



Pulse One Cloud Administration Guide

Supporting Pulse One Appliance 2.0.1902

| | |
|------------------|-----------------------|
| Product Release | 2.0.1902 |
| Published | 15 August 2019 |
| Document Version | 1.0 |

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

<https://www.pulsesecure.net>

© 2019 Pulse Secure, LLC. All rights reserved. Pulse Secure and the Pulse Secure logo are trademarks of Pulse Secure, LLC in the United States.

All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

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 | 1 |
| DOCUMENT CONVENTIONS | 1 |
| TEXT FORMATTING CONVENTIONS | 1 |
| COMMAND SYNTAX CONVENTIONS..... | 1 |
| NOTES AND WARNINGS | 2 |
| REQUESTING TECHNICAL SUPPORT | 2 |
| SELF-HELP ONLINE TOOLS AND RESOURCES | 2 |
| OPENING A CASE WITH PSGSC | 3 |
| GETTING STARTED WITH PULSE ONE | 5 |
| OVERVIEW OF PULSE ONE | 5 |
| LOGGING INTO PULSE ONE | 6 |
| CHANGING THE USER PASSWORD | 9 |
| ADDING PULSE ONE LICENSES | 9 |
| SETTING A SESSION TIMEOUT THRESHOLD..... | 12 |
| WORKING WITH THE PULSE ONE DASHBOARD..... | 13 |
| VIEWING OVERALL SYSTEM HEALTH | 13 |
| CUSTOMIZING DASHBOARDS AND WIDGETS | 14 |
| ADDING A NEW WIDGET | 16 |
| EDITING THE DASHBOARD LAYOUT..... | 17 |
| EDITING WIDGET CONFIGURATION | 19 |
| APPLIANCE MANAGEMENT | 21 |
| REGISTERING AN EXISTING PCS/PPS APPLIANCE | 21 |
| EDITING APPLIANCE INFORMATION | 23 |
| LAUNCHING THE USER INTERFACE FOR AN APPLIANCE..... | 24 |
| CONFIGURING AN APPLIANCE TO CONNECT TO PULSE ONE | 25 |
| COMPLETING REGISTRATION OF AN APPLIANCE | 25 |
| CONFIGURING ACTIVESYNC HANDLER | 25 |
| CONFIGURING CPU, MEMORY AND DISK UTILIZATION..... | 27 |
| WORKING WITH APPLIANCE GROUPS | 27 |
| CREATING AN APPLIANCE GROUP..... | 28 |
| ADDING APPLIANCES TO AN APPLIANCE GROUP..... | 32 |
| DISTRIBUTING A MASTER CONFIGURATION | 34 |
| VIEWING THE ACTIVITIES LOG FOR AN APPLIANCE | 38 |
| VIEWING THE CONFIGURATION CHANGE HISTORY FOR AN APPLIANCE | 39 |

| | |
|--|----|
| COMPARING APPLIANCES | 40 |
| REBOOTING AN APPLIANCE..... | 42 |
| REMOVING AN APPLIANCE FROM PULSE ONE | 43 |
| PREPARING A TARGET APPLIANCE | 44 |
| PREPARING AN RSA AGENT INSTANCE FOR THE TARGET APPLIANCE | 44 |
| REMOVING AN APPLIANCE FROM AN APPLIANCE GROUP | 44 |
| EDITING AN APPLIANCE GROUP..... | 45 |
| DELETING AN APPLIANCE GROUP | 47 |
| VIEWING ANALYTICS AND REPORTS..... | 49 |
| VIEWING THE LOGIN ATTEMPTS REPORT..... | 49 |
| VIEWING THE APPLIANCE HEALTH REPORT..... | 50 |
| VIEWING THE APPLIANCE ACTIVITIES REPORT | 51 |
| VIEWING APPLIANCE ACTIVITIES | 51 |
| USER MANAGEMENT | 53 |
| ADDING AN ADMIN USER..... | 53 |
| EDITING USER DETAILS..... | 54 |
| REMOVING AN ADMIN USER..... | 55 |
| RESETTING A USER PASSWORD | 55 |
| SUSPENDING A USER..... | 56 |
| ROLE MANAGEMENT | 57 |
| ADDING AN ADMIN DEFINED ROLE | 57 |
| EDITING AN ADMIN ROLE | 58 |
| REMOVING AN ADMIN ROLE..... | 58 |
| WORKING WITH PULSE ONE PROPERTIES | 59 |
| VIEWING PULSE ONE PROPERTIES..... | 59 |
| EDITING PULSE ONE PROPERTIES | 59 |
| UNDERSTANDING PULSE ONE PROPERTIES | 60 |
| ENTERPRISE CONNECTION PROPERTIES | 60 |
| PASSWORD PROPERTIES..... | 60 |
| MISCELLANEOUS PROPERTIES | 61 |
| SESSION PROPERTIES | 61 |
| CONFIGURING ENTERPRISE SSO USING SAML | 63 |
| OVERVIEW..... | 63 |
| CONFIGURING SAML IDP IN PULSE CONNECT SECURE SERVER | 64 |
| AUTOMATICALLY CONFIGURING A SAML IDP ON PULSE ONE..... | 68 |
| CONFIGURING A METADATA PROVIDER IN PULSE CONNECT SECURE | 70 |

| | |
|---|----|
| ENABLING ENTERPRISE SSO IN PULSE ONE APPLIANCE..... | 71 |
| CONFIGURING SAML METADATA IN PULSE ONE | 71 |
| ADDING SAML SP METADATA IN PULSE CONNECT SECURE SERVER..... | 72 |
| AUTOMATICALLY CREATING PULSE ONE USERS FOR SAML SSO LOGINS..... | 76 |
| TESTING SIGN IN WITH ENTERPRISE SSO..... | 78 |
| APPENDIX: CHECKLIST FOR PREPARING A TARGET APPLIANCE..... | 79 |

Preface

- **Document Conventions** 1
- **Requesting Technical Support** 2

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 |
| <i>italic text</i> | 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. |
| <i>italic text</i> | 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://www.pulsesecure.net/support/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://www.pulsesecure.net/support>
- Search for known bugs: <https://www.pulsesecure.net/support>
- Find product documentation: <https://www.pulsesecure.net/techpubs>

- Download the latest versions of software and review release notes: <https://www.pulsesecure.net/support>
- Open a case online in the CSC Case Management tool: <https://www.pulsesecure.net/support>
- To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: <https://www.pulsesecure.net/support>

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: <http://kb.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://www.pulsesecure.net/support>.
- Call 1-844 751 7629 (Toll Free, US).

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

Getting Started With Pulse One

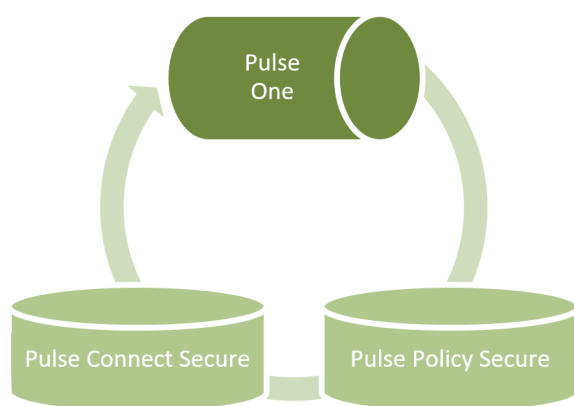
- **Overview of Pulse One** 5
- **Logging Into Pulse One** 6
- **Changing the User Password** 9
- **Adding Pulse One Licenses** 9
- **Setting a Session Timeout Threshold** 12

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.
- **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 60](#).

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**.

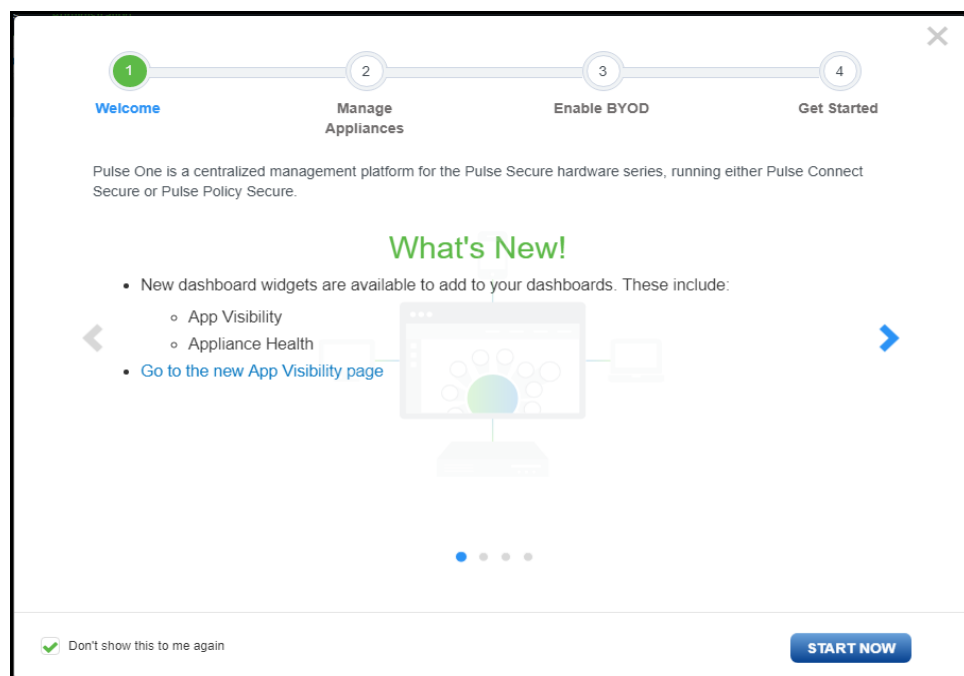
An email that contains a **Reset your password** link will be sent to your registered mail id. Use this link to launch Pulse One and provide your new password and confirm the new password.

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

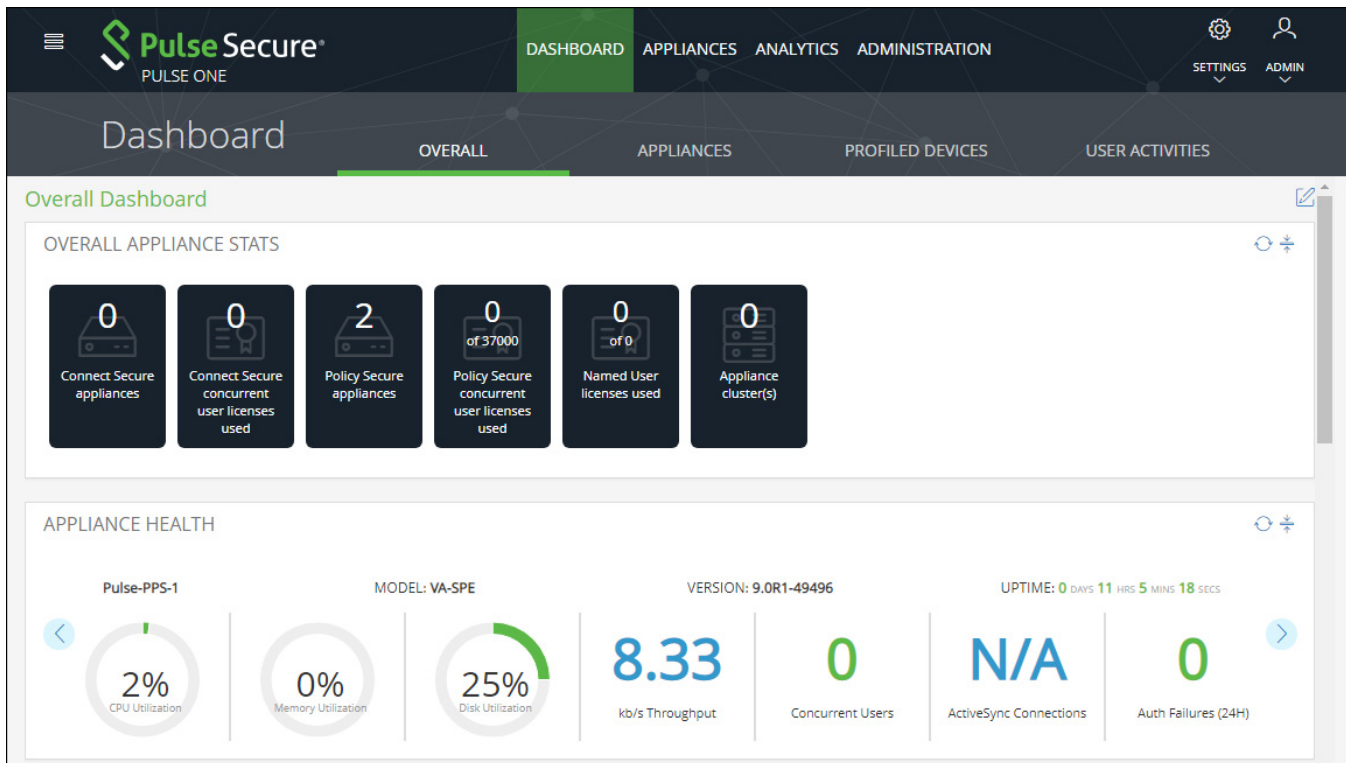


In the Welcome wizard, click the right-arrow button until the **Get Started** option appears. If required, select the **Don't show this to me again** check box and then click **Start Now**.

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



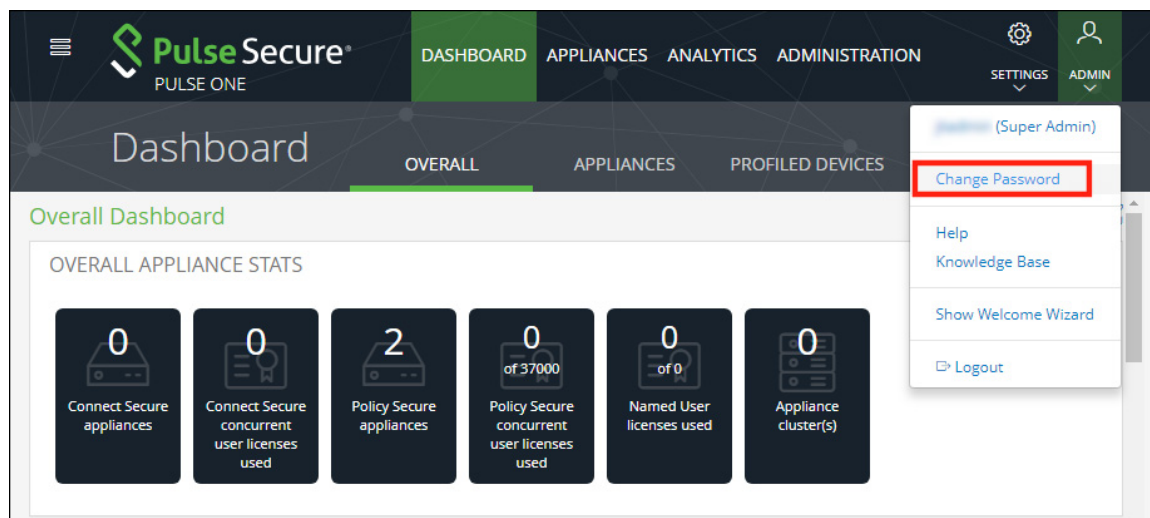
Select the appropriate tab, settings icon or user icon, and get started with the administration.

