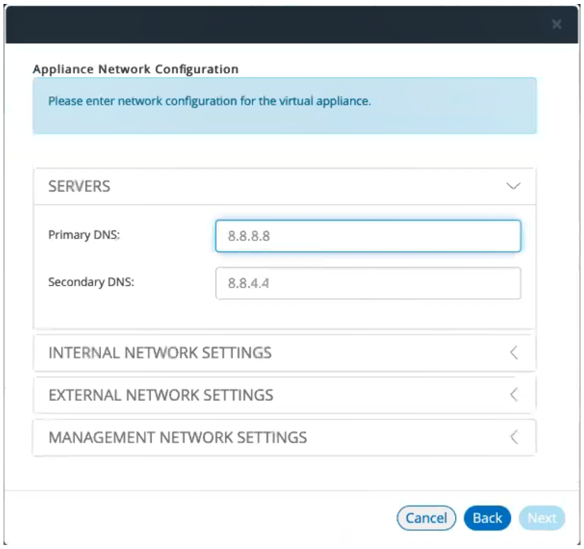
8. Specify additional information for the appliance:

   - A **Company Name**.
   - (Optional) A **License Auth Code** can be recorded if required.
   - The **Appliance Username**, **Password** (and **Confirm Password**) for a required user on the appliance. This user will be created after the appliance is created.

9. Click **Next**.

   The **Appliance Network Configuration** panel of the wizard appears.

   FIGURE 85 Appliance Network Configuration: Servers



Appliance Network Configuration

Please enter network configuration for the virtual appliance.

SERVERS

Primary DNS: 8.8.8.8

Secondary DNS: 8.8.4.4

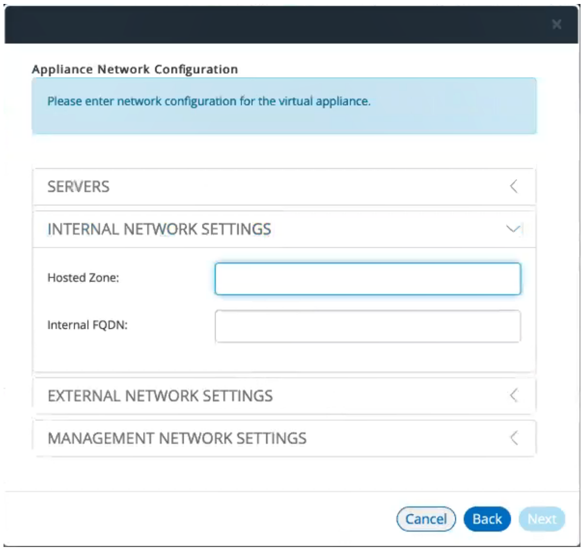
INTERNAL NETWORK SETTINGS
EXTERNAL NETWORK SETTINGS
MANAGEMENT NETWORK SETTINGS
Cancel
Back
Next

10. Specify the **Primary DNS** and the **Secondary DNS** for your network.

    Note: The displayed values are examples, and not defaults.

11. Expand the **Internal Network Settings** panel.

FIGURE 86 Appliance Network Configuration: Internal Network Settings



Appliance Network Configuration

Please enter network configuration for the virtual appliance.

SERVERS
INTERNAL NETWORK SETTINGS
Hosted Zone:
Internal FQDN:
EXTERNAL NETWORK SETTINGS
MANAGEMENT NETWORK SETTINGS
Cancel
Back
Next

12. In the **Internal Network Settings**:

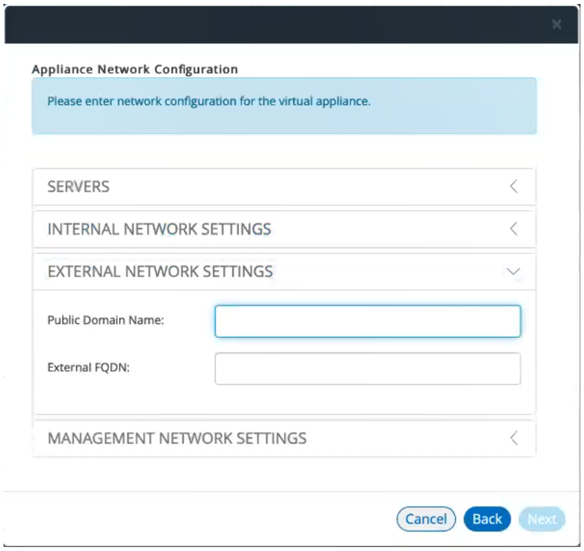
- For the **Hosted Zone**, enter the internal domain name (internal Route 53 hosted zone) for your appliance. See **“Identifying the Required Route 53 Zones” on page 57**.

  Note: When you shift focus away from this property, the internal **Hosted Zone** setting is displayed as a suffix to **Internal FQDN**.

- For the **Internal FQDN**, complete the FQDN by adding a unique appliance identifier to the left-hand side of the internal domain name in this field. Typically, you will specify the **Appliance Name** you specified in the **Appliance Configuration** dialog, and the internal **Hosted Zone** is used as a suffix.

13. Expand the **External Network Settings** panel.

FIGURE 87 Appliance Network Configuration: External Network Settings



Appliance Network Configuration

Please enter network configuration for the virtual appliance.

×
SERVERS
INTERNAL NETWORK SETTINGS
EXTERNAL NETWORK SETTINGS
MANAGEMENT NETWORK SETTINGS
Cancel
Back
Next

Public Domain Name:

External FQDN:

14. In the **External Network Settings**:

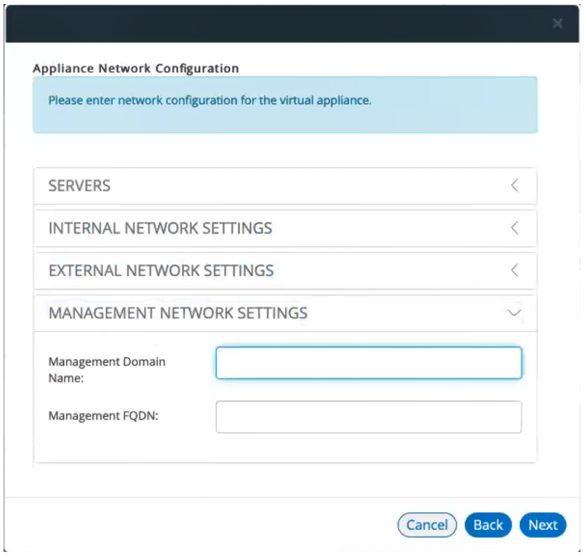
- For the **Public Domain Name**, enter the external domain name (external Route 53 hosted zone) for your appliance. See **"Identifying the Required Route 53 Zones" on page 57**.

  Note: When you shift focus away from this property, the external **Hosted Zone** setting is displayed as a suffix to **External FQDN**.

- For the **External FQDN**, complete the FQDN by adding a unique appliance identifier to the left-hand side of the external domain name in this field. Typically, you will specify the **Appliance Name** you specified in the **Appliance Configuration** dialog, and the external **Hosted Zone** is a suffix.

15. Expand the **Management Network Settings** panel.

FIGURE 88 Appliance Network Configuration: Management Network Settings



Appliance Network Configuration

Please enter network configuration for the virtual appliance.

SERVERS
INTERNAL NETWORK SETTINGS
EXTERNAL NETWORK SETTINGS
MANAGEMENT NETWORK SETTINGS

Management Domain Name:

Management FQDN:

16. In the **Management Network Settings**:

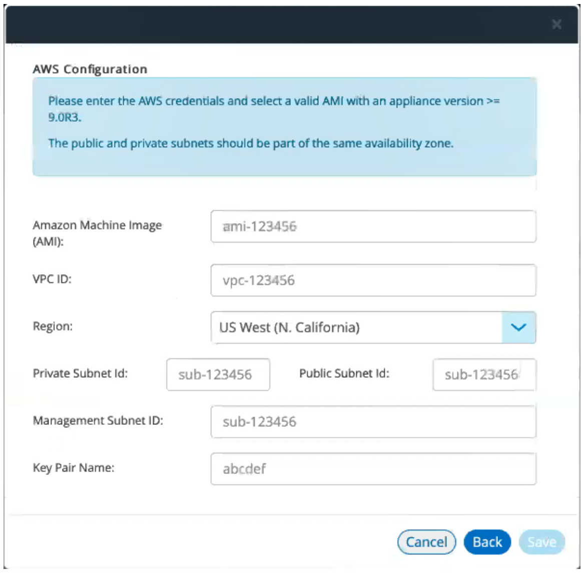
- For **Management Domain Name**, enter a name for the AWS network.

  Note: When you shift focus away from this property, the **Management Domain Name** setting is displayed as a suffix to **Management FQDN**.

- For the **Management FQDN**, complete the FQDN by adding a unique appliance identifier to the left-hand side of the external domain name in this field. Typically, you will specify the **Appliance Name** you specified in the **Appliance Configuration** dialog, and the **Management Domain Name** is a suffix.

17. Click **Next**. The **AWS Configuration** panel of the wizard appears.

FIGURE 89 AWS Configuration



AWS Configuration

Please enter the AWS credentials and select a valid AMI with an appliance version >= 9.0R3.

The public and private subnets should be part of the same availability zone.

Amazon Machine Image (AMI): ami-123456

VPC ID: vpc-123456

Region: US West (N. California)

Private Subnet Id: sub-123456 Public Subnet Id: sub-123456

Management Subnet ID: sub-123456

Key Pair Name: abcdef

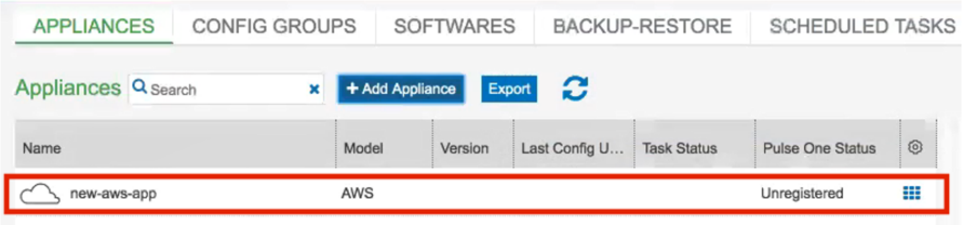
18. Specify the following properties:

- **Amazon Machine Image (AMI)** is the AMI ID that you identified in **"Identifying the EC2 Deployment Key and AMI ID" on page 62**.
- **VPC ID** is the value that you identified in **"Identifying the Required VPC ID and Subnet IDs" on page 60**.
- **Region** is automatically populated from your chosen region.
- **Private Subnet ID**, **Public Subnet ID**, and **Management Subnet ID** are the three subnet IDs that you identified in **"Identifying the Required VPC ID and Subnet IDs" on page 60**.
- **Deployment Key** is the key pair that you identified in **"Identifying the EC2 Deployment Key and AMI ID" on page 62**.

19. Click **Save**.

The wizard closes, and the new *Unregistered* AWS appliance is added to the list of appliances. For example:

FIGURE 90 New Unregistered Appliance



Name	Model	Version	Last Config U...	Task Status	Pulse One Status
new-aws-app	AWS				Unregistered

20. Click the **Actions** icon for the appliance and select **Start Appliance**.

21. The status of the new appliance goes through a series of states until it successfully created.

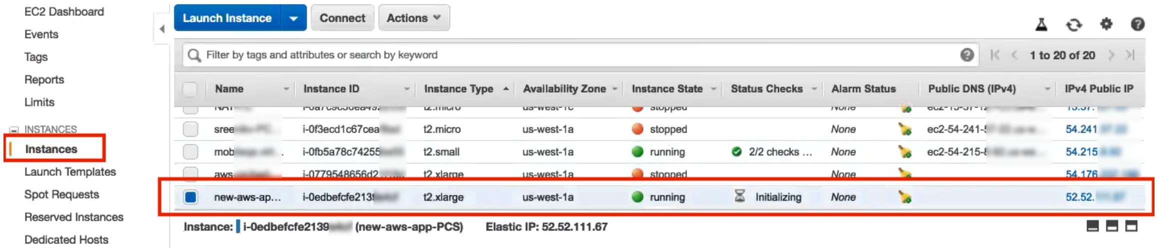
    - *Unregistered*
    - *Creating*
    - *Starting*
    - *Started*

22. Wait until the appliance is created.

23. Go to the **EC2 Dashboard** in AWS and view **Instances**.

24. The new appliance is listed and reports a **Status Check** of Initializing. For example:

FIGURE 91 AWS Initializing Appliance



Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)	IPv4 Public IP
sree[redacted]	i-0f3ecd1c67cea[redacted]	t2.micro	us-west-1a	stopped		None	ec2-54-241-[redacted]	54.241[redacted]
mob[redacted]	i-0fb5a78c74255[redacted]	t2.small	us-west-1a	running	2/2 checks ...	None	ec2-54-215-[redacted]	54.215[redacted]
aws[redacted]	i-0779548656d2[redacted]	t2.xlarge	us-west-1a	stopped		None		54.176[redacted]
new-aws-ap...	i-0edbefcfe2139[redacted]	t2.xlarge	us-west-1a	running	Initializing	None		52.52.[redacted]

Instance: i-0edbefcfe2139[redacted] (new-aws-app-PCS) Elastic IP: 52.52.111.67

Note: The appliance is auto-registered. That is, you do not need to manually complete the registration of the appliance from the appliance GUI.

The creation and registration of a PCS appliance as a virtual machine on AWS is now complete.

Configuring CPU, Memory and Disk Utilization

The **Appliances** tab displays all the added appliances. When you select an online appliance, a detailed panel shows the health of the appliance.

The panel shows the following status:

- CPU, memory and disk utilization.
- The number of concurrent users connected.
- The throughput of the appliance.
- The number of authentication failures.

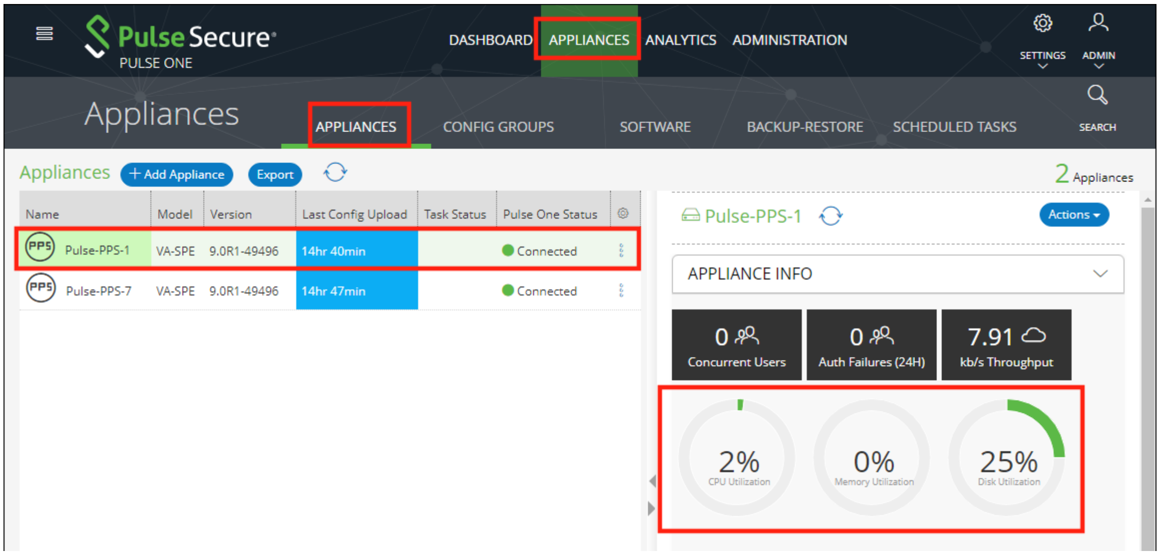
To view the health of an appliance:

1. Log into Pulse One as an administrator.
2. Click the **Appliances** menu and then the **Appliances** tab.

   The **Appliances** tab displays all current appliances.
3. Select an appliance whose **Pulse One Status** is *Connected*.

   The panel on the right gives a pictorial representation of the CPU, memory, and disk usage information. For example:

FIGURE 92 Appliance Health



Name	Model	Version	Last Config Upload	Task Status	Pulse One Status
Pulse-PPS-1	VA-SPE	9.0R1-49496	14hr 40min		Connected
Pulse-PPS-7	VA-SPE	9.0R1-49496	14hr 47min		Connected

Backing up and Restoring Appliance Configurations

Pulse One supports the backup and restore of the configuration of any managed appliance of v9.0R2 or later.

Each appliance can have a single configuration backup only.

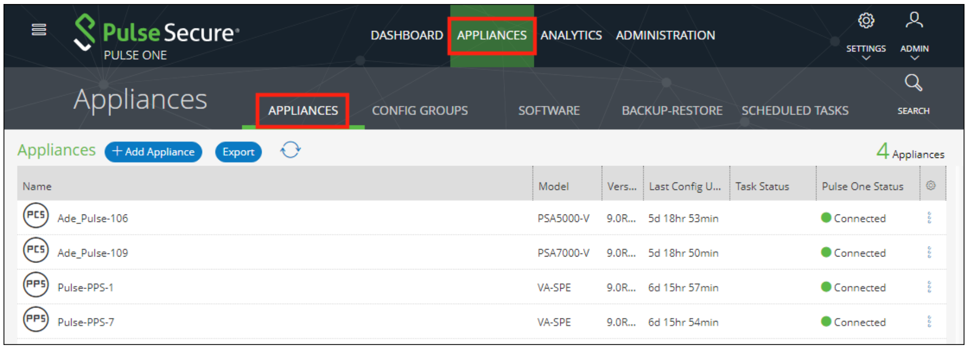
When a new backup for an appliance is started, the previous backup (if present) is deleted.

Backing up the Configuration of an Appliance

1. Log into Pulse One as an administrator.
2. Click the **Appliances** menu and then the **Appliances** tab.

   The **Appliances** tab displays all current appliances.

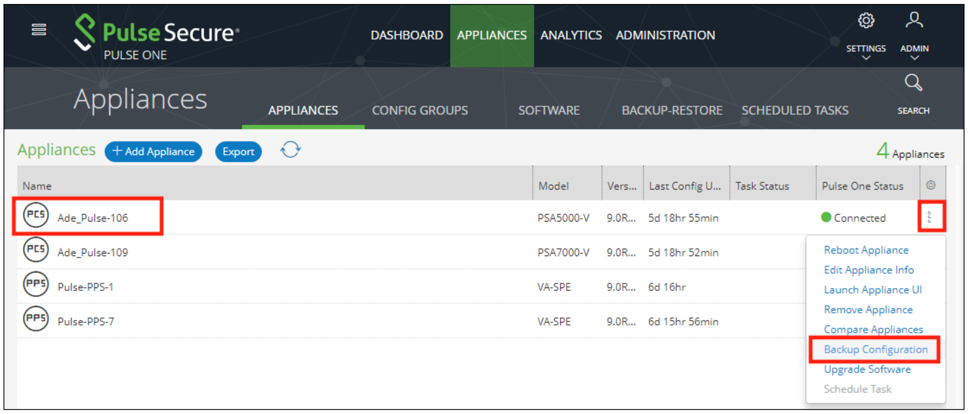
   FIGURE 93 Pulse One Appliances Tab



Name	Model	Vers...	Last Config U...	Task Status	Pulse One Status
PCS Ade_Pulse-106	PSA5000-V	9.0R...	5d 18hr 53min		Connected
PCS Ade_Pulse-109	PSA7000-V	9.0R...	5d 18hr 50min		Connected
PPS Pulse-PPS-1	VA-SPE	9.0R...	6d 15hr 57min		Connected
PPS Pulse-PPS-7	VA-SPE	9.0R...	6d 15hr 54min		Connected

3. Locate the appliance that you want to backup and click its **Actions** icon.

   FIGURE 94 Appliance Menu



Name	Model	Vers...	Last Config U...	Task Status	Pulse One Status
PCS Ade_Pulse-106	PSA5000-V	9.0R...	5d 18hr 55min		Connected
PCS Ade_Pulse-109	PSA7000-V	9.0R...	5d 18hr 52min		
PPS Pulse-PPS-1	VA-SPE	9.0R...	6d 16hr		
PPS Pulse-PPS-7	VA-SPE	9.0R...	6d 15hr 56min		

   In this example, the *pcs-174* appliance is at version 9.0R2. As a result, its menu includes the **Backup Configuration** option.

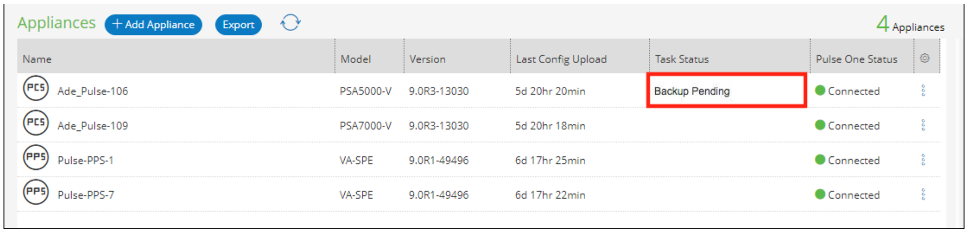
4. Click **Backup Configuration**.

   The **Backup Appliance** dialog appears.

5. Specify a **Description** for the configuration backup and click **Save**.

The configuration backup is initially marked as *Backup Pending* in the **Task Status** column.

FIGURE 95 Monitoring a Pending Backup



Name	Model	Version	Last Config Upload	Task Status	Pulse One Status
PCS Ade_Pulse-106	PSA5000-V	9.0R3-13030	5d 20hr 20min	Backup Pending	● Connected
PCS Ade_Pulse-109	PSA7000-V	9.0R3-13030	5d 20hr 18min		● Connected
PPS Pulse-PPS-1	VA-SPE	9.0R1-49496	6d 17hr 25min		● Connected
PPS Pulse-PPS-7	VA-SPE	9.0R1-49496	6d 17hr 22min		● Connected

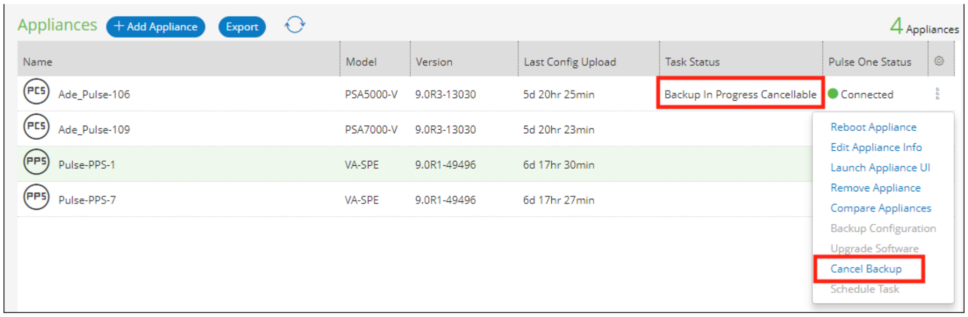
The **Task Status** changes to *Backup in Progress Cancellable* after the configuration backup starts.

After the configuration backup completes, the **Task Status** entry for the appliance is cleared.

6. (Optional) If required, you can cancel the configuration backup while it is in progress.

   To do this, click the **Actions** icon for the appliance, and then click **Cancel Backup**.

FIGURE 96 Canceling a Backup



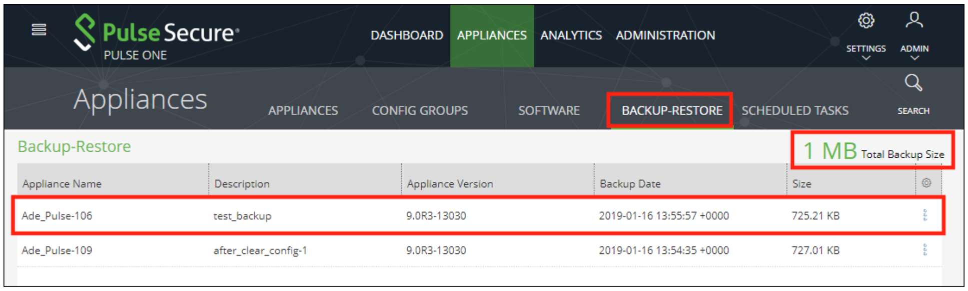
Name	Model	Version	Last Config Upload	Task Status	Pulse One Status
PCS Ade_Pulse-106	PSA5000-V	9.0R3-13030	5d 20hr 25min	Backup In Progress Cancellable	● Connected
PCS Ade_Pulse-109	PSA7000-V	9.0R3-13030	5d 20hr 23min		
PPS Pulse-PPS-1	VA-SPE	9.0R1-49496	6d 17hr 30min		
PPS Pulse-PPS-7	VA-SPE	9.0R1-49496	6d 17hr 27min		

The cancellation is then confirmed.

7. After the configuration backup completes, click the **Backup-Restore** tab.

   The **Backup-Restore** tab lists all configuration backups taken, plus a total size of all backups. For example:

FIGURE 97 Viewing Backup Files



Appliance Name	Description	Appliance Version	Backup Date	Size
Ade_Pulse-106	test_backup	9.0R3-13030	2019-01-16 13:55:57 +0000	725.21 KB
Ade_Pulse-109	after_clear_config-1	9.0R3-13030	2019-01-16 13:54:35 +0000	727.01 KB

In this example:

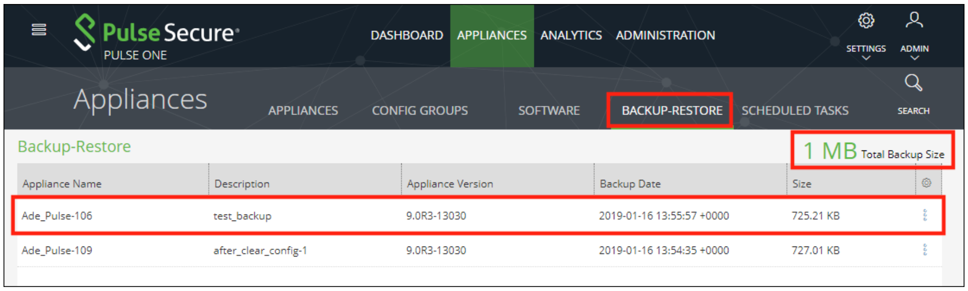
- The configuration backup for *Ade_Pulse-106* is at the top of the list.
- The total size of all backups is 1 MB.

Deleting the Configuration Backup for an Appliance

1. Log into Pulse One as an administrator.
2. Click the **Appliances** menu and then the **Backup-Restore** tab.

   The **Backup-Restore** tab lists all configuration backups taken. For example:

   FIGURE 98 Viewing Backup Files Before Delete

Appliance Name	Description	Appliance Version	Backup Date	Size
Ade_Pulse-106	test_backup	9.0R3-13030	2019-01-16 13:55:57 +0000	725.21 KB
Ade_Pulse-109	after_clear_config-1	9.0R3-13030	2019-01-16 13:54:35 +0000	727.01 KB

   In this example, the configuration backup for *Ade_Pulse-106* is at the top of the list.
3. Locate the configuration backup that you want to delete.
4. Click the **Actions** icon for the appliance, and then click **Delete Configuration**.

   A confirmation dialog appears.
5. Confirm the deletion.

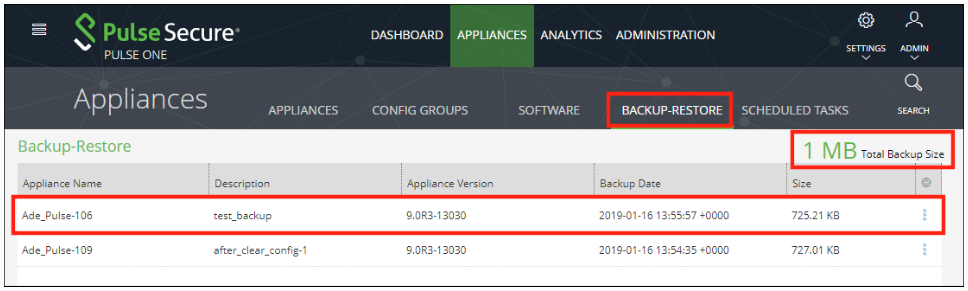
   The configuration backup is deleted and removed from the list of configuration backups.

Restoring the Configuration of an Appliance

1. Log into Pulse One as an administrator.
2. Click the **Appliances** menu and then the **Backup-Restore** tab.

   The **Backup-Restore** tab lists all configuration backups taken. For example:

   FIGURE 99 Viewing Backup Files

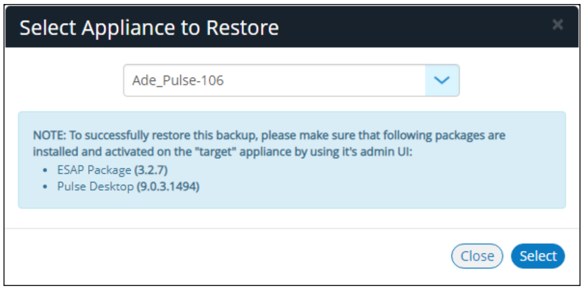
Appliance Name	Description	Appliance Version	Backup Date	Size
Ade_Pulse-106	test_backup	9.0R3-13030	2019-01-16 13:55:57 +0000	725.21 KB
Ade_Pulse-109	after_clear_config-1	9.0R3-13030	2019-01-16 13:54:35 +0000	727.01 KB

   In this example, the configuration backup for *pcs-174* is at the top of the list.

3. Locate the configuration backup that you want to restore.
4. Click the **Actions** icon for the appliance, and then click **Restore Configuration**.

   The **Select Appliance to Restore** dialog appears. This dialog lists all appliances for which there is a configuration backup file, and which are also in a connected state. For example:

   FIGURE 100 Selecting an Appliance

   Select Appliance to Restore

   Ade_Pulse-106

   NOTE: To successfully restore this backup, please make sure that following packages are installed and activated on the "target" appliance by using it's admin UI:
   - ESAP Package (3.2.7)
   - Pulse Desktop (9.0.3.1494)

   Note: This dialog also lists the ESAP Package version and the Pulse Desktop version that must be installed on the appliance manually before initiating the restore.

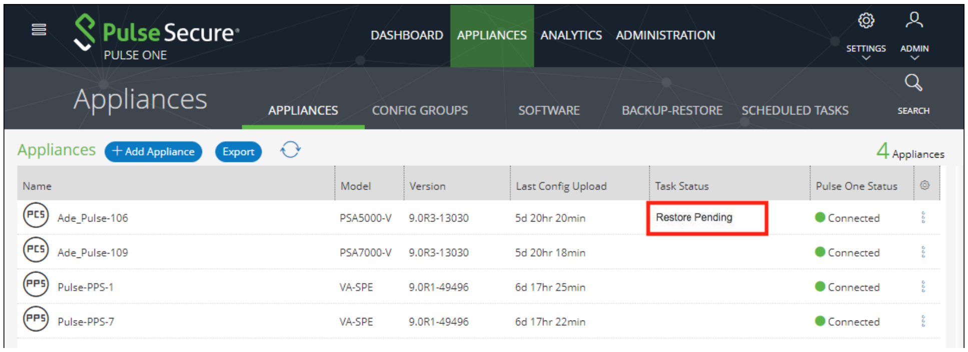
5. Select the required appliance and click **Select**.

   The configuration restore for the selected appliance is scheduled.

6. Click the **Appliances** tab.

   The **Task Status** for the selected appliance is shown as *Restore Pending*. For example:

   FIGURE 101 Monitoring a Configuration Restore for an Appliance

Name	Model	Version	Last Config Upload	Task Status	Pulse One Status
PCS Ade_Pulse-106	PSA5000-V	9.0R3-13030	5d 20hr 20min	Restore Pending	● Connected
PCS Ade_Pulse-109	PSA7000-V	9.0R3-13030	5d 20hr 18min		● Connected
PPS Pulse-PPS-1	VA-SPE	9.0R1-49496	6d 17hr 25min		● Connected
PPS Pulse-PPS-7	VA-SPE	9.0R1-49496	6d 17hr 22min		● Connected

   The **Task Status** changes to *Restore in Progress Not Cancellable* after the configuration restore starts.

   After the configuration restore completes, the **Task Status** for the appliance is cleared.

   Note: During a configuration restore of an appliance, you cannot schedule a backup. This restriction clears after the restore completes.

7. (Optional) While the **Task Status** for a selected appliance is *Restore Pending*, you can cancel the restore process. To do this, click the **Actions** icon for the appliance, and then click **Cancel Restore**.
8. (Optional) View the activities for an appliance to see the results of backup and restore operations, see **"Viewing the Activities Log for an Appliance" on page 112**.

Working with Appliance Groups

Two or more appliances can be collected into an appliance group to enable group operations:

- **"Creating an Appliance Group" on page 78**.
- **"Adding Appliances to an Appliance Group" on page 83**.
- **"Distributing a Master Configuration" on page 84**.

Creating an Appliance Group

An Appliance Group uses a single base configuration from a *master* appliance in Pulse One and applies that configuration to all the other *target* appliances in the group. This master appliance is always used to change the configuration settings for the group. You can add appliances to the group or remove appliances from the group at any time.

All appliances in a group must run the same firmware version and must be the same appliance type as the master. However, the appliance group may contain member appliances using any form factor.