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 5 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. Beyond this time, you will have to make a new request for setting the new password.

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

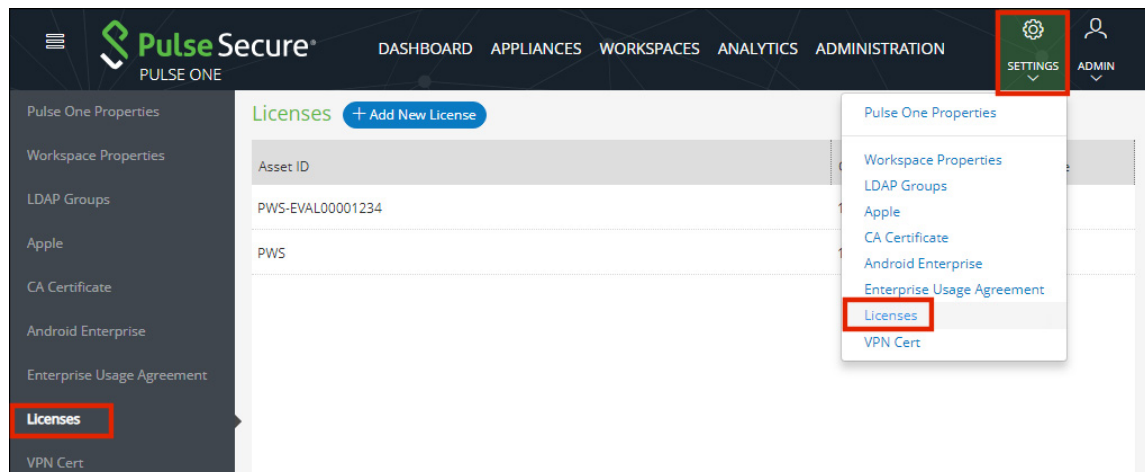
Adding Pulse One Licenses

To view and install a licenses on Pulse One Cloud:

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

3. Select **Licenses**. The **Licenses** page appears.

FIGURE 6 Installed Licenses

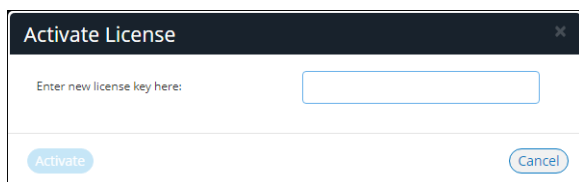


Note: Any expired licenses (none shown in this example) are displayed in red.

4. Click **Add New License**.

The **Activate License** dialog appears.

FIGURE 7 Add New License



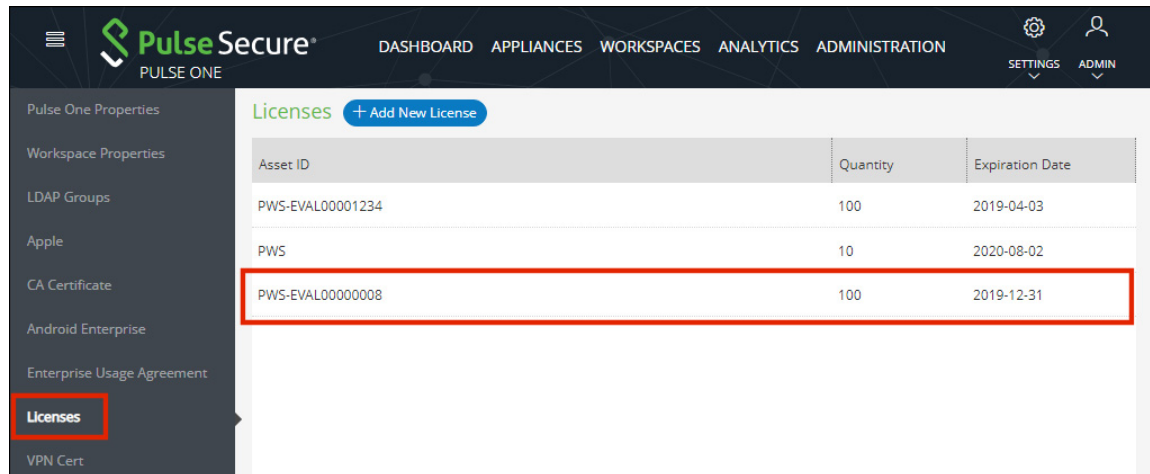
5. Enter the license key.

6. Click **Activate**.

The new license is confirmed.

The new license appears in the list of licenses. For example:

FIGURE 8 New Pulse Workspace License



| Asset ID | Quantity | Expiration Date |
|------------------|----------|-----------------|
| PWS-EVAL00001234 | 100 | 2019-04-03 |
| PWS | 10 | 2020-08-02 |
| PWS-EVAL00000008 | 100 | 2019-12-31 |

Setting a Session Timeout Threshold

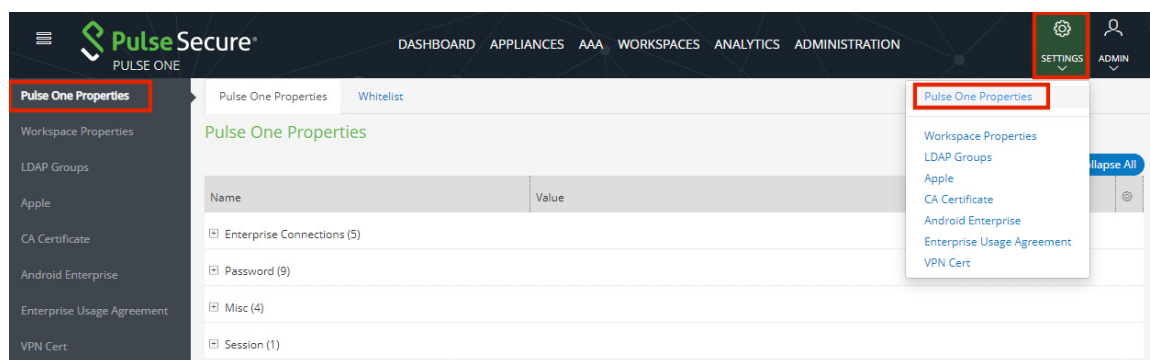
You can set a session timeout threshold. After a period of activity reaches this threshold, the user is logged out, and must log in again to continue.

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 9 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.

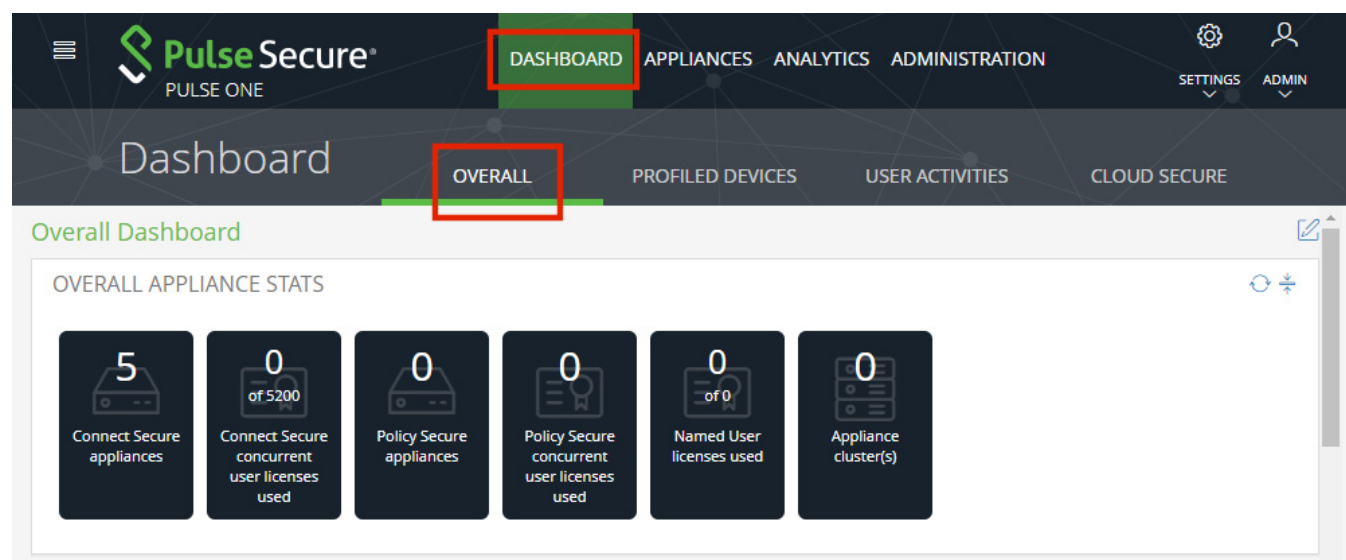
Working with the Pulse One Dashboard

- [Viewing Overall System Health](#) 13
- [Customizing Dashboards and Widgets](#) 14

Viewing Overall System Health

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

FIGURE 10 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** (⌵).

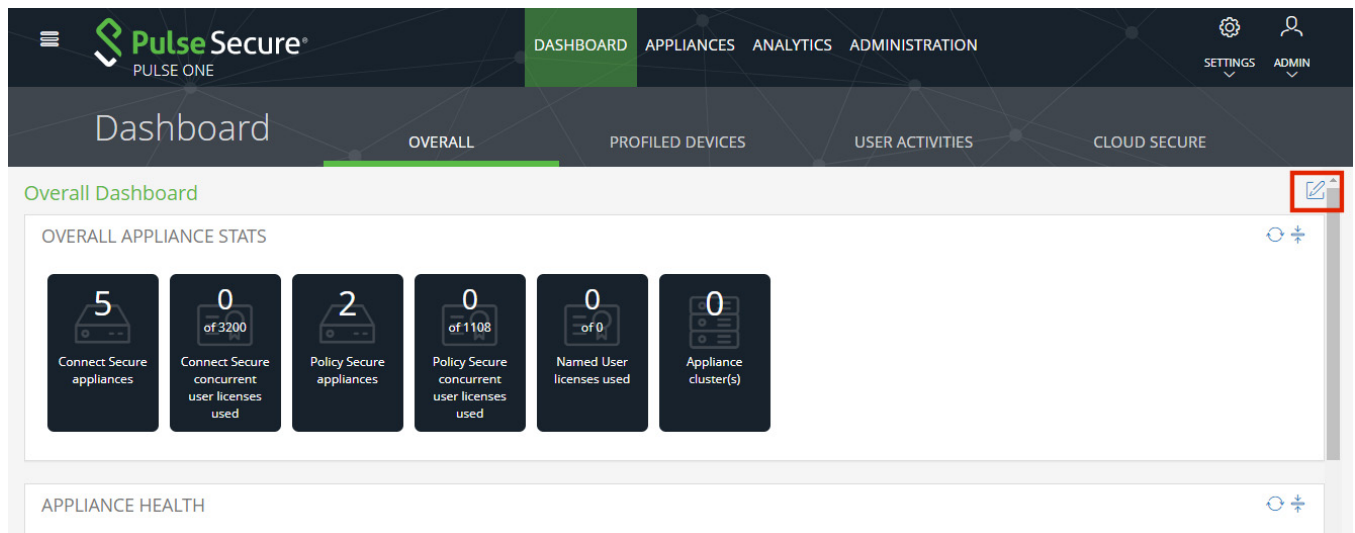
Customizing Dashboards and Widgets

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 11 Customizing the Dashboard

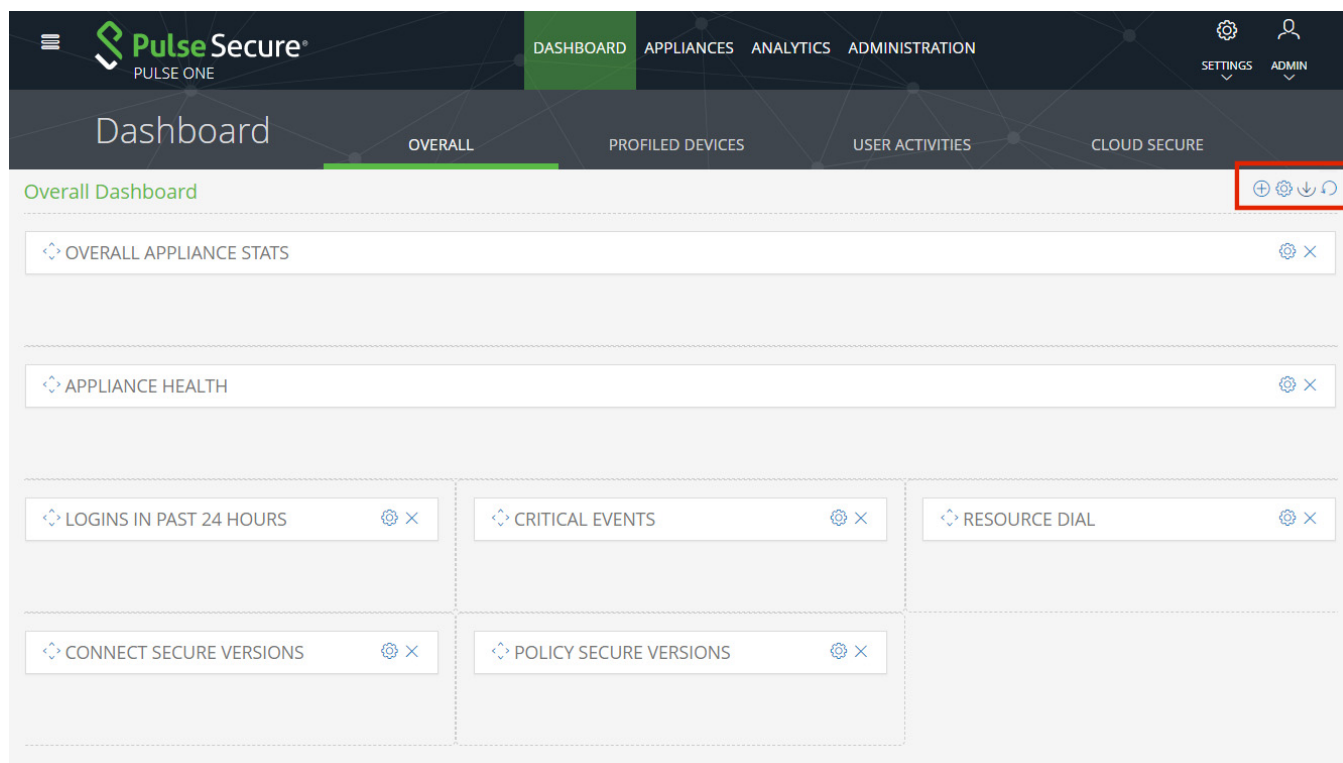


Note: The inclusion of individual menus and tabs will reflect all loaded licenses. Your view may differ from that shown above.