Examples:

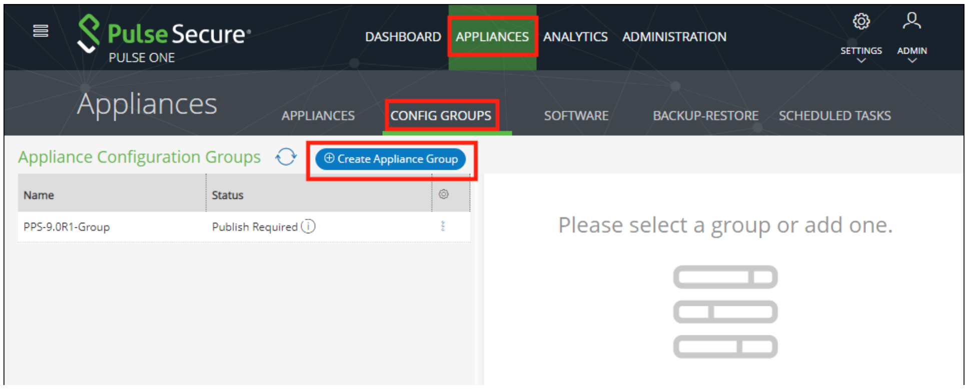
- If the master is a Pulse Connect Secure appliance running firmware version 8.2R5, all other appliances in the group must also be Pulse Connect Secure – either virtual appliances or hardware appliances (PSAs, MAGs, and SAs) - that also run firmware version 8.2R5.
- If the master is Pulse Policy Secure, all other appliances in the group must also be Pulse Policy Secure.

To create an appliance group:

1. Select the **Appliances** menu.
2. Select the **Config Groups** tab.

3. Click **Create Appliance Group**.

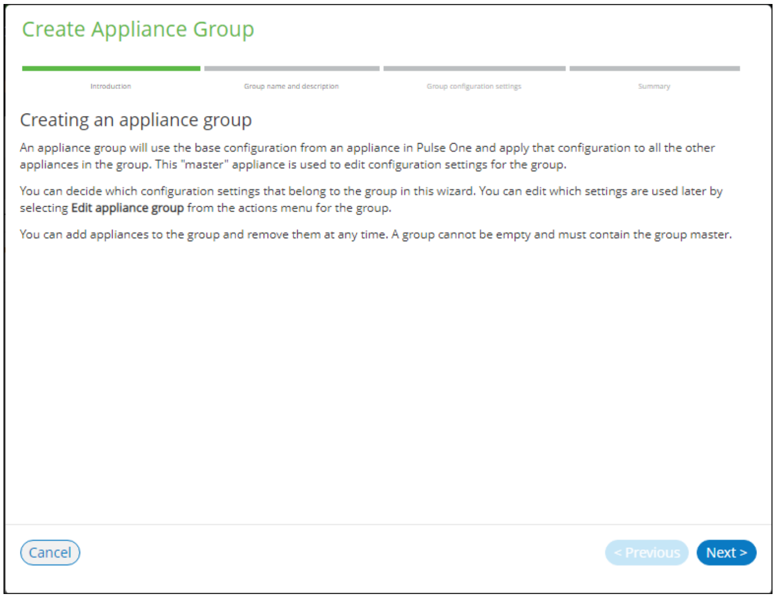
FIGURE 102 Create Appliance Group



Name	Status
PPS-9.0R1-Group	Publish Required ⓘ

The **Create Appliance Group Wizard** appears.

FIGURE 103 Create Appliance Group Wizard



Creating an appliance group

An appliance group will use the base configuration from an appliance in Pulse One and apply that configuration to all the other appliances in the group. This "master" appliance is used to edit configuration settings for the group.

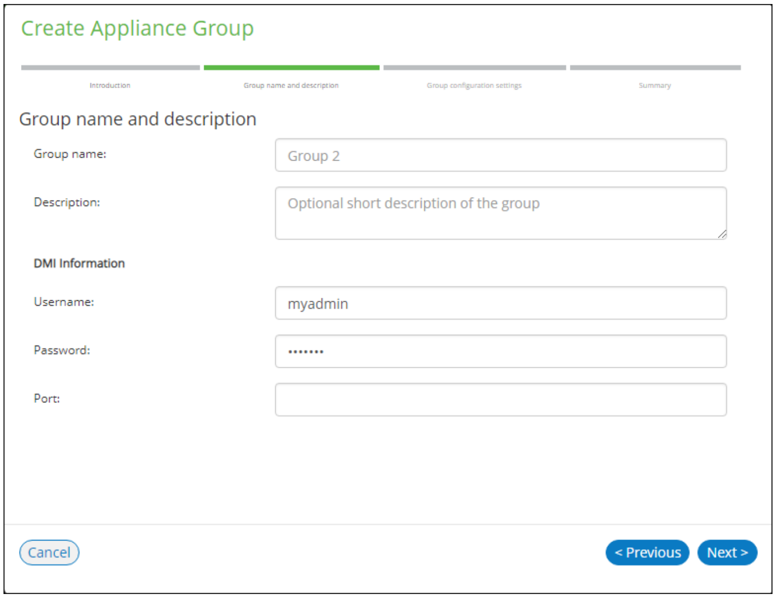
You can decide which configuration settings that belong to the group in this wizard. You can edit which settings are used later by selecting **Edit appliance group** from the actions menu for the group.

You can add appliances to the group and remove them at any time. A group cannot be empty and must contain the group master.

4. Click **Next**.

The **Group name and description** panel of the wizard appears.

FIGURE 104 Group Name and Description Wizard Panel



Create Appliance Group

Group name and description

Group name: Group 2

Description: Optional short description of the group

DMI Information

Username: myadmin

Password: •••••••

Port:

5. In this wizard panel:

    - Enter the **Group name** and a **Description**.

      Note: The **Group name** should be at least 3 characters and not more than 50 characters.

    - Enter a common admin **Username** and **Password** for all the appliances under this group, with which all appliances can receive DMI requests from Pulse One.

      Note: These credentials must be valid for all group members.

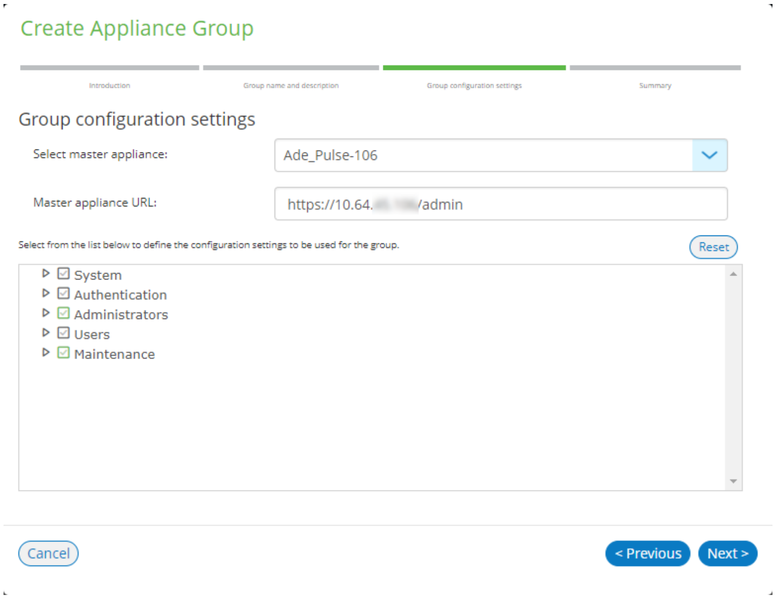
    - Specify a common **Port** number on which all appliances under this group will receive DMI requests. The default value is 830.

    For full details of appliance upgrades, see "Upgrading Managed Appliances" on page 89.

6. Click **Next**.

The **Group configuration settings** panel of the wizard appears.

FIGURE 105 Group Configuration Settings Wizard Panel



Create Appliance Group

Group configuration settings

Select master appliance: Ade_Pulse-106

Master appliance URL: https://10.64.[redacted]/admin

Select from the list below to define the configuration settings to be used for the group.

7. In this panel:

    - For **Select master appliance**, select an appliance to be the master appliance.

      Note: An appliance can be configured as master appliance in one or more groups.

    - Enter the **Master appliance URL**. This is the Internet-facing admin login URL. For example:

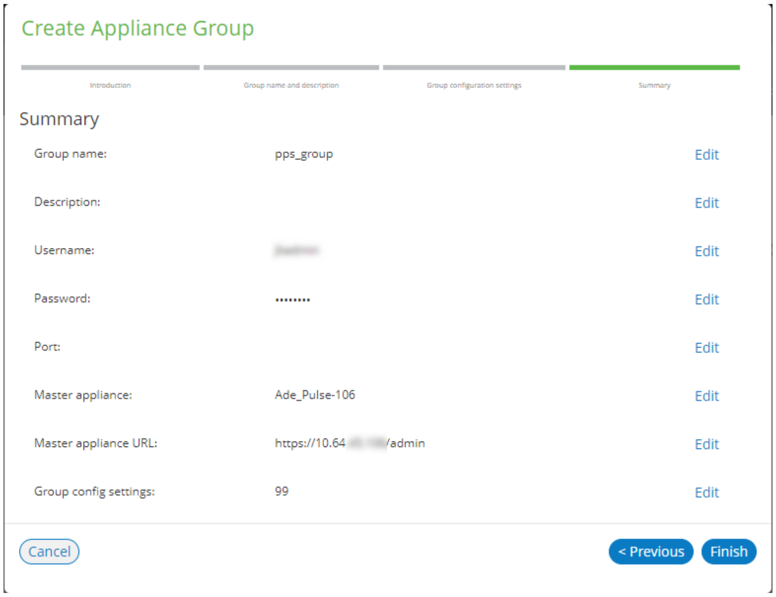
      ```
      https://<ip_address>/admin
      ```

    - Select the configuration settings that must be shared between all group members.

8. Click **Next**.

   The **Summary** panel of the wizard appears. For example:

   FIGURE 106 Summary Wizard Panel



Create Appliance Group

Summary

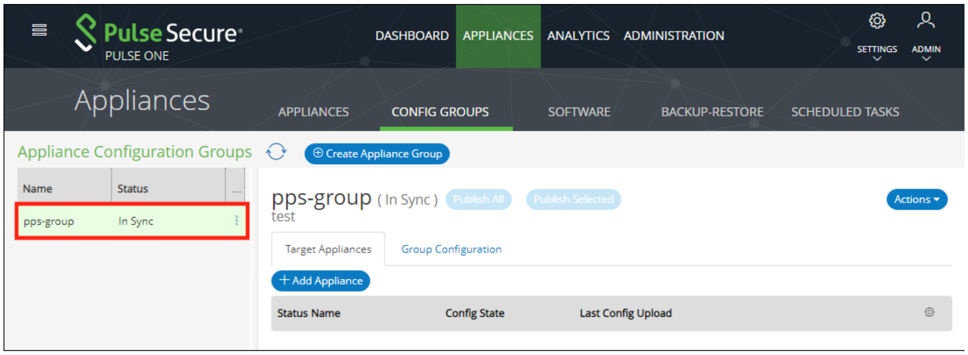
Group name:	pps_group	Edit
Description:		Edit
Username:	[redacted]	Edit
Password:	••••••••	Edit
Port:		Edit
Master appliance:	Ade_Pulse-106	Edit
Master appliance URL:	https://10.64[redacted]/admin	Edit
Group config settings:	99	Edit

9. (Optional) If you want to make any changes, click on the corresponding **Edit** link and make the changes.

10. Click **Finish**.

    The new appliance group is listed in the **Appliances** page. For example:

    FIGURE 107 New Appliance Group



Name	Status
pps-group	In Sync

Status Name	Config State	Last Config Upload

You can now add appliances to the group as target appliances, see **"Adding Appliances to an Appliance Group" on page 83**.

Adding Appliances to an Appliance Group

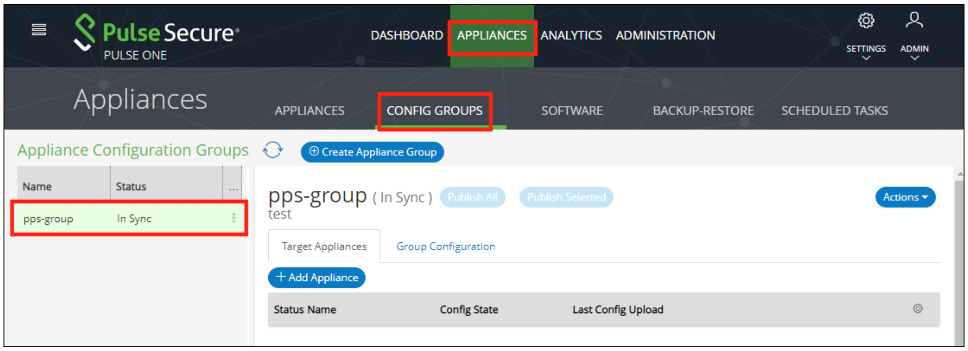
To add an appliance into an appliance group as a *target* appliance:

1. Select the **Appliances** menu.
2. Select the **Config Groups** tab.
3. Select the appliances group to which you want to add the appliance.

   The right-hand panel updates to show group details.

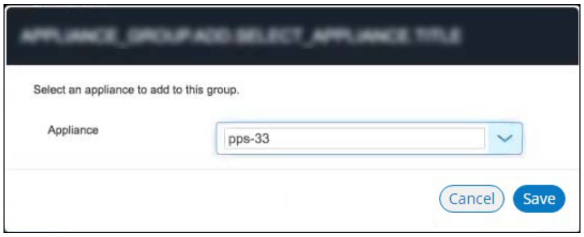
4. Select the **Target Appliances** tab. For example:

   FIGURE 108 Target Appliances Empty



5. Click **Add Appliance**. A dialog appears.

   FIGURE 109 Select Target Appliance


Select an appliance to add to this group.

Appliance: pps-33

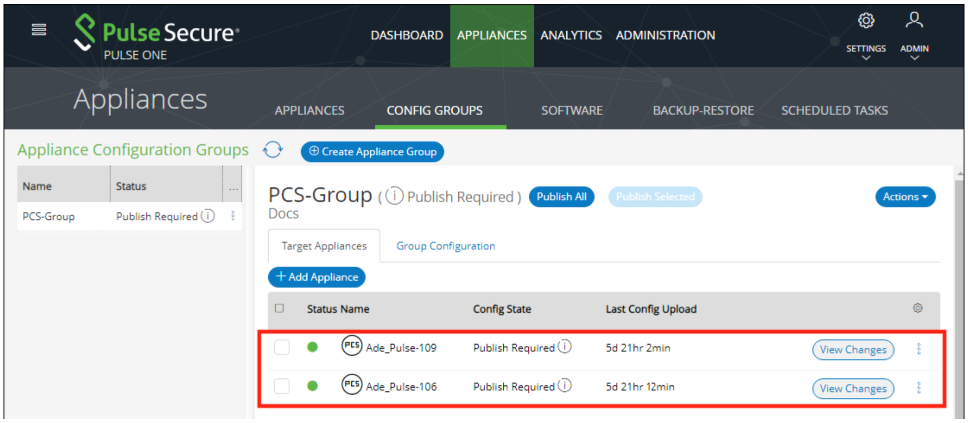
6. In this dialog, select an appliance to be added as a target appliance to the selected group.

   Note: Group configuration is only supported for appliances that are of same security appliance type and running the same software version.

7. Click **Save** to add the appliance to the group.

8. Repeat steps 5, 6 and 7 until the group contains all required target appliances. For example:

FIGURE 110 Target Appliances Added



Name	Status
PCS-Group	Publish Required

□	Status	Name	Config State	Last Config Upload	
□	●	Ade_Pulse-109	Publish Required	5d 21hr 2min	View Changes
□	●	Ade_Pulse-106	Publish Required	5d 21hr 12min	View Changes

Distributing a Master Configuration

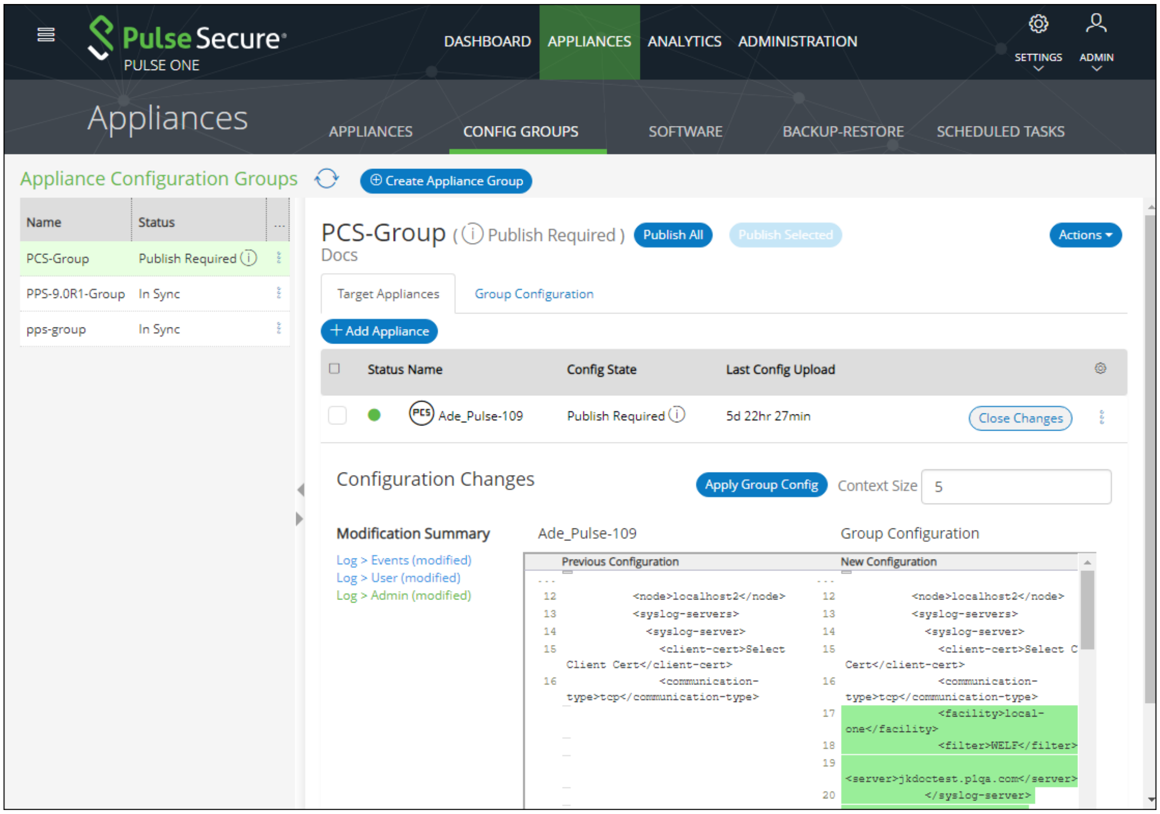
This section details the steps to distribute the configuration of the master appliance to all target appliances.

- "Viewing Configuration Changes" on page 84.
- "Publishing Configuration Changes Manually to Group Members" on page 85.
- "Publishing Configuration Changes to Group Members as a Scheduled Task" on page 87.

Viewing Configuration Changes

To view configuration changes between the master appliance and target appliances, click the **View Changes** button. The button changes to **Close Changes**. The configuration changes will be displayed on the same page.

FIGURE 111 View Configuration Changes



Name	Status
PCS-Group	Publish Required
PPS-9.0R1-Group	In Sync
pps-group	In Sync

PCS-Group (Publish Required)
Docs

	Status	Name	Config State	Last Config Upload
□	●	Ade_Pulse-109	Publish Required	5d 22hr 27min

Context Size: 5

Modification Summary

- Log > Events (modified)
- Log > User (modified)
- Log > Admin (modified)

Ade_Pulse-109 — Previous Configuration

```
...
            <node>localhost2</node>
            <syslog-servers>
              <syslog-server>
                <client-cert>Select
Client Cert</client-cert>
                <communication-
type>tcp</communication-type>
```

Group Configuration — New Configuration

```
...
            <node>localhost2</node>
            <syslog-servers>
              <syslog-server>
                <client-cert>Select C
Cert</client-cert>
                <communication-
type>tcp</communication-type>
                <facility>local-
one</facility>
                <filter>WELF</filter>

<server>jkdoctest.plqa.com</server>
              </syslog-server>
```

To close the configuration changes view, click **Close Changes**.

Publishing Configuration Changes Manually to Group Members

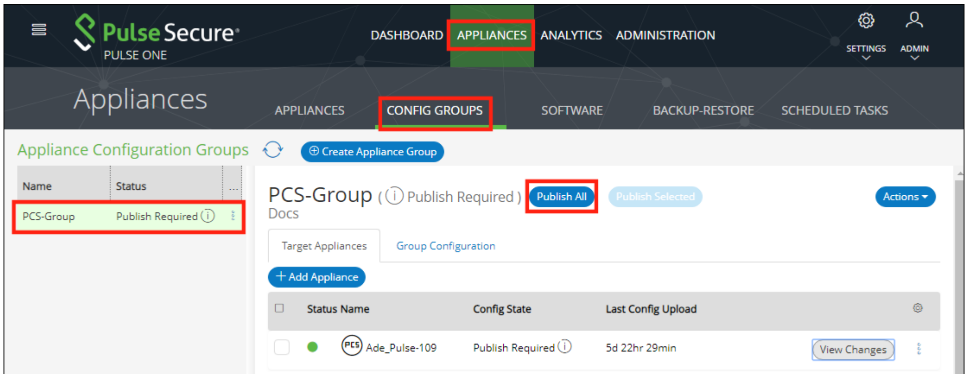
If the configuration of the master appliance differs from the configuration of the target appliances in its group, a *Publish Required* notification is displayed, and the **Publish All** button is enabled.

Note: Publishing to a group can also be performed as a scheduled task for groups. See **"Publishing Configuration Changes to Group Members as a Scheduled Task" on page 87**.

To manually publish a configuration to all appliances in a group:

1. Select the **Appliances** menu and then the **Config Groups** tab.
2. In the Appliance Group panel, click **Publish All**.

   FIGURE 112 Publish All

Name	Status
PCS-Group	Publish Required

Status	Name	Config State	Last Config Upload
●	Ade_Pulse-109	Publish Required	5d 22hr 29min

   The **Configuration Changes** view closes if it is open.

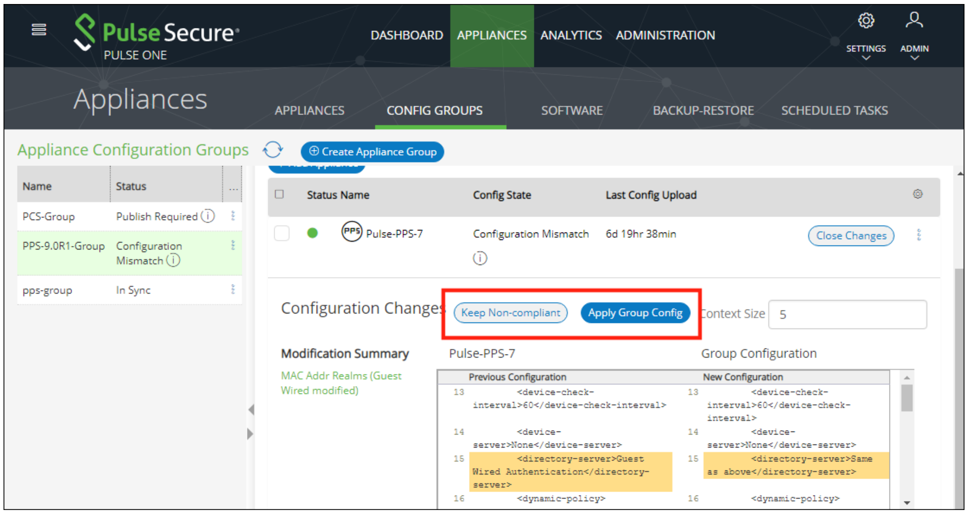
   A confirmation dialog appears.

3. In the confirmation dialog, click **Yes** to confirm the publication.

   Pulse One then publishes the master appliance configuration to the target appliances within the group.

4. To view configuration mismatch scenarios, click the **View Changes** button and then click the **Apply Group Config** button. The **Publish All** button will be disabled.

   FIGURE 113 Configuration Change in Member Appliance

Name	Status
PCS-Group	Publish Required
PPS-9.0R1-Group	Configuration Mismatch
pps-group	In Sync

Status	Name	Config State	Last Config Upload
●	Pulse-PPS-7	Configuration Mismatch	6d 19hr 38min

	Previous Configuration		New Configuration
13	`<device-check-interval>60</device-check-interval>`	13	`<device-check-interval>60</device-check-interval>`
14	`<device-server>None</device-server>`	14	`<device-server>None</device-server>`
15	`<directory-server>Guest Wired Authentication</directory-server>`	15	`<directory-server>Same as above</directory-server>`
16	`<dynamic-policy>`	16	`<dynamic-policy>`

   The **Configuration Changes** panel shows the changes in the member appliance configuration compared to the master configuration.

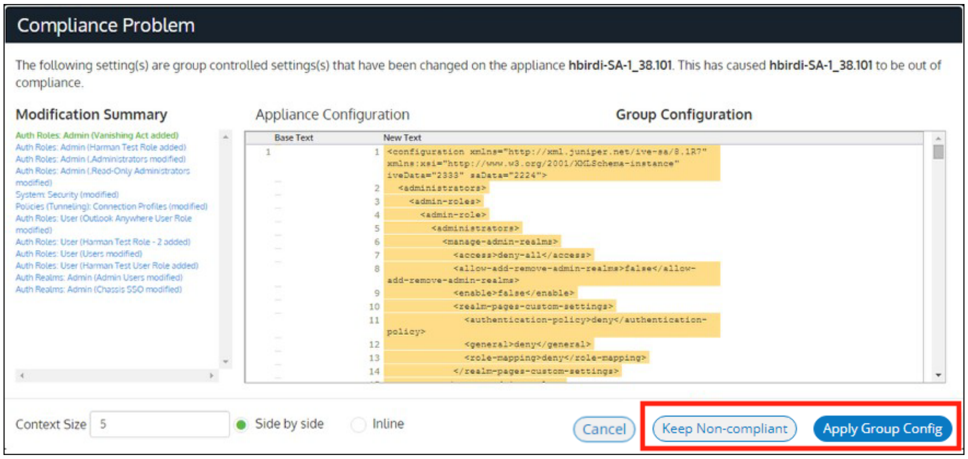
5. You can either:

    - Retain the changes by clicking **Keep Non-compliant**, OR
    - Apply the group configuration by clicking **Apply Group Config**.

    In either case, the compliance conflict is ignored, and the configuration will be published.

6. If you choose to remain non-compliant, then the *Configuration Mismatch* notification changes to a *Mismatch Ignored* notification, indicating that it is intentionally being kept out of compliance.

FIGURE 114 Configuration Mismatch



Compliance Problem

The following setting(s) are group controlled settings(s) that have been changed on the appliance **hbirdi-SA-1_38.101**. This has caused **hbirdi-SA-1_38.101** to be out of compliance.

Modification Summary

Auth Roles: Admin (Vanishing Act added)
Auth Roles: Admin (Harman Test Role added)
Auth Roles: Admin (.Administrators modified)
Auth Roles: Admin (.Read-Only Administrators modified)
System: Security (modified)
Policies (Tunneling): Connection Profiles (modified)
Auth Roles: User (Outlook Anywhere User Role modified)
Auth Roles: User (Harman Test Role - 2 added)
Auth Roles: User (Users modified)
Auth Roles: User (Harman Test User Role added)
Auth Realms: Admin (Admin Users modified)
Auth Realms: Admin (Chassis SSO modified)

Appliance Configuration | **Group Configuration**

```
<configuration xmlns="http://xml.juniper.net/ive-sa/8.1R7"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
iveData="2333" saData="2224">
  <administrators>
    <admin-roles>
      <admin-role>
        <administrators>
          <manage-admin-realms>
            <access>deny-all</access>
            <allow-add-remove-admin-realms>false</allow-
add-remove-admin-realms>
            <enable>false</enable>
            <realm-pages-custom-settings>
              <authentication-policy>deny</authentication-
policy>
              <general>deny</general>
              <role-mapping>deny</role-mapping>
            </realm-pages-custom-settings>
```

Context Size 5 ● Side by side ○ Inline

Publishing Configuration Changes to Group Members as a Scheduled Task

If the configuration of the master appliance differs from the configuration of the target appliances in its group, a *Publish Required* notification is displayed.

To publish configuration changes at a specific time, you can create a scheduled task to perform this action.

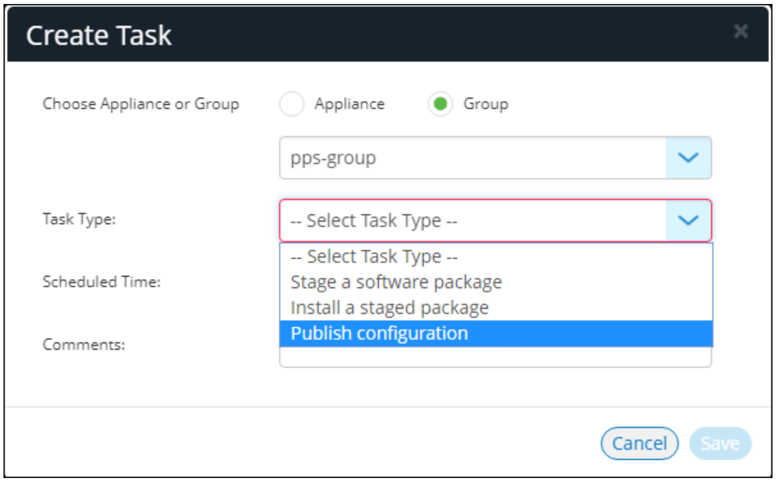
Note: Publishing configuration changes to an appliance group can also be performed manually, see **"Publishing Configuration Changes Manually to Group Members" on page 85**.

To publish configuration changes from a master appliance to all target appliances as a scheduled task:

1. Select the **Appliances** menu and then the **Config Groups** tab.
2. Click the **Actions** icon (⋮) for the appliance group you want to upgrade, and then click **Schedule Task**.

The **Create Task** dialog appears.

FIGURE 115 Create Publish Configuration Task



Create Task

Choose Appliance or Group ○ Appliance ● Group

pps-group

Task Type: -- Select Task Type --

Scheduled Time:

Comments:

3. In the **Create Task** dialog, for **Task Type**, select *Publish configuration*.

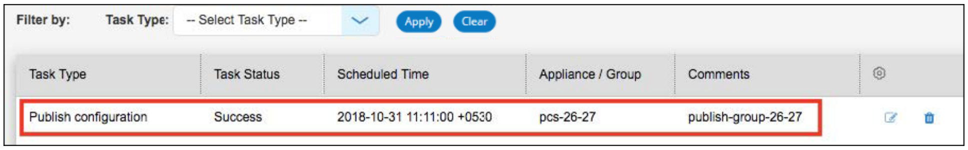
4. For **Scheduled Time**, select the required start time for the task.

5. (Optional) Add **Comments** as required. These appear on the **Scheduled Tasks** list.

6. Click **Save**.

   The new task is added to the list of scheduled tasks in the **Scheduled Tasks** tab.

FIGURE 116 Scheduled Publish Configuration Task



Filter by: Task Type: -- Select Task Type --

Task Type	Task Status	Scheduled Time	Appliance / Group	Comments
Publish configuration	Success	2018-10-31 11:11:00 +0530	pcs-26-27	publish-group-26-27

7. (Optional) You can edit the details for a scheduled task by clicking the **Edit** icon (✎) for the task.

8. (Optional) You can cancel a scheduled task by clicking the **Delete** icon for the task.

9. (Optional) You can monitor the progress of scheduled tasks using one of the following methods:

   - On the **Scheduled Tasks** tab. Here, the **Task Status** updates as a task starts and proceeds through to completion.
   - From the **Appliance Activities** panel. To access this, click the **Administration** tab, and then the **Appliance Activities** option.
   - From the **Config Group** tab, you can see status updates for the group as a whole.
   - From the **Appliances** tab, you can see status updates for each appliance group member.
   - From the **Activities** panel for an individual appliance on the right side of the **Appliances** tab.

Upgrading Managed Appliances

After an appliance is registered on Pulse One, several upgrade operations are supported. You can:

- Upload one or more appliance system software packages on Pulse One, see **"Uploading an Appliance Software Package to Pulse One" on page 90**.

  Note: You must ensure that each appliance has its DMI enabled and configured correctly, see **"Checking DMI Settings" on page 93**.

- Upload one or more ESAP packages on Pulse One, see **"Uploading an Endpoint Security Assessment Plug-In Package" on page 106**.

  Note: An ESAP package is included in every system software package. However, Pulse Secure releases ESAP upgrade packages more frequently than system software versions. You may choose to upgrade the ESAP package more regularly than system software.

- Upgrade a single appliance, see **"Upgrading Software on an Appliance" on page 94**.
- Upgrade all appliances in an appliance group, see **"Upgrading Software on all Target Appliances in a Group" on page 96**.
- Upgrade both appliances in a cluster, see **"Upgrading Software on all Appliances in a Cluster" on page 98**.
- Schedule the upgrade of an appliance in two stages:
  - First, schedule the upload of an image to a staging area on an appliance.
  - Second, schedule the installation of a staged software package on an appliance.

  For details, see **"Scheduling Upgrade-Related Tasks" on page 99**.

Uploading an Appliance Software Package to Pulse One

Before you can perform any software upgrade operations on PPS/PCS appliances, you must upload one or more appliance software packages to Pulse One.

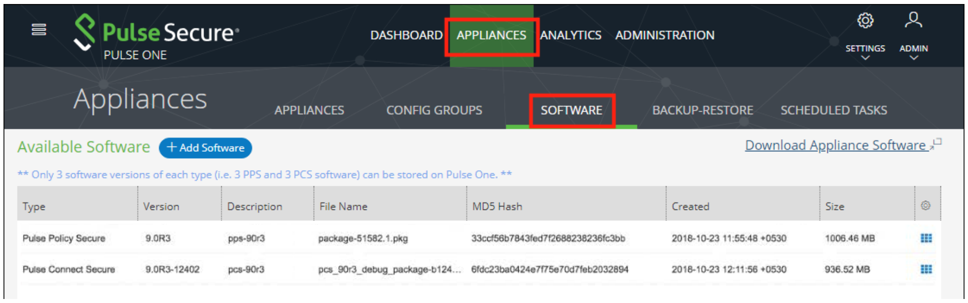
You can upload up to three PPS appliance software packages and up to three PCS software packages.

To upload an appliance software package:

1. Log into Pulse One as an administrator.
2. Click the **Appliances** menu and then the **Software** tab.

   The **Software** tab lists all **Available Software** packages present on Pulse One. For example:

   FIGURE 117 Available Software

   ** Only 3 software versions of each type (i.e. 3 PPS and 3 PCS software) can be stored on Pulse One. **

Type	Version	Description	File Name	MD5 Hash	Created	Size	⚙
Pulse Policy Secure	9.0R3	pps-90r3	package-51582.1.pkg	33ccf56b7843fed7f2688238236fc3bb	2018-10-23 11:55:48 +0530	1006.46 MB	▦
Pulse Connect Secure	9.0R3-12402	pcs-90r3	pcs_90r3_debug_package-b124...	6fdc23ba0424e7f75e70d7feb2032894	2018-10-23 12:11:56 +0530	936.52 MB	▦

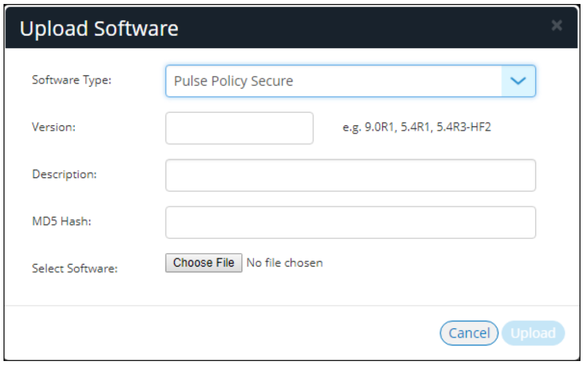
3. (Optional) If you do not have the required software images, click **Download Appliance Software** and download them from Pulse Support.

   Note: Any software package downloaded from the Pulse Support site should be available in local storage (not in Pulse One). It is the responsibility of the admin to upload packages to Pulse One.

4. Click **Add Software**.

The **Upload Software** dialog appears.

FIGURE 118 Upload Software


Upload Software

Software Type: Pulse Policy Secure

Version: e.g. 9.0R1, 5.4R1, 5.4R3-HF2

Description:

MD5 Hash:

Select Software: Choose File No file chosen

5. In the **Upload Software** dialog:

    - For **Software Type**, select whether your software package is for *Pulse Policy Secure* or *Pulse Connect Secure*.
    - Enter a **Version** number and a **Description** for the software package.

      Note: The version number is case sensitive and should use capital letters.

    - Enter the **MD5 Hash** value for the software package.

      You can get the MD5 value from the Pulse Support site. Alternatively, log into any LINUX machine where the file is downloaded, locate the software package file, and run the **md5<package_file_name>** command from the command line.

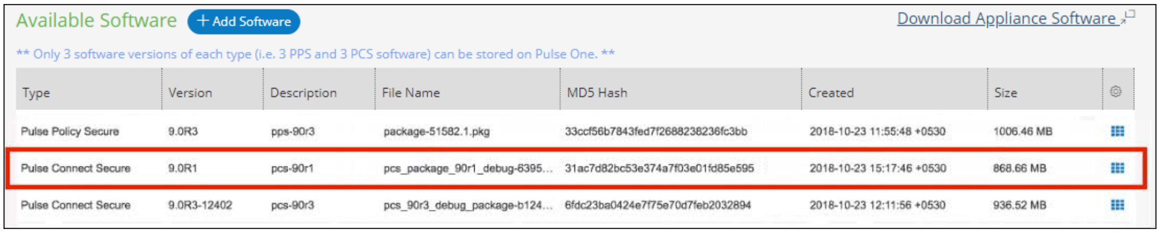
    - For **Select Software**, click **Browse** and locate the software package file.

6. Click **Upload**.

   The upload may take several minutes.

   After the upload completes, the new package is added to the **Available Software** list. For example:

FIGURE 119 Appliance Software Package Added


Available Software

** Only 3 software versions of each type (i.e. 3 PPS and 3 PCS software) can be stored on Pulse One. **

Type	Version	Description	File Name	MD5 Hash	Created	Size	⚙
Pulse Policy Secure	9.0R3	pps-90r3	package-51582.1.pkg	33ccf56b7843fed7f2688238236fc3bb	2018-10-23 11:55:48 +0530	1006.46 MB	▦
Pulse Connect Secure	9.0R1	pcs-90r1	pcs_package_90r1_debug-6395...	31ac7d82bc53e374a7f03e01fd85e595	2018-10-23 15:17:46 +0530	868.66 MB	▦
Pulse Connect Secure	9.0R3-12402	pcs-90r3	pcs_90r3_debug_package-b124...	6fdc23ba0424e7f75e70d7feb2032894	2018-10-23 12:11:56 +0530	936.52 MB	▦

7. (Optional) If required, you can edit the details for an uploaded software package.

   To do this, click the **Actions** icon for the software package, and then click **Edit Software**.

8. (Optional) If required, you can delete an uploaded software package.

To do this, click the **Actions** icon for the software package, and then click **Delete Software**.

You can now perform one or more appliance software upgrades.

Checking DMI Settings

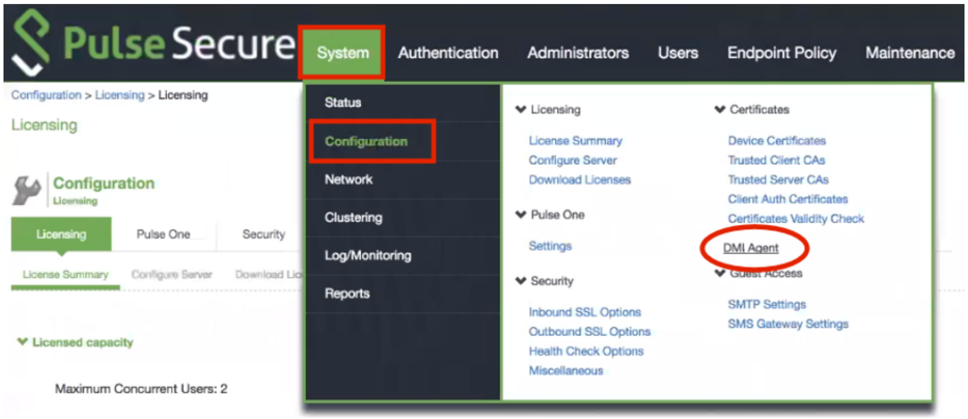
Before you can upgrade an appliance from Pulse One, you must ensure that the appliance has Device Management Interface (DMI) enabled and configured correctly.

To check DMI settings:

1. Log into the appliance as an administrator.
2. Access the DMI Agent settings for the appliance.

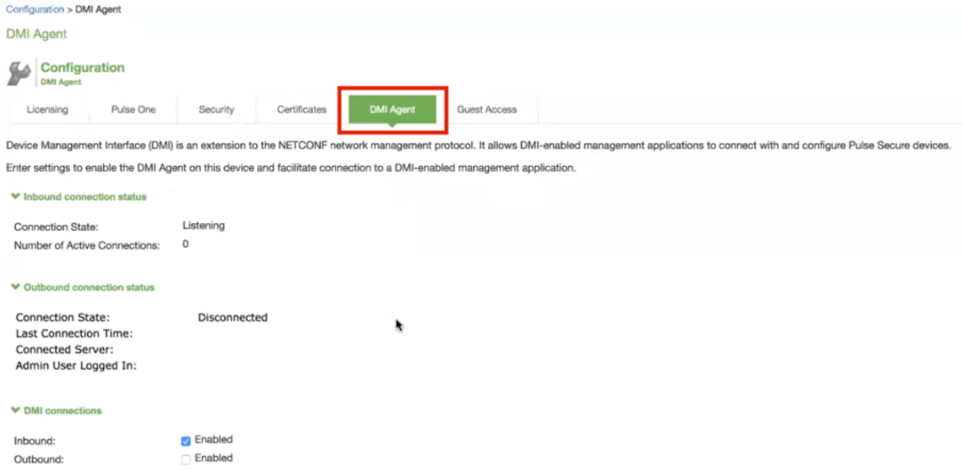
   For example, on Pulse Policy Secure, click the **System** menu, then **Configuration > DMI Agent**.

   FIGURE 120 Accessing Pulse Policy Secure DMI Agent Settings

3. The **DMI Agent** settings appear. For example, on Pulse Policy Secure:

   FIGURE 121 Pulse Policy Secure DMI Agent Settings

   Device Management Interface (DMI) is an extension to the NETCONF network management protocol. It allows DMI-enabled management applications to connect with and configure Pulse Secure devices.

   Enter settings to enable the DMI Agent on this device and facilitate connection to a DMI-enabled management application.

   Inbound connection status

   Connection State: Listening
   Number of Active Connections: 0

   Outbound connection status

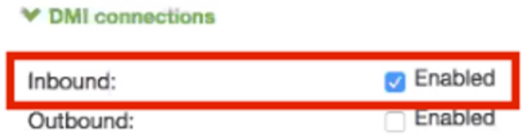
   Connection State: Disconnected
   Last Connection Time:
   Connected Server:
   Admin User Logged In:

   DMI connections

   Inbound: ☑ Enabled
   Outbound: ☐ Enabled

4. Ensure that inbound DMI connections are enabled. For example, on Pulse Policy Secure:

FIGURE 122 Pulse Policy Secure DMI Agent Settings



DMI connections

Inbound: ☑ Enabled

Outbound: □ Enabled

5. Ensure that inbound DMI connections are received on the correct port type and port number.

   To do this, you need the DMI settings that you used when you registered the appliance, see **"Registering an Existing PCS/PPS Appliance" on page 33**. Specifically, you need the choice of whether to perform DMI over the internal port or the management port.

   - For the **Accept connections on** setting, select the required interface type. That is, either the *Internal Port* or the *Management Port*.
   - The **TCP port** number. The default is *830*.

6. The DMI settings on the appliance are now configured correctly for software upgrades from Pulse One.

Upgrading Software on an Appliance

You can perform an immediate software upgrade on any registered appliance.

Note: Alternatively, you can schedule one or more upgrade processes for a later time, see **"Scheduling Upgrade-Related Tasks" on page 99**.

Before you can perform an immediate software upgrade on an appliance, you must upload the required appliance software package, see **"Uploading an Appliance Software Package to Pulse One" on page 90**.

Note: The appliance will continue to operate while it uploads the software package, but it will then reboot. The appliance will be offline until the upgrade completes. After the appliance is online again the upgrade is complete, but it may take several more minutes for the appliance to reconnect to Pulse One.

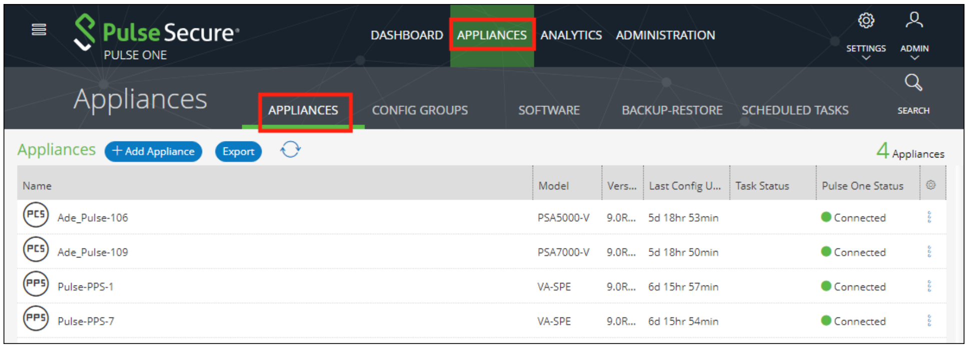
To perform a software upgrade for an appliance:

1. Log into Pulse One as an administrator.
2. Click the **Appliances** menu and then the **Appliances** tab.

   The **Appliances** tab lists all appliances on Pulse One.

For example:

FIGURE 123 Available Appliances

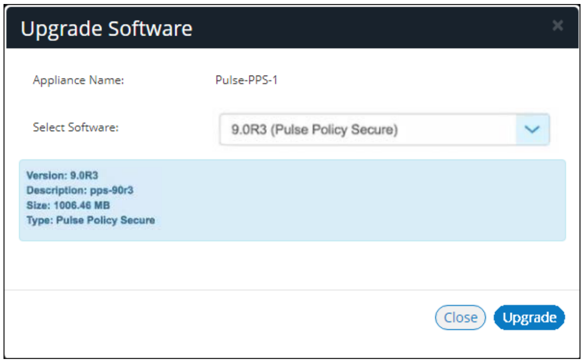


Name	Model	Vers...	Last Config U...	Task Status	Pulse One Status
PCS Ade_Pulse-106	PSA5000-V	9.0R...	5d 18hr 53min		● Connected
PCS Ade_Pulse-109	PSA7000-V	9.0R...	5d 18hr 50min		● Connected
PPS Pulse-PPS-1	VA-SPE	9.0R...	6d 15hr 57min		● Connected
PPS Pulse-PPS-7	VA-SPE	9.0R...	6d 15hr 54min		● Connected

3. Click the **Actions** icon for the appliance you want to upgrade, and then click **Upgrade Software**.

   The **Upgrade Software** dialog appears. For example:

FIGURE 124 Upgrade Software



Appliance Name: Pulse-PPS-1

Select Software: 9.0R3 (Pulse Policy Secure)

Version: 9.0R3
Description: pps-90r3
Size: 1006.46 MB
Type: Pulse Policy Secure

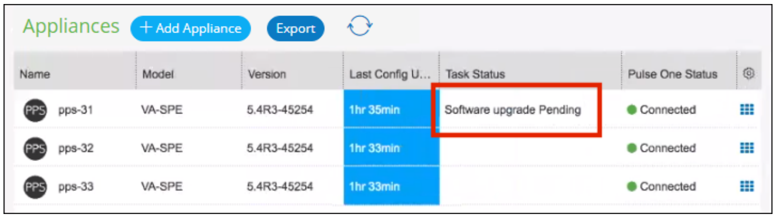
4. For **Select Software**, choose the required software package for the upgrade.

   Full details for the selected package are displayed.

5. To start the upgrade, click **Upgrade**.

   The **Task Status** of the appliance updates to show that the upgrade of the appliance is pending. For example:

FIGURE 125 Upgrade Pending



Name	Model	Version	Last Config U...	Task Status	Pulse One Status
PPS pps-31	VA-SPE	5.4R3-45254	1hr 35min	Software upgrade Pending	● Connected
PPS pps-32	VA-SPE	5.4R3-45254	1hr 33min		● Connected
PPS pps-33	VA-SPE	5.4R3-45254	1hr 33min		● Connected

The **Task Status** changes as the process continues.

Note: The entire upgrade process may take up to an hour.

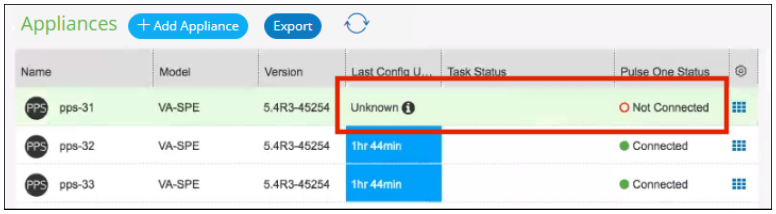
Note: All appliance configuration is preserved during this process.

- After the software update begins, the appliance uploads the specified software package. At this point, the appliance is still operational.

  Note: Do not log into an appliance during an upgrade using the credentials used for DMI. This may cause the upgrade to fail.

- After the software package upload is complete, the appliance reboots to complete the upgrade, and the connection between Pulse One and the appliance is lost. For example:

  FIGURE 126 Appliance Rebooting



Name	Model	Version	Last Config U...	Task Status	Pulse One Status
PPS pps-31	VA-SPE	5.4R3-45254	Unknown		○ Not Connected
PPS pps-32	VA-SPE	5.4R3-45254	1hr 44min		● Connected
PPS pps-33	VA-SPE	5.4R3-45254	1hr 44min		● Connected

- After the appliance reboots, the upgrade is complete, but it may take several minutes to reconnect to the appliance from Pulse One.

Upgrading Software on all Target Appliances in a Group

You can perform an immediate software upgrade on the master appliance in an appliance group.

The target appliances in the group are upgraded automatically.

Note: Alternatively, you can schedule one or more upgrade tasks for the master appliance at a later time, see “Scheduling a Full Upgrade of an Appliance Group” on page 104.

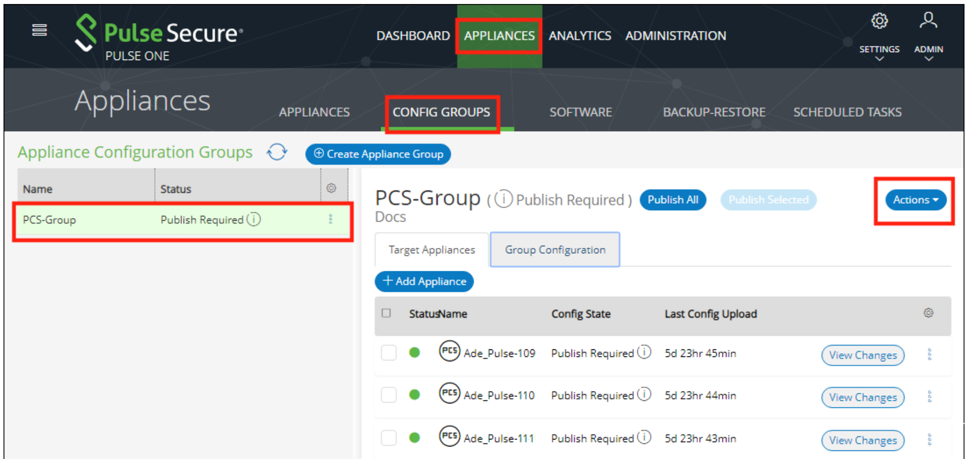
To upgrade all members of an appliance group:

1. Log into Pulse One as an administrator.
2. Click the **Appliances** menu and then the **Config Groups** tab.

   The **Appliance Configuration Groups** tab lists all appliance groups on Pulse One.

For example:

FIGURE 127 Available Appliance Groups



Name	Status
PCS-Group	Publish Required

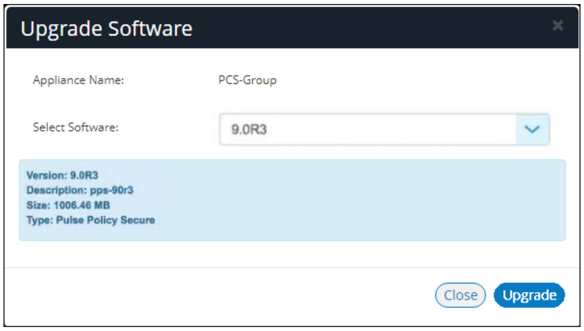
PCS-Group (Publish Required)
Docs

Status	Name	Config State	Last Config Upload
●	Ade_Pulse-109	Publish Required	5d 23hr 45min
●	Ade_Pulse-110	Publish Required	5d 23hr 44min
●	Ade_Pulse-111	Publish Required	5d 23hr 43min

3. Click the **Actions** button for the appliance group you want to upgrade, and then click **Upgrade Software**.

   The **Upgrade Software** dialog appears. For example:

FIGURE 128 Appliance Group Upgrade Software



Appliance Name: PCS-Group

Select Software: 9.0R3

Version: 9.0R3
Description: pps-90r3
Size: 1006.46 MB
Type: Pulse Policy Secure

4. For **Select Software**, choose the required software package for the upgrade.

   Full details for the selected package are displayed.

5. To start the upgrade, click **Upgrade**.

6. Click the **Appliances** tab.

   The **Task Status** of each appliance updates to show that the upgrade of the appliance is pending.

   The **Task Status** of each appliance changes as the process continues.

   Note: The entire upgrade process for an appliance may take up to an hour.

   Note: All appliance configuration is preserved during this process.

   - After an appliance software update begins, the appliance uploads the specified software package. At this point, the appliance is still operational.

     Note: Do not log into an appliance during an upgrade using the credentials used for DMI. This may cause the upgrade to fail.

   - After the software package upload to an appliance is complete, the appliance reboots to complete the upgrade, and the connection between Pulse One and the appliance is lost.

   - After the appliance reboots, the upgrade of the appliance is complete, but it may take several minutes to reconnect to the appliance from Pulse One.

   After all members of the group (master and target appliances) have been upgraded, the upgrade of the group is complete.

Upgrading Software on all Appliances in a Cluster

Upgrading all appliances in a cluster is similar to the upgrade of a single appliance, see **"Upgrading Software on an Appliance" on page 94**.

You can perform an immediate software upgrade on one of the appliances in a cluster, as follows:

- For *Active/Active* clusters, you can only upgrade the *Leader node*. All other nodes upgrade automatically.
- For *Active/Passive* clusters, you can only upgrade the Passive node. The Active node upgrades automatically.

In both cases, all nodes will be offline for some time during the upgrade.

Note: Alternatively, you can schedule the upgrade processes for a later time, see **"Scheduling Upgrade-Related Tasks" on page 99**.

Scheduling Upgrade-Related Tasks

You can schedule upgrade-related tasks so that they are performed automatically at specified times.

There are three types of scheduled task:

1. The publication of configuration changes from a master appliance to all group members.

   Note: This scheduled task type is only supported for appliance groups. It is not a requirement to publish all configuration changes before performing an upgrade, but you can optionally publish your configuration as part of your workflow if required.

2. The upload of a software package to a staging area on an appliance.

   No installation is performed, and there is no loss of service.

3. The upgrade of an appliance based on a pre-staged software package.

   There is a loss of service during the upgrade as the appliance must be rebooted.

To perform a full upgrade on an appliance or an appliance group, you must perform both task types.

The scheduling of these tasks can be suited to your network requirements.

The scheduling of tasks is supported for:

- Single appliances.
- Appliance groups. You schedule the tasks against the group, and all group members will automatically perform the designated task.
- Appliance clusters:
  - For *Active/Active* clusters, you can only schedule tasks for the *Leader node*. After both the upload and the installation tasks are complete, all other nodes upgrade automatically.
  - For *Active/Passive* clusters, you can only upgrade the Passive node. After both the upload and the installation tasks are complete, the Active node upgrades automatically.

You can initiate appliance upgrades using scheduled tasks as follows:

- **“Scheduling a Full Upgrade from the Scheduled Tasks Tab” on page 100**.
- **“Scheduling a Full Upgrade from the Appliances Tab” on page 102**.
- **“Scheduling a Full Upgrade of an Appliance Group” on page 104**.

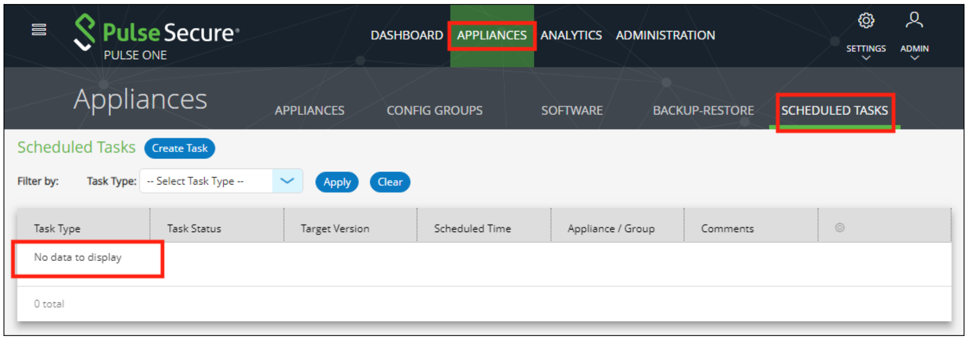
Scheduling a Full Upgrade from the Scheduled Tasks Tab

To schedule an upgrade of an individual appliance using a pair of tasks from the **Scheduled Tasks** tab:

1. Log into Pulse One as an administrator.
2. Click the **Appliances** menu and then the **Scheduled Tasks** tab.

   The **Scheduled Tasks** tab lists all scheduled tasks on Pulse One. For example:

   FIGURE 129 Scheduled Tasks

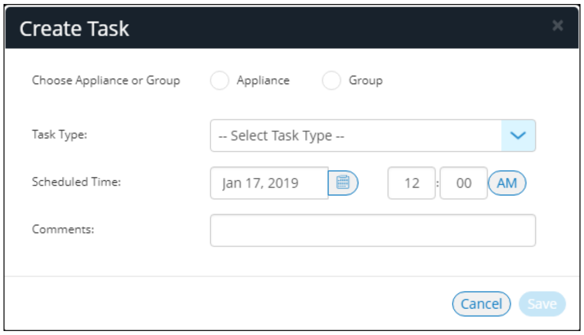
Task Type	Task Status	Target Version	Scheduled Time	Appliance / Group	Comments
No data to display					

   0 total

3. Click **Create Task**.

   The **Create Task** dialog appears.

   FIGURE 130 Create Task

   Choose Appliance or Group ○ Appliance ○ Group

   Task Type: -- Select Task Type --

   Scheduled Time: Jan 17, 2019 12 : 00 AM

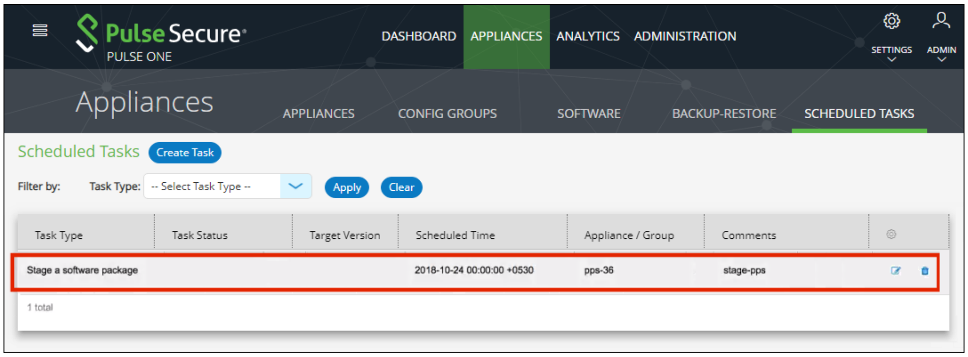
   Comments:

4. In the **Create Task** dialog:
   - For **Choose Appliance or Group**, select either *Appliance* or *Group*. An additional property appears, from which your select the required appliance or group.
   - For **Task Type**, select *Stage a software package*.
   - For **Target Version**, select the required software upgrade package.
   - For **Scheduled Time**, select the start time for the task.
   - (Optional) Add **Comments** as required. These appear on the **Scheduled Tasks** list.

5. Click **Save**.

   The new task is added to the list of **Scheduled Tasks**. For example:

   FIGURE 131 Scheduled Staging Task Added



Task Type	Task Status	Target Version	Scheduled Time	Appliance / Group	Comments
Stage a software package			2018-10-24 00:00:00 +0530	pps-36	stage-pps

1 total

6. To add the second task, click **Create Task** again.

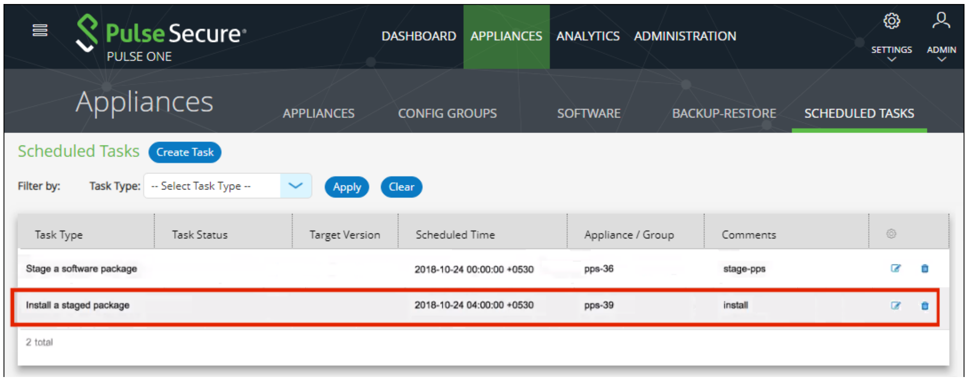
7. In the **Create Task** dialog:

   - For **Choose Appliance or Group**, select the same setting as for the first task, and select the same appliance or group.
   - For **Task Type**, select *Install a staged package*.
   - For **Target Version**, select the same package as for the first task.
   - For **Scheduled Time**, select the start time for the task. This must allow sufficient time for the first task to complete.
   - (Optional) Add **Comments** as required. These appear on the **Scheduled Task** list.

8. Click **Save**.

   The new task is added to the list of **Scheduled Tasks**. For example:

   FIGURE 132 Scheduled Install Task Added



Task Type	Task Status	Target Version	Scheduled Time	Appliance / Group	Comments
Stage a software package			2018-10-24 00:00:00 +0530	pps-36	stage-pps
Install a staged package			2018-10-24 04:00:00 +0530	pps-39	install

2 total

9. (Optional) You can edit the details for a scheduled task by clicking the **Edit** icon for the task.

10. (Optional) You can cancel a scheduled task by clicking the **Delete** icon for the task.
11. (Optional) You can monitor the progress of scheduled tasks using one of the following methods:
    - On the **Scheduled Tasks** tab. Here, the **Task Status** updates as a task starts and proceeds through to completion.
    - From the **Appliance Activities** panel. To access this, click the **Administration** tab, and then the **Appliance Activities** option.
    - From the **Appliances** tab, you can see status updates for individual appliances.
    - From the **Activities** panel for an appliance on the right side of the **Appliances** tab.

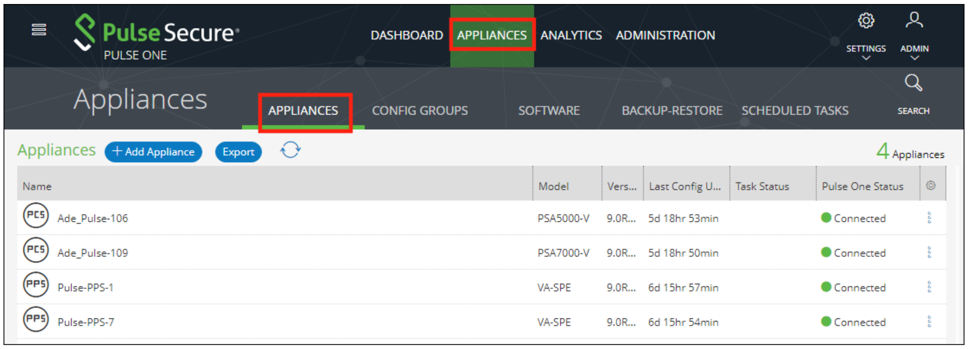
Scheduling a Full Upgrade from the Appliances Tab

To schedule an upgrade of an individual appliance using a pair of scheduled tasks from the **Appliances** tab:

1. Log into Pulse One as an administrator.
2. Click the **Appliances** menu and then the **Appliances** tab.

   The **Appliances** tab lists all appliances on Pulse One. For example:

   FIGURE 133 List of Appliances



Name	Model	Vers...	Last Config U...	Task Status	Pulse One Status
PCS Ade_Pulse-106	PSA5000-V	9.0R...	5d 18hr 53min		● Connected
PCS Ade_Pulse-109	PSA7000-V	9.0R...	5d 18hr 50min		● Connected
PPS Pulse-PPS-1	VA-SPE	9.0R...	6d 15hr 57min		● Connected
PPS Pulse-PPS-7	VA-SPE	9.0R...	6d 15hr 54min		● Connected

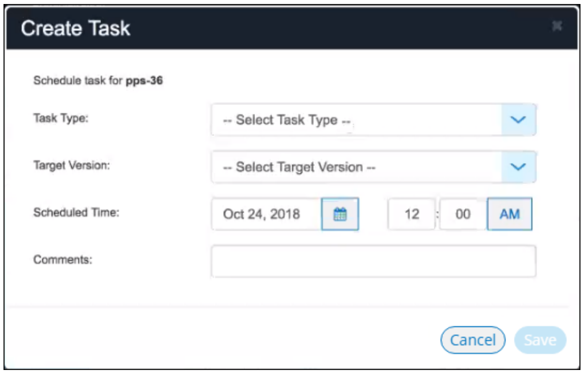
3. Click the **Actions** icon for the appliance you want to upgrade, and then click **Schedule Task**.

   The **Schedule Task** option is unavailable for:

    - Target appliances. That is, appliances that are in an appliance group, other than the master.
    - All non-*Leader* appliances in an Active/Active cluster.
    - The Active node in an Active/Passive cluster.

The **Create Task** dialog appears.

FIGURE 134 Create Task



Schedule task for **pps-36**

Task Type: -- Select Task Type --

Target Version: -- Select Target Version --

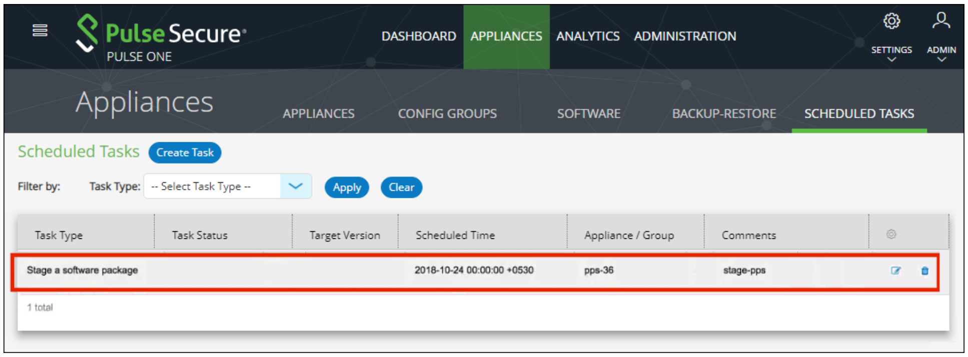
Scheduled Time: Oct 24, 2018 12 : 00 AM

Comments:

4. In the **Create Task** dialog:
   - For **Task Type**, select *Stage a software package*.
   - For **Target Version**, select the required software upgrade package.
   - For **Scheduled Time**, select the start time for the task.
   - (Optional) Add **Comments** as required. These appear on the **Scheduled Tasks** list.
5. Click **Save**.