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 12 Dashboard Widget Layout



3. (Optional) Click **Add New Widget** (+) to add a widget to the current layout, see [“Adding a New Widget” on page 16](#).
4. (Optional) Click **Edit Dashboard** (⚙️) to select a new layout, see [“Editing the Dashboard Layout” on page 17](#).
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 19](#).
7. (Optional) Remove a widget by clicking its **Remove Widget** (X) 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:

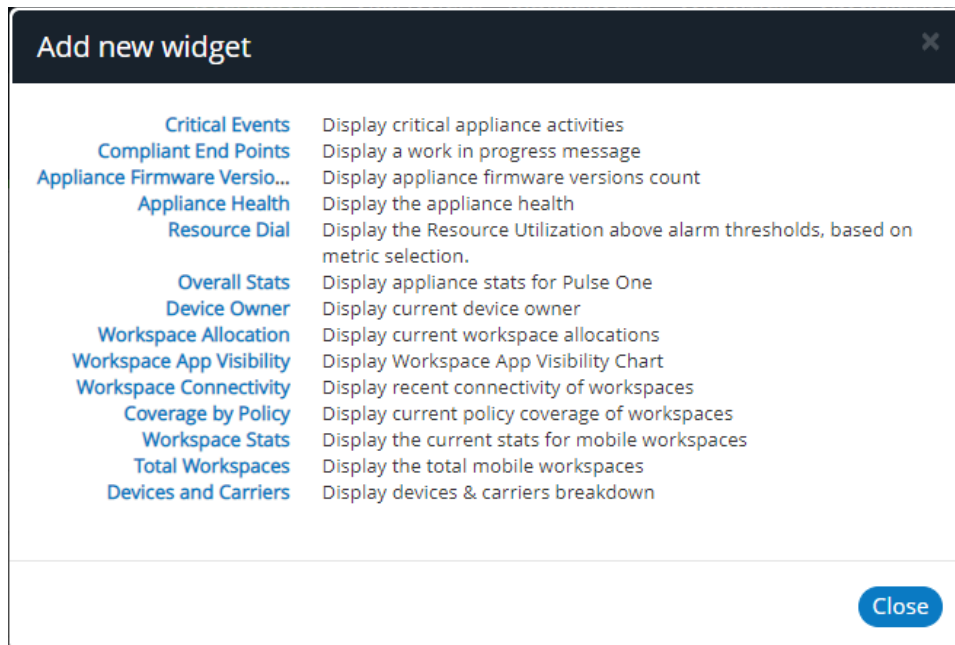
1. Display the required dashboard tab. That is, either the **Overall** tab or the **Workspaces** tab.
2. Click the **Enable Edit mode** icon () on the top-right of the tab.

A widget layout summary for the dashboard appears.

3. Click the **Add New Widget** () control.




A list of widgets appears.

FIGURE 13 Add New Widget



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 19](#).
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.

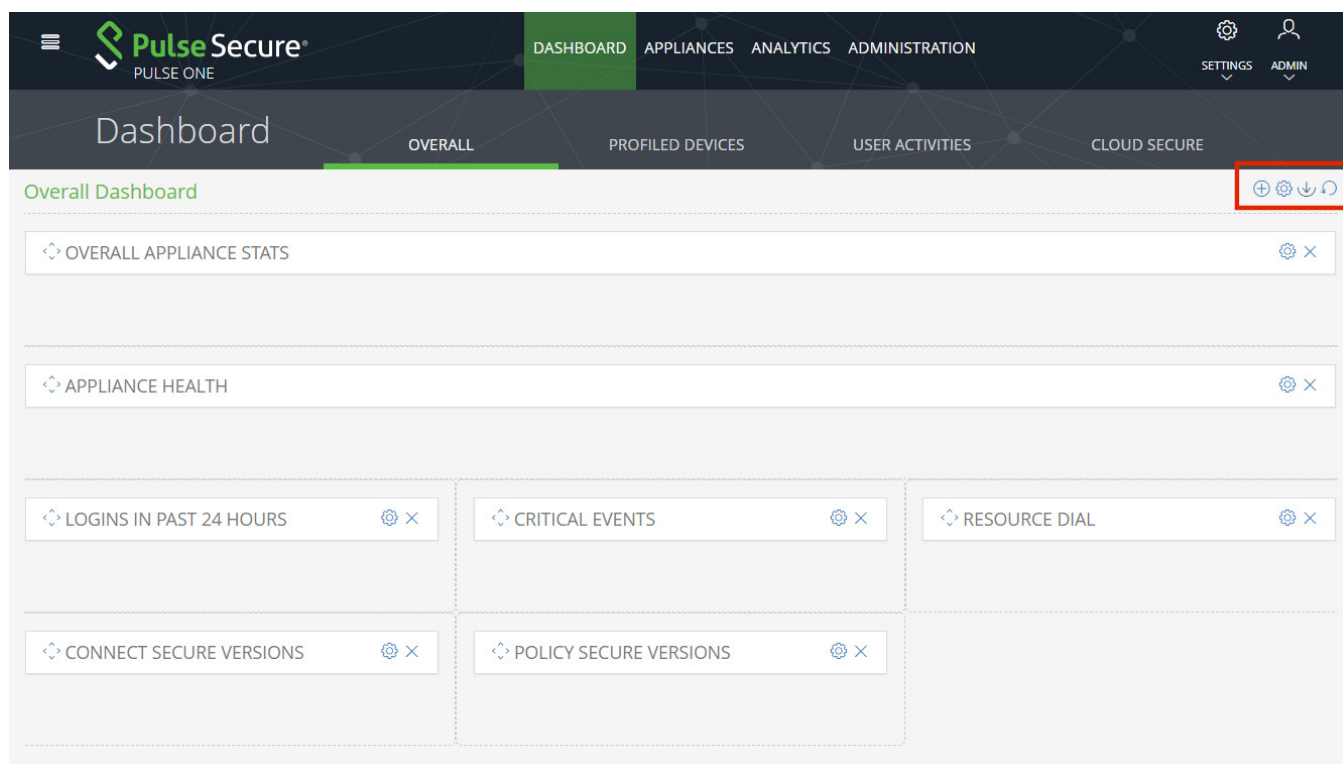
Editing the Dashboard Layout

To change the layout of a dashboard tab:

1. Display the required dashboard tab. That is, either the **Overall** tab or the **Workspaces** 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:

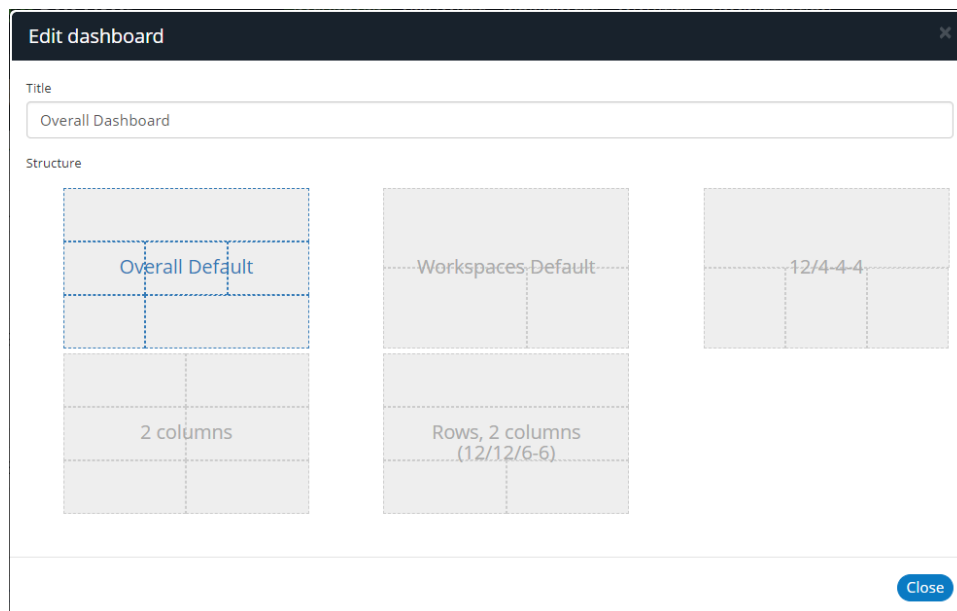
FIGURE 14 Dashboard Widget Layout



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

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

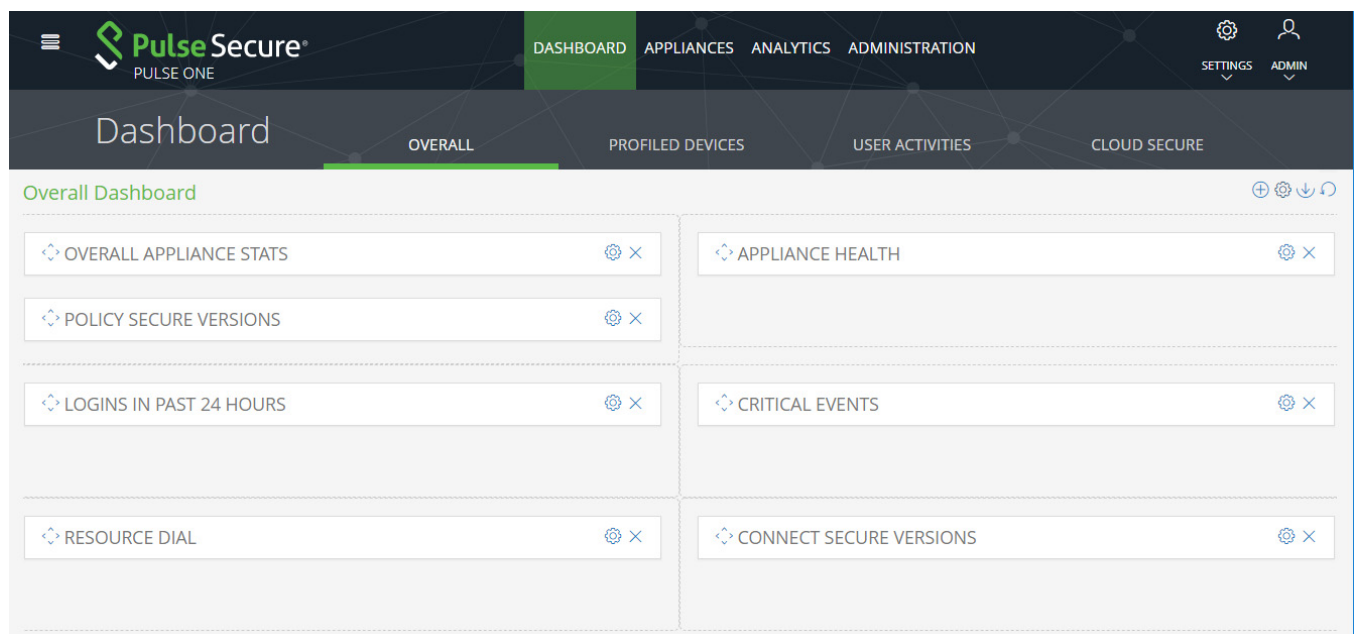
FIGURE 15 Edit Dashboard Layout



- 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 16 Updated Dashboard Widget Layout



- (Optional) Click **Undo Changes** (↶) to reset all unsaved changes and close the layout summary.
- 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. That is, either the **Overall** tab or the **Workspaces** 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 17 Appliance Health Widget



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 | 21 |
| • Configuring an Appliance to Connect to Pulse One | 25 |
| • Configuring CPU, Memory and Disk Utilization | 27 |
| • Working with Appliance Groups | 27 |
| • Viewing the Activities Log for an Appliance | 38 |
| • Viewing the Configuration Change History for an Appliance | 39 |
| • Comparing Appliances | 40 |
| • Rebooting an Appliance | 42 |
| • Removing an Appliance from Pulse One | 43 |
| • Preparing a Target Appliance | 44 |
| • Removing an Appliance from an Appliance Group | 44 |
| • Editing an Appliance Group | 45 |
| • Deleting an Appliance Group | 47 |

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.

To register an existing appliance:

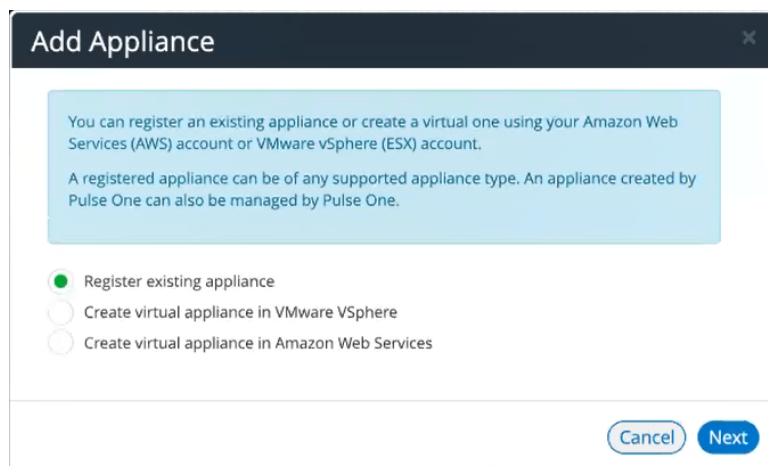
1. Log into Pulse One as an administrator.
2. Click the **Appliances** menu and then the **Appliances** tab.

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

3. Click **Add Appliance**.

The **Add Appliance** dialog box appears.

FIGURE 18 Add Appliance



The **Add Appliance** dialog box has a dark header with the title and a close button. Below the header is a light blue informational box containing text about registering or creating virtual appliances. Underneath are three radio button options: 'Register existing appliance' (which is selected), 'Create virtual appliance in VMware vSphere', and 'Create virtual appliance in Amazon Web Services'. At the bottom right are 'Cancel' and 'Next' buttons.

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.