   The new task is added to the list of scheduled tasks in the **Scheduled Tasks** tab. For example:

FIGURE 135 Scheduled Staging Task Added



Filter by: Task Type: -- Select Task Type --

Task Type	Task Status	Target Version	Scheduled Time	Appliance / Group	Comments	⚙
Stage a software package			2018-10-24 00:00:00 +0530	pps-36	stage-pps	✎ 🗑

1 total

6. In the **Appliances** tab, click the **Actions** icon for the appliance you want to upgrade, and then click **Schedule Task**.

   The **Create Task** dialog appears.

7. In the **Create Task** dialog:

    - For **Task Type**, select *Install a staged package*.
    - For **Target Version**, select the same package as for the first task.
    - For **Scheduled Time**, select the start time for the task. This must allow sufficient time for the first task to complete.
    - (Optional) Add **Comments** as required. These appear on the **Scheduled Tasks** list.

8. Click **Save**.

    The new task is added to the list of scheduled tasks in the **Scheduled Tasks** tab.

9. (Optional) You can edit the details for a scheduled task by clicking the **Edit** icon for the task.
10. (Optional) You can cancel a scheduled task by clicking the **Delete** icon for the task.
11. (Optional) You can monitor the progress of scheduled tasks using one of the following methods:

    - On the **Scheduled Tasks** tab. Here, the **Task Status** updates as a task starts and proceeds through to completion.
    - From the **Appliance Activities** panel. To access this, click the **Administration** tab, and then the **Appliance Activities** option.
    - From the **Appliances** tab, you can see status updates for individual appliances.
    - From the **Activities** panel for an appliance on the right side of the **Appliances** tab.

Scheduling a Full Upgrade of an Appliance Group

You can schedule an upgrade of an all target appliances in an appliance group as a single task from the **Config Groups** tab. When each task triggers, the same operation is initiated simultaneously on all group members.

Note: Before you upgrade a group, you can optionally publish any configuration changes from the master appliance to all group members. This can be performed as a separate scheduled task. You can also choose to publish a configuration to a group at any other time, see **"Distributing a Master Configuration" on page 84**.

To schedule an upgrade of an appliance group using a pair of scheduled tasks from the **Config Groups** tab:

1. Log into Pulse One as an administrator.
2. Click the **Appliances** menu and then the **Config Groups** tab.

    The **Config Groups** tab lists all appliance groups on Pulse One.

3. (Optional) If there are unpublished configuration changes for the group, you can choose to publish the configuration changes to all target appliances before performing other scheduled tasks. To do this:

    - Click the **Actions** icon for the appliance group you want to upgrade, and then click **Schedule Task**. The **Create Task** dialog appears.
    - In the **Create Task** dialog, for **Task Type**, select *Publish configuration*.
    - For **Scheduled Time**, select the start time for the task.
    - (Optional) Add **Comments** as required. These appear on the **Scheduled Tasks** list.
    - Click **Save**.

    The new task is added to the list of scheduled tasks in the **Scheduled Tasks** tab.

4. Click the **Actions** icon for the appliance group you want to upgrade, and then click **Schedule Task**.

    The **Create Task** dialog appears.

5. In the **Create Task** dialog:

    - For **Task Type**, select *Stage a software package*.
    - For **Target Version**, select the required software upgrade package.
    - For **Scheduled Time**, select the start time for the task.

      Note: If you scheduled a *Publish configuration* task for this group, you must leave sufficient time for that task to complete.
    - (Optional) Add **Comments** as required. These appear on the **Scheduled Tasks** list.

6. Click **Save**.

    The new task is added to the list of scheduled tasks in the **Scheduled Tasks** tab.

7. In the **Appliances** tab, click the **Actions** icon for the appliance you want to upgrade, and then click **Schedule Task**.

    The **Create Task** dialog appears.

8. In the **Create Task** dialog:

    - For **Task Type**, select *Install a staged package*.
    - For **Target Version**, select the same package as for the first task.
    - For **Scheduled Time**, select the start time for the task.

      Note: Ensure that you leave sufficient time for the *Stage a software package* task to complete.
    - (Optional) Add **Comments** as required. These appear on the **Scheduled Tasks** list.

9. Click **Save**.

   The new task is added to the list of scheduled tasks in the **Scheduled Tasks** tab.

10. (Optional) You can edit the details for a scheduled task by clicking the **Edit** icon for the task.

11. (Optional) You can cancel a scheduled task by clicking the **Delete** icon for the task.

12. (Optional) You can monitor the progress of scheduled tasks using one of the following methods:

    - On the **Scheduled Tasks** tab. Here, the **Task Status** updates as a task starts and proceeds through to completion.
    - From the **Appliance Activities** panel. To access this, click the **Administration** tab, and then the **Appliance Activities** option.
    - From the **Config Group** tab, you can see status updates for the group as a whole.
    - From the **Appliances** tab, you can see status updates for each appliance group member.
    - From the **Activities** panel for an individual appliance on the right side of the **Appliances** tab.

Uploading an Endpoint Security Assessment Plug-In Package

The Endpoint Security Assessment Plug-in (ESAP) is required by both Pulse Connect Secure and Pulse Policy Secure appliances. The ESAP package is used by the appliance to check third-party applications on endpoints for compliance with the predefined rules configured in a Host Checker policy.

Pulse Secure frequently adds enhancements, bug fixes, and support for new third-party applications to the plug-in. New plug-in package releases are available independently and more frequently than new releases of the system software package. If necessary, you can upload (and optionally activate) an ESAP package independently of upgrading the system software package.

Note: ESAP uploads from Pulse One are supported on PCS/PPS appliances at version 9.1R1 or later.

Note: For full details of ESAP use on PCS/PPS appliances, see the specific product documentation for the appliance.

To upload (and optionally activate) an ESAP package from Pulse One, you must perform the following tasks:

- Download the required ESAP package to local storage, see **"Downloading an ESAP Package" on page 107**.
- Upload the ESAP package to Pulse One, see **"Uploading an ESAP Package to Pulse One" on page 107**.
- Upload (and optionally activate) the ESAP package to individual appliances or appliance groups, see **"Uploading ESAP Packages onto Appliances and Appliance Groups" on page 108**.

Downloading an ESAP Package

Download the Endpoint Security Assessment Plug-in from the Pulse Secure Global Support Center (PSGSC) Center to your computer:

1. Open the following page:

   https://support.pulsesecure.net

2. Click the **Software** tab.
3. Navigate to the ESAP release you want, and click the link to download the package file to accessible local storage.

After you have downloaded the ESAP package, you can upload it to Pulse One, see **"Uploading an ESAP Package to Pulse One" on page 107**.

Uploading an ESAP Package to Pulse One

The process of uploading an ESAP package to Pulse One is similar to the upload of system software to Pulse One, see **"Uploading an Appliance Software Package to Pulse One" on page 90**.

You can upload up to three ESAP packages to Pulse One.

To upload an ESAP package to Pulse One:

1. Log into Pulse One as an administrator.
2. Click the **Appliances** menu and then the **Software** tab.

   The **Software** tab lists all **Available Software** packages present on Pulse One.

3. Click **Add Software**.

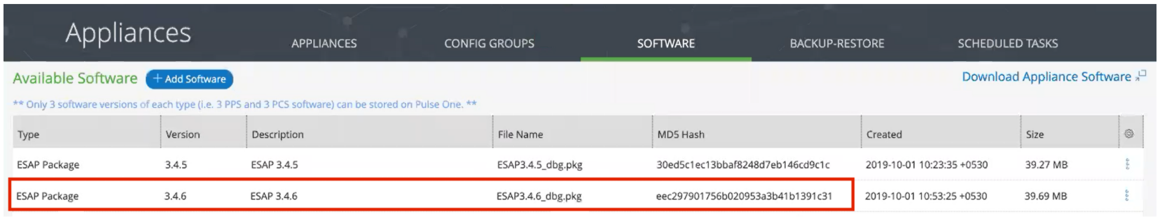
   The **Upload Software** dialog appears.

4. In the **Upload Software** dialog:
   - For **Software Type**, select *ESAP Package*.
   - Enter a **Version** number and a **Description** for the software package.
   - Enter the **MD5 Hash** value for the software package.
   - For **Select Software**, click **Browse** and locate the ESAP package file.
5. Click **Upload**.

   Note: The upload may take several minutes.

After the upload completes, the new ESAP package is added to the **Available Software** list on Pulse One. For example:

FIGURE 136 Appliance Software Package Added



** Only 3 software versions of each type (i.e. 3 PPS and 3 PCS software) can be stored on Pulse One. **

Type	Version	Description	File Name	MD5 Hash	Created	Size
ESAP Package	3.4.5	ESAP 3.4.5	ESAP3.4.5_dbg.pkg	30ed5c1ec13bbaf8248d7eb146cd9c1c	2019-10-01 10:23:35 +0530	39.27 MB
ESAP Package	3.4.6	ESAP 3.4.6	ESAP3.4.6_dbg.pkg	eec297901756b020953a3b41b1391c31	2019-10-01 10:53:25 +0530	39.69 MB

6. (Optional) If required, you can edit the details for an uploaded ESAP package.

   To do this, click the **Actions** icon for the ESAP package, and then click **Edit Software**.

7. (Optional) If required, you can delete an uploaded ESAP package from Pulse One.

   To do this, click the **Actions** icon for the ESAP package, and then click **Delete Software**.

After you have uploaded the ESAP package to Pulse One, you can upload (and optionally activate) individual appliances and appliance groups, see **"Uploading ESAP Packages onto Appliances and Appliance Groups" on page 108**.

Uploading ESAP Packages onto Appliances and Appliance Groups

After you have uploaded the ESAP package to Pulse One, you can:

- Upload (and optionally activate) ESAP on a single appliance, see **"Uploading an ESAP Package onto an Appliance" on page 109**.
- Upload (and optionally activate) on all appliances in an appliance group, see **"Uploading an ESAP Package onto all Target Appliances in a Group" on page 110**.
- Upload (and optionally activate) ESAP on both appliances in a cluster, see **"Uploading an ESAP Package onto all Appliances in a Cluster" on page 111**.

If you do not activate an uploaded ESAP package, you can activate it later. Please refer to the specific appliance product documentation for details of this procedure.

Note: ESAP uploads from Pulse One are supported on PCS/PPS appliances at version 9.1R1 or later.

Uploading an ESAP Package onto an Appliance

You can upload (and optionally activate) an ESAP package on any registered appliance at version 9.1R1 or later.

Before you can perform an ESAP upload to an appliance, you must upload the required ESAP package onto Pulse One, see **"Uploading an ESAP Package to Pulse One" on page 107**.

Note: The appliance will continue to operate during the upload, and will not reboot.

To upload (and optionally activate) an ESAP package on a single appliance:

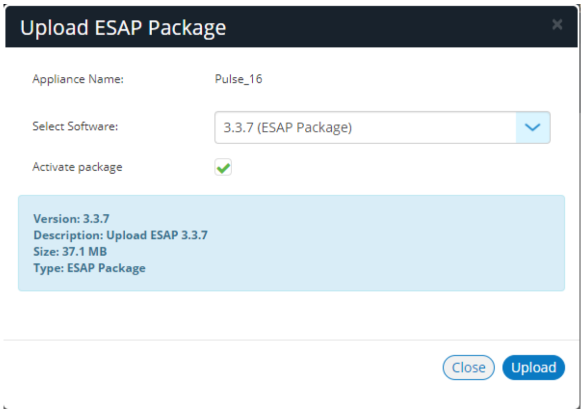
1. Log into Pulse One as an administrator.
2. Click the **Appliances** menu and then the **Appliances** tab.

   The **Appliances** tab lists all appliances on Pulse One.
3. Click the **Actions** icon for the required appliance, and then click **Upload ESAP Package**.

   The **Upload ESAP Package** dialog appears.
4. For **Select Software**, choose the required ESAP package.

   Full details for the selected package are displayed.
5. (Optional) To automatically activate an uploaded package, select the **Activate package** check box. For example:

   FIGURE 137 Upload Software



Upload ESAP Package

Appliance Name: Pulse_16

Select Software: 3.3.7 (ESAP Package)

Activate package ☑

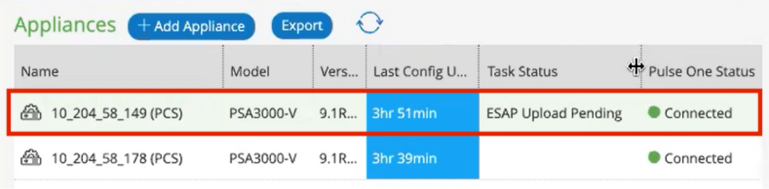
Version: 3.3.7
Description: Upload ESAP 3.3.7
Size: 37.1 MB
Type: ESAP Package

Note: If you do not select the **Activate package** check box, the package is uploaded but not activated. You can activate it later in the UI for the appliance. Please refer to the specific appliance product documentation for details of this procedure.

6. To start the upload/activation, click **Upload**.

   The **Task Status** of the appliance updates to show that the upload of the appliance is pending. For example:

   FIGURE 138 Upload Pending



Name	Model	Vers...	Last Config U...	Task Status	Pulse One Status
10_204_58_149 (PCS)	PSA3000-V	9.1R...	3hr 51min	ESAP Upload Pending	● Connected
10_204_58_178 (PCS)	PSA3000-V	9.1R...	3hr 39min		● Connected

   The **Task Status** changes as the process continues, including activation if selected.

   Note: The upload (and optional activation) may take several minutes. No reboot is performed.

After this operation completes, the ESAP package upload is complete.

Uploading an ESAP Package onto all Target Appliances in a Group

You can upload (and optionally activate) an ESAP package on the master appliance in an appliance group. When an ESAP package is activated, the other appliances in the group are then updated automatically.

Note: The appliances must be at version 9.1R1 or later.

To perform an ESAP upload on all members of an appliance group:

1. Log into Pulse One as an administrator.
2. Click the **Appliances** menu and then the **Config Groups** tab.

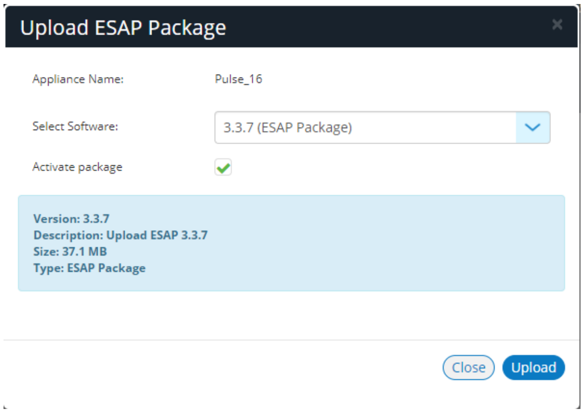
   The **Appliance Configuration Groups** tab lists all appliance groups on Pulse One.
3. Click the **Actions** button for the required appliance group, and then click **Upload ESAP Package**.

   The **Upload ESAP Package** dialog appears.
4. For **Select Software**, choose the required ESAP package for the upload.

   Full details for the selected package are displayed.

5. (Optional) To automatically activate an uploaded ESAP package, select the **Activate package** check box. For example:

FIGURE 139 Upload Software



Upload ESAP Package

Appliance Name: Pulse_16

Select Software: 3.3.7 (ESAP Package)

Activate package ☑

Version: 3.3.7
Description: Upload ESAP 3.3.7
Size: 37.1 MB
Type: ESAP Package

Note: If you do not select the **Activate package** check box, the package is uploaded but not activated. You can activate it later in the UI for the Master appliance. Please refer to the specific appliance product documentation for details of this procedure.

6. To start the upload/activation, click **Upload**.

7. Click the **Appliances** tab.

   The **Task Status** of each appliance updates to show that the upload is pending.

   The **Task Status** of each appliance changes as the process continues.

   Note: Each upload (and optional activation) may take several minutes. No reboots are performed.

   After the ESAP package has been uploaded (and optionally activated) on all members of the group (master and target appliances), the ESAP package upload to the group is complete.

Uploading an ESAP Package onto all Appliances in a Cluster

Uploading (and optionally activating) an ESAP package on all appliances in a cluster is similar to the ESAP upload of a single appliance, see **"Uploading an ESAP Package onto an Appliance" on page 109**.

Note: The appliances must be at version 9.1R1 or later.

You can perform an immediate ESAP upload (and optional activation) on one of the appliances in a cluster, as follows:

- For *Active/Active* clusters, you can only upload (and optionally activate) an ESAP package on the *Leader node*. When the ESAP package is activated, all other nodes update automatically.
- For *Active/Passive* clusters, you can only upload (and optionally activate) the Passive node. When the ESAP package is activated, the Active node updates automatically.

In both cases, no reboot is required.

Viewing the Activities Log for an Appliance

Viewing the log details of the activities between the Pulse One console and various appliances will help the Administrator to troubleshoot and resolve any issues. The **Appliances > Activities** panel in Pulse One provides details of appliance reboots, configuration uploads, and so on.

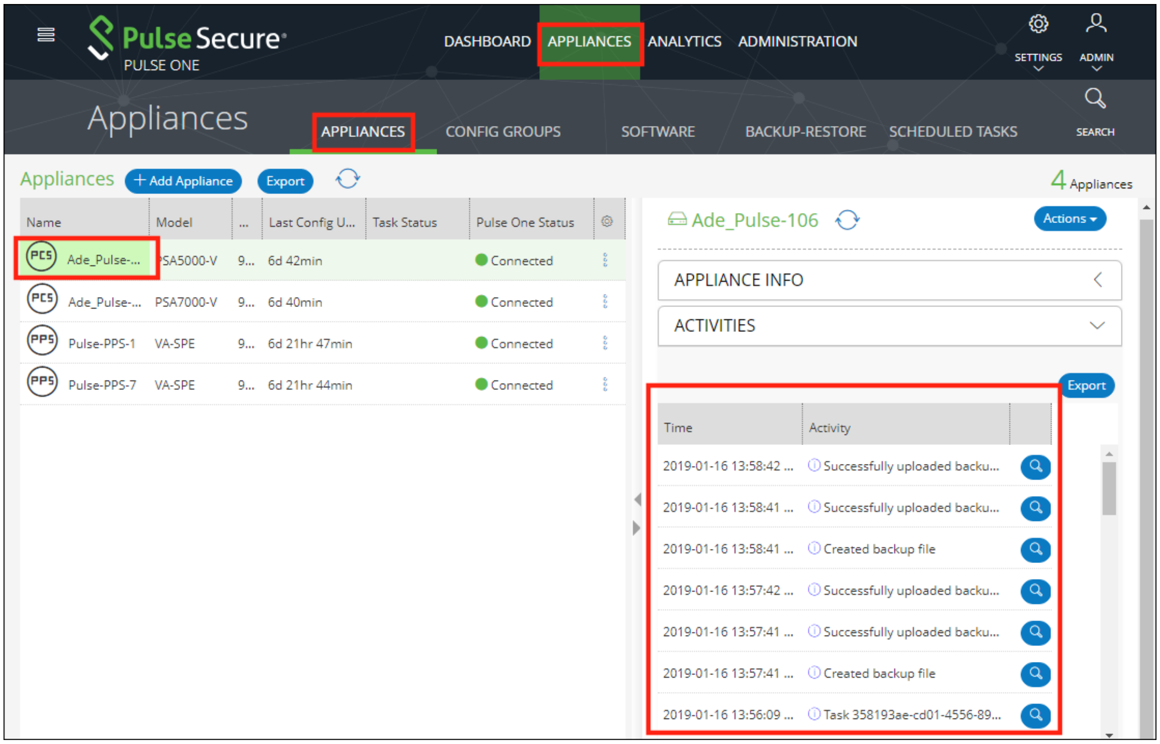
To view the activities log for an appliance:

1. Log into Pulse One as an administrator.
2. Click the **Appliances** menu and then the **Appliances** tab.

   The **Appliances** tab displays all current appliances.
3. Select an appliance whose **Pulse One Status** is status *Connected*.
4. In the panel on the right, expand **Activities** to display details of all activities.

   For example:

FIGURE 140 Activities Details



Name	Model	...	Last Config U...	Task Status	Pulse One Status
Ade_Pulse-...	PSA5000-V	9...	6d 42min		Connected
Ade_Pulse-...	PSA7000-V	9...	6d 40min		Connected
Pulse-PPS-1	VA-SPE	9...	6d 21hr 47min		Connected
Pulse-PPS-7	VA-SPE	9...	6d 21hr 44min		Connected

Time	Activity
2019-01-16 13:58:42 ...	Successfully uploaded backu...
2019-01-16 13:58:41 ...	Successfully uploaded backu...
2019-01-16 13:58:41 ...	Created backup file
2019-01-16 13:57:42 ...	Successfully uploaded backu...
2019-01-16 13:57:41 ...	Successfully uploaded backu...
2019-01-16 13:57:41 ...	Created backup file
2019-01-16 13:56:09 ...	Task 358193ae-cd01-4556-89...

Viewing the Configuration Change History for an Appliance

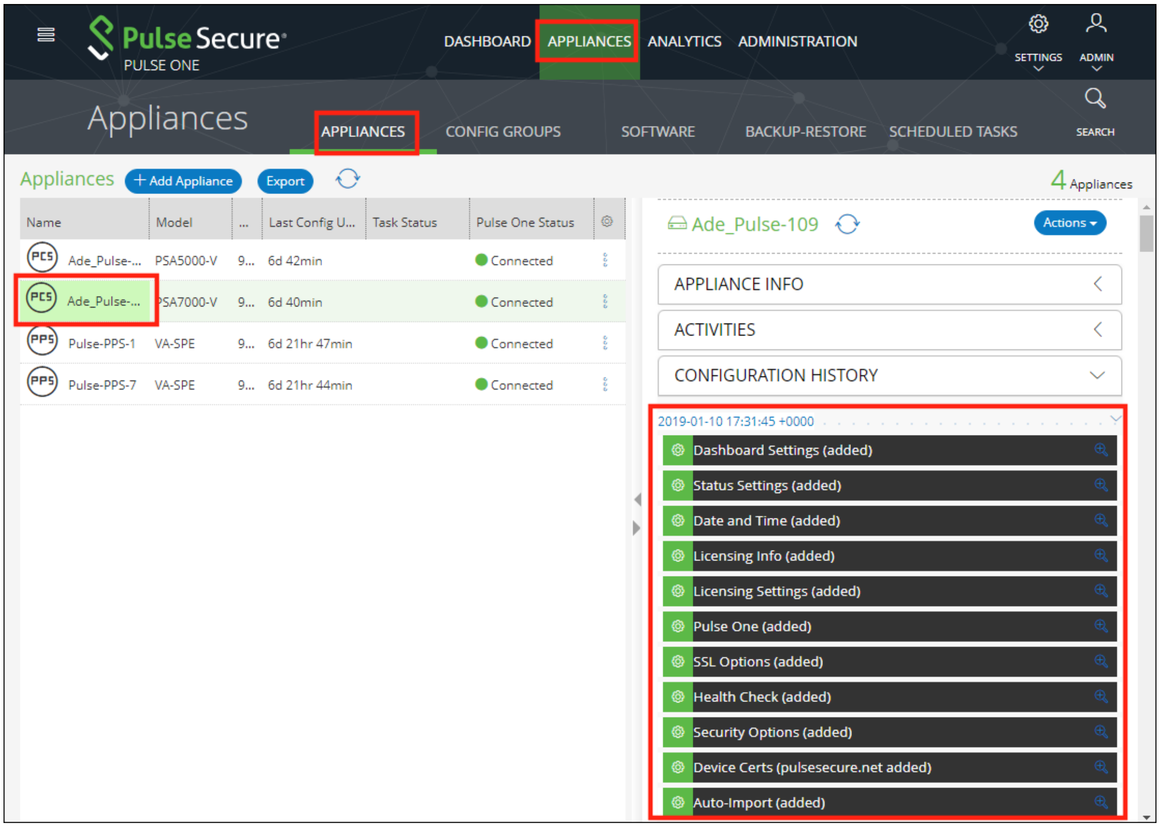
The Configuration Changes panel in the Appliances tab provides the configuration change history for each appliance.

To view the configuration changes history:

1. Log into Pulse One as an administrator.
2. Click the **Appliances** menu and then the **Appliances** tab.

   The **Appliances** tab displays all current appliances.
3. Select an appliance whose **Pulse One Status** is status *Connected*.
4. In the panel on the right, select **Configuration History**. This displays the configuration changes history for the appliance, including timestamps for each change.
5. Expand the required timestamp to view the changes made at that time. For example:

FIGURE 141 View Configuration Changes



Name	Model	...	Last Config U...	Task Status	Pulse One Status
Ade_Pulse-...	PSA5000-V	9...	6d 42min		Connected
Ade_Pulse-...	PSA7000-V	9...	6d 40min		Connected
Pulse-PPS-1	VA-SPE	9...	6d 21hr 47min		Connected
Pulse-PPS-7	VA-SPE	9...	6d 21hr 44min		Connected

Ade_Pulse-109

2019-01-10 17:31:45 +0000

- Dashboard Settings (added)
- Status Settings (added)
- Date and Time (added)
- Licensing Info (added)
- Licensing Settings (added)
- Pulse One (added)
- SSL Options (added)
- Health Check (added)
- Security Options (added)
- Device Certs (pulsesecure.net added)
- Auto-Import (added)

Comparing Appliances

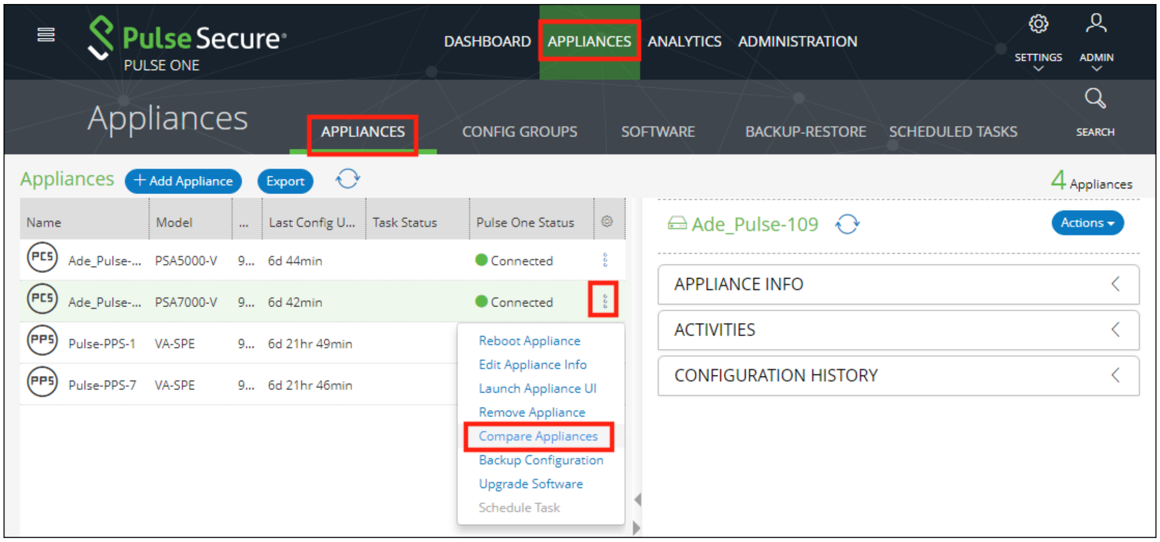
The Compare Appliances feature allows you to compare two appliances based on their settings.

To compare two appliances:

1. Log into Pulse One as an administrator.
2. Click the **Appliances** menu and then the **Appliances** tab.

   The **Appliances** tab displays all current appliances.
3. Select the source appliance that you want to compare and click its **Actions** icon (✎).
4. On the drop-down menu, click **Compare Appliances**.

   FIGURE 142 Compare Appliances

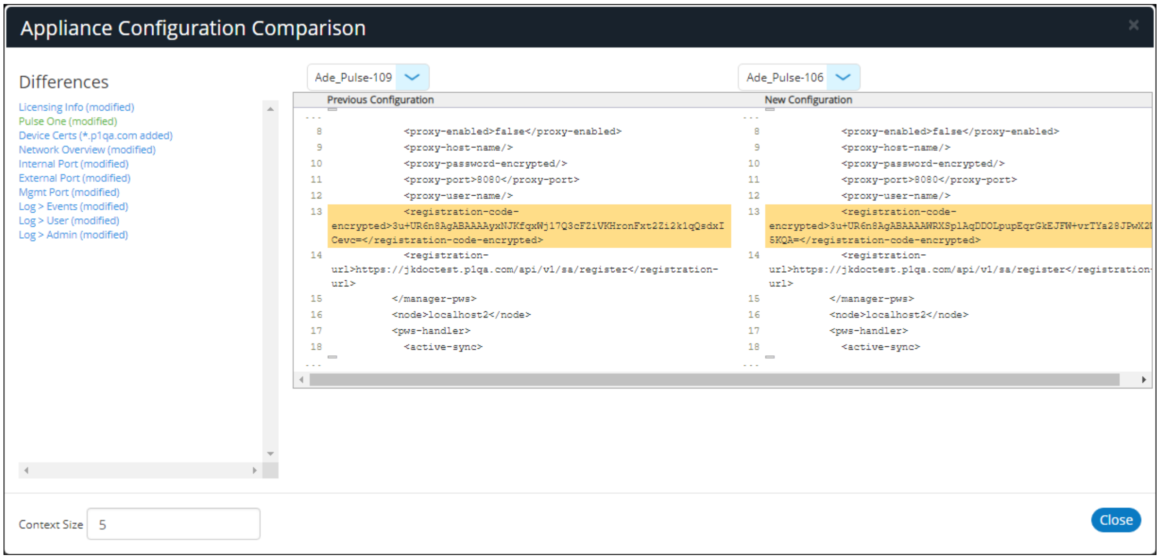
Name	Model	...	Last Config U...	Task Status	Pulse One Status
PCS Ade_Pulse-...	PSA5000-V	9...	6d 44min		Connected
PCS Ade_Pulse-...	PSA7000-V	9...	6d 42min		Connected
PPS Pulse-PPS-1	VA-SPE	9...	6d 21hr 49min		
PPS Pulse-PPS-7	VA-SPE	9...	6d 21hr 46min		

5. In the **Appliance Configuration Comparison** window, select the source appliance and the target appliance to compare.

   The **Differences** panel shows a list of settings that the two selected appliances have differences.
6. Select a setting. For example, *Pulse One (Modified)*.

   In the **Results** pane, the **Base** text and **New** text highlight the differences in the two appliances for that setting. For example:

FIGURE 143 Appliance Configuration Comparison



Previous Configuration

```
...
            <proxy-enabled>false</proxy-enabled>
            <proxy-host-name/>
            <proxy-password-encrypted/>
            <proxy-port>8080</proxy-port>
            <proxy-user-name/>
            <registration-code-
encrypted>3u+UR6n8AgABAAAAyxNJKfqxWj17Q3cFZiVKHronFxt2Zi2k1qQsdxI
Cevc=</registration-code-encrypted>
            <registration-
url>https://jkdoctest.p1qa.com/api/v1/sa/register</registration-
url>
          </manager-pws>
          <node>localhost2</node>
          <pws-handler>
            <active-sync>
...
```

New Configuration

```
...
            <proxy-enabled>false</proxy-enabled>
            <proxy-host-name/>
            <proxy-password-encrypted/>
            <proxy-port>8080</proxy-port>
            <proxy-user-name/>
            <registration-code-
encrypted>3u+UR6n8AgABAAAAWRXSp1AqDDOLpupEqrGkEJFW+vrTYa28JPwX2
5KQA=</registration-code-encrypted>
            <registration-
url>https://jkdoctest.p1qa.com/api/v1/sa/register</registration
url>
          </manager-pws>
          <node>localhost2</node>
          <pws-handler>
            <active-sync>
...
```

Rebooting an Appliance

Rebooting an appliance is necessary when the services on the appliance must be restarted, or when there are other issues with an appliance that must be resolved.

After the reboot, the appliance will connect back to the network and Pulse One will indicate the status of the appliance in the dashboard.

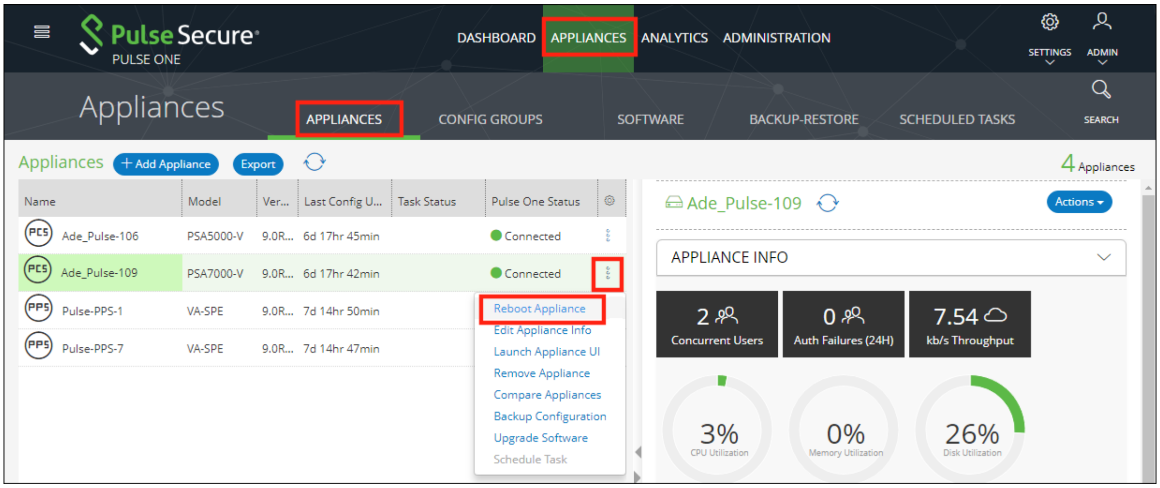
To reboot an appliance:

1. Log into Pulse One as an administrator.
2. Click the **Appliances** menu and then the **Appliances** tab.

   The **Appliances** tab displays all current appliances.
3. Select the appliance that you want to reboot and click the **Actions** icon (⋮).

4. On the drop-down menu, click **Reboot Appliance**.

FIGURE 144 Reboot Appliance



Name	Model	Ver...	Last Config U...	Task Status	Pulse One Status
Ade_Pulse-106	PSA5000-V	9.0R...	6d 17hr 45min		Connected
Ade_Pulse-109	PSA7000-V	9.0R...	6d 17hr 42min		Connected
Pulse-PPS-1	VA-SPE	9.0R...	7d 14hr 50min		
Pulse-PPS-7	VA-SPE	9.0R...	7d 14hr 47min		

The **Reboot Appliance** confirmation dialog appears.

5. Ensure that you have selected the correct appliance and click **Yes**.

   The selected appliance reboots.

Removing an Appliance from Pulse One

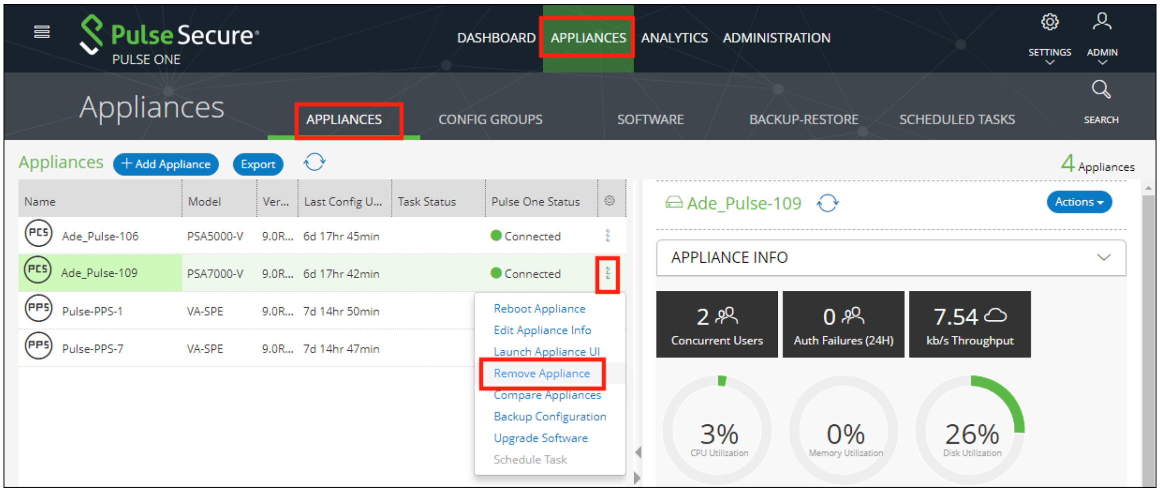
If you no longer want to use an appliance with Pulse One, or want to re-provision it, you can remove the appliance.

To remove an appliance:

1. Log into Pulse One as an administrator.
2. Click the **Appliances** menu and then the **Appliances** tab.

   The **Appliances** tab displays all current appliances.
3. Select the appliance that you want to remove and click its **Actions** icon (⁝).
4. Click **Remove Appliance to remove the appliance from Pulse One.**

   FIGURE 145 Remove Appliance

Name	Model	Ver...	Last Config U...	Task Status	Pulse One Status
PCS Ade_Pulse-106	PSA5000-V	9.0R...	6d 17hr 45min		Connected
PCS Ade_Pulse-109	PSA7000-V	9.0R...	6d 17hr 42min		Connected
PPS Pulse-PPS-1	VA-SPE	9.0R...	7d 14hr 50min		
PPS Pulse-PPS-7	VA-SPE	9.0R...	7d 14hr 47min		

   Note: For PCS appliance virtual machines on either vSphere or AWS, an additional command is available. Click **Destroy Appliance** to remove the appliance from Pulse One, and to also destroy the appliance on the vSphere/AWS platform.

   The **Remove Appliance From Pulse One** confirmation dialog appears.
5. Click **Yes** to remove the selected appliance.

Preparing a Target Appliance

This section details the steps to add an agent instance for the target appliance, and a checklist for preparing the target appliance for configuration distribution.

Preparing an RSA Agent Instance for the Target Appliance

The Pulse One administrator must ensure that the *sdconf.rec* file is uploaded to the master appliance that contains the agent instance for the target appliance.

To add a new target appliance:

1. In **RSA Authentication Manager**, add the agent instance for the target appliance.
2. Download the *sdconf.rec* file.
3. Upload the *sdconf.rec* file to the master appliance.

   Note: Some configuration blocks that are distributed by Pulse One may refer to other blocks that are not distributed. In such cases, the configuration distribution fails at the target appliance while importing the configuration. The administrator must manually configure the target appliance before distributing the configuration through Pulse One.

A checklist for preparing the target appliance for configuration distribution is provided in **“Appendix: Checklist for Preparing a Target Appliance” on page 161**.

Removing an Appliance from an Appliance Group

You can remove any appliance other than the master appliance from the appliance group.

This section details the steps to remove an appliance from the group.

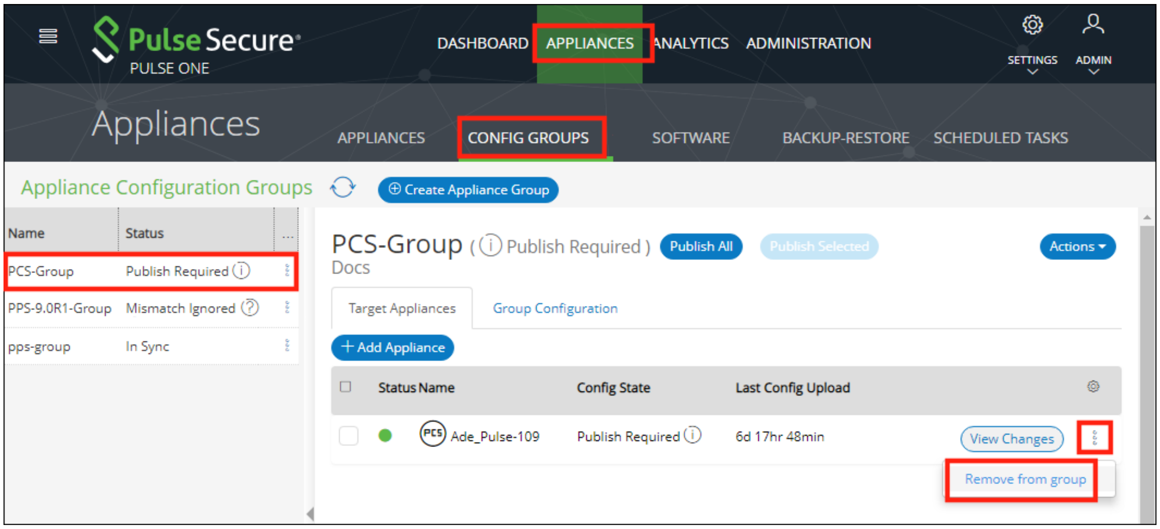
To remove an appliance from the group:

1. Select the **Appliances** menu.
2. Select the **Config Groups** tab.

   A list of configuration groups is displayed.
3. Select the group from which the appliance needs to be removed.
4. Select the **Target Appliances** tab.
5. Click the **Actions** icon (⋮) for the appliance you want to remove.

6. From the menu options, select **Remove from Group**. For example:

FIGURE 146 Remove from Group



Name	Status
PCS-Group	Publish Required
PPS-9.0R1-Group	Mismatch Ignored
pps-group	In Sync

Status	Name	Config State	Last Config Upload
●	Ade_Pulse-109	Publish Required	6d 17hr 48min

An alert message confirms the removal of the appliance from the group.

Editing an Appliance Group

This section details the steps to modify an appliance group.

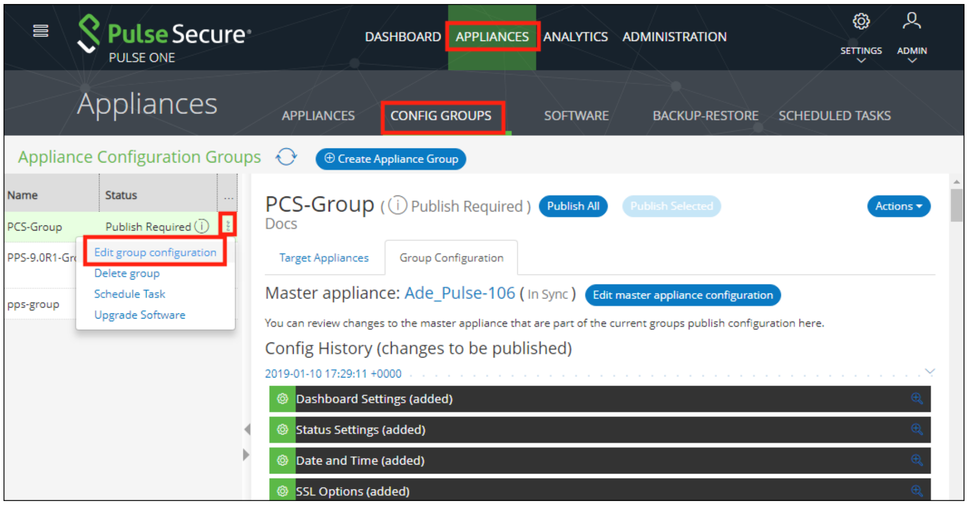
To edit an appliance group:

1. Select the **Appliances** menu.
2. Select the **Config Groups** tab.

   A list of configuration groups is displayed.
3. Select the group that you want to modify and click its **Actions** (⋮) icon.

4. From the menu options, select **Edit Group Configuration**.

FIGURE 147 Edit Group Configuration



Name	Status
PCS-Group	Publish Required
PPS-9.0R1-Gr	
pps-group	

PCS-Group (Publish Required)
Docs

Master appliance: Ade_Pulse-106 (In Sync)

You can review changes to the master appliance that are part of the current groups publish configuration here.

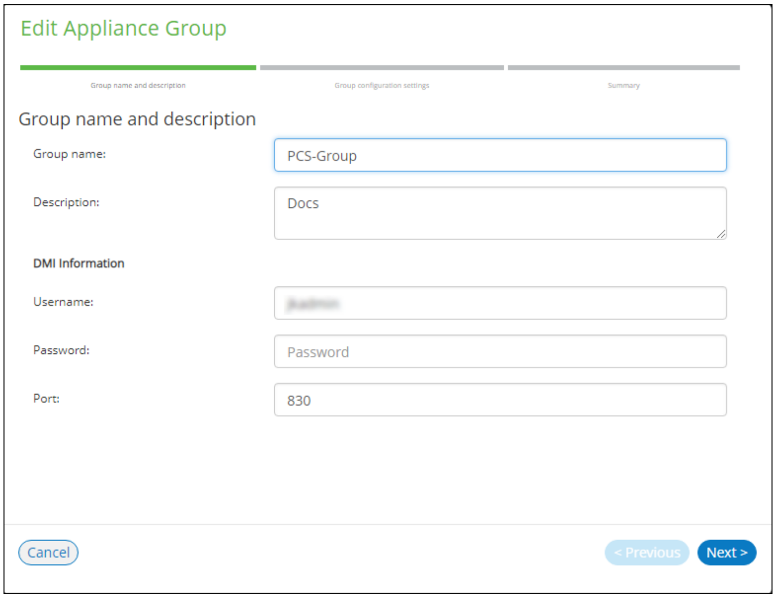
Config History (changes to be published)

2019-01-10 17:29:11 +0000

- Dashboard Settings (added)
- Status Settings (added)
- Date and Time (added)
- SSL Options (added)

The **Edit Appliance Group** wizard appears. For example:

FIGURE 148 Edit Appliance Group Wizard



Group name and description

Group name: PCS-Group

Description: Docs

DMI Information

Username: [redacted]

Password: Password

Port: 830

5. Work through the wizard, making the required changes to the group name, master appliance, and configuration settings.

6. Click **Finish**.

Deleting an Appliance Group

This section details the steps to delete an appliance group.

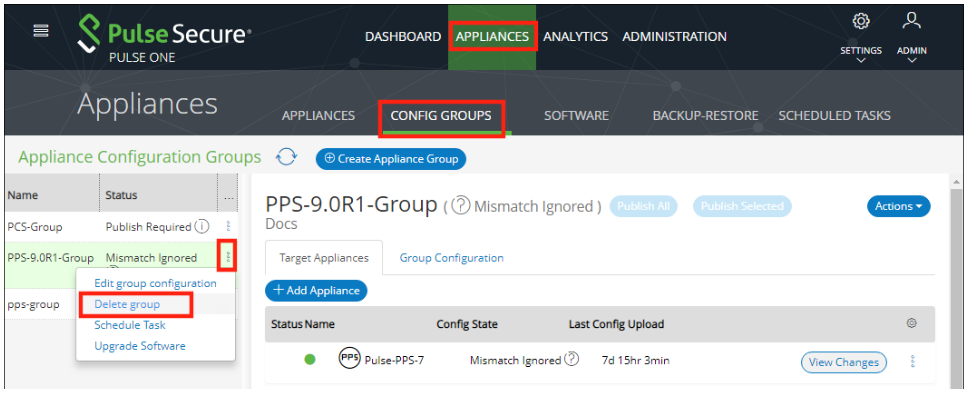
Note: The appliances within the appliance group are not deleted when you the delete the group, and can be viewed as normal in the **Appliances** tab.

1. Select the **Appliances** menu.
2. Select the **Config Groups** tab.

   A list of all configuration groups is displayed.

3. Click the group that you want to delete and click its **Actions** icon (⋮).

   FIGURE 149 Delete Group

Name	Status
PCS-Group	Publish Required
PPS-9.0R1-Group	Mismatch Ignored
pps-group	

Status	Name	Config State	Last Config Upload
●	Pulse-PPS-7	Mismatch Ignored	7d 15hr 3min

4. From the menu options, select **Delete Group**.
5. In the **Delete Group** confirmation window, click **Yes** to delete the group.

Viewing Analytics and Reports

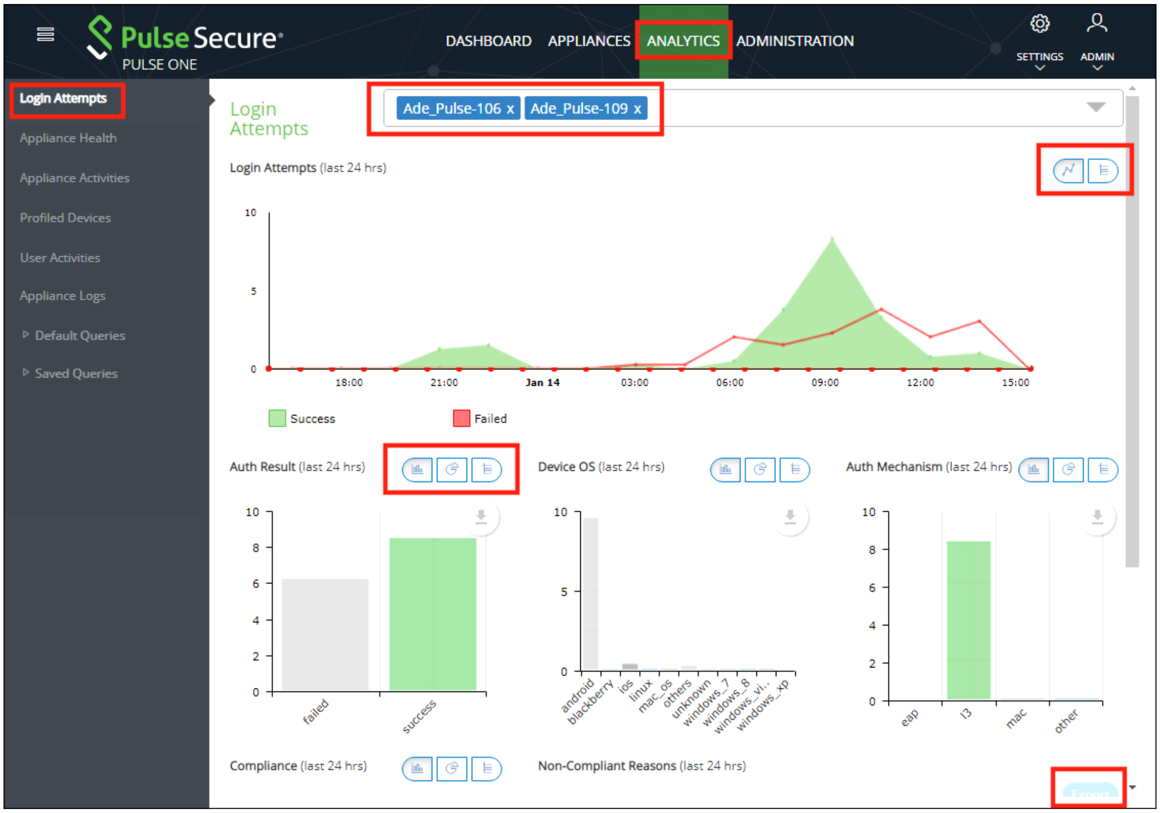
Viewing the Login Attempts Report

To view the **Login Attempts** report:

1. Select the **Analytics** menu.
2. Select **Login Attempts**.
3. From the **Login Attempts** drop-down, select one or more appliances for the report.
4. Select the graph type.

The report shows the login attempts, authentication mechanism and result, and device OS in the last 24 hours.

FIGURE 150 Login Attempts Report



5. (Optional) Choose bar chart, line graph, pie chart or table data for each graph.

6. (Optional) Click **Export** to download displayed information as a *.csv* format file.

Viewing the Appliance Health Report

To view the **Appliance Health** report:

1. Select the **Analytics** menu.

2. Select **Appliance Health**.

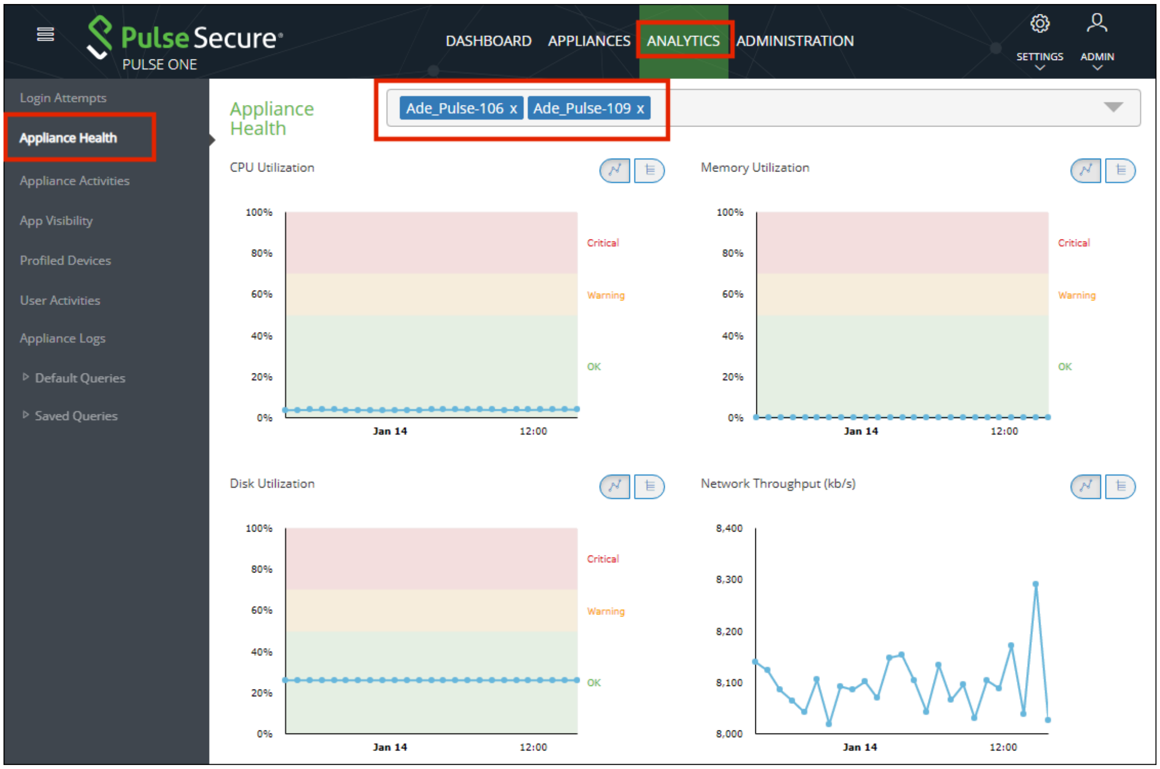
3. From the **Appliance Health** drop-down, select one or more appliances for the report.

   The following reports for the selected appliance over the last 24 hours are displayed:

   - CPU Utilization
   - Memory Utilization
   - Disk Utilization
   - Network Throughput (kb/s)

For example:

FIGURE 151 Appliance Health Report



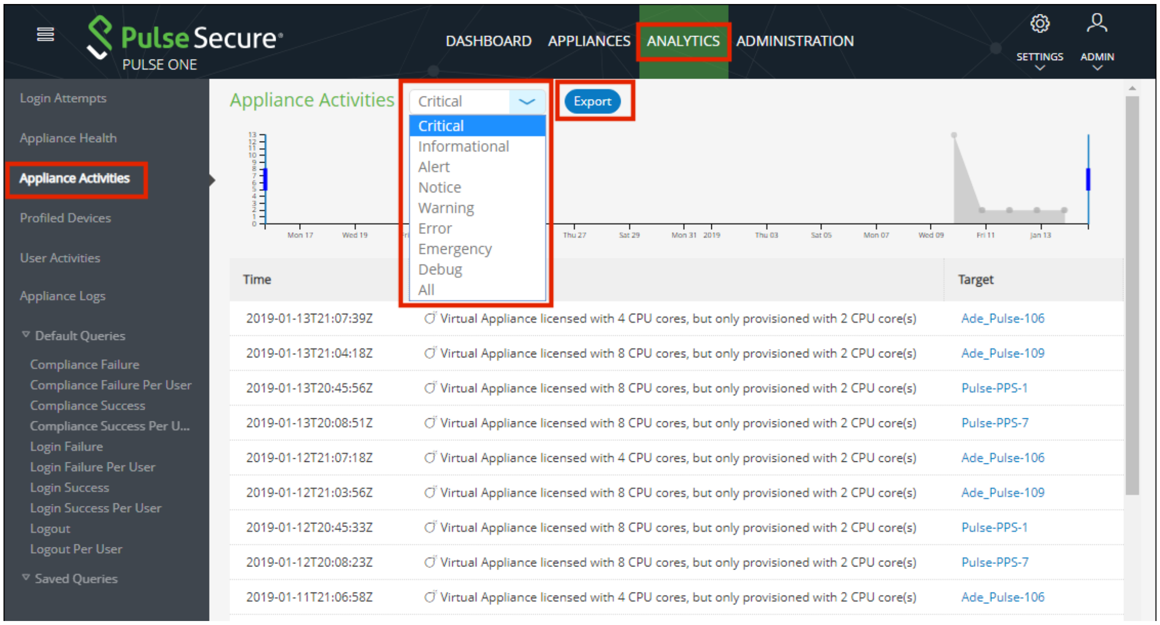
Viewing the Appliance Activities Report

To view the **Appliance Activities** report:

1. Select the **Analytics** menu.
2. Select **Appliance Activities**.

3. From the **Appliance Activities** drop-down, select the required filter (*Critical*, *Alert*, *Notice*, and so on) for the report.

FIGURE 152 Appliance Activities



Time		Target
2019-01-13T21:07:39Z	Virtual Appliance licensed with 4 CPU cores, but only provisioned with 2 CPU core(s)	Ade_Pulse-106
2019-01-13T21:04:18Z	Virtual Appliance licensed with 8 CPU cores, but only provisioned with 2 CPU core(s)	Ade_Pulse-109
2019-01-13T20:45:56Z	Virtual Appliance licensed with 8 CPU cores, but only provisioned with 2 CPU core(s)	Pulse-PPS-1
2019-01-13T20:08:51Z	Virtual Appliance licensed with 8 CPU cores, but only provisioned with 2 CPU core(s)	Pulse-PPS-7
2019-01-12T21:07:18Z	Virtual Appliance licensed with 4 CPU cores, but only provisioned with 2 CPU core(s)	Ade_Pulse-106
2019-01-12T21:03:56Z	Virtual Appliance licensed with 8 CPU cores, but only provisioned with 2 CPU core(s)	Ade_Pulse-109
2019-01-12T20:45:33Z	Virtual Appliance licensed with 8 CPU cores, but only provisioned with 2 CPU core(s)	Pulse-PPS-1
2019-01-12T20:08:23Z	Virtual Appliance licensed with 8 CPU cores, but only provisioned with 2 CPU core(s)	Pulse-PPS-7
2019-01-11T21:06:58Z	Virtual Appliance licensed with 4 CPU cores, but only provisioned with 2 CPU core(s)	Ade_Pulse-106

4. (Optional) Click **Export** to download displayed information as a *.csv* format file.

Viewing the Profiled Devices Report

Pulse Secure Profiler dynamically identifies and classifies both managed and unmanaged endpoint devices, enabling control of access to networks and resources based on the type of the device.

The **Profiled Devices** report in Pulse One displays the list of devices that are discovered in the network.

To view profiled devices in Pulse One reports, a Pulse Policy Secure appliance must be registered in Pulse One and this Pulse Policy Secure appliance should have the Local Profiler Authentication server configured.

For details about configuring Local Profiler Authentication server in the Pulse Policy Secure appliance, refer to *Pulse Secure Profiler Deployment Guide*.

For details about registering the Pulse Policy Secure appliance, see **“Registering an Existing PCS/PPS Appliance” on page 33**.

To view **Profiled Devices** report:

1. Select **Analytics > Profiled Devices.**

   The **Profiled Devices** page appears. This includes a table of devices and a **Device Details** area.

2. (Optional) Type a text entry (such as an IP address, a MAC address or a manufacturer name) into the **Filter** field and click **Apply**. The table updates to show entries that match that string.

3. (Optional) Select a **Collector Type** to filter the table based on the selected type and click **Apply**. The table updates to show entries that match that type: *DHCP*, *SNMP*, *NMAP*, *SSH*, *WMI*, *MDM*, *TRAP*, *USER AGENT*.

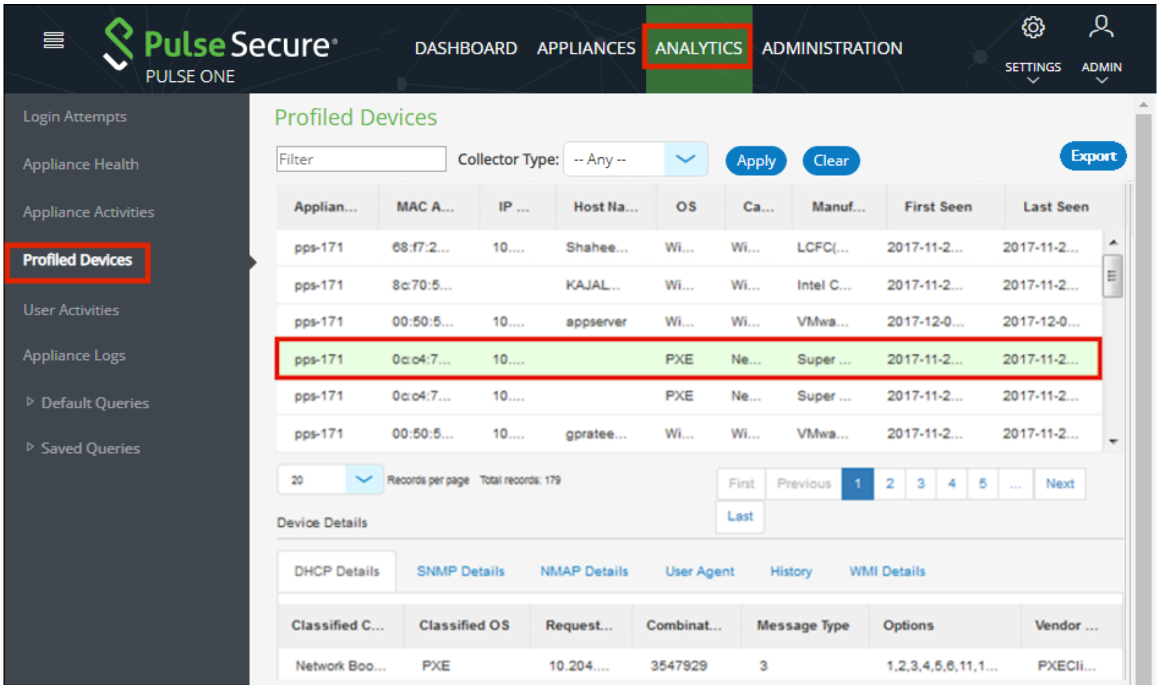
4. (Optional) Select the required number of **Records per page**. The default is *20*.

5. Select a device in the table to update the **Device Detail** category tabs at the bottom of the page: **DHCP Details**, **SNMP Details**, **NMAP Details**, **User Agent**, **History**, **WMI Details**, **MDM Details** and **SSH Details**.

   Note: Some devices will not populate the **Device Details** tabs. These devices have been imported into a PPS appliance from another PPS appliance using the PPS GUI. See the *Pulse Policy Secure* documentation for details.

6. Click **Export** to download the details in a *.csv* format file.

FIGURE 153 Profiled Devices



Profiled Devices

Filter Collector Type: -- Any --

Applian...	MAC A...	IP ...	Host Na...	OS	Ca...	Manuf...	First Seen	Last Seen
pps-171	68:f7:2...	10....	Shahee...	Wi...	Wi...	LCFC(...	2017-11-2...	2017-11-2...
pps-171	8c:70:5...		KAJAL...	Wi...	Wi...	Intel C...	2017-11-2...	2017-11-2...
pps-171	00:50:5...	10....	appserver	Wi...	Wi...	VMwa...	2017-12-0...	2017-12-0...
pps-171	0c:c4:7...	10....		PXE	Ne...	Super ...	2017-11-2...	2017-11-2...
pps-171	0c:c4:7...	10....		PXE	Ne...	Super ...	2017-11-2...	2017-11-2...
pps-171	00:50:5...	10....	gpratee...	Wi...	Wi...	VMwa...	2017-11-2...	2017-11-2...

20 Records per page Total records: 179

Device Details

Classified C...	Classified OS	Request...	Combinat...	Message Type	Options	Vendor ...
Network Boo...	PXE	10.204....	3547929	3	1,2,3,4,5,6,11,1...	PXECli...

The above table is populated as endpoints join the network. It might take a few hours (to several days) for all the endpoints to be profiled.

Viewing the User Activities Report

Pulse One administrators can aggregate user activities information as consolidated reports in Pulse One.

Note: Displayed information is based on data from registered appliances with version 9.0R1 or above.

This report provides the aggregated view of list of all users and their last login activities, compliance status, session length, appliance names, login success and failures.

- **Users Summary** table - information of all the users such as username, last login time, last login IP and their session lengths. This list can be filtered by date range, username and realm.
- **Selected User Sign-in Activities** table - information of selected user's authentication results, timestamps, authentication type, authentication mechanism, compliance information. The user details can be filtered by mac address, realm, compliance results, authentication mechanism and authentication results.

Note: PCS/PPS appliances with versions 9.0R1 or above must be registered with Pulse One to view user activity reports.

To view the **User Activities** report:

1. Select **Analytics > User Activities**.
2. Click a user to view the sessions details of that user in the Activities table.
3. Use the **View** drop-down to change the number of rows to be displayed.
4. Use the **Columns** drop-down to customize the columns to be displayed.
5. Use the filters to narrow down the search results.
6. Use the **Export** button to save the report in the .csv format.

If the device from which user performed sign-in was profiled by any registered PPS/Profiler in Pulse One, a hyperlink will be shown in MAC Address column. Upon clicking, it will take that device's profiler report.

Viewing the UEBA Analytics Reports

User and Entity Behavior Analytics (UEBA) software analyzes user activity data from logs, network traffic and endpoints. It correlates this data with threat intelligence to identify activities/behaviours that might indicate a malicious presence in your environment.

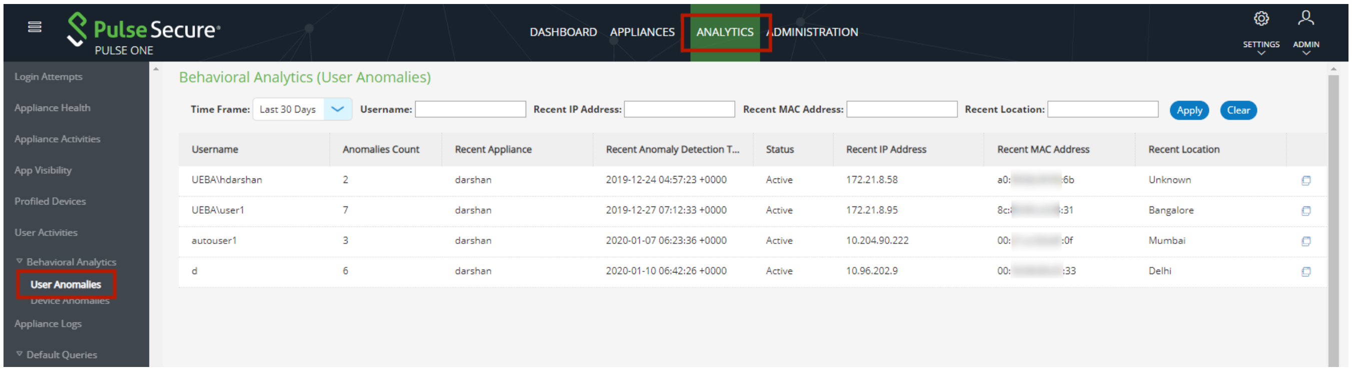
Note: To view UEBA analytics reports, you must install an analytics-enabled license.