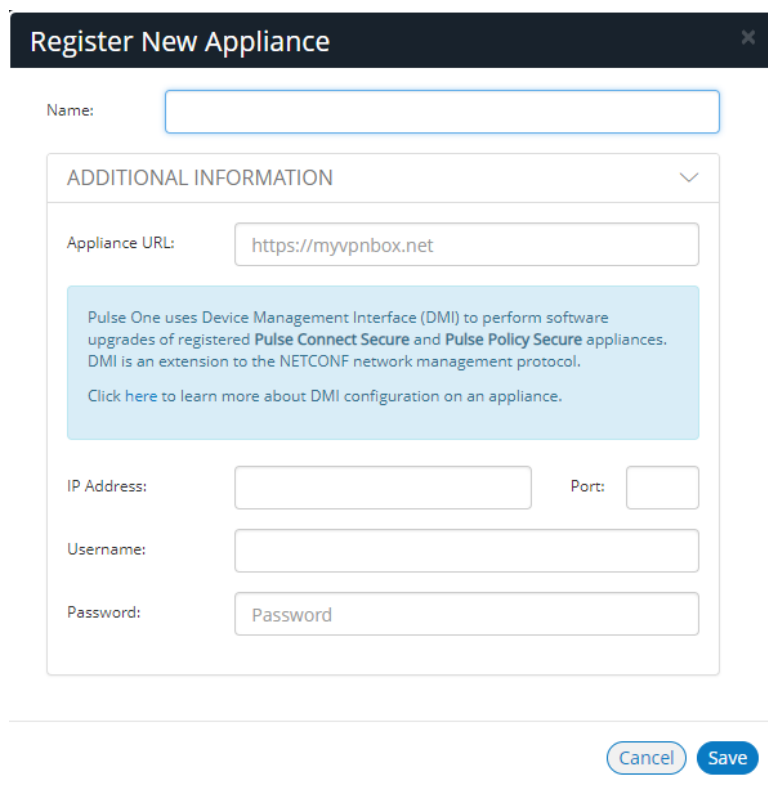
☒ Register existing appliance
☐ Create virtual appliance in VMware vSphere
☐ Create virtual appliance in Amazon Web Services

Cancel Next

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

The **Register Appliance** dialog appears.

FIGURE 19 Register New Appliance



The **Register New Appliance** dialog box has a dark header with the title and a close button. Below the header is a text input field for 'Name'. Underneath is an 'ADDITIONAL INFORMATION' section with a dropdown arrow. Inside this section is an 'Appliance URL' field with the value 'https://myvpnbox.net', followed by a light blue informational box about DMI. Below that are fields for 'IP Address', 'Port', 'Username', and 'Password'. At the bottom right are 'Cancel' and 'Save' buttons.

Register New Appliance

Name:

ADDITIONAL INFORMATION

Appliance URL:

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:

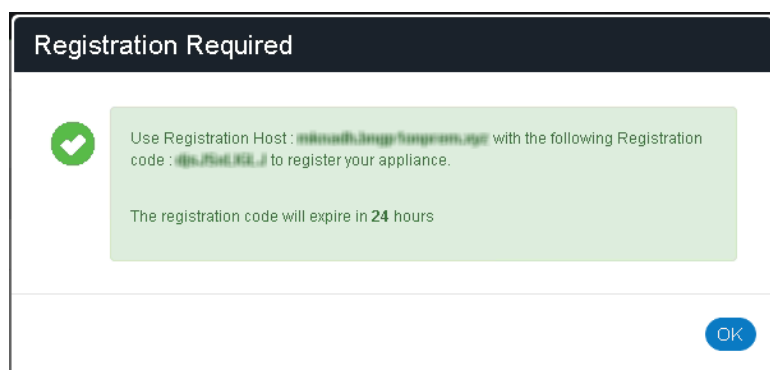
Cancel Save

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.
8. Click **Save**.

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

FIGURE 20 Registration Required



- Record the **Registration Host** and **Registration Code** and close the dialog.
- 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 25.

When the auto-registration process is complete, 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.


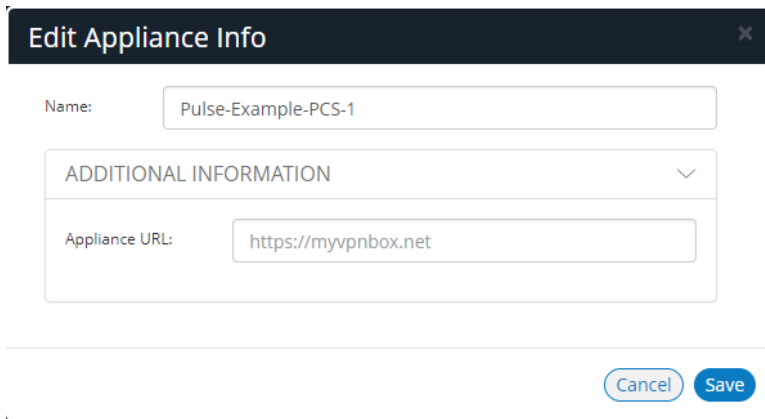
3. Select the required appliance from the list and click its **Actions** icon ().
4. From the menu options, select **Edit Appliance Info**.
5. In the **Edit Appliance Info** dialog, make the required changes.

FIGURE 21 Edit Appliance Information



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 23](#).

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.

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 25](#).
- Configure the ActiveSync handler on the appliance as required, see [“Configuring ActiveSync Handler” on page 25](#).

Completing Registration of an Appliance

To complete registration of an appliance in Pulse Connect Secure:

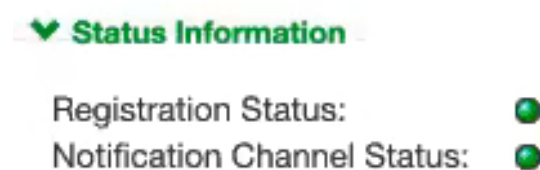
1. Log into the PCS/PPS appliance.
2. Select the **System > Configuration > Pulse One > Settings** tab.
3. Enter the **Registration Host** and **Registration Code**.

Note: These were displayed during [“Registering an Existing PCS/PPS Appliance” on page 21](#).

4. Click **Save Changes**.

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

FIGURE 22 Pulse Connect Secure: Pulse One Settings



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:

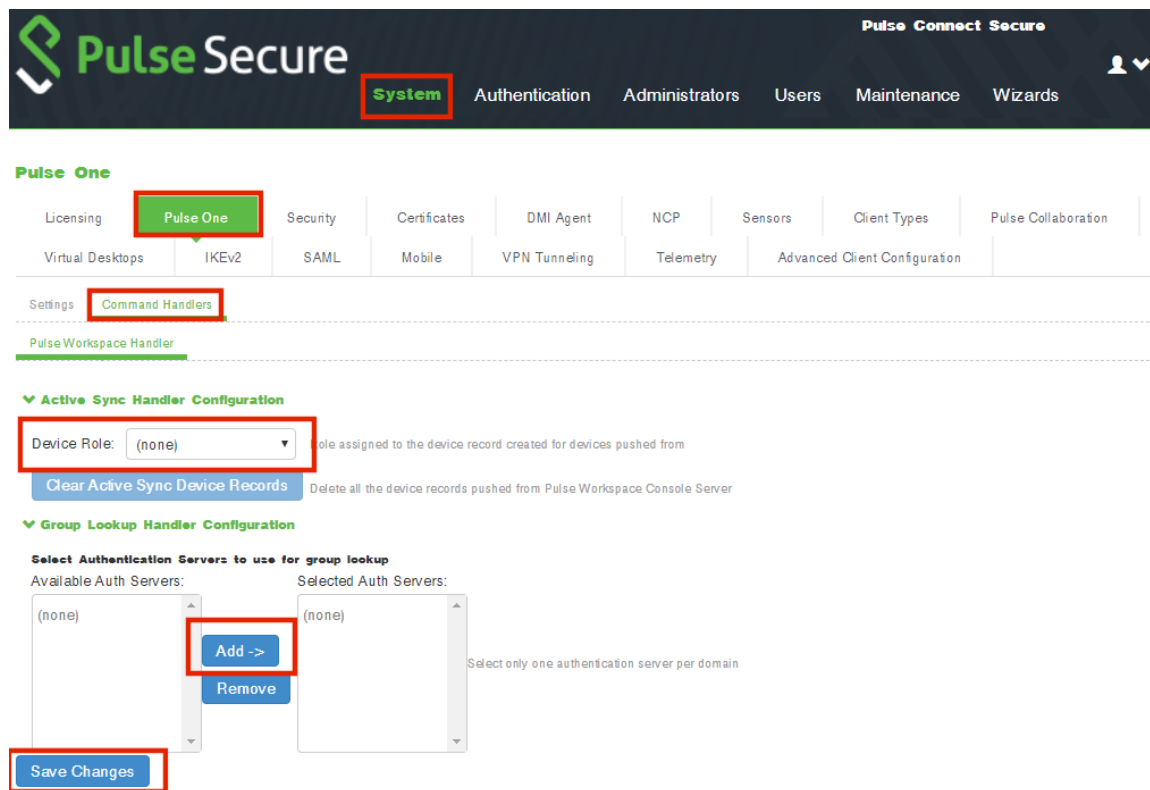
- Filter out and reject ActiveSync connection requests coming from unauthorized Mobile devices.
- Allow only those devices that have been successfully provisioned on Pulse Workspace Server.

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 23 Pulse Connect Secure: Command Handlers



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)

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:

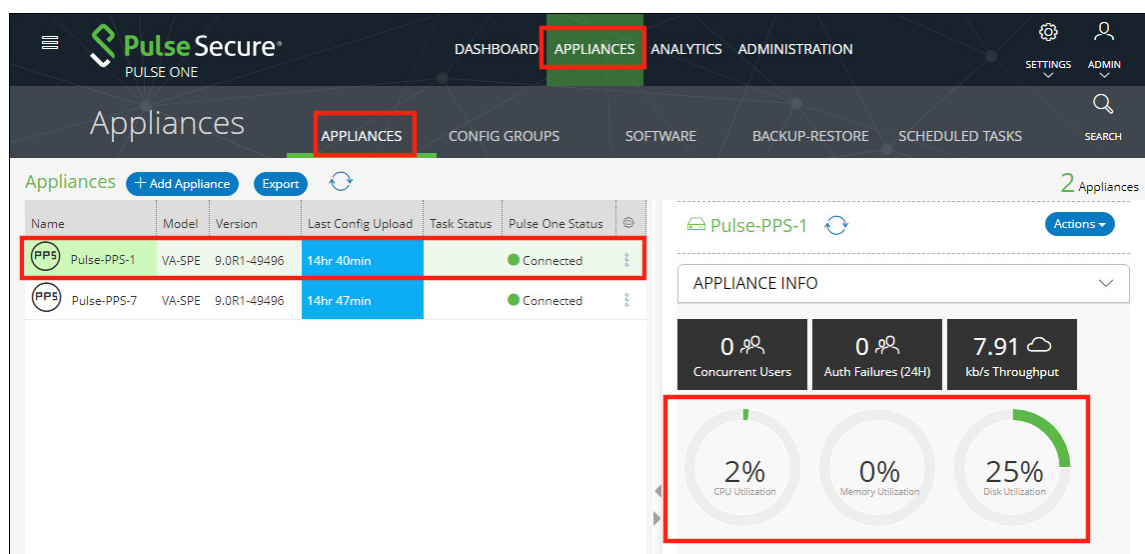
1. Log into Pulse One as an administrator.
2. Click the **Appliances** menu and then the **Appliances** tab.

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 24 Appliance Health



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 28.**

- “Adding Appliances to an Appliance Group” on page 32.
- “Distributing a Master Configuration” on page 34.

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.

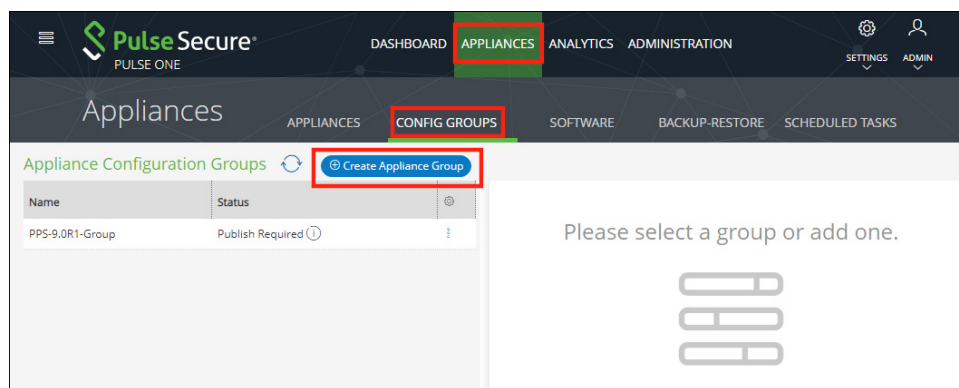
Examples:

- 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 25 Create Appliance Group



The **Create Appliance Group Wizard** appears.

FIGURE 26 Create Appliance Group Wizard

The screenshot shows the 'Create Appliance Group' wizard with the 'Introduction' step selected. The progress bar at the top has four segments: 'Introduction' (active), 'Group name and description', 'Group configuration settings', and 'Summary'. The main content area contains the following text:

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.

At the bottom, there are three buttons: 'Cancel', '< Previous', and 'Next >'.

4. Click **Next**.

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

FIGURE 27 Group Name and Description Wizard Panel

The screenshot shows the 'Create Appliance Group' wizard with the 'Group name and description' step selected. The progress bar at the top has four segments: 'Introduction', 'Group name and description' (active), 'Group configuration settings', and 'Summary'. The main content area contains the following form fields:

Group name and description

Group name:

Description:

DMI Information

Username:

Password:

Port:

At the bottom, there are three buttons: 'Cancel', '< Previous', and 'Next >'.

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.

6. Click **Next**.

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

FIGURE 28 Group Configuration Settings Wizard Panel

Create Appliance Group

Group configuration settings

Select master appliance: Ade_Pulse-106

Master appliance URL: https://10.64. /admin

Select from the list below to define the configuration settings to be used for the group. [Reset](#)

- ☒ System
- ☒ Authentication
- ☒ Administrators
- ☒ Users
- ☒ Maintenance

[Cancel](#) [< Previous](#) [Next >](#)

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.

- Click **Next**.

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

FIGURE 29 Summary Wizard Panel

Create Appliance Group

Introduction Group name and description Group configuration settings **Summary**

Summary

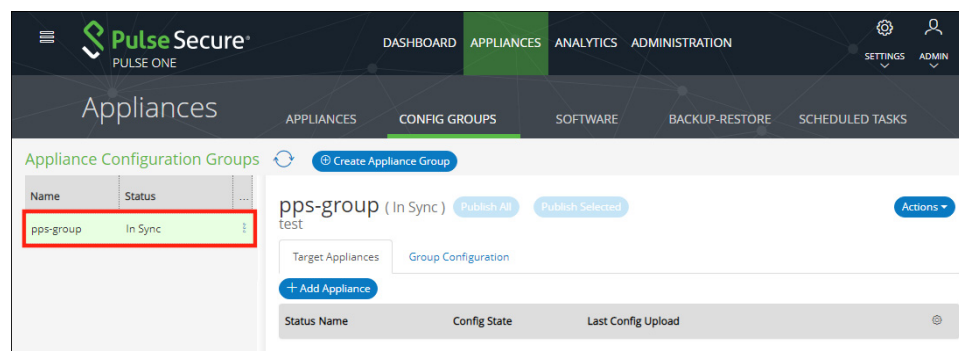
| | | |
|------------------------|------------------------|------|
| Group name: | pps_group | Edit |
| Description: | | Edit |
| Username: | | Edit |
| Password: | ***** | Edit |
| Port: | | Edit |
| Master appliance: | Ade_Pulse-106 | Edit |
| Master appliance URL: | https://10.64.../admin | Edit |
| Group config settings: | 99 | Edit |

Cancel < Previous Finish

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

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

FIGURE 30 New Appliance Group



You can now add appliances to the group as target appliances, see **“Adding Appliances to an Appliance Group” on page 32**.

Adding Appliances to an Appliance Group

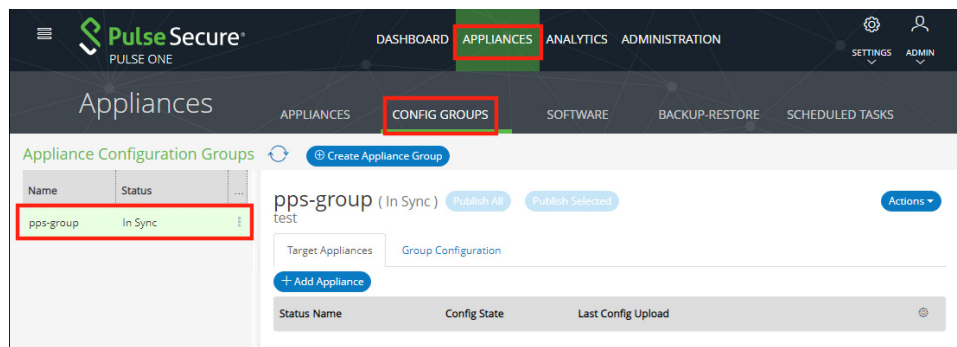
To add an appliance into an appliance group as a *target* appliance:

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 31 Target Appliances Empty



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

FIGURE 32 Select Target Appliance



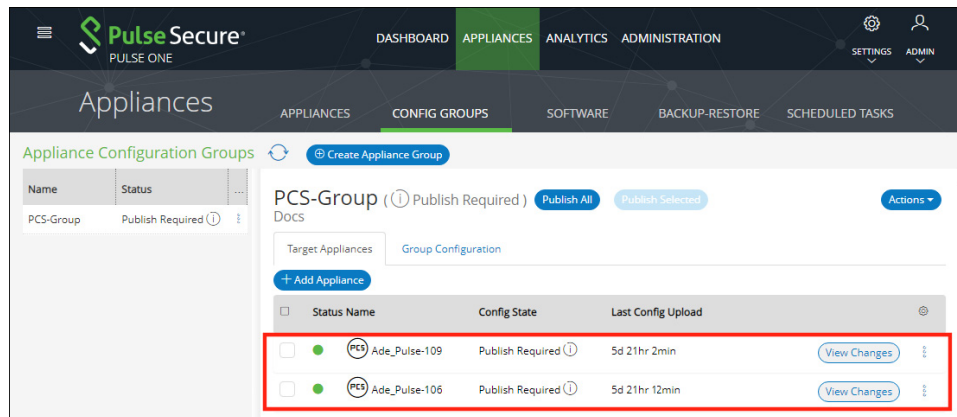
6. In this dialog, select an appliance to be added as a target appliance to the selected group.

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 33 Target Appliances Added



Distributing a Master Configuration

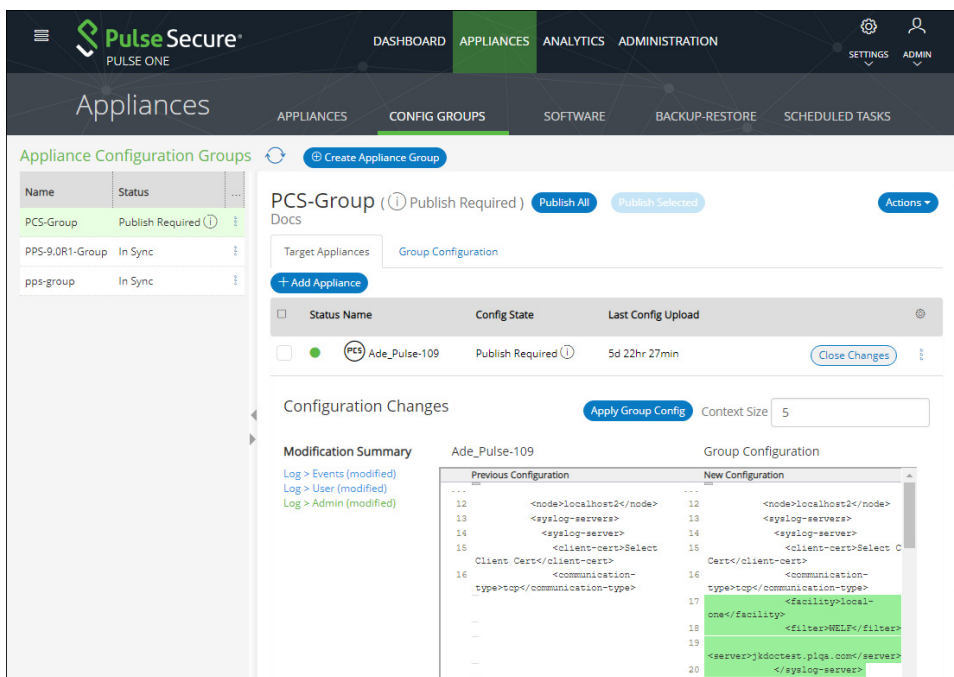
This section details the steps to distribute the configuration of the master appliance to all target appliances.

- “Viewing Configuration Changes” on page 34.
- “Publishing Configuration Changes Manually to Group Members” on page 34.
- “Publishing Configuration Changes to Group Members as a Scheduled Task” on page 37.

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 34 View Configuration Changes



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

Publishing Configuration Changes Manually to Group Members

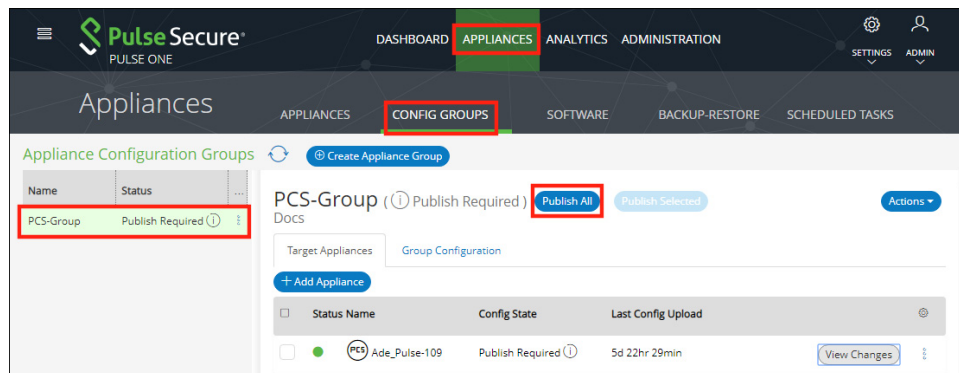
If the configuration of the master appliance differs from the configuration of the target appliances in its group, a *Publish Required* notification is displayed, and the **Publish All** button is enabled.

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 37.

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 35 Publish All



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

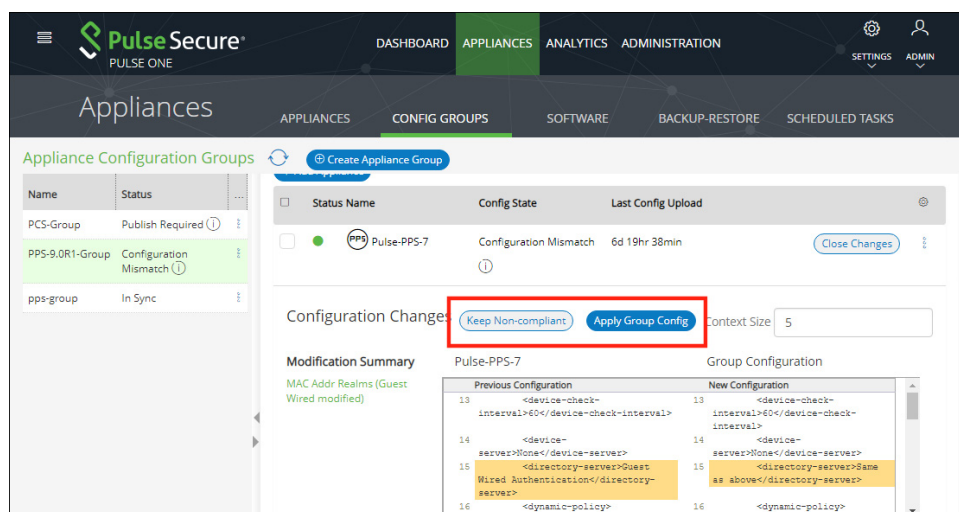
A confirmation dialog appears.

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 36 Configuration Change in Member Appliance



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

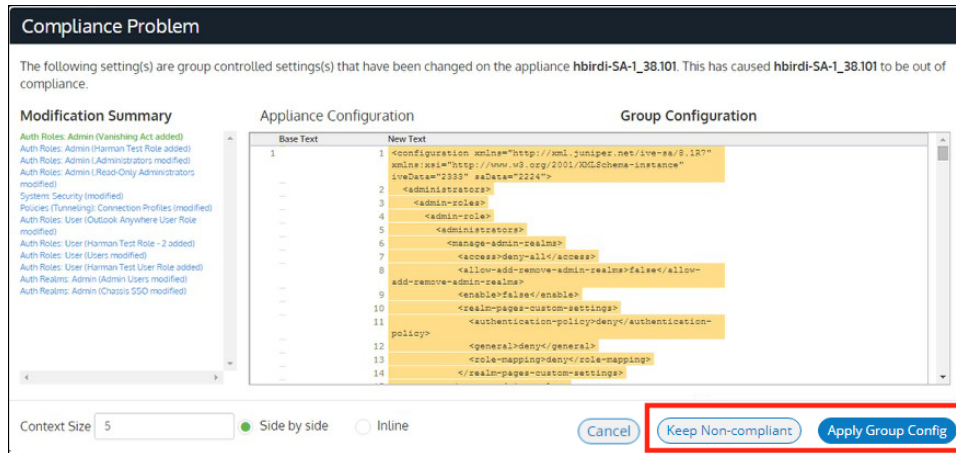
5. You can either:

- 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 37 Configuration Mismatch




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.

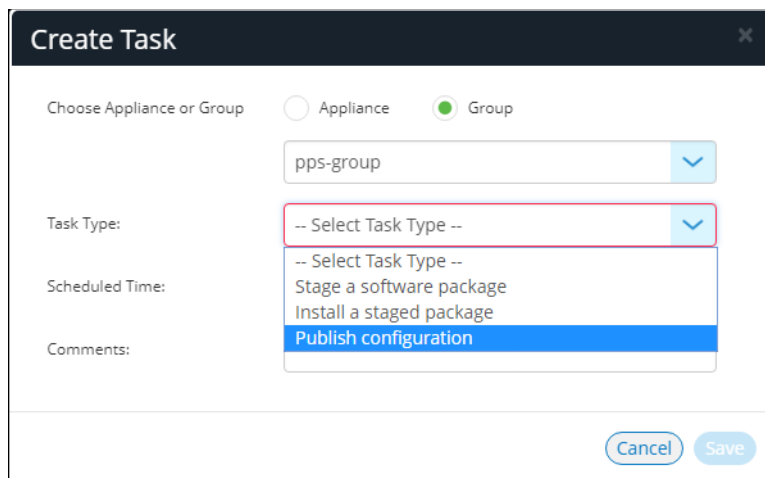
Note: Publishing configuration changes to an appliance group can also be performed manually, see [“Publishing Configuration Changes Manually to Group Members” on page 34](#).

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 38 Create Publish Configuration Task

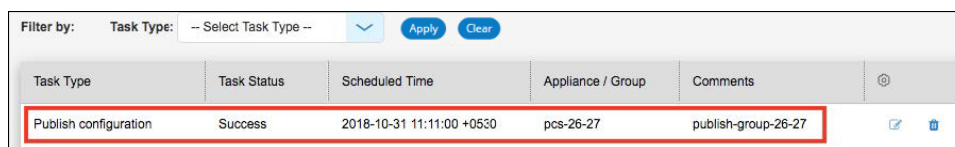




The **Create Task** dialog box is shown. It has a title bar with a close button. Below the title bar, there are two radio buttons: **Appliance** and **Group**, with **Group** selected. Below the radio buttons is a dropdown menu showing **pps-group**. Below that is a **Task Type:** dropdown menu with a red border, showing **-- Select Task Type --**. Below the **Task Type:** dropdown is a **Scheduled Time:** dropdown menu showing **-- Select Task Type --**, **Stage a software package**, **Install a staged package**, and **Publish configuration** (highlighted in blue). Below the **Scheduled Time:** dropdown is a **Comments:** text input field. At the bottom right are **Cancel** and **Save** buttons.


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 39 Scheduled Publish Configuration Task



| Filter by: Task Type: -- Select Task Type -- Apply Clear | | | | | |
|--|-------------|---------------------------|-------------------|---------------------|---|
| 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.

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.