Pulse One supports the following analytics reports:

- The Behavioral Analytics (User Anomalies) report.

  To view this report, click the **Analytics** tab, and then click the **User Anomalies** report. For example:

FIGURE 154 Behavioral Analytics User Anomalies Report



Behavioral Analytics (User Anomalies)

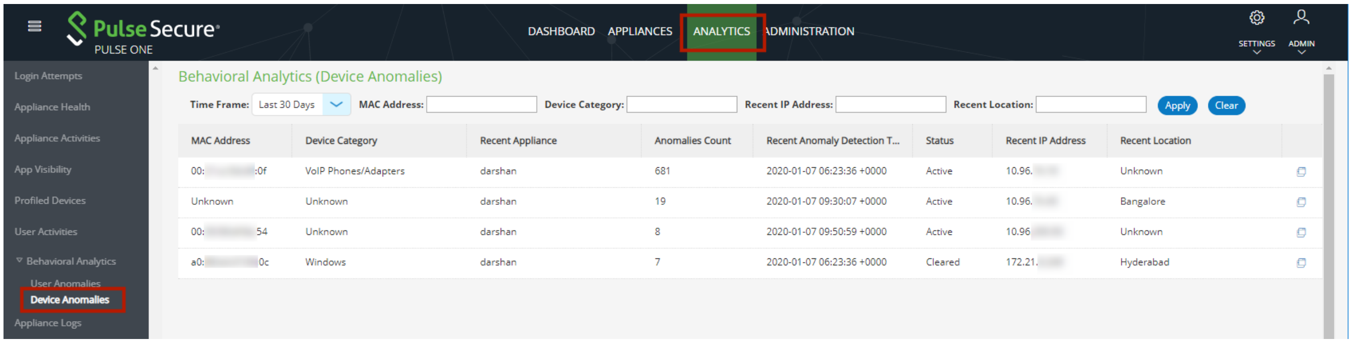
Time Frame: Last 30 Days Username: Recent IP Address: Recent MAC Address: Recent Location:

Username	Anomalies Count	Recent Appliance	Recent Anomaly Detection T...	Status	Recent IP Address	Recent MAC Address	Recent Location
UEBA\hdarshan	2	darshan	2019-12-24 04:57:23 +0000	Active	172.21.8.58	a0:[redacted]6b	Unknown
UEBA\user1	7	darshan	2019-12-27 07:12:33 +0000	Active	172.21.8.95	8c:[redacted]:31	Bangalore
autouser1	3	darshan	2020-01-07 06:23:36 +0000	Active	10.204.90.222	00:[redacted]:0f	Mumbai
d	6	darshan	2020-01-10 06:42:26 +0000	Active	10.96.202.9	00:[redacted]:33	Delhi

- The Behavioral Analytics (Device Anomalies) report.

  To view this report, click the **Analytics** tab, and then click the **User Anomalies** report. For example:

FIGURE 155 Behavioral Analytics Device Anomalies Report



Behavioral Analytics (Device Anomalies)

Time Frame: Last 30 Days MAC Address: Device Category: Recent IP Address: Recent Location:

MAC Address	Device Category	Recent Appliance	Anomalies Count	Recent Anomaly Detection T...	Status	Recent IP Address	Recent Location
00:[redacted]:0f	VoIP Phones/Adapters	darshan	681	2020-01-07 06:23:36 +0000	Active	10.96.[redacted]	Unknown
Unknown	Unknown	darshan	19	2020-01-07 09:30:07 +0000	Active	10.96.[redacted]	Bangalore
00:[redacted]54	Unknown	darshan	8	2020-01-07 09:50:59 +0000	Active	10.96[redacted]	Unknown
a0:[redacted]0c	Windows	darshan	7	2020-01-07 06:23:36 +0000	Cleared	172.21.[redacted]	Hyderabad

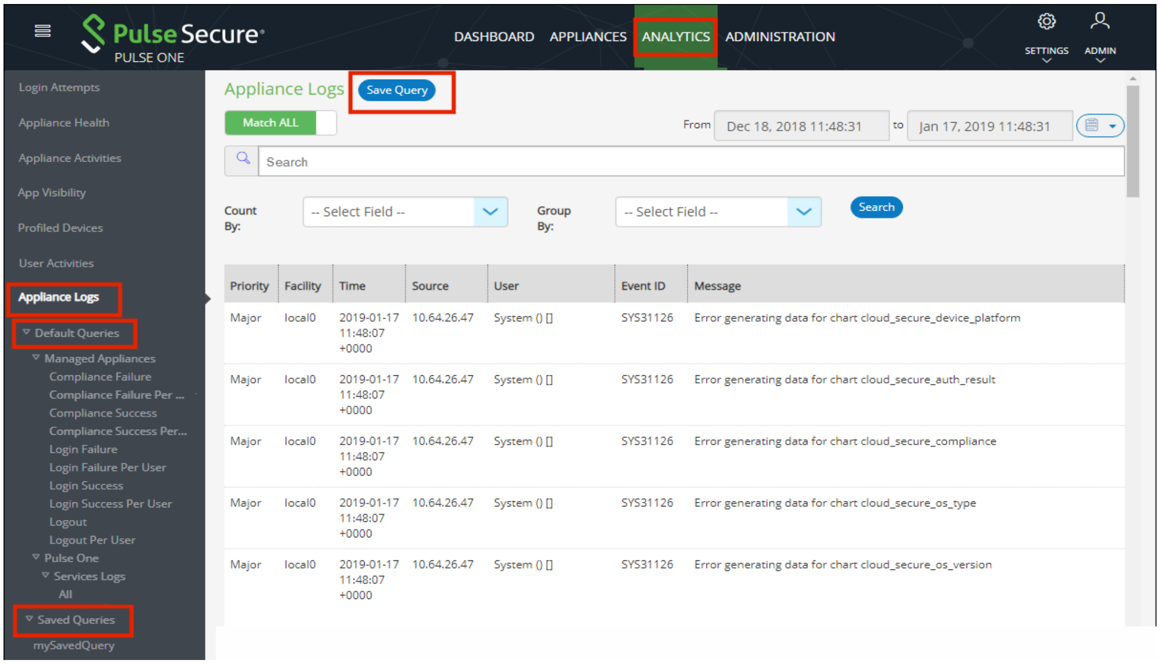
Note: You can also view a dashboard of graphs and maps for UEBA anomalies, see **"Viewing UEBA Metrics" on page 23**.

Viewing Log Aggregation and Analysis

The syslog forwarded from the configured PCS/PPS appliances can be viewed in **Appliance Logs > Default Queries > Managed Appliances**. Here, users have a consolidated view of logs generated by every PPS/PCS appliance that is configured to forward syslogs to the Pulse One server.

Note: To view logs output by Pulse One, see **"Viewing Services Logs" on page 132**.

FIGURE 156 Appliance Logs



From Dec 18, 2018 11:48:31 to Jan 17, 2019 11:48:31

Count By: -- Select Field --

Group By: -- Select Field --

Priority	Facility	Time	Source	User	Event ID	Message
Major	local0	2019-01-17 11:48:07 +0000	10.64.26.47	System () []	SYS31126	Error generating data for chart cloud_secure_device_platform
Major	local0	2019-01-17 11:48:07 +0000	10.64.26.47	System () []	SYS31126	Error generating data for chart cloud_secure_auth_result
Major	local0	2019-01-17 11:48:07 +0000	10.64.26.47	System () []	SYS31126	Error generating data for chart cloud_secure_compliance
Major	local0	2019-01-17 11:48:07 +0000	10.64.26.47	System () []	SYS31126	Error generating data for chart cloud_secure_os_type
Major	local0	2019-01-17 11:48:07 +0000	10.64.26.47	System () []	SYS31126	Error generating data for chart cloud_secure_os_version

The system provides a set of **Appliance Logs > Managed Appliances > Default Queries** in the navigation pane.

To view logs from any of the default queries, expand **Appliance Logs > Default Queries** and click on the required query.

The Administrator can also customize the queries and save them for future use. These customized queries are then listed below **Saved Queries**, see **"Working with Log Queries" on page 131**.

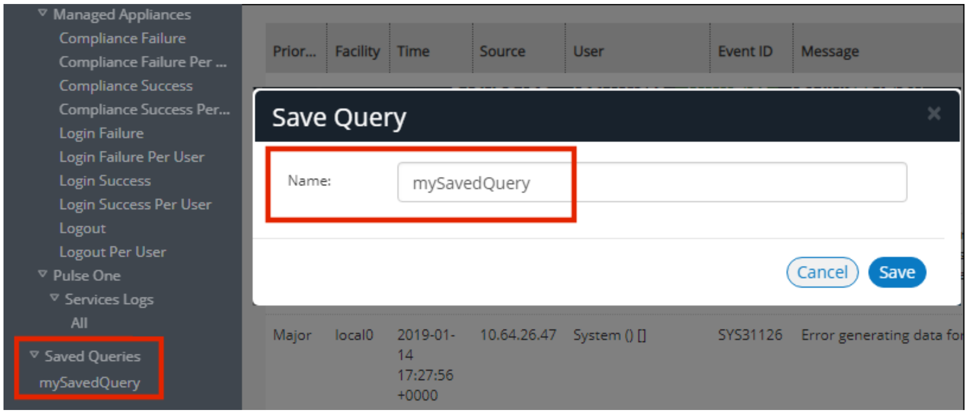
Working with Log Queries

The **Appliance Logs > Default Queries** page supports filtering using a string token. Type the token in the search bar or double-clicking a string in the logs details. The view is then filtered to display all messages with the token that is being searched for. Users can enter multiple tokens separated by space.

This customized query can then be saved using **Save As**.

To view logs from a customized query, expand **Saved Queries** and click on the required query. For example:

FIGURE 157 Save Query



Name: mySavedQuery

Prior...	Facility	Time	Source	User	Event ID	Message
Major	local0	2019-01-14 17:27:56 +0000	10.64.26.47	System () []	SYS31126	Error generating data for

It is also possible to filter the logs by timestamp. This can be done by choosing a **From date** and **To date** in the date fields on the top-right corner of the panel.

Users can also choose to filter search results by **Match All** (which will display search results that have all specified tokens) or **Match Any** (which will display search results that include any of the specified tokens).

The number of search results to be displayed on the screen can be 50, 100, 250, 500 by making a choice on the bottom left corner of the screen. Finally, the search results can span over multiple pages and navigated using the buttons on the bottom right corner of the screen.

Note: Saved queries can be deleted using the **Delete Query** feature.

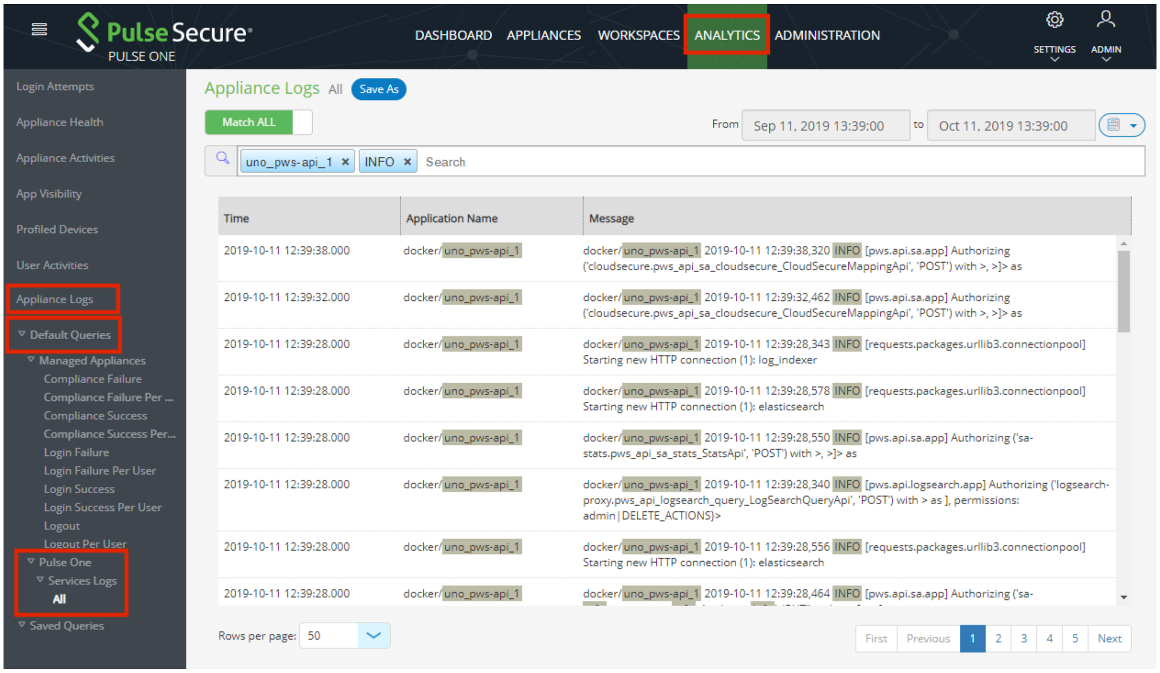
Viewing Services Logs

The logs generated by Pulse One can be viewed in **Appliance Logs > Default Queries > Pulse One > Services Logs**. These log entries fall into two categories:

- Services logs generated by Pulse One.
- Unitycom logs generated by Pulse One.

Note: To view logs output by appliances that are registered on Pulse One, see **"Viewing Log Aggregation and Analysis" on page 130**.

FIGURE 158 Services Logs



From: Sep 11, 2019 13:39:00 to Oct 11, 2019 13:39:00

uno_pws-api_1 × INFO ×

Time	Application Name	Message
2019-10-11 12:39:38.000	docker/uno_pws-api_1	docker/uno_pws-api_1 2019-10-11 12:39:38,320 INFO [pws.api.sa.app] Authorizing ('cloudsecure.pws_api_sa_cloudsecure_CloudSecureMappingApi', 'POST') with >, >]> as
2019-10-11 12:39:32.000	docker/uno_pws-api_1	docker/uno_pws-api_1 2019-10-11 12:39:32,462 INFO [pws.api.sa.app] Authorizing ('cloudsecure.pws_api_sa_cloudsecure_CloudSecureMappingApi', 'POST') with >, >]> as
2019-10-11 12:39:28.000	docker/uno_pws-api_1	docker/uno_pws-api_1 2019-10-11 12:39:28,343 INFO [requests.packages.urllib3.connectionpool] Starting new HTTP connection (1): log_indexer
2019-10-11 12:39:28.000	docker/uno_pws-api_1	docker/uno_pws-api_1 2019-10-11 12:39:28,578 INFO [requests.packages.urllib3.connectionpool] Starting new HTTP connection (1): elasticsearch
2019-10-11 12:39:28.000	docker/uno_pws-api_1	docker/uno_pws-api_1 2019-10-11 12:39:28,550 INFO [pws.api.sa.app] Authorizing ('sa-stats.pws_api_sa_stats_StatsApi', 'POST') with >, >]> as
2019-10-11 12:39:28.000	docker/uno_pws-api_1	docker/uno_pws-api_1 2019-10-11 12:39:28,340 INFO [pws.api.logsearch.app] Authorizing ('logsearch-proxy.pws_api_logsearch_query_LogSearchQueryApi', 'POST') with > as], permissions: admin|DELETE_ACTIONS}>
2019-10-11 12:39:28.000	docker/uno_pws-api_1	docker/uno_pws-api_1 2019-10-11 12:39:28,556 INFO [requests.packages.urllib3.connectionpool] Starting new HTTP connection (1): elasticsearch
2019-10-11 12:39:28.000	docker/uno_pws-api_1	docker/uno_pws-api_1 2019-10-11 12:39:28,464 INFO [pws.api.sa.app] Authorizing ('sa-

Rows per page: 50

The system provides **Default Queries > Pulse One > Services Logs** in the navigation pane.

To view logs from any of the default queries, expand **Service Logs > Default Queries** and click on the required query.

The Administrator can also create custom queries and save them for future use. These customized queries are then listed below **Saved Queries**, see **"Working with Log Queries" on page 131**.

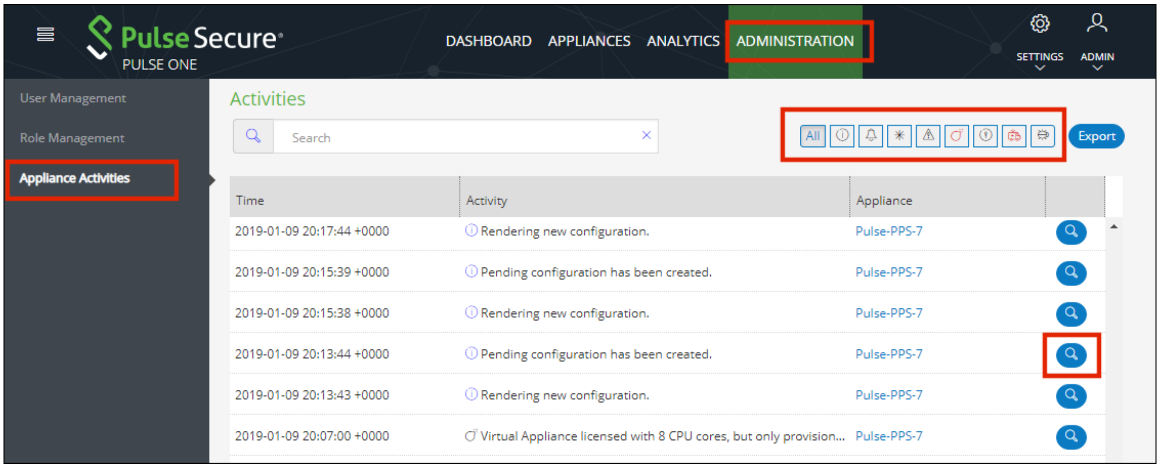
Viewing Appliance Activities

The **Appliance Activities** page displays information about the events registered in the Management Server. You can view filtered activities for appliances.

To view appliance activities:

1. Select the **Administration** tab
2. Click **Appliance Activities.**
3. Click an **Event Type** button to filter for a specific event type.

FIGURE 159 Filter Activities

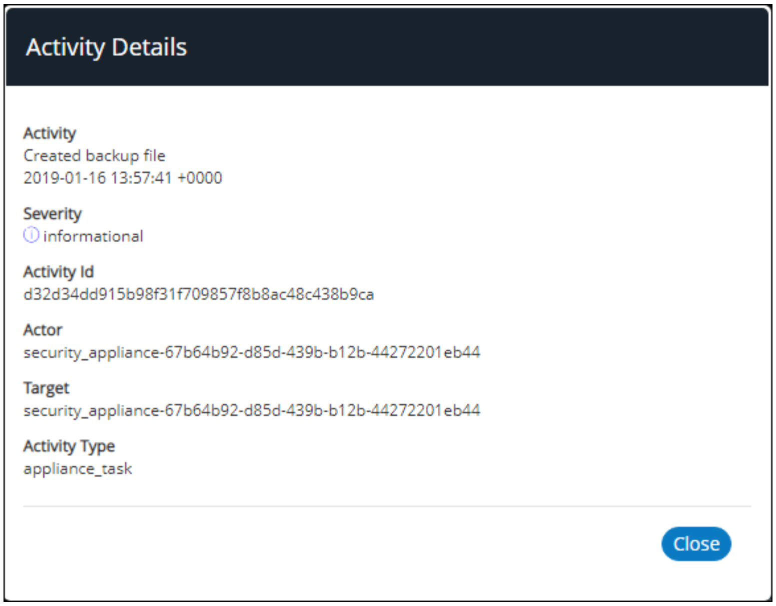


Time	Activity	Appliance
2019-01-09 20:17:44 +0000	Rendering new configuration.	Pulse-PPS-7
2019-01-09 20:15:39 +0000	Pending configuration has been created.	Pulse-PPS-7
2019-01-09 20:15:38 +0000	Rendering new configuration.	Pulse-PPS-7
2019-01-09 20:13:44 +0000	Pending configuration has been created.	Pulse-PPS-7
2019-01-09 20:13:43 +0000	Rendering new configuration.	Pulse-PPS-7
2019-01-09 20:07:00 +0000	Virtual Appliance licensed with 8 CPU cores, but only provision...	Pulse-PPS-7

4. Click the **Details** button associated with the activity you want to view the details.

   The **Activity Details** dialog displays the additional details.

FIGURE 160 Activity Details



Activity Details

Activity
Created backup file
2019-01-16 13:57:41 +0000

Severity
informational

Activity Id
d32d34dd915b98f31f709857f8b8ac48c438b9ca

Actor
security_appliance-67b64b92-d85d-439b-b12b-44272201eb44

Target
security_appliance-67b64b92-d85d-439b-b12b-44272201eb44

Activity Type
appliance_task

User Management

Adding an Admin User

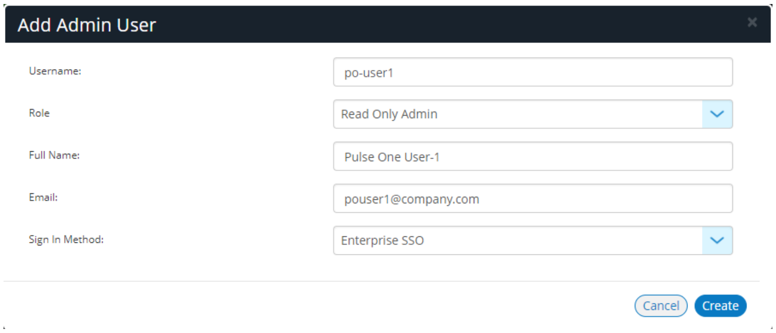
To add an admin user:

1. Select the **Administration** tab.
2. Select **User Management**.

   A list of existing admin users is displayed.
3. Click **Add User** to add an admin user.

   The **Add Admin User** window appears.

   FIGURE 161 Add Admin User

   Add Admin User

   Username: po-user1

   Role: Read Only Admin

   Full Name: Pulse One User-1

   Email: pouser1@company.com

   Sign In Method: Enterprise SSO

   Note: If Role is set to **Read Only Admin**, then the user will not be given the permissions to create/ update/ delete functions.
4. In the Add Admin User window, enter the **Username**, **Full Name** and **Email** for the user.
5. Select a **Role** from the drop-down list:
   - *Super Admin* - This role has full access to the admin console. Super admin can create other admins.
   - *Read Only Admin* - This role has read-only access to the entire system. Read-only admin can view dashboard and report, perform search function, and run pre-defined queries.

6. Select a Sign in Method. Either:

    - Select **Enterprise SSO** if the same user ID exists on both Pulse One (Service Provider) and the Pulse Connect Secure (Identity Provider), OR

    - Select **Local Authentication**.

7. Click **Create**. The new user is displayed in the list of users.

Editing User Details

To modify a user's details:

1. Select the **Administration** tab.

2. Select **User Management**.

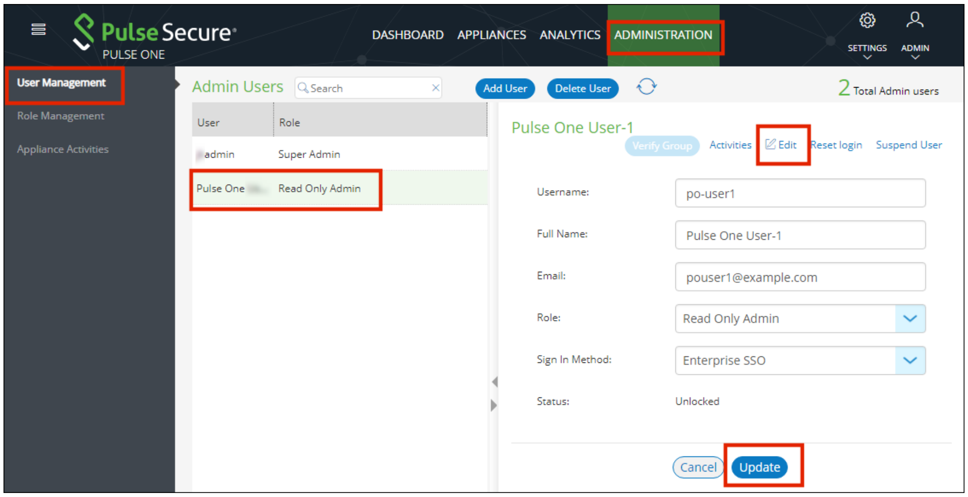
    A list of existing admin users is displayed.

3. Select the user from the list.

4. In the user details panel click the **Edit** icon and make the required changes.

5. Click **Update**.

FIGURE 162 Edit User Details



User	Role
[redacted]admin	Super Admin
Pulse One [redacted]	Read Only Admin

Username: po-user1

Full Name: Pulse One User-1

Email: pouser1@example.com

Role: Read Only Admin

Sign In Method: Enterprise SSO

Status: Unlocked

Removing an Admin User

To remove an admin user:

1. Select the **Administration** tab.
2. Select **User Management**.

   A list of existing admin users is displayed.
3. Select the user from the list.
4. Click **Delete User**.
5. In the **Remove Admin User** confirmation message box, click **OK**.

   The user is removed as an administrator.

Resetting a User Password

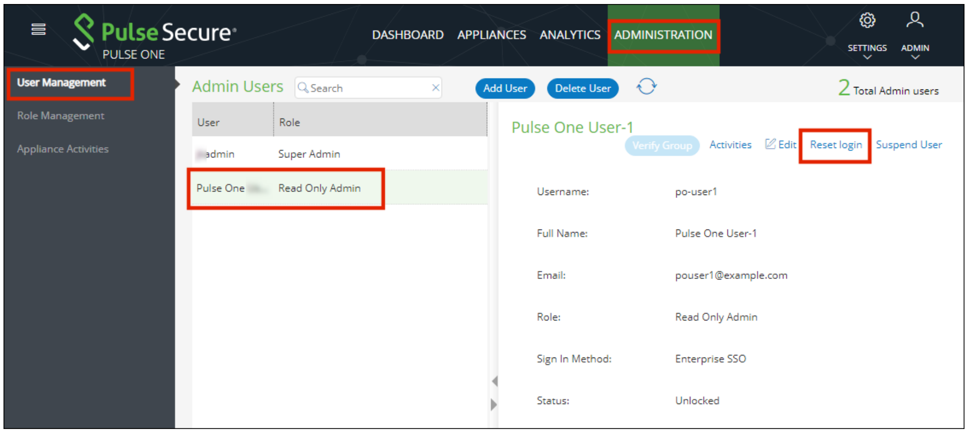
To reset a user's password:

1. Select the user from the list.
2. Click the **Reset login** link in the user details pane.

   An email that contains the **Set new password** link will be sent to the registered email address.
3. Click the **Set new password** link in the email.
4. In the Pulse One page that appears, provide the new password and confirm the new password. The new password will be saved in the database.
5. Then log in to Pulse One with the new password.

   Note: The **Set new password** link that you received in the email has an expiration time of 1 hour. Beyond this time, you should make a new request for setting the new password.

   FIGURE 163 Reset Login



User	Role
[redacted]admin	Super Admin
Pulse One [redacted]	Read Only Admin

Username: po-user1

Full Name: Pulse One User-1

Email: pouser1@example.com

Role: Read Only Admin

Sign In Method: Enterprise SSO

Status: Unlocked

Suspending a User

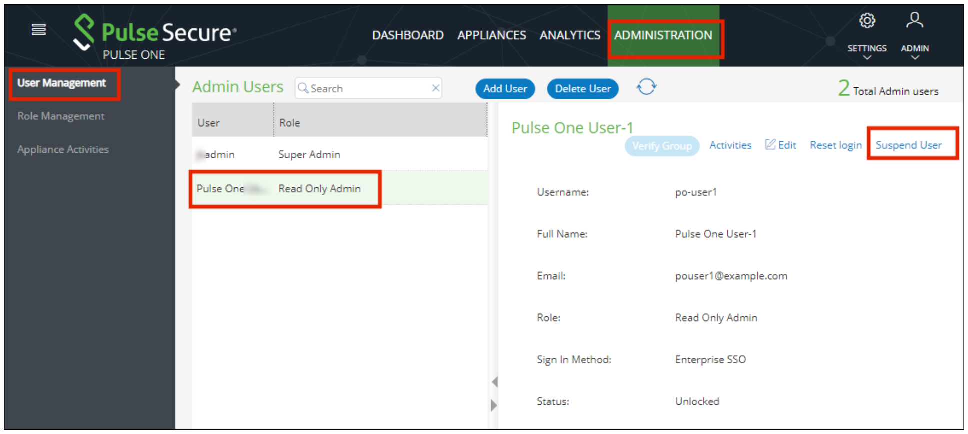
To suspend an admin user:

1. Select the user from the list.
2. Click **Suspend User**.

   The user will be locked and will not be able to log in.

   The **Forgot Password** option in the **Login** page will not send email to reset the password.
3. (Optional) To unlock the suspended user, select the user and click **Reset Login**. This will send a mail to the user with a set new password link.

FIGURE 164 Suspend User



User	Role
[redacted]admin	Super Admin
Pulse One [redacted]	Read Only Admin

Username: po-user1

Full Name: Pulse One User-1

Email: pouser1@example.com

Role: Read Only Admin

Sign In Method: Enterprise SSO

Status: Unlocked

Role Management

Adding an Admin Defined Role

To add a new admin-defined role:

1. Select the **Administration** tab.

2. Select **Role Management**.

3. Click **Add Role** to add a new admin-defined role.

   Note: To create a role from an existing role, click **Duplicate** corresponding to the existing role.

4. In the **Create New Role** window, enter the role name.

5. In the **Role Assignment** section, select the permissions for *Dashboard*, *Appliances*, *Settings*, *Users*, and *Roles* from the drop-down list.

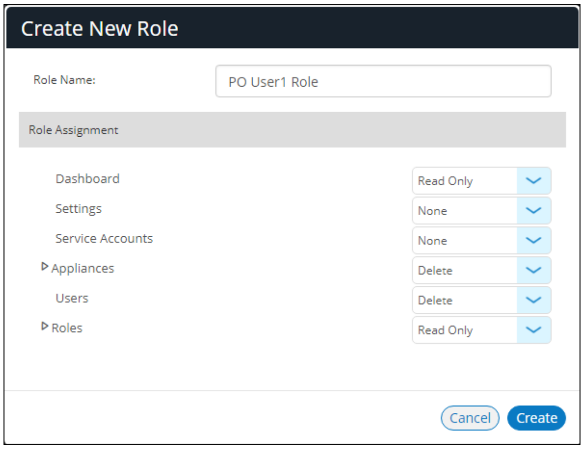
   - *None* - This permission disables the assigned feature. For example, if the *Appliances* permission is set to *None*, then **Appliances** page will not be visible in Pulse One console for this role.

   - *Read Only* - This permission will disable create/edit/delete options for the assigned feature.

   - *Edit* - This permission allows create/view/edit operations.

   - *Delete* - This permission allows all operations.

   FIGURE 165 Create New Role



Create New Role

Role Name: PO User1 Role

Role Assignment

Dashboard	Read Only
Settings	None
Service Accounts	None
▷ Appliances	Delete
Users	Delete
▷ Roles	Read Only

6. Click **Create**.

Editing an Admin Role

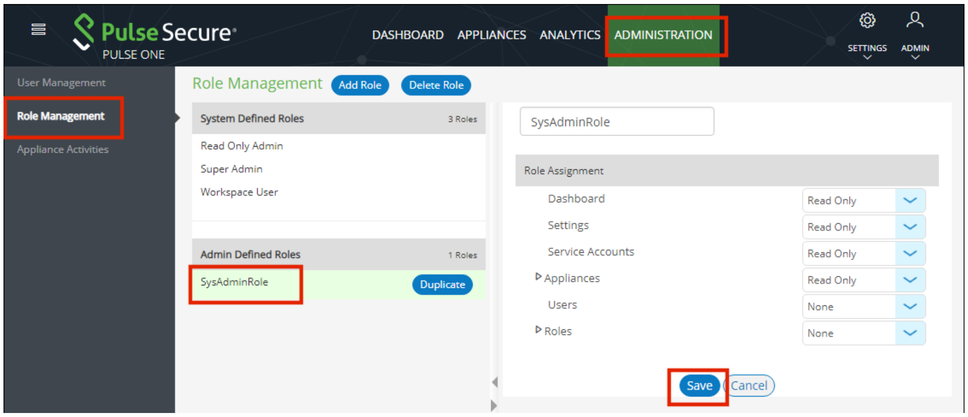
You can modify only the admin defined roles.

To modify a role's permissions:

1. Select the **Administration** tab.
2. Select **Role Management**.

   A list of system defined roles is displayed.
3. Select the role from the list.
4. In the role details pane, click **Edit**.
5. Make the required changes and click **Save**.

FIGURE 166 Modify Role



SysAdminRole

Role Assignment	
Dashboard	Read Only
Settings	Read Only
Service Accounts	Read Only
Appliances	Read Only
Users	None
Roles	None

Removing an Admin Role

You can remove only the admin defined roles.

To remove an admin defined role:

1. Select the **Administration** tab.
2. Select **Role Management**.

   A list of system defined roles is displayed.
3. Select the role from the list and click **Delete Role**.

   In the Confirmation message box, click **Yes** to remove the selected role.