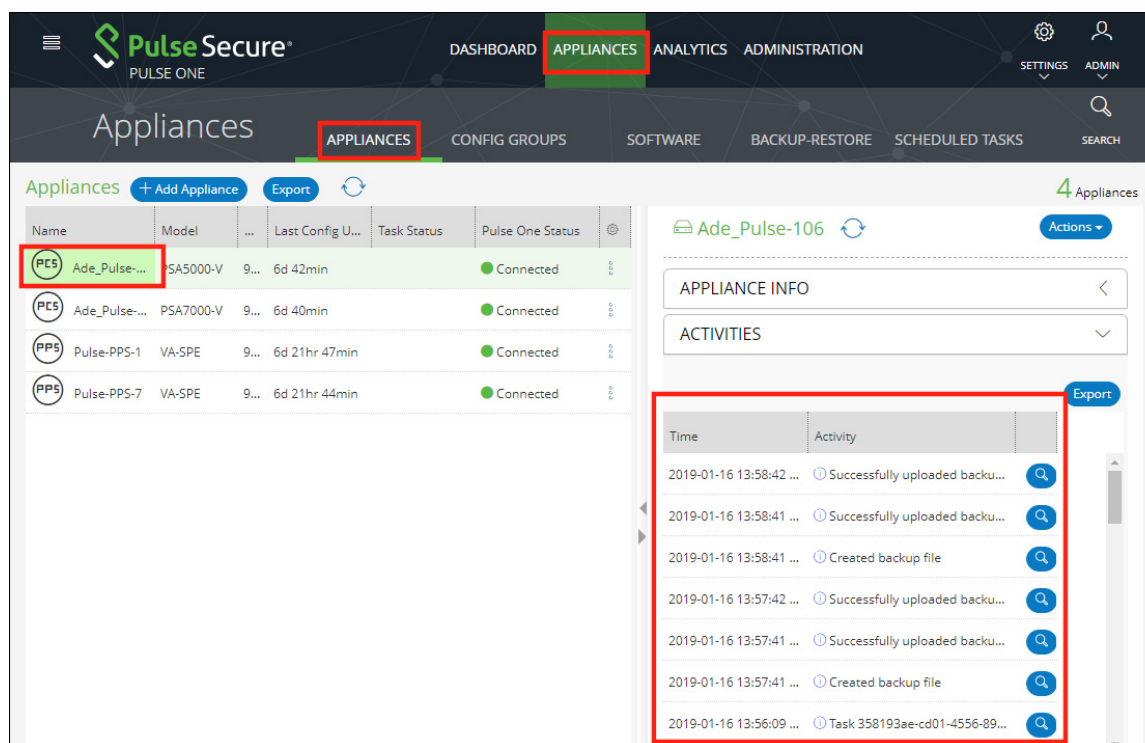
The **Appliances** tab displays all current appliances.

3. Select an appliance whose **Pulse One Status** is status *Connected*.

- In the panel on the right, expand **Activities** to display details of all activities.

For example:

FIGURE 40 Activities Details



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:

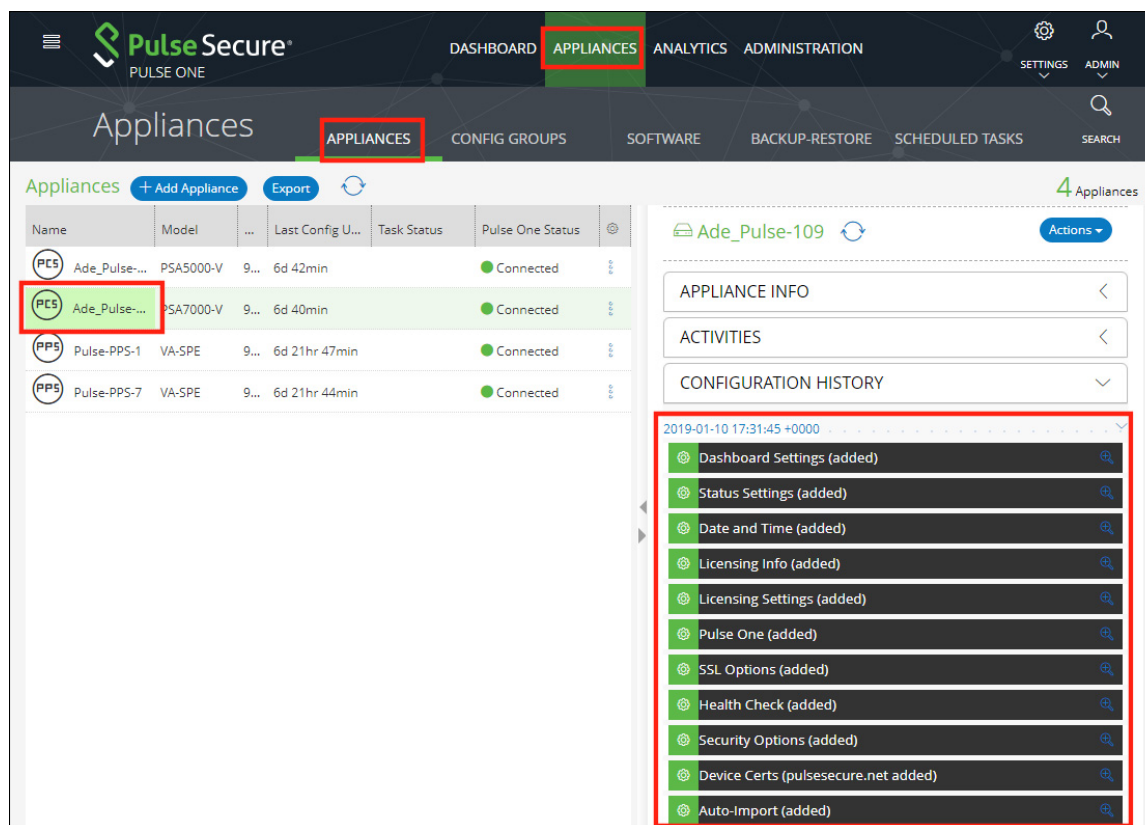
- Log into Pulse One as an administrator.
- Click the **Appliances** menu and then the **Appliances** tab.

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

- Select an appliance whose **Pulse One Status** is status *Connected*.
- In the panel on the right, select **Configuration History**. This displays the configuration changes history for the appliance, including timestamps for each change.

- Expand the required timestamp to view the changes made at that time. For example:

FIGURE 41 View Configuration Changes



Comparing Appliances

The Compare Appliances feature allows you to compare two appliances based on their settings.

To compare two appliances:

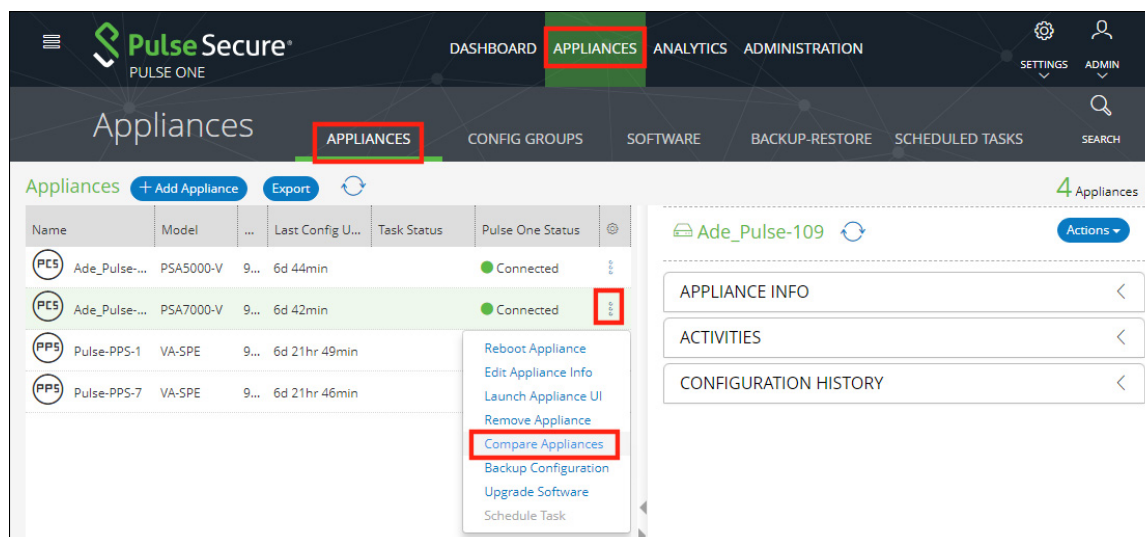
- Log into Pulse One as an administrator.
- Click the **Appliances** menu and then the **Appliances** tab.

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

- Select the source appliance that you want to compare and click its **Actions** icon (🔗).

- On the drop-down menu, click **Compare Appliances**.

FIGURE 42 Compare Appliances



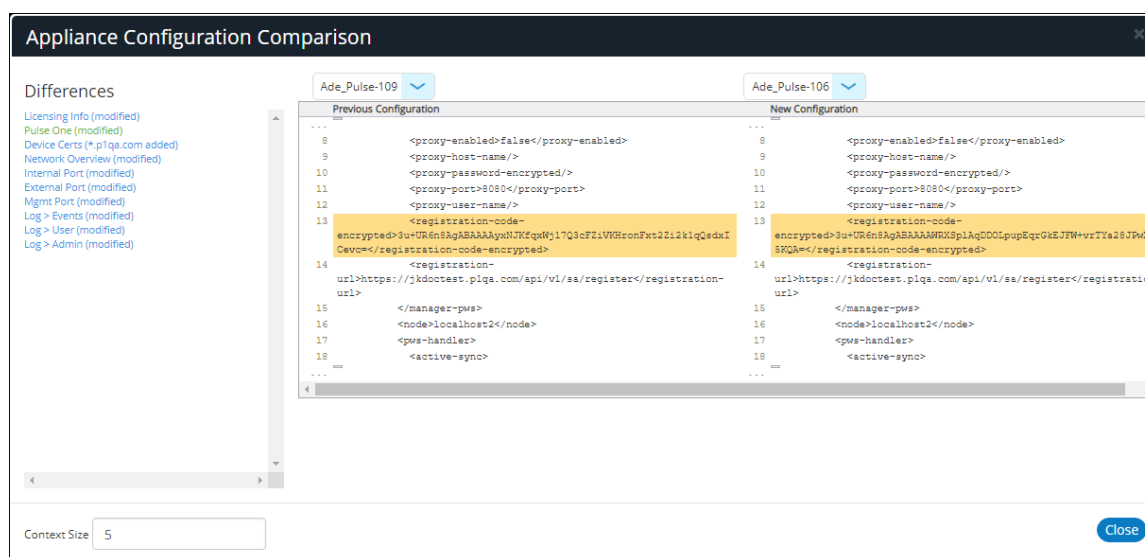
- In the **Appliance Configuration Comparison** window, select the source appliance and the target appliance to compare.

The **Differences** panel shows a list of settings that the two selected appliances have differences.

- 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 43 Appliance Configuration Comparison



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.


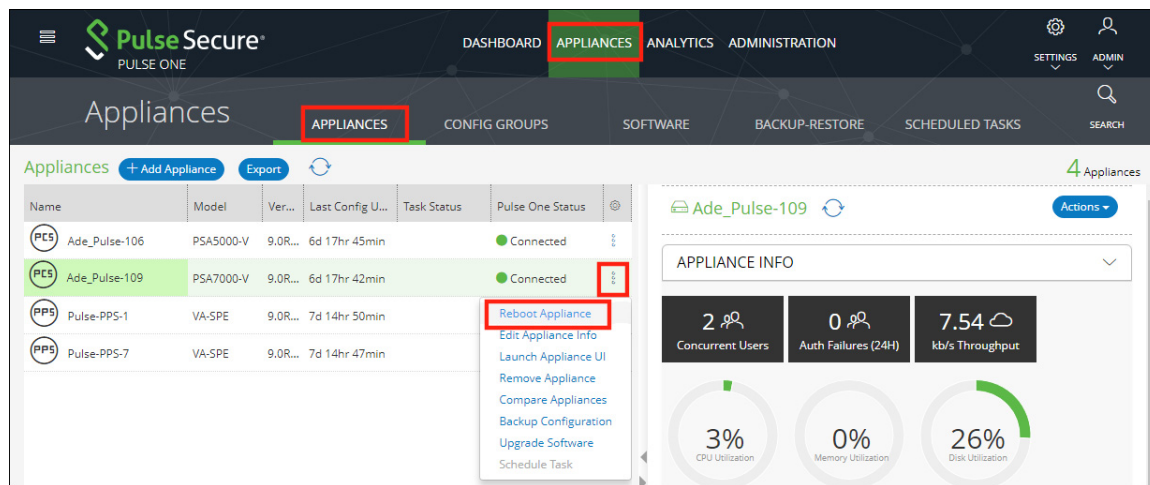
3. Select the appliance that you want to reboot and click the **Actions** icon ().
4. On the drop-down menu, click **Reboot Appliance**.

FIGURE 44 Reboot Appliance



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.

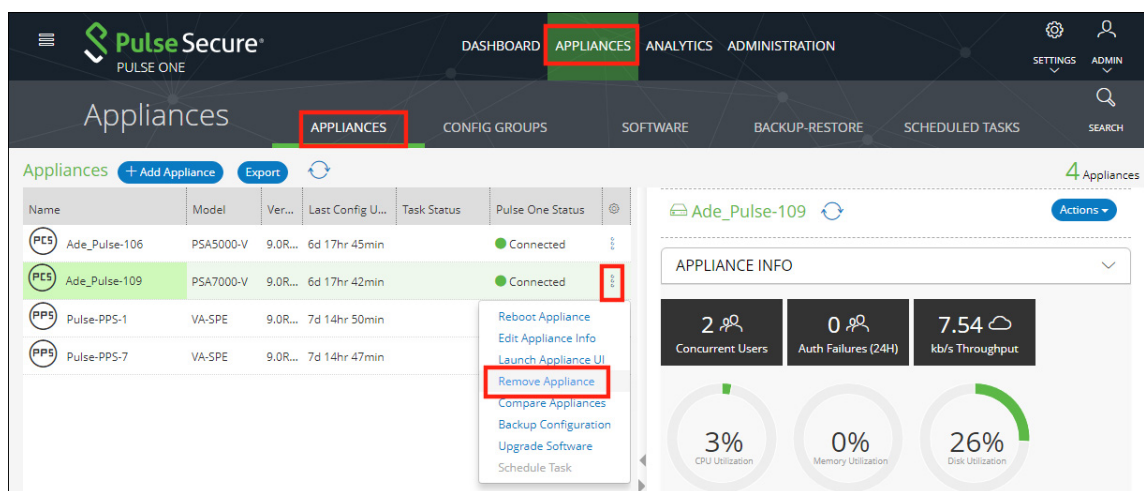
To remove an appliance:

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 45 Remove Appliance



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 79**.

Removing an Appliance from an Appliance Group

You can remove any appliance other than the master appliance from the appliance group.

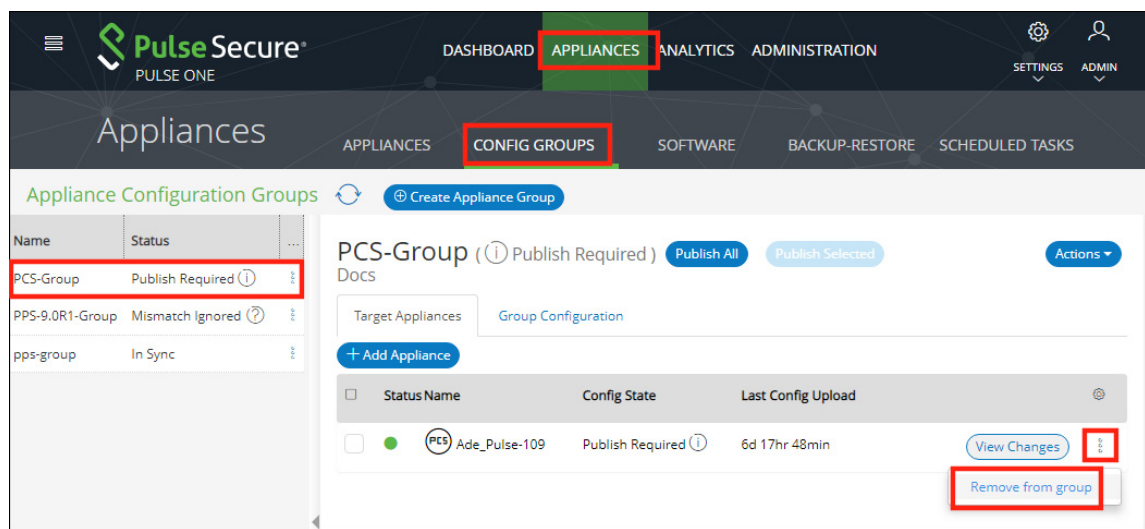
This section details the steps to remove an appliance from the group.

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.

- From the menu options, select **Remove from Group**. For example:

FIGURE 46 Remove from Group



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:

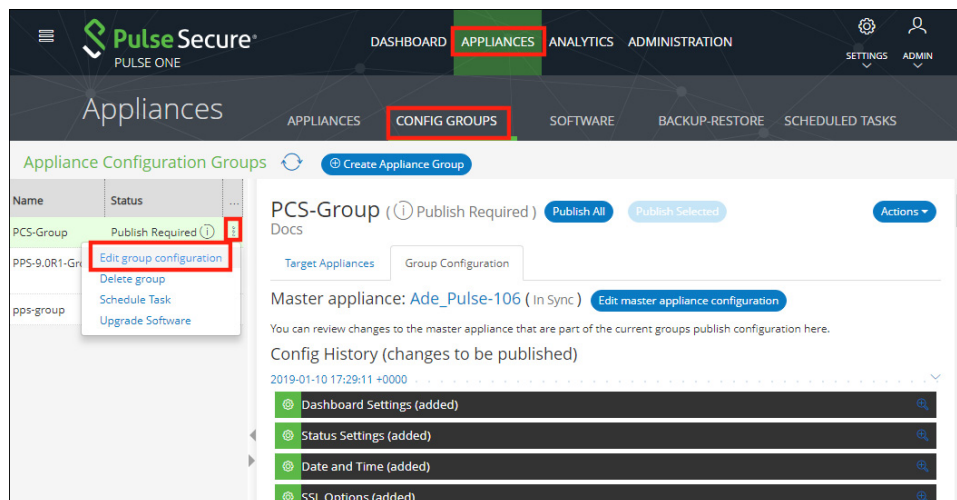
- Select the **Appliances** menu.
- Select the **Config Groups** tab.

A list of configuration groups is displayed.

- Select the group that you want to modify and click its **Actions** (⋮) icon.

- From the menu options, select **Edit Group Configuration**.

FIGURE 47 Edit Group Configuration



The **Edit Appliance Group** wizard appears. For example:

FIGURE 48 Edit Appliance Group Wizard

- Work through the wizard, making the required changes to the group name, master appliance, and configuration settings.
- 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 delete the group, and can be viewed as normal in the **Appliances** tab.

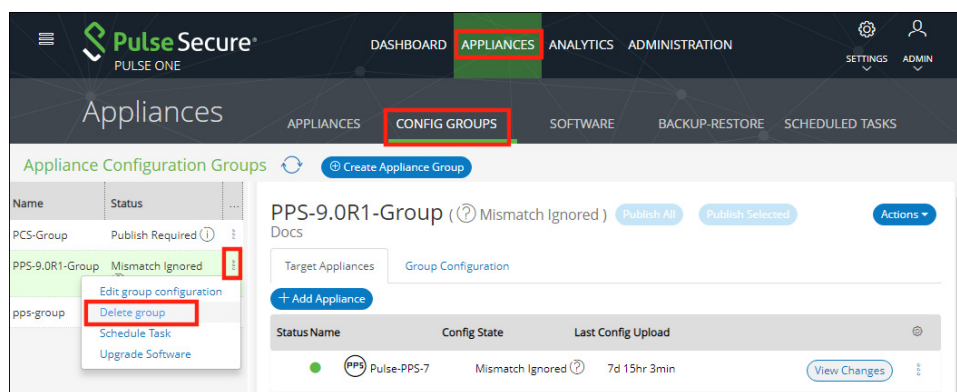
1. Select the **Appliances** menu.

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 49 Delete Group



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** 49
- **Viewing the Appliance Health Report** 50
- **Viewing the Appliance Activities Report** 51
- **Viewing Appliance Activities** 51

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 50 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:

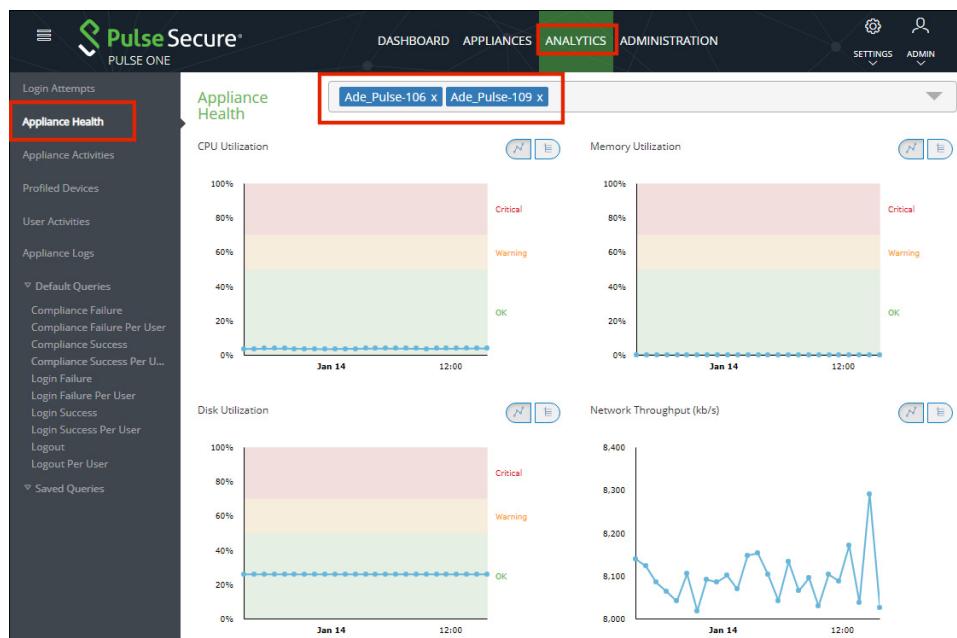
1. Select the **Analytics** menu.
2. Select **Appliance Health**.
3. From the **Appliance Health** drop-down, select one or more appliances for the report.

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 51 Appliance Health Report

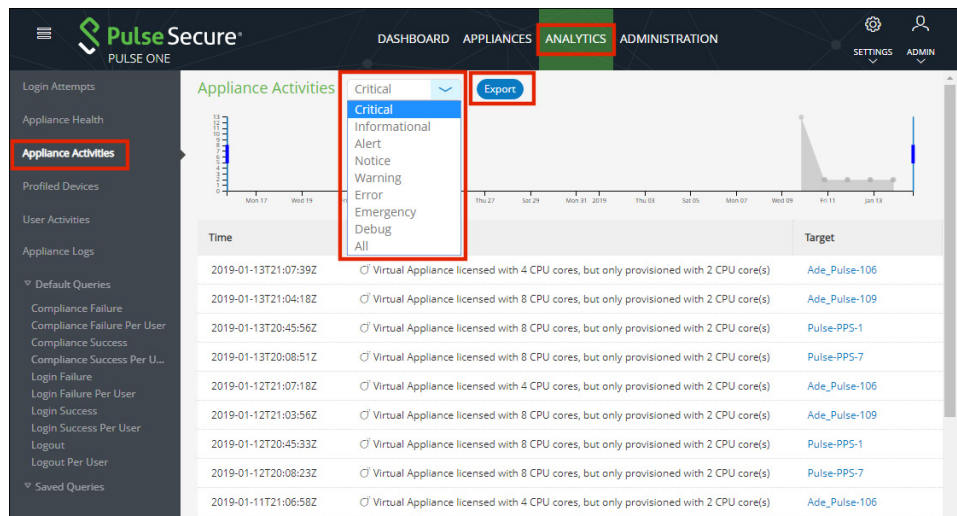


Viewing the Appliance Activities Report

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 52 Appliance Activities



4. (Optional) Click **Export** to download displayed information as a .csv format file.

Viewing Appliance Activities

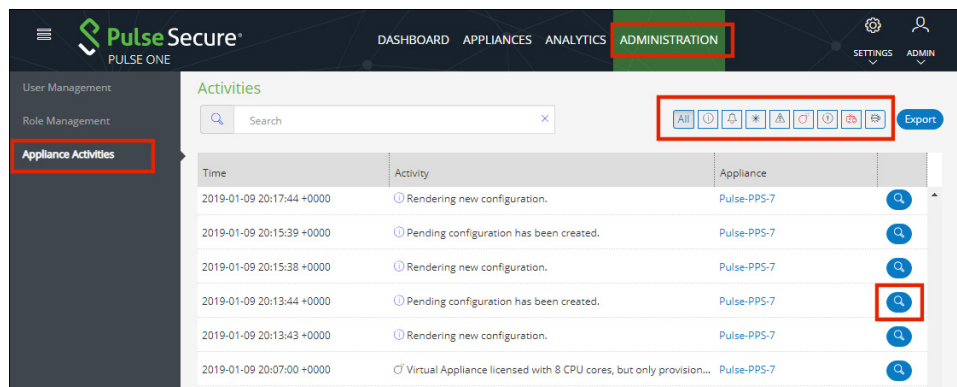
The **Appliance Activities** page displays information about the events registered in the Management Server. You can view filtered activities for appliances.

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.

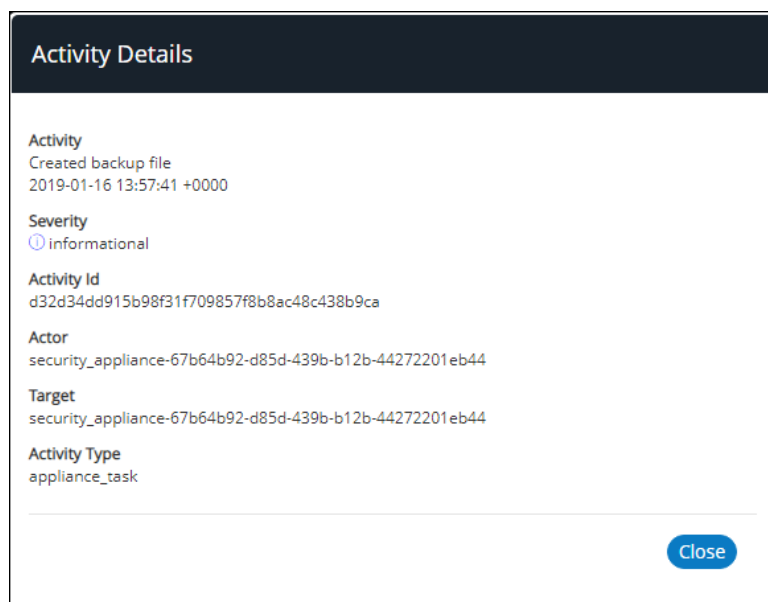
FIGURE 53 Filter Activities



4. Click the **Details** button associated with the activity you want to view the details.

The **Activity Details** dialog displays the additional details.

FIGURE 54 Activity Details



User Management

- **Adding an Admin User** 53
- **Editing User Details** 54
- **Removing an Admin User** 55
- **Resetting a User Password** 55
- **Suspending a User** 56

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 55 Add Admin User

The screenshot shows the 'Add Admin User' dialog box. It has a dark title bar with the text 'Add Admin User' and a close icon. Below the title bar are five input fields arranged vertically. The first field is 'Username' with the value 'po-user1'. The second field is 'Role' with a dropdown menu showing 'Read Only Admin'. The third field is 'Full Name' with the value 'Pulse One User-1'. The fourth field is 'Email' with the value 'pouser1@company.com'. The fifth field is 'Sign In Method' with a dropdown menu showing 'Enterprise SSO'. At the bottom right of the dialog are two buttons: 'Cancel' and 'Create'.

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.

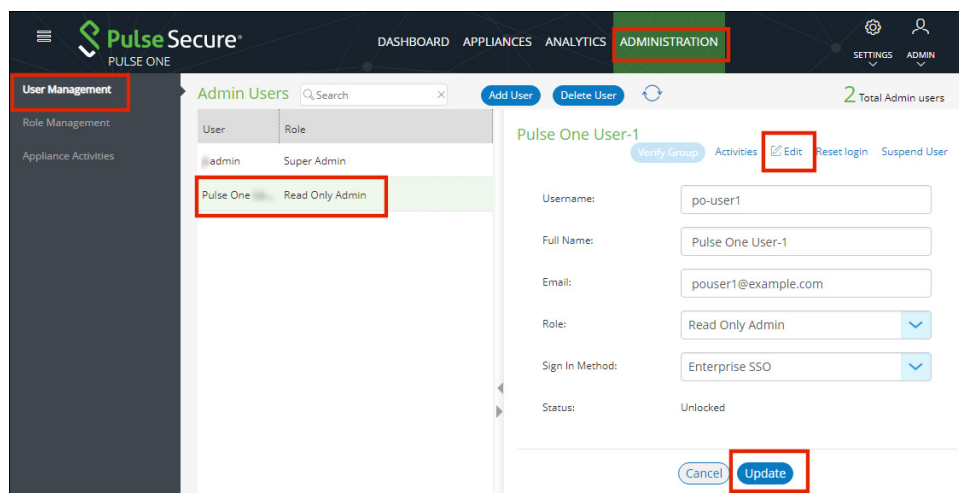
Editing User Details

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 56 Edit User Details



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.