Working With Pulse One Properties

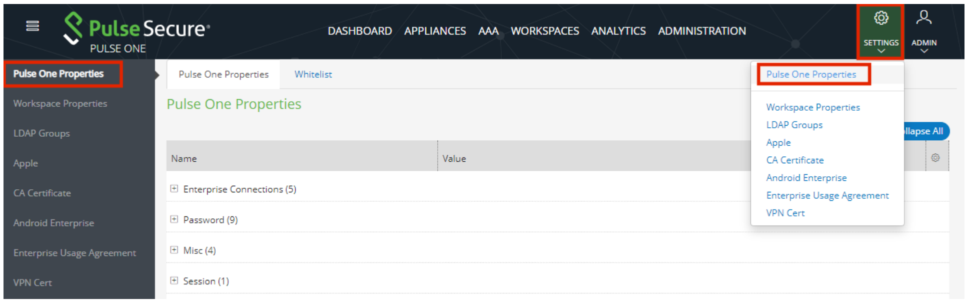
Viewing Pulse One Properties

To open the **Pulse One Properties** page:

1. Click the **Settings** icon on top-right-corner of the page.
2. Select **Pulse One Properties**.

   The **Pulse One Properties** page appears.

FIGURE 167 Pulse One Properties



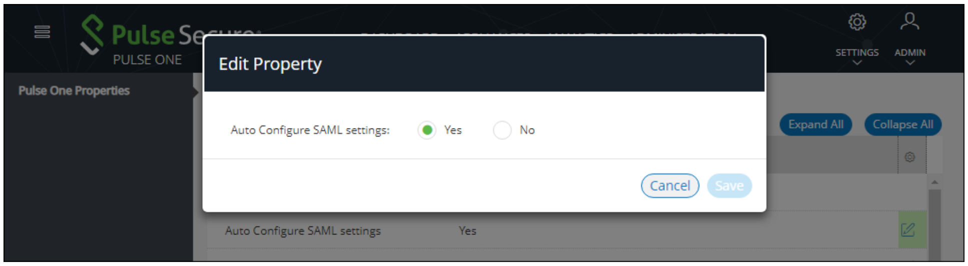
Name	Value
⊞ Enterprise Connections (5)	
⊞ Password (9)	
⊞ Misc (4)	
⊞ Session (1)	

Editing Pulse One Properties

To edit a Pulse One property:

1. View Pulse One properties, see Viewing Pulse One Properties<XREF>.
2. Click the **Edit** (✎ button corresponding to the field you want to edit.
3. Change the value and then click **Save**. For example:

FIGURE 168 Edit Properties



Auto Configure SAML settings: ● Yes ○ No

Auto Configure SAML settings Yes

Understanding Pulse One Properties

All Pulse One properties are described in the following sections:

- **"Enterprise Connection Properties" on page 142**
- **"Password Properties" on page 142**
- **"Miscellaneous Properties" on page 143**
- **"Session Properties" on page 143**

Enterprise Connection Properties

The **Enterprise Connections** settings are described below:

- **Auto Configure SAML Settings** – Boolean. If *True*, Pulse One automates the SAML Metadata configuration flow for both Appliance and Pulse One SAML settings.
- **Create Users and Roles from SAML** – Boolean. If *True*, a Pulse One user is created automatically whenever a user from a linked SAML idP (PCS) authentication server logs into Pulse One for the first time using Enterprise SSO.

  Note: Further configuration is required to use this feature, see **"Automatically Creating Pulse One Users for SAML SSO Logins" on page 158**.
- **SAML Identity Provider** – The Pulse Connect Secure appliance that is configured for Pulse One server SAML auto-provisioning.
- **SAML Identity Provider Metadata** – Required metadata for the SAML identity provider.
- **SAML Service Provider Metadata**– Required metadata for the SAML service provider.

Password Properties

The **Password** settings are described below:

- **Console Minimum Password Length** – The minimum length of a console password.
- **Console Password Expiration Days** – The number of days after which an Administrator must change their console password.
- **Console Password Require Lowercase** – Boolean. If *True*, the console password must contain at least one lowercase letter.
- **Console Password Require Number** – Boolean. If *True*, the console password must contain at least one number.
- **Console Password Require Special** – Boolean. If *True*, the console password must contain at least one special character.

- **Console Password Require Uppercase** – Boolean. If *True*, the console password must contain at least one uppercase letter.
- **Console Password Reset Timeout Hours** – The number of hours a console password reset email link is valid.
- **Domain Allowed Password Attempts** – The number of login attempts until a console account is locked.
- **Welcome Timeout Hours** –The number of hours a registration token in a welcome email is valid.

Miscellaneous Properties

The miscellaneous (**Misc**) settings are described below:

- **Created On** – The date on which the management console was created.
- **Locale** – The console language code.
- **Page Footer** – The footer information that will be displayed at the bottom of the admin console.
- **Server Version** – The current Management Server version that will be displayed at the bottom of the admin console.

Note: You cannot edit the **Created On** and **Server Version** properties.

Session Properties

The Session properties are described below:

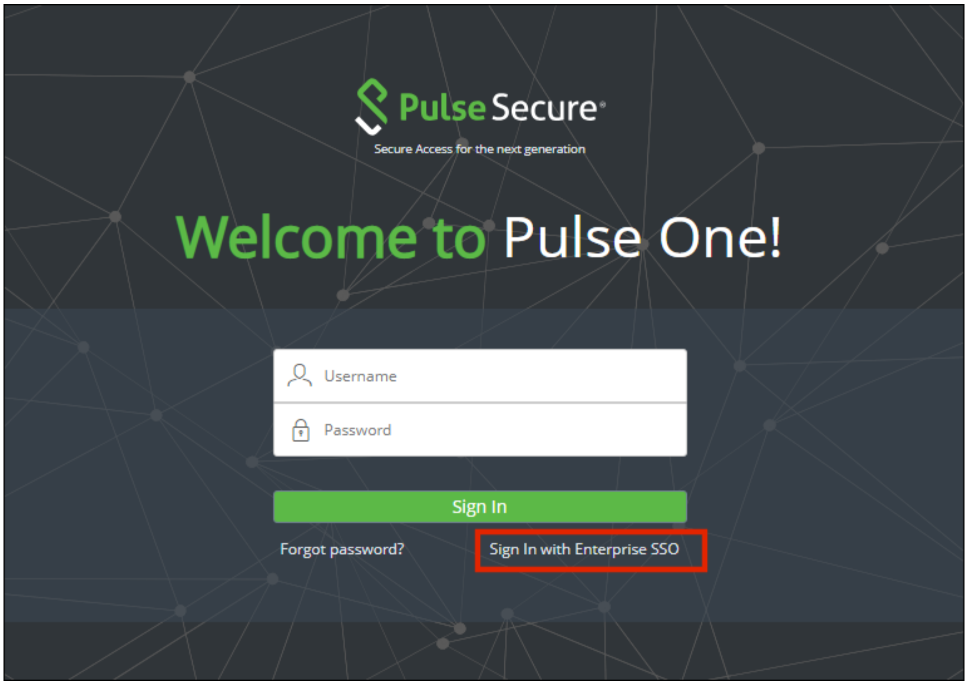
- **Session idle timeout (minutes)** – The timeout for an idle session. After this timeout is reached, the user is logged out automatically. The default is *20*.

Configuring Enterprise SSO Using SAML

Overview

By setting up Enterprise Single Sign On (SSO) with SAML, Enterprise users can sign into Pulse One by delegating authentication to their Pulse Connect Secure appliance.

FIGURE 169 Sign In with Enterprise SSO



If your authentication is performed by a PCS appliance at v8.3r1 or later, many of the configuration steps are automated. You must perform the following processes:

- **"Configuring SAML idP in Pulse Connect Secure Server" on page 146**.
- **"Automatically Configuring a SAML idP on Pulse One" on page 150**.
- (Optional) **"Automatically Creating Pulse One Users for SAML SSO Logins" on page 158**.
- **"Testing Sign In with Enterprise SSO" on page 160**.

If your authentication is performed by a PCS appliance that is earlier than v8.3r1, you must perform all stages of the following manual processes:

- **"Configuring SAML idP in Pulse Connect Secure Server" on page 146**.
- **"Configuring a Metadata Provider in Pulse Connect Secure" on page 152**.
- **"Enabling Enterprise SSO in Pulse One Appliance" on page 153**.
- **"Configuring SAML Metadata in Pulse One" on page 153**.
- **"Adding SAML SP Metadata in Pulse Connect Secure Server" on page 154**.
- (Optional) **"Automatically Creating Pulse One Users for SAML SSO Logins" on page 158**.
- **"Testing Sign In with Enterprise SSO" on page 160**.

Configuring SAML idP in Pulse Connect Secure Server

Note: This section is required for all PCS appliance versions.

This section provides the steps to configure a SAML Identity Provider on Pulse Connect Secure server.

Before proceeding with the configuration, ensure that the Pulse Connect Secure appliance that you intend to use as the Identity Provider is registered with Pulse One, see **"Registering an Existing PCS/PPS Appliance" on page 33**.

Note: If the PCS server is already configured as a SAML identity provider, make sure that POST binding is enabled and the **Accept Unsigned AuthnRequest** option is selected.

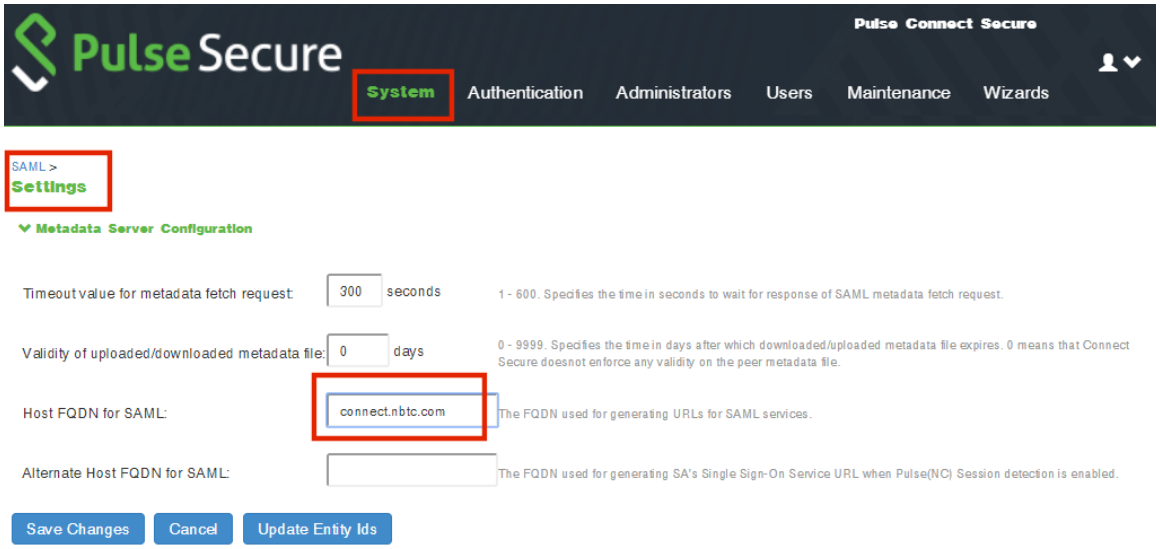
To configure SAML IdP on the Pulse Connect Secure server:

1. Log in to the Pulse Connect Secure server that is identified as an Identity Provider.
2. Navigate to **System > Configuration > SAML > Settings**.

3. Configure the following Metadata Server Configuration:

    - **Timeout value for metadata fetch request** to *300*.
    - **Host FQDN for SAML** to the Fully Qualified Domain Name, noting the host FQDN guidance below.

FIGURE 170 SAML Settings



Timeout value for metadata fetch request: 300 seconds — 1 - 600. Specifies the time in seconds to wait for response of SAML metadata fetch request.

Validity of uploaded/downloaded metadata file: 0 days — 0 - 9999. Specifies the time in days after which downloaded/uploaded metadata file expires. 0 means that Connect Secure doesnot enforce any validity on the peer metadata file.

Host FQDN for SAML: connect.nbtc.com — The FQDN used for generating URLs for SAML services.

Alternate Host FQDN for SAML: — The FQDN used for generating SA's Single Sign-On Service URL when Pulse(NC) Session detection is enabled.

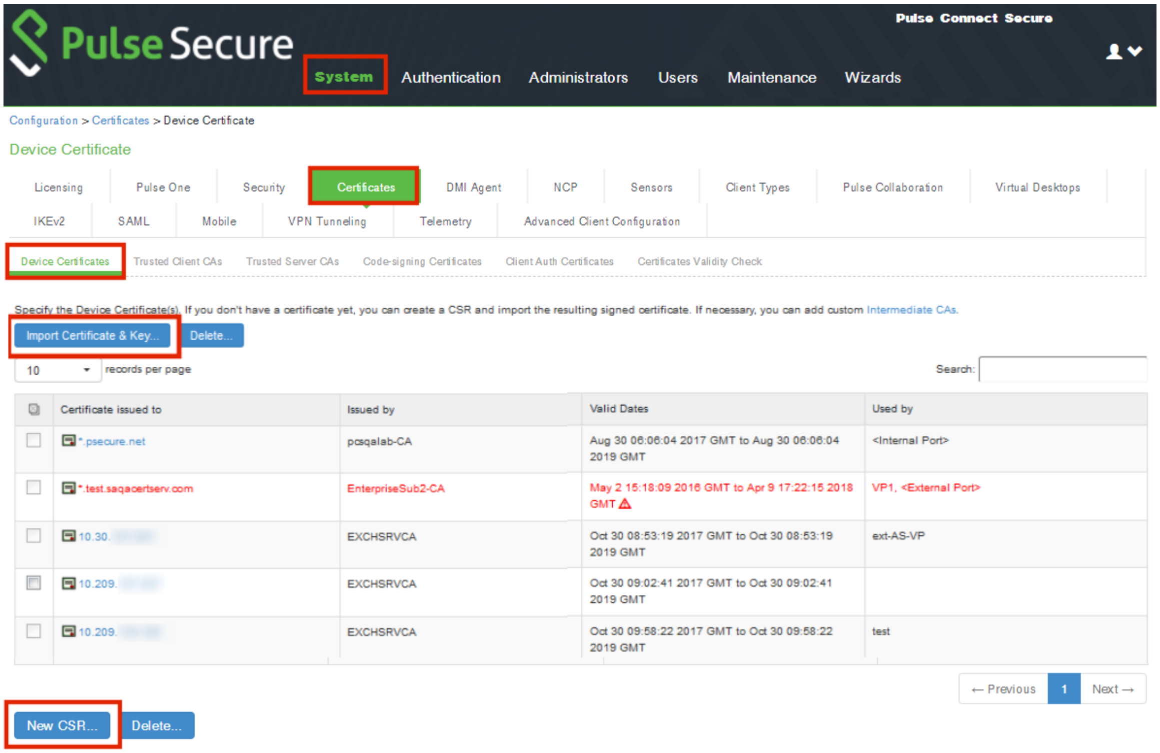
The host FQDN specified here is used in the SAML entity ID, used by browsers to connect to PCS, and used in the URLs for SAML services. Typically:

- If the PCS is standalone, the FQDN should resolve to the IP address of the external interface / internal interface, whichever is chosen.
- If the PCS is an Active-Passive cluster, the FQDN should resolve to the external VIP / Internal VIP, whichever is chosen.
- If the PCS is an Active-Active cluster behind an in-line load balancer, the FQDN should resolve to the load balancer's external VIP / Internal VIP, whichever is chosen.

4. Click **Save Changes**.

5. Navigate to **System > Configuration > Certificates > Device Certificate**, create a new CSR, and import certificate and keys. Skip this step if the PCS external interface / internal interface (whichever is chosen) already provides a certificate that matches the host's Fully Qualified Domain Name.

FIGURE 171 Import Certificate and Keys



Configuration > Certificates > Device Certificate

Device Certificate

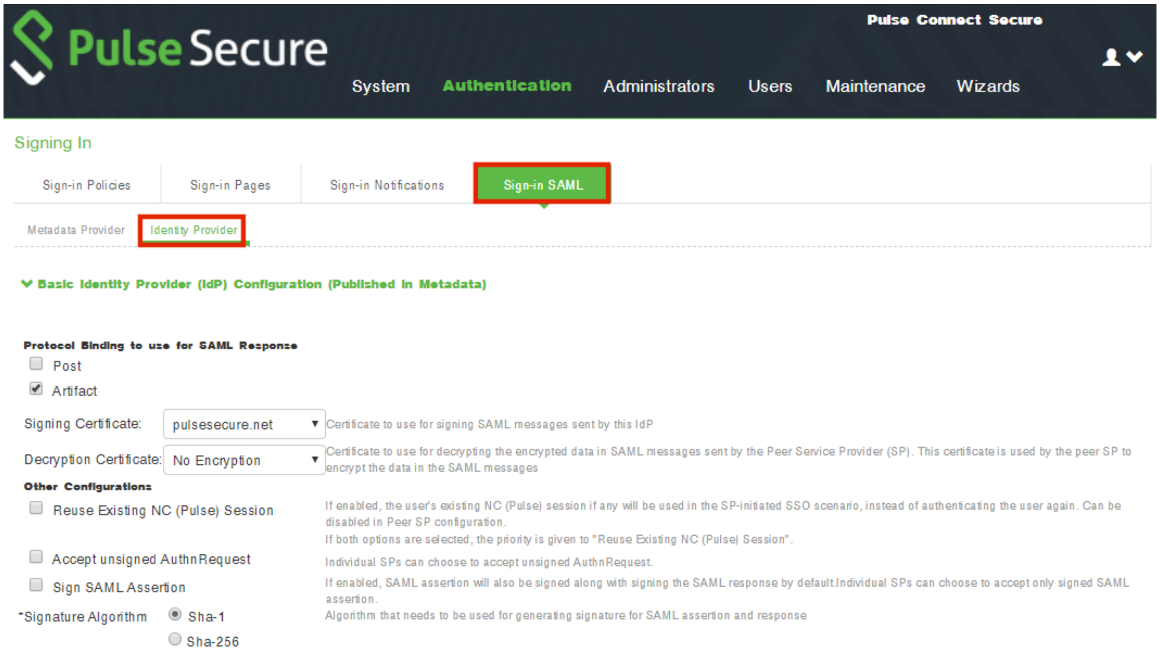
Specify the Device Certificate(s). If you don't have a certificate yet, you can create a CSR and import the resulting signed certificate. If necessary, you can add custom Intermediate CAs.

□	Certificate issued to	Issued by	Valid Dates	Used by
□	*.psecure.net	pcsqalab-CA	Aug 30 06:06:04 2017 GMT to Aug 30 06:06:04 2019 GMT	<Internal Port>
□	*.test.saqacertserv.com	EnterpriseSub2-CA	May 2 15:18:09 2016 GMT to Apr 9 17:22:15 2018 GMT ⚠	VP1, <External Port>
□	10.30.[redacted]	EXCHSRVCA	Oct 30 08:53:19 2017 GMT to Oct 30 08:53:19 2019 GMT	ext-AS-VP
□	10.209.[redacted]	EXCHSRVCA	Oct 30 09:02:41 2017 GMT to Oct 30 09:02:41 2019 GMT	
□	10.209.[redacted]	EXCHSRVCA	Oct 30 09:58:22 2017 GMT to Oct 30 09:58:22 2019 GMT	test

6. Navigate to **Authentication > Signing In > Sign In SAML > Identity Provider**.

7. Locate the the **Basic Identity Provider (idP) Configuration** section. For example:

FIGURE 172 Basic Identity Provider Configuration



Basic Identity Provider (IdP) Configuration (Published in Metadata)

Protocol Binding to use for SAML Response

□ Post
☑ Artifact

Signing Certificate: pulsesecure.net — Certificate to use for signing SAML messages sent by this IdP

Decryption Certificate: No Encryption — Certificate to use for decrypting the encrypted data in SAML messages sent by the Peer Service Provider (SP). This certificate is used by the peer SP to encrypt the data in the SAML messages

Other Configurations

□ Reuse Existing NC (Pulse) Session — If enabled, the user's existing NC (Pulse) session if any will be used in the SP-initiated SSO scenario, instead of authenticating the user again. Can be disabled in Peer SP configuration.
If both options are selected, the priority is given to "Reuse Existing NC (Pulse) Session".

□ Accept unsigned AuthnRequest — Individual SPs can choose to accept unsigned AuthnRequest.

□ Sign SAML Assertion — If enabled, SAML assertion will also be signed along with signing the SAML response by default.Individual SPs can choose to accept only signed SAML assertion.

*Signature Algorithm ● Sha-1 ○ Sha-256 — Algorithm that needs to be used for generating signature for SAML assertion and response

8. In the **Basic Identity Provider (idP) Configuration** section, do the following:

   - Select the **Post** check box for protocol binding to use for SAML response.

     Note: If the PCS server is already configured as a SAML identity provider, make sure that POST binding is enabled and the **Accept Unsigned AuthnRequest** option is selected.

   - Select a **Signing Certificate** from the list.
   - For **Decryption Certificate**, select *No Encryption*.
   - Clear the **Reuse Existing NC (Pulse) Session** check box.
   - Select the **Accept Unsigned AuthnRequest** check box.

   For more details, refer to the "Configuring Sign-in SAML Identity Provider Settings" section in the *Pulse Connect Secure Administration Guide*.

9. Click **Save Changes** to save the Identity Provider configuration.

Automatically Configuring a SAML idP on Pulse One

Note: This section is only applicable if your PCS appliance is at v8.3r1 or later. If your PCS is at an earlier release, you must perform a number of manual processes, see **"Overview" on page 145**.

To automatically configure a SAML idP, you must have already completed the following tasks:

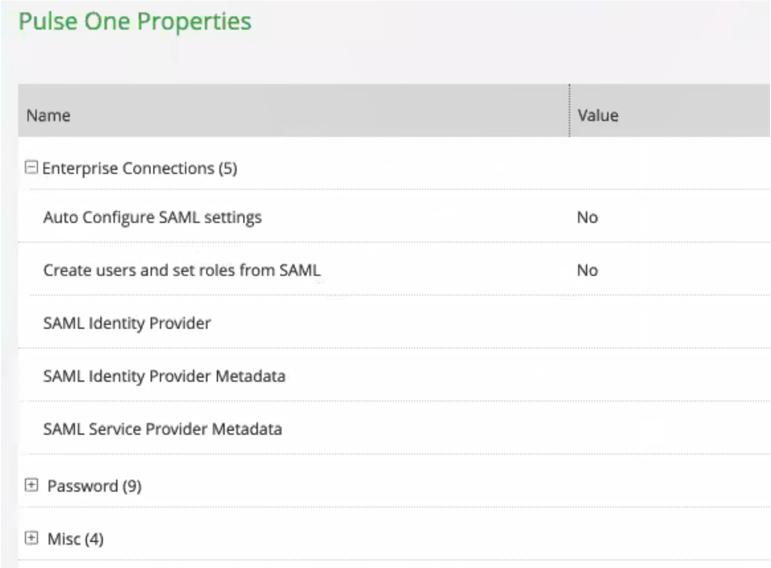
- Registered the Pulse Connect Secure appliance that you intend to use as the SAML idP with Pulse One, see **"Registering an Existing PCS/PPS Appliance" on page 33**.
- Configured the SAML idP on Pulse Connect Secure, see **"Configuring SAML idP in Pulse Connect Secure Server" on page 146**.

To auto-configure the SAML idP:

1. Log into Pulse One as an administrator.
2. Click the **Settings** icon on top-right-corner of the page.
3. Select **Pulse One Properties**.

   The **Pulse One Properties** page appears.
4. Expand the *Enterprise Connections* group to view its properties. For example:

   FIGURE 173 Pulse One Properties Enterprise Connections



Pulse One Properties

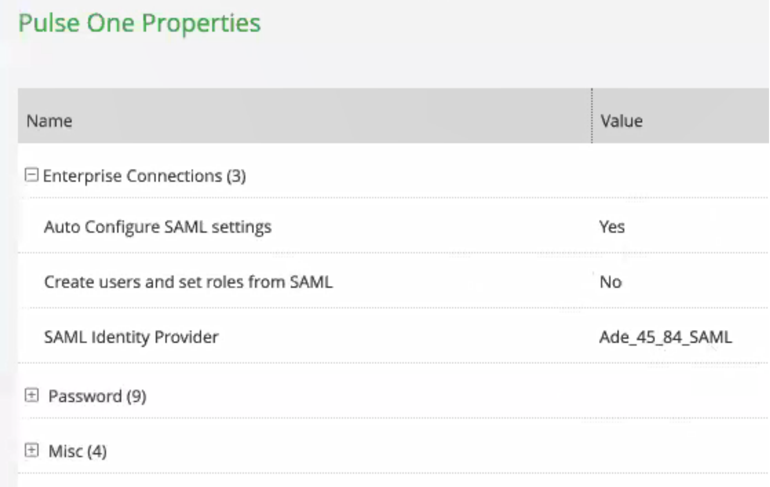
Name	Value
⊟ Enterprise Connections (5)	
Auto Configure SAML settings	No
Create users and set roles from SAML	No
SAML Identity Provider	
SAML Identity Provider Metadata	
SAML Service Provider Metadata	
⊞ Password (9)	
⊞ Misc (4)	

5. Set the **Auto Configure SAML Properties** property to *Yes*.

   Note: When you set **Auto Configure SAML Properties** to *Yes*, the **SAML Identity Provider Metadata** and the **SAML Service Provider Metadata** properties are removed. These are not required when auto-configuration is enabled.

6. Set the **SAML Identity Provider** property to match the appliance name, as registered on Pulse One. For example:

FIGURE 174 Pulse One Properties Configure Auto SAML



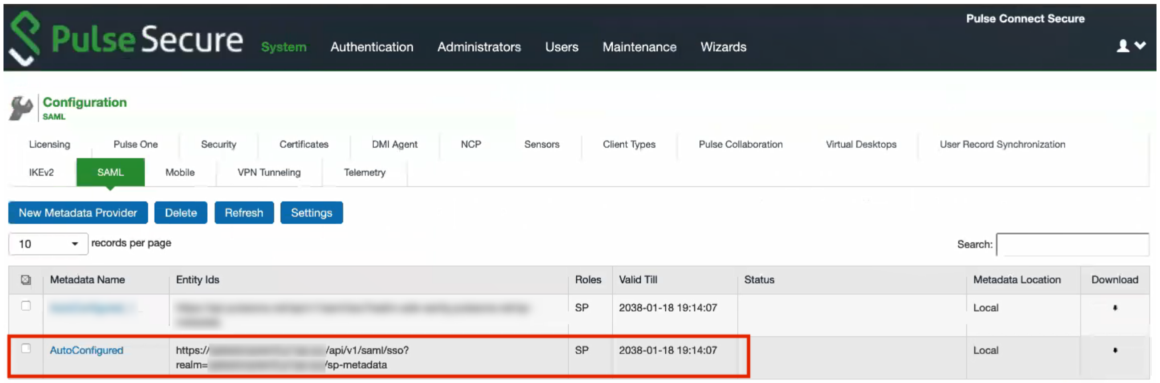
Pulse One Properties

Name	Value
⊟ Enterprise Connections (3)	
Auto Configure SAML settings	Yes
Create users and set roles from SAML	No
SAML Identity Provider	Ade_45_84_SAML
⊞ Password (9)	
⊞ Misc (4)	

After this process is complete, auto-configuration of the SAML idP will be performed.

7. (Optional) To confirm the auto-configuration of the SAML idP, log into Pulse Connect Secure and access the **System > Configuration > SAML** settings page. There will now be a **Metadata Name** called *AutoConfigured*. For example:

FIGURE 175 Pulse Connect Secure SAML Auto-configuration



☒	Metadata Name	Entity Ids	Roles	Valid Till	Status	Metadata Location	Download
□	[redacted]	[redacted]	SP	2038-01-18 19:14:07		Local	•
□	AutoConfigured	https://[redacted]/api/v1/saml/sso? realm=[redacted]/sp-metadata	SP	2038-01-18 19:14:07		Local	•

The auto-configuration of the SAML idP is complete.

You can then either:

- Continue with an optional activity **“Automatically Creating Pulse One Users for SAML SSO Logins” on page 158**.
- Move directly to testing the SSO login, see **“Testing Sign In with Enterprise SSO” on page 160**.

Configuring a Metadata Provider in Pulse Connect Secure

Note: You do not have to perform the process in the section if your appliance is at v8.3r1 or later, and you have already performed auto-configuration of SAML, see **“Automatically Configuring a SAML idP on Pulse One” on page 150**.

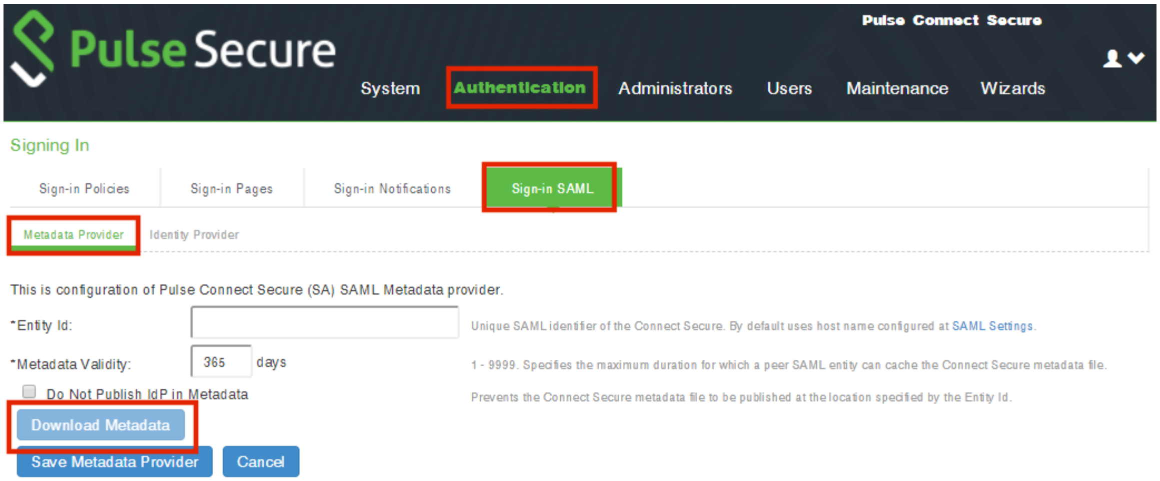
This section provides the steps to configure Metadata Provider on Pulse Connect Secure.

Note: If the PCS server is already configured to operate as a SAML IdP, skip the steps 2 to 6.

To configure a Metadata Provider in the PCS server:

1. Log in to Pulse Connect Secure server.
2. Navigate to **Authentication > Signing-In > Sign In SAML > Metadata Provider**.
3. The SAML Metadata Provider **Entity Id** property is pre-populated. It is generated by the system, based on the value for the **Host FQDN for SAML** setting on the **System > Configuration > SAML > Settings** page.
4. Set **Metadata Validity** to *365* days.
5. Clear the **Do Not Publish IdP in Metadata** check box.
6. Click **Save Metadata Provider**.
7. Click **Download Metadata** and save the file to your computer.

FIGURE 176 Metadata Provider



This is configuration of Pulse Connect Secure (SA) SAML Metadata provider.

*Entity Id: Unique SAML identifier of the Connect Secure. By default uses host name configured at SAML Settings.

*Metadata Validity: 365 days 1 - 9999. Specifies the maximum duration for which a peer SAML entity can cache the Connect Secure metadata file.

□ Do Not Publish IdP in Metadata Prevents the Connect Secure metadata file to be published at the location specified by the Entity Id.

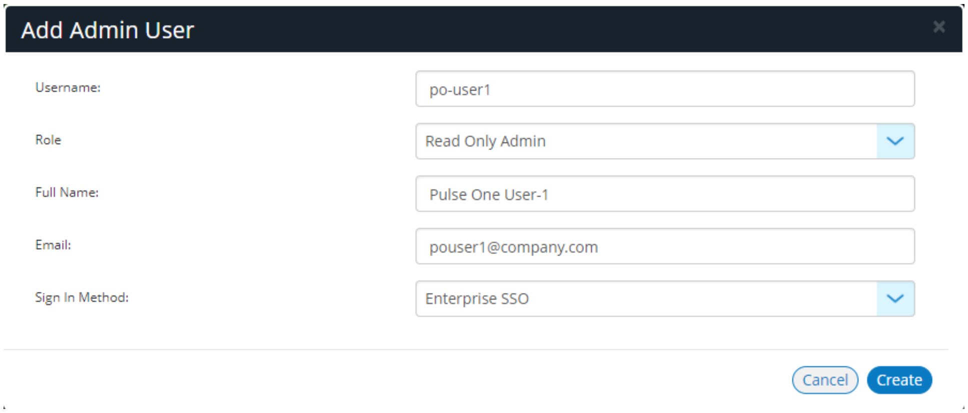
Enabling Enterprise SSO in Pulse One Appliance

Note: You do not have to perform the process in the section if your appliance is at v8.3r1 or later, and you have already performed auto-configuration of SAML, see **"Automatically Configuring a SAML idP on Pulse One" on page 150**.

To enable Enterprise SSO:

1. Log into Pulse One as an administrator.
2. Select the **Administration** tab.
3. Select **User Management**.
4. In the **User Management** page, add (or edit) all the admin users who need to use Enterprise SSO by setting their corresponding **Sign In Method** to *Enterprise SSO*. For example:

FIGURE 177 Sign In Method



Add Admin User

Username: po-user1

Role: Read Only Admin

Full Name: Pulse One User-1

Email: pouser1@company.com

Sign In Method: Enterprise SSO

Note: To use Enterprise SSO login, the same user identity (username) must exist on both Pulse One (Service Provider) and the Identity Provider (Pulse Connect Secure).

Configuring SAML Metadata in Pulse One

Note: You do not have to perform the process in the section if your appliance is at v8.3r1 or later, and you have already performed auto-configuration of SAML, see **"Automatically Configuring a SAML idP on Pulse One" on page 150**.

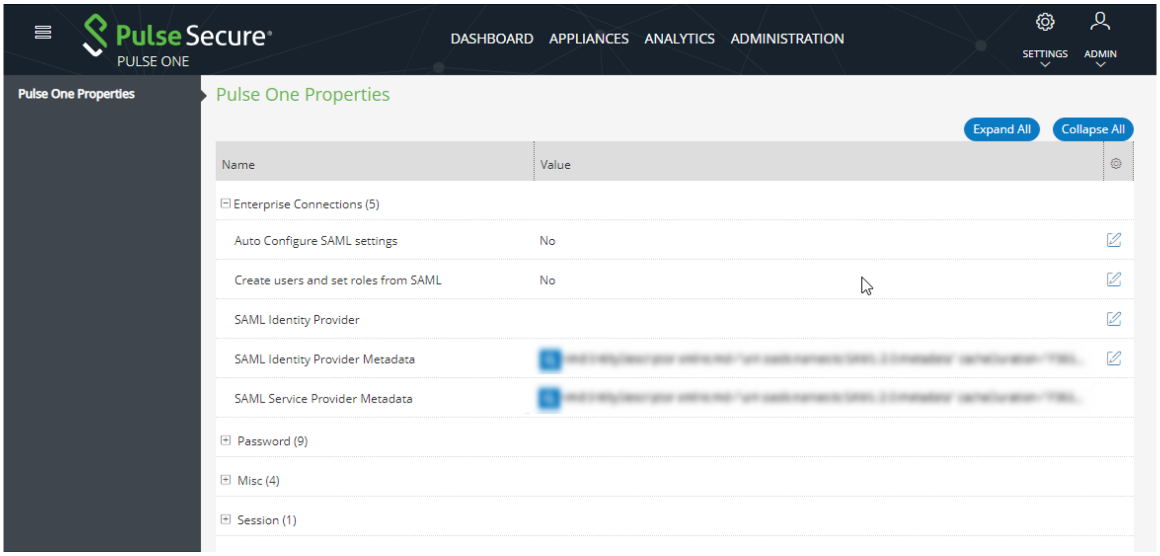
To configure metadata in Pulse One:

1. In the Pulse One admin console, click the settings icon on top-right-corner of the page and select **Pulse One Properties**.
2. Click the **Edit** icon corresponding to **SAML Identity Provider** and select the Pulse Connect Secure appliance that you are setting up as the Identity Provider.
3. Click the **Edit** icon corresponding to **SAML Identity Provider Metadata**.

4. Copy the contents of the metadata file that you downloaded from Pulse Connect Secure, paste it into the **Edit Property** window, and click **Save**. The **SAML Service Provider Metadata** will automatically be populated.

5. Click **SAML Service Provider Metadata**, copy the metadata content, paste it into a file such as *saml-metadata-pws.xml* and save the file to your computer. This file will be used when configuring Pulse Connect Secure later.

FIGURE 178 Pulse One Properties



Pulse One Properties

Name	Value
⊟ Enterprise Connections (5)	
Auto Configure SAML settings	No
Create users and set roles from SAML	No
SAML Identity Provider	
SAML Identity Provider Metadata	[redacted]
SAML Service Provider Metadata	[redacted]
⊞ Password (9)	
⊞ Misc (4)	
⊞ Session (1)	

Adding SAML SP Metadata in Pulse Connect Secure Server

Note: You do not have to perform the process in the section if your appliance is at v8.3r1 or later, and you have already performed auto-configuration of SAML, see **"Automatically Configuring a SAML idP on Pulse One" on page 150**.

This section provides the steps to add SAML Service Provider metadata in PCS server.

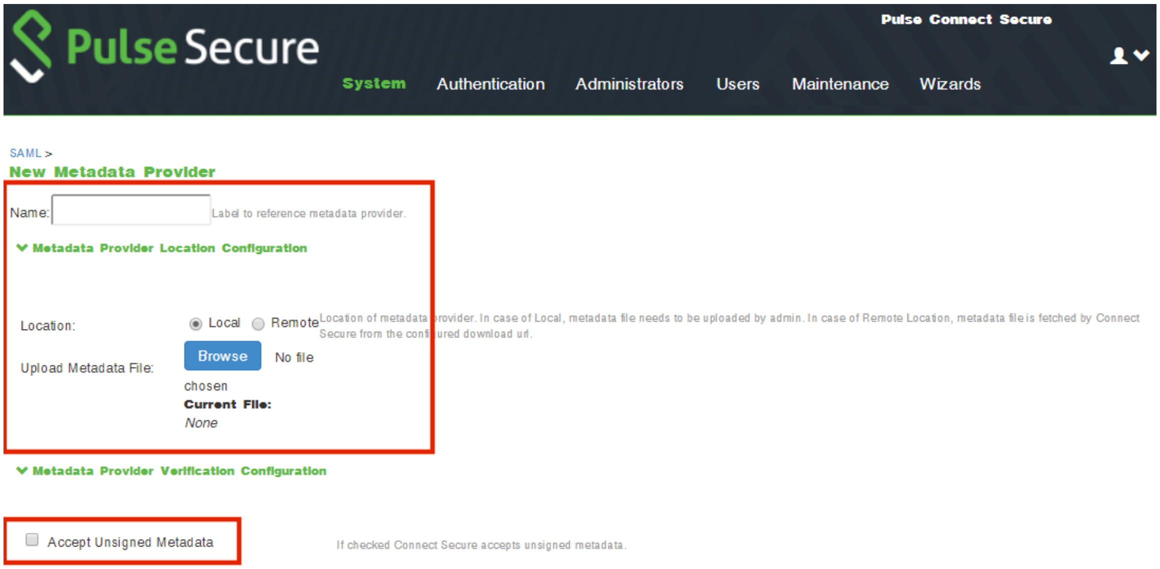
1. Navigate to **System > Configuration > SAML**.

2. Click **New Metadata Provider**.

3. Enter a **Name** for the metadata provider.

4. Under **Metadata Provider Location Configuration**:
   - For **Location**, select *Local*.
   - For **Upload Metadata File**, click **Browse** and select the SP metadata file *saml-metadata-pws.xml* that you saved on your computer in the previous process.

FIGURE 179 Metadata Provider Location Configuration



Name: Label to reference metadata provider.

Metadata Provider Location Configuration

Location: ● Local ○ Remote Location of metadata provider. In case of Local, metadata file needs to be uploaded by admin. In case of Remote Location, metadata file is fetched by Connect Secure from the configured download url.

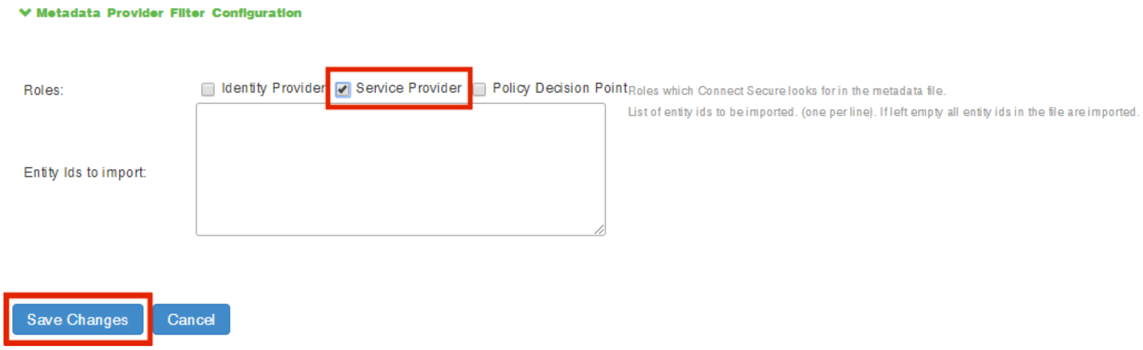
Upload Metadata File: No file chosen
Current File: *None*

Metadata Provider Verification Configuration

□ Accept Unsigned Metadata If checked Connect Secure accepts unsigned metadata.

5. Under **Metadata Provider Verification Configuration**:
   - Select the **Accept Unsigned Metadata** check box.
6. Under **Metadata Provider Filter Configuration**:
   - For **Roles**, select the **Service Provider** check box.

FIGURE 180 Service Provider



Metadata Provider Filter Configuration

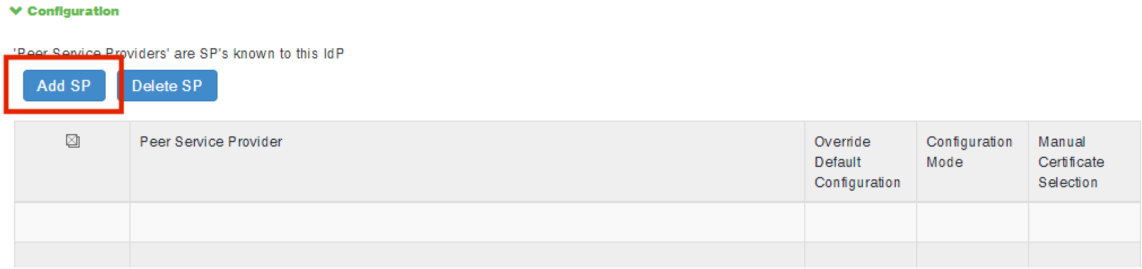
Roles: □ Identity Provider ☑ Service Provider □ Policy Decision Point Roles which Connect Secure looks for in the metadata file.

Entity Ids to import: List of entity ids to be imported. (one per line). If left empty all entity ids in the file are imported.

7. Click **Save Changes**.
8. Navigate to **Authentication > Signing In > Sign-In SAML > Identity Provider**.

9. In the **Configuration** section, click **Add SP**.

FIGURE 181 SAML Identity Provider



Configuration

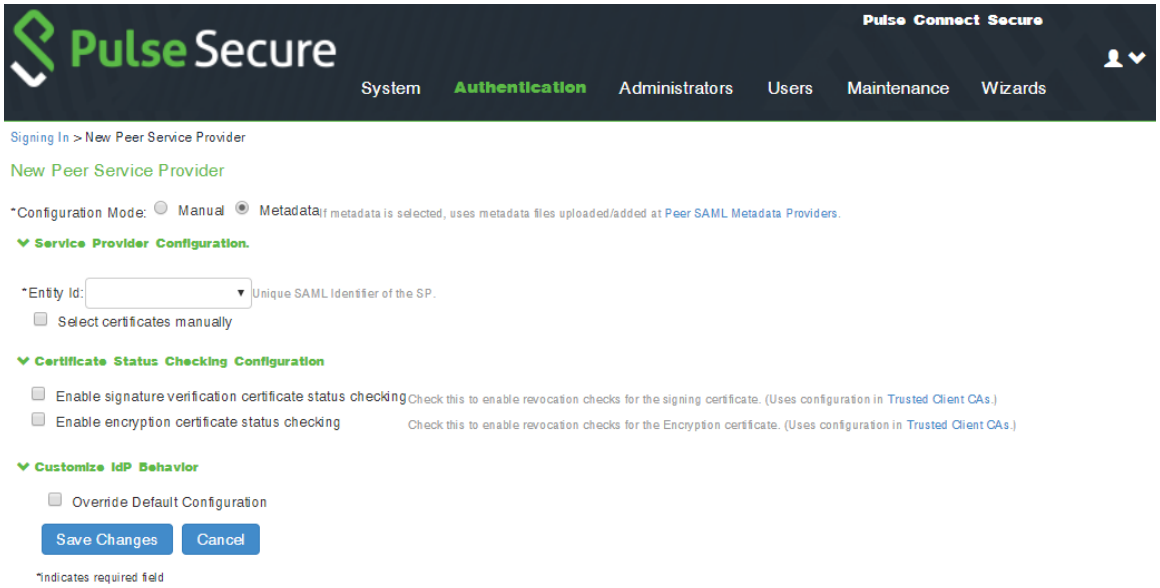
'Peer Service Providers' are SP's known to this IdP

☐	Peer Service Provider	Override Default Configuration	Configuration Mode	Manual Certificate Selection

The **New Peer Service Provider** page appears.

10. In the **Service Provider Configuration** and **Certificate Status Checking Configuration** sections, make the necessary service provider specific settings. For more details, refer to the "Configuring Sign-in SAML Identity Provider Settings" section in the *Pulse Connect Secure Administration Guide*.

FIGURE 182 New Peer Service Provider



Signing In > New Peer Service Provider

New Peer Service Provider

*Configuration Mode: ○ Manual ● Metadata If metadata is selected, uses metadata files uploaded/added at Peer SAML Metadata Providers.

Service Provider Configuration

*Entity Id: ▾ Unique SAML Identifier of the SP.

☐ Select certificates manually

Certificate Status Checking Configuration

☐ Enable signature verification certificate status checking Check this to enable revocation checks for the signing certificate. (Uses configuration in Trusted Client CAs.)

☐ Enable encryption certificate status checking Check this to enable revocation checks for the Encryption certificate. (Uses configuration in Trusted Client CAs.)

Customize IdP Behavior

☐ Override Default Configuration

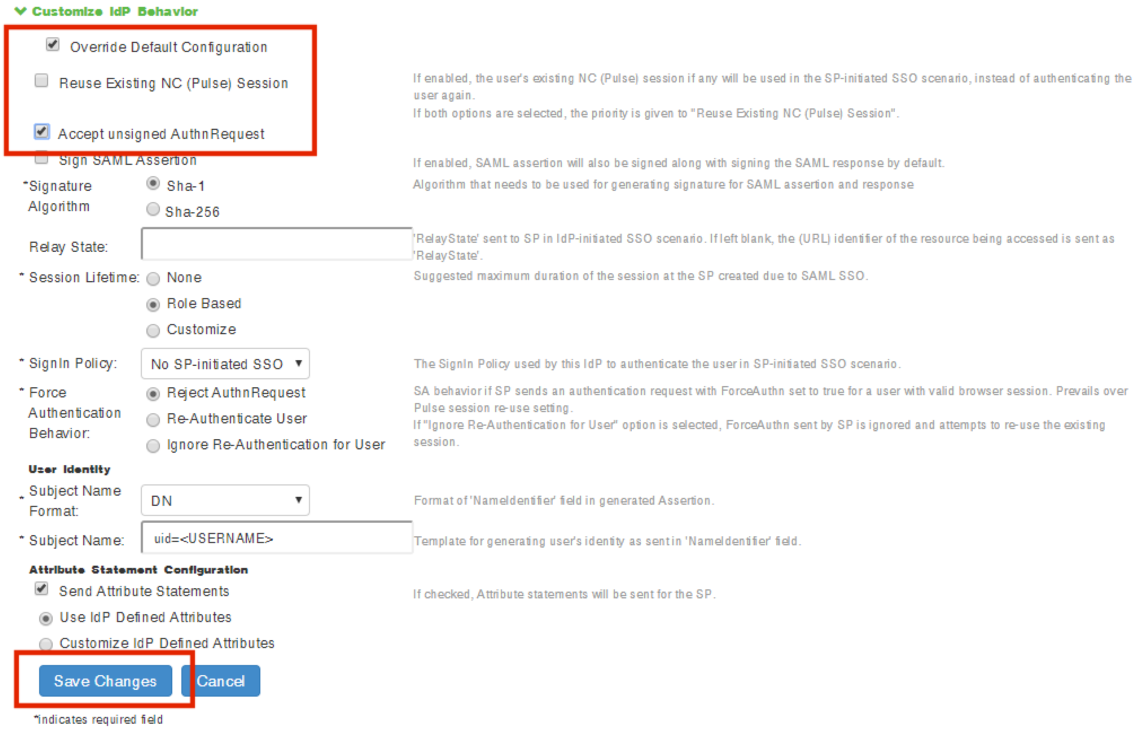
*indicates required field

11. In the **Customize IdP Behavior** section, select the **Override Default Configuration** check box.

12. Clear the **Reuse Existing NC (Pulse) Session** check box.

13. Select the **Accept unsigned AuthnRequest** check box.

FIGURE 183 Customize IdP Behavior



Customize IdP Behavior

☑ Override Default Configuration

☐ Reuse Existing NC (Pulse) Session — If enabled, the user's existing NC (Pulse) session if any will be used in the SP-initiated SSO scenario, instead of authenticating the user again. If both options are selected, the priority is given to "Reuse Existing NC (Pulse) Session".

☑ Accept unsigned AuthnRequest

☐ Sign SAML Assertion — If enabled, SAML assertion will also be signed along with signing the SAML response by default.

*Signature Algorithm: ● Sha-1 ○ Sha-256 — Algorithm that needs to be used for generating signature for SAML assertion and response

Relay State: — 'RelayState' sent to SP in IdP-initiated SSO scenario. If left blank, the (URL) identifier of the resource being accessed is sent as 'RelayState'.

* Session Lifetime: ○ None ● Role Based ○ Customize — Suggested maximum duration of the session at the SP created due to SAML SSO.

* SignIn Policy: No SP-initiated SSO — The SignIn Policy used by this IdP to authenticate the user in SP-initiated SSO scenario.

* Force Authentication Behavior: ● Reject AuthnRequest ○ Re-Authenticate User ○ Ignore Re-Authentication for User — SA behavior if SP sends an authentication request with ForceAuthn set to true for a user with valid browser session. Prevails over Pulse session re-use setting. If "Ignore Re-Authentication for User" option is selected, ForceAuthn sent by SP is ignored and attempts to re-use the existing session.

User Identity

* Subject Name Format: DN — Format of 'NameIdentifier' field in generated Assertion.

* Subject Name: uid=<USERNAME>

Template for generating user's identity as sent in 'NameIdentifier' field.

Attribute Statement Configuration

☑ Send Attribute Statements — If checked, Attribute statements will be sent for the SP.

● Use IdP Defined Attributes

○ Customize IdP Defined Attributes

*indicates required field

14. At the bottom of the page, click **Save Changes**.

SAML configuration is complete.

You can then either:

- Continue with an optional activity **"Automatically Creating Pulse One Users for SAML SSO Logins" on page 158**.
- Move directly to testing the SSO login, see **"Testing Sign In with Enterprise SSO" on page 160**.

Automatically Creating Pulse One Users for SAML SSO Logins

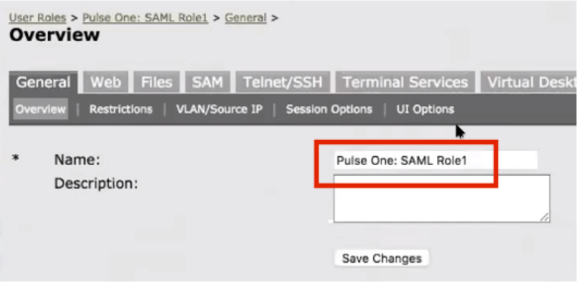
Note: This section is optional for all PCS appliance versions.

After you have a linked a SAML idP (PCS) server to Pulse One, users can log into Pulse One using their Enterprise SSO. However, by default there is no Pulse One user created for these Enterprise SSO users. A Pulse One user is required for features such as appliance configuration management, and the addition of workspaces and devices.

You can configure roles on PCS and Pulse One so that a Pulse One user will be created automatically whenever an Enterprise SSO user logs into Pulse One for the first time.

1. Log into the PCS appliance.
2. Access user roles.
3. Create a user role with a name that starts with "Pulse One: ", followed by a defined Pulse One admin-defined role. For example:

   FIGURE 184 PCS User Roles



User Roles > Pulse One: SAML Role1 > General >

Overview

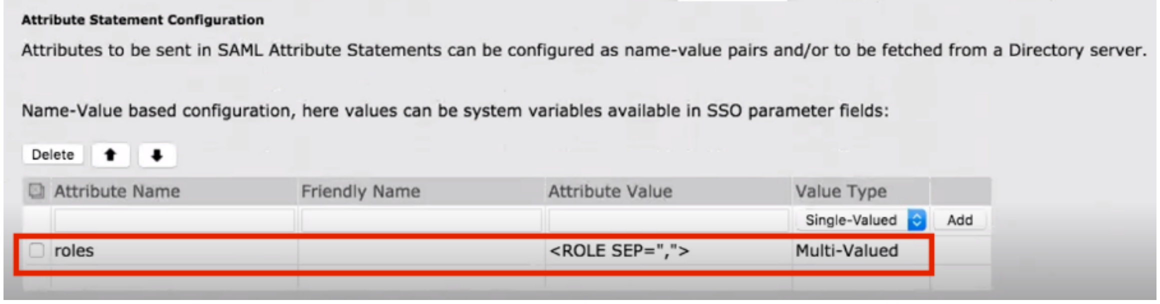
* Name: Pulse One: SAML Role1

Description:

   In this example, there must be a role called *SAML Role1* on Pulse One.

4. Access the SAML idP configuration, see **Configuring SAML idP in Pulse Connect Secure Server**<XREF>
5. In the **Services-Provider-related idP Configuration** section, ensure that there is an **Attribute Statement Configuration** entry that matches the following entry:

   FIGURE 185 Attribute Statement Configuration



Attribute Statement Configuration

Attributes to be sent in SAML Attribute Statements can be configured as name-value pairs and/or to be fetched from a Directory server.

Name-Value based configuration, here values can be system variables available in SSO parameter fields:

□	Attribute Name	Friendly Name	Attribute Value	Value Type
				Single-Valued
□	roles		<ROLE SEP=",">	Multi-Valued

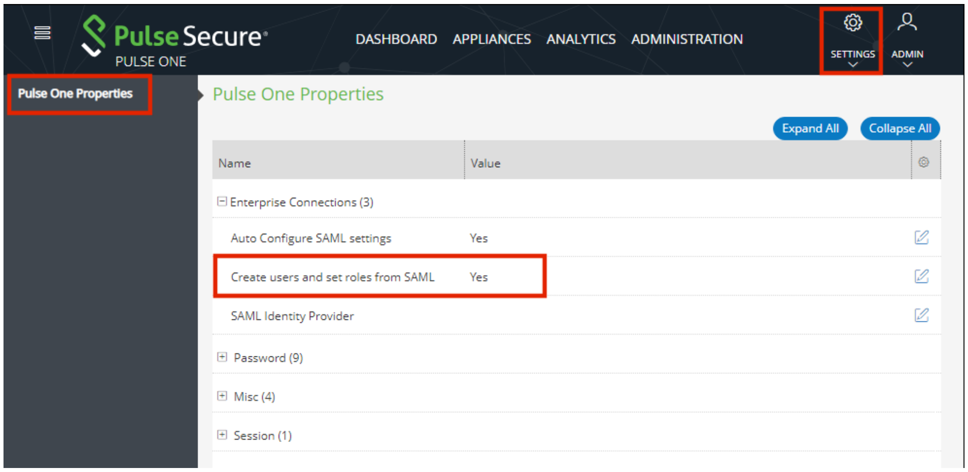
6. Log into Pulse One.

7. Click the **Settings** icon on top-right-corner of the page.

8. Select **Pulse One Properties**.

9. Under **Enterprise Connections**, ensure that the **Create users and roles from SAML** property is set to *Yes*.

FIGURE 186 Pulse One Properties Enterprise Connections



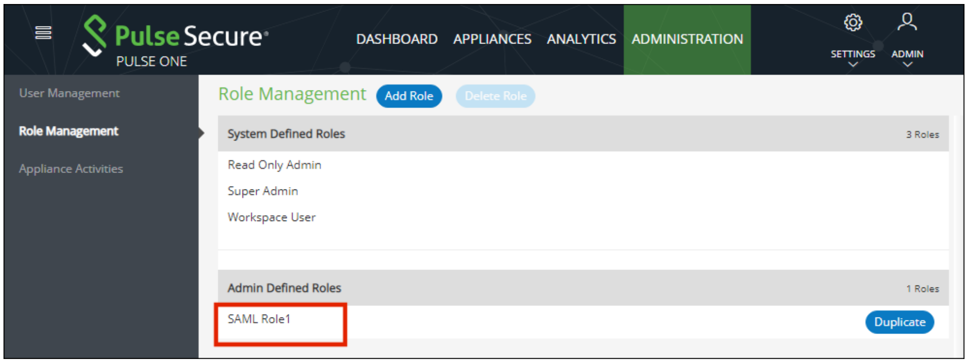
Pulse One Properties

Name	Value
⊟ Enterprise Connections (3)	
Auto Configure SAML settings	Yes
Create users and set roles from SAML	Yes
SAML Identity Provider	
⊞ Password (9)	
⊞ Misc (4)	
⊞ Session (1)	

10. Select the **Administration** menu, and then click **Role Management**.

11. Ensure that there is an admin-defined role whose name was referenced in step 3. For example:

FIGURE 187 Pulse One Admin Defined Roles



Role Management

System Defined Roles — 3 Roles
- Read Only Admin
- Super Admin
- Workspace User

Admin Defined Roles — 1 Roles
- SAML Role1

The configuration is now complete.

Whenever a SAML user logs into Pulse One using their Enterprise SSO, an equivalent Pulse One user is created for them automatically.

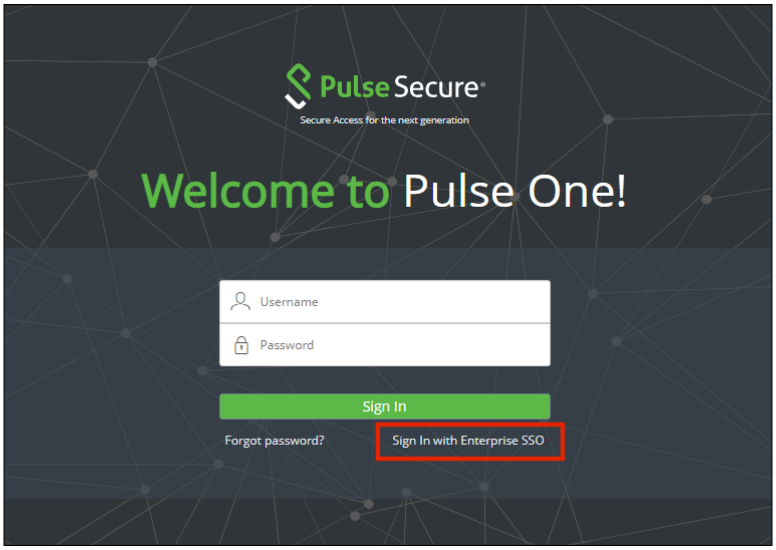
Note: The user will continue to log in with their Enterprise SSO. However, their Pulse One user will enable them to use features such as appliance configuration management, and the addition of workspaces and devices.

Testing Sign In with Enterprise SSO

To test signing in using Enterprise SSO:

1. Navigate to the Pulse One admin login page and click **Sign In with Enterprise SSO**.

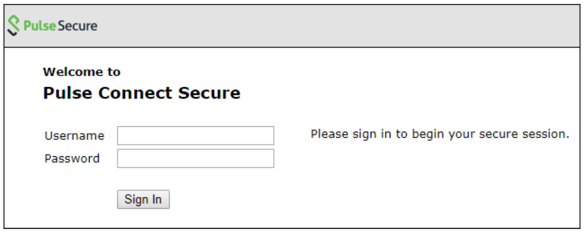
   FIGURE 188 Pulse One Properties

   You are navigated to the Pulse Connect Secure login page.

2. Enter your Username and Password, and click **Sign In**.

   FIGURE 189 Pulse Connect Secure Login Page

3. If this is the first time you're logging in to Pulse One, you are prompted to access the **End User License Agreement (EULA)**. Read and scroll to the bottom of the EULA. Click **Agree** and you will be signed in to Pulse One using your SAML SSO credentials.

Note: If you have configured the automatic creation of Pulse One users from SAML Enterprise SSO users, an equivalent Pulse One user is created for the SAML Enterprise SSO user. See **Automatically Creating Pulse One Users for SAML SSO Logins<XREF>**.

Note: The user will continue to log in with their Enterprise SSO. However, their Pulse One user will enable them to use features such as appliance configuration management, and the addition of workspaces and devices.

Appendix: Checklist for Preparing a Target Appliance

Block Type (which is distributed) (Names as in Pulse One Console)	Requires Preparation of (which is not distributed) (Names as in Appliances Menu	Sample Log Messages	How to Prepare the Target Appliance
Client > Components	Pulse Secure Client > Pulse Secure Versions	Import of configuration from Pulse One returned an Error: [/users/junos-pulse/component-settings/client-version-settings/active-version] Invalid reference: no 'Client Version' object found with identifier '5.2.1.226'.	Navigate to Pulse Secure Client > Components. Upload the required Pulse Client version.
	Endpoint Security > Host Checker > ESAP Versions		Navigate to Authentication > Endpoint Security > Host Checker. Upload the required ESAP package.
Auth > Realms > Admin, Auth > Realms > User	Auth. Servers (Local Auth Servers are not distributed)		Configure the Local Auth Server
Policies > Tunneling > Bandwidth Mgmt	Network > Internal Port, Network > External Port, Network > Management Port	Import of configuration from Pulse One returned an Error: [/users/resource-policies/network-connect-policies/network-connector-bandwidth-policy[name=vpm-tun-bandwidth-policy]] Bandwidth Management Not Enabled! The VPN Tunnels Maximum Bandwidth must be configured on the network overview page.	On the network overview page configure VPN Tunnels Maximum Bandwidth.
Policies > Web > Client Auth	Configuration > Certificates	Import of configuration from Pulse One returned an Error: [/users/resource-policies/web-policies/client-authentications/client-authentication [name=client-auth-policy,parent-type=none]/certificate] Invalid reference: no 'Client Auth Certificate' object found with identifier 'qa.pulsesecure.net'.	Configure the appropriate CA certificate under System > Configuration > Certificates
Policies > Web > Client Auth	Resource Policies > Email Client		An SAnnnn (for example, SA6500), if it has been configured with Resource Policies > Email Client, should not be a master appliance.
Policies > Web > Compression	Options		On the Options page select "Enable gzip compression"
Policies > Web > Java Code Signing	Configuration > Certificates > Code-signing Certificates		Save the policy with the default code-signing certificates.
Policies > Web > PTP	Network > Overview	Import of configuration from Pulse One returned an Error: [/users/resource-policies/web-policies/ptp[application=ptp_policy_2,parent-type=none]] Please specify the IVE hostname on the Network Settings page under Network Identify.	Configure a valid hostname under System > Network > Overview.
Policies > Secure Email	Network > Overview	Import of configuration from Pulse One returned an Error: [/users/resource-profiles/mobile/secure-mail-profiles/secure-mail-profile[virtual-hostname=myhost.myco.com]] Please specify the IVE hostname on the Network Settings page under Network Identify	Configure a valid hostname under System > Network > Overview.
Security	Network Settings > Internal Port > Virtual Port	Import of configuration from Pulse One returned an Error: [/system/configuration/security/ssl-options] Virtual port number virtual_internal is not a valid Virtual Port	
	Network Settings > External Port > Virtual Port	Import of configuration from Pulse One returned an Error: [/system/configuration/security/ssl-options] Virtual port number virtual_external is not a valid Virtual Port	
SAML Auth-Server	System > Configuration > SAML > Settings		Configure a valid "Host FQDN for SAML" on the System > Configuration > SAML > Settings page.

Block Type (which is distributed) (Names as in Pulse One Console)	Requires Preparation of (which is not distributed) (Names as in Appliances Menu	Sample Log Messages	How to Prepare the Target Appliance
Signing in > Sign-in SAML	System > Configuration > SAML > Settings	Import of configuration from Pulse One returned an Error:[/authentication/signin/saml/identity-provider/sp-default-configuration/source-id] Modification of this attribute is not allowed.	Configure a valid "Host FQDN for SAML" on the System > Configuration > SAML > Settings page.
(PPS) Policies > Enforcer > Access	Policies > Enforcer > Connection	Import of configuration from Pulse One returned an Error: Failed to resolve path references. Import of configuration from Pulse One returned an Error:[/uac/infranet-enforcer/resource-access-policies/resource-access-policy[name=enforcer_access_policy]/infranet-enforcer] Invalid reference: no 'Infranet Enforcer' object found with identifier 'screenOS1'.	
(PPS) Policies > Enforcer > Auth Table Mapping	Policies > Enforcer > Connection	Import of configuration from Pulse One returned an Error: Failed to resolve path references. Import of configuration from Pulse One returned an Error:[/uac/infranet-enforcer/auth-table-mapping-policies/auth-table-mapping[name= auth_table_mapping_policy]/infranet-enforcer] Invalid reference: no 'Infranet Enforcer' object found with identifier 'screenOS1'.	
(PPS) Policies > Enforcer > IP Address Pools	Policies > Enforcer > Connection	Import of configuration from Pulse One returned an Error: Failed to resolve path references. Import of configuration from Pulse One returned an Error:[/uac/infranet-enforcer/ip-address-pools-policies/ip-address-pools-policy[name= ip_pool_policy]/infranet-enforcer] Invalid reference: no 'Infranet Enforcer' object found with identifier 'screenOS1'.	
(PPS) Policies > Enforcer > IPSec Routing	Policies > Enforcer > Connection	Import of configuration from Pulse One returned an Error: Failed to resolve path references. Import of configuration from Pulse One returned an Error:[/uac/infranet-enforcer/ipsec-routing-policies/ipsec-routing -policy [name= ipsec_policy]/infranet-enforcer] Invalid reference: no 'Infranet Enforcer' object found with identifier 'screenOS1'.	
(PPS) Policies > Enforcer > Source Interface	Policies > Enforcer > Connection	No error message. Enforcer is a required field for Source Interface Policy.	
Pulse Secure Client > Connections	System > Configuration > Certificates > Trusted Server CAs	Import of configuration from Pulse One returned an Error:[/users/junos-pulse/connection-sets/connection-set[name=PPS_PCS_Combo]/connections/connection [name=L2_Connection_WIRED]/trusted-servers/trusted-server[dn=ANY,ca=PMDRoorCA]/ca] Invalid reference: no 'Trusted Server CA' object found with identifier 'PMDRootCA'.	Configure the appropriate 'Trusted Server CA' under System > Configuration > Certificates > Trusted Server CAs, by importing the 'Trusted Server CA'.
(PPS) Auth > Realms > Users	Endpoint Policy > Network Access > Radius Attributes	Import of configuration from Pulse One returned an Error:[/users/user-realms/realm[name=TestRealm1]/authentication-policy/radius-request-attributes-policies/selected-policies] Invalid reference: no 'RADIUS Request Attributes Policy' object found with identifier '2nd Request Policy'.	Configure the appropriate 'RADIUS Request Attributes Policy' under Endpoint Policy > Network Access > Radius Attributes.