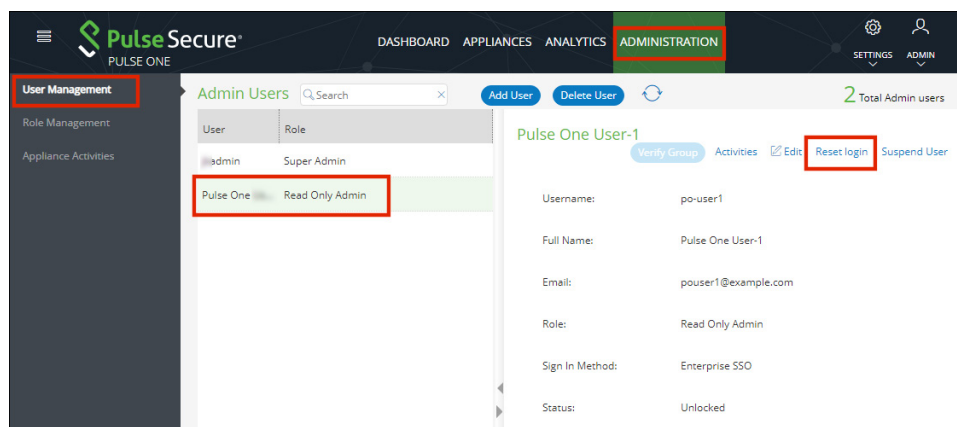
Resetting a User Password

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 57 Reset Login



Suspending a User

To suspend an admin user:

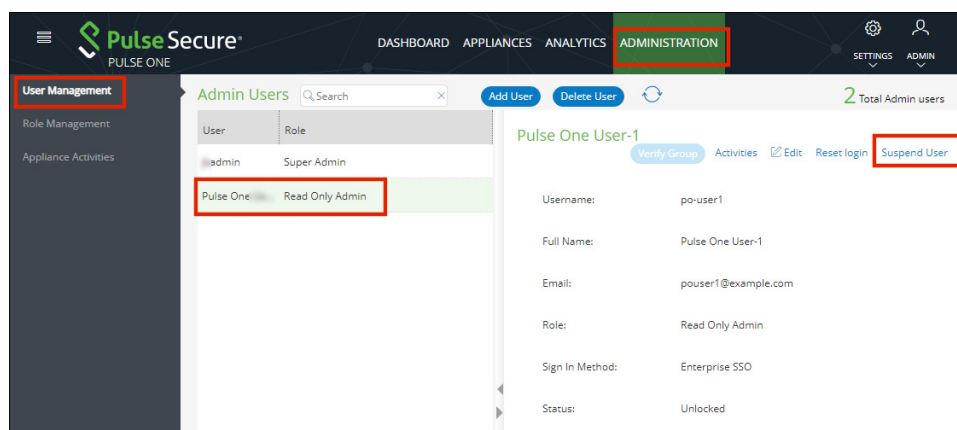
1. Select the user from the list.
2. Click **Suspend User**.

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 58 Suspend User



Role Management

- **Adding an Admin Defined Role** 57
- **Editing an Admin Role** 58
- **Removing an Admin Role** 58

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 59 Create New Role

Create New Role

Role Name:

Role Assignment

| | |
|------------------|-----------|
| Dashboard | Read Only |
| Settings | None |
| Service Accounts | None |
| ▶ Appliances | Delete |
| Users | Delete |
| ▶ Roles | Read Only |

6. Click **Create**.

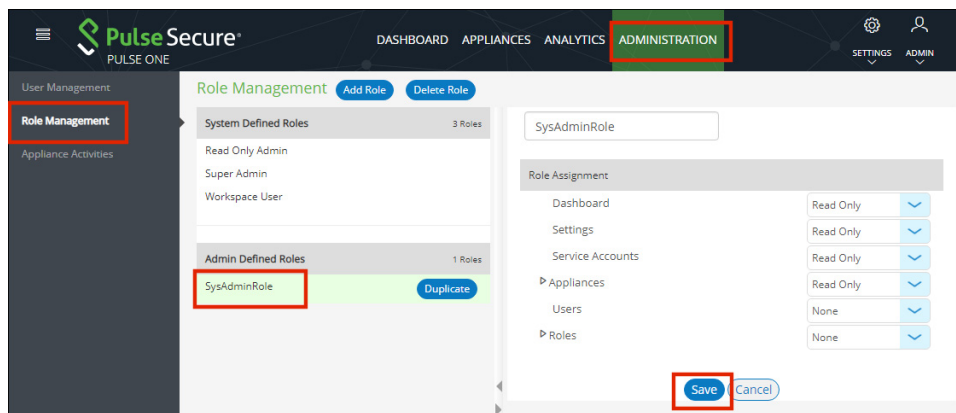
Editing an Admin Role

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 60 Modify Role



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](#) 59
- [Editing Pulse One Properties](#) 59
- [Understanding Pulse One Properties](#) 60

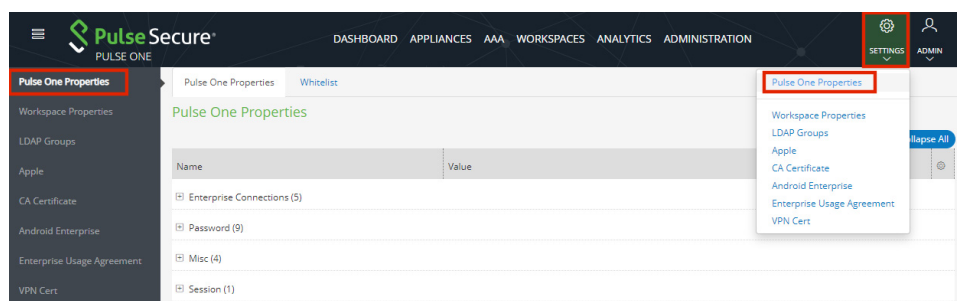
Viewing Pulse One Properties

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 61 Pulse One Properties

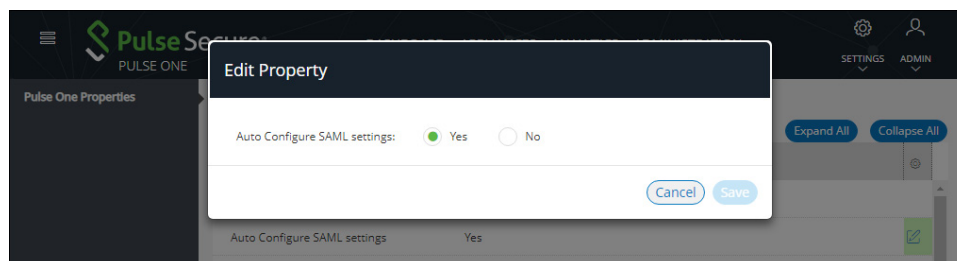


Editing Pulse One Properties

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 62 Edit Properties



Understanding Pulse One Properties

All Pulse One properties are described in the following sections:

- [“Enterprise Connection Properties” on page 60](#)
- [“Password Properties” on page 60](#)
- [“Miscellaneous Properties” on page 61](#)
- [“Session Properties” on page 61](#)

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 76](#).
- **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.

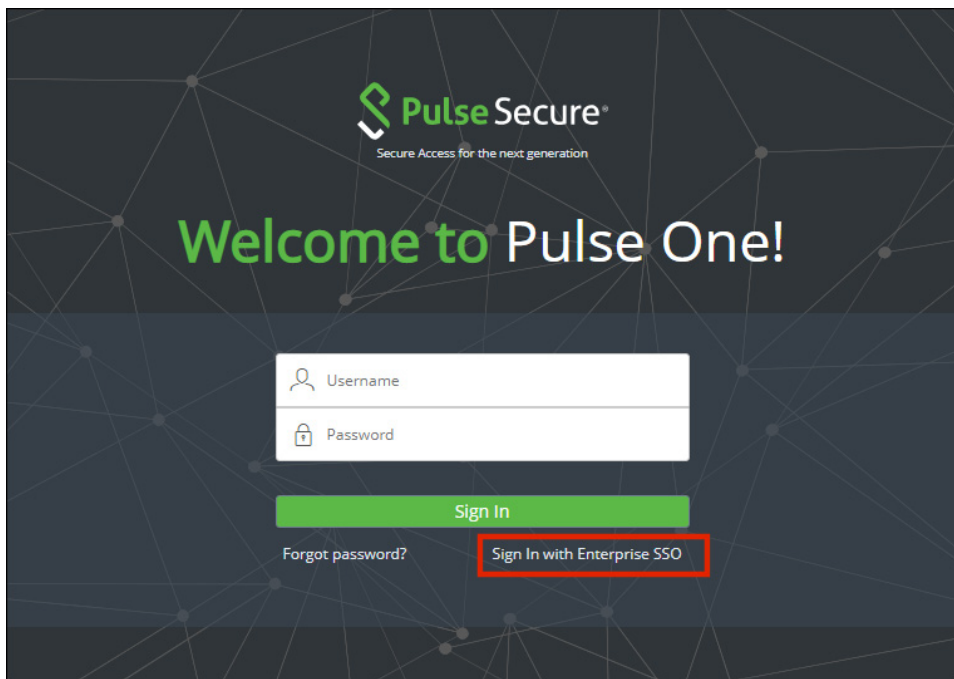
Configuring Enterprise SSO Using SAML

- **Overview** 63
- **Configuring SAML idP in Pulse Connect Secure Server**..... 64
- **Automatically Configuring a SAML idP on Pulse One** 68
- **Configuring a Metadata Provider in Pulse Connect Secure**..... 70
- **Enabling Enterprise SSO in Pulse One Appliance**..... 71
- **Configuring SAML Metadata in Pulse One** 71
- **Adding SAML SP Metadata in Pulse Connect Secure Server** 72
- **Automatically Creating Pulse One Users for SAML SSO Logins**..... 76
- **Testing Sign In with Enterprise SSO** 78

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 63 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 64.](#)
- [“Automatically Configuring a SAML idP on Pulse One” on page 68.](#)
- (Optional) [“Automatically Creating Pulse One Users for SAML SSO Logins” on page 76.](#)
- [“Testing Sign In with Enterprise SSO” on page 78.](#)

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 64.](#)
- [“Configuring a Metadata Provider in Pulse Connect Secure” on page 70.](#)
- [“Enabling Enterprise SSO in Pulse One Appliance” on page 71.](#)
- [“Configuring SAML Metadata in Pulse One” on page 71.](#)
- [“Adding SAML SP Metadata in Pulse Connect Secure Server” on page 72.](#)
- (Optional) [“Automatically Creating Pulse One Users for SAML SSO Logins” on page 76.](#)
- [“Testing Sign In with Enterprise SSO” on page 78.](#)

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 21.](#)

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 64 SAML Settings

Pulse Secure **Pulse Connect Secure**

System Authentication Administrators Users Maintenance Wizards

SAML > **Settings**

▼ Metadata Server Configuration

Timeout value for metadata fetch request: seconds 1 - 600. Specifies the time in seconds to wait for response of SAML metadata fetch request.

Validity of uploaded/downloaded metadata file: days 0 - 9999. Specifies the time in days after which downloaded/uploaded metadata file expires. 0 means that Connect Secure does not enforce any validity on the peer metadata file.

Host FQDN for SAML: 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.

Save Changes **Cancel** **Update Entity Ids**

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**.

- 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 65 Import Certificate and Keys

The screenshot shows the Pulse Secure web interface. The top navigation bar has 'System' highlighted. Under 'Configuration', 'Certificates' is highlighted. The 'Device Certificate' page is displayed. A red box highlights the 'Import Certificate & Key...' button. Below the table, another red box highlights the 'New CSR...' button.

| | Certificate issued to | Issued by | Valid Dates | Used by |
|--------------------------|-----------------------|-------------------|--|----------------------|
| <input type="checkbox"/> | secure.net | psqalab-CA | Aug 30 06:06:04 2017 GMT to Aug 30 06:06:04 2019 GMT | <Internal Port> |
| <input type="checkbox"/> | test.seqaertserv.com | EnterpriseSub2-CA | May 2 15:18:09 2016 GMT to Apr 9 17:22:15 2018 GMT ⚠ | VP1, <External Port> |
| <input type="checkbox"/> | 10.30. | EXCHSRVCA | Oct 30 08:53:19 2017 GMT to Oct 30 08:53:19 2019 GMT | ext-AS-VP |
| <input type="checkbox"/> | 10.209. | EXCHSRVCA | Oct 30 09:02:41 2017 GMT to Oct 30 09:02:41 2019 GMT | |
| <input type="checkbox"/> | 10.209. | EXCHSRVCA | Oct 30 09:58:22 2017 GMT to Oct 30 09:58:22 2019 GMT | test |

- Navigate to **Authentication > Signing In > Sign In SAML > Identity Provider**.

7. Locate the the **Basic Identity Provider (idP) Configuration** section. For example:

FIGURE 66 Basic Identity Provider Configuration

Pulse Secure Pulse Connect Secure

System **Authentication** Administrators Users Maintenance Wizards

Signing In

Sign-in Policies Sign-in Pages Sign-in Notifications **Sign-in SAML**

Metadata Provider **Identity Provider**

▼ **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 Algorithm that needs to be used for generating signature for SAML assertion and response

☐ Sha-256

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 63](#).

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 21](#).
- Configured the SAML idP on Pulse Connect Secure, see [“Configuring SAML idP in Pulse Connect Secure Server” on page 64](#).

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 67 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.

- Set the **SAML Identity Provider** property to match the appliance name, as registered on Pulse One. For example:

FIGURE 68 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.

- (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 69 Pulse Connect Secure SAML Auto-configuration

| Pulse Connect Secure | | | | | | | |
|---|----------------|--------------------|-----------------------------------|---------------------|--------|-------------------|----------|
| <div> <div>Pulse Secure</div> <div>System Authentication Administrators Users Maintenance Wizards</div> </div> | | | | | | | |
| <div> <div>Configuration</div> <div>SAML</div> <div>Licensing Pulse One Security Certificates DMI Agent NCP Sensors Client Types Pulse Collaboration Virtual Desktops User Record Synchronization</div> <div>IKEv2 SAML Mobile VPN Tunneling Telemetry</div> </div> | | | | | | | |
| <div> <div>New Metadata Provider Delete Refresh Settings</div> <div>10 records per page</div> <div>Search:</div> </div> | | | | | | | |
| | Metadata Name | Entity Ids | Roles | Valid Till | Status | Metadata Location | Download |
| <input type="checkbox"/> | | | SP | 2038-01-18 19:14:07 | | Local | • |
| <input type="checkbox"/> | AutoConfigured | https:// realm= | /api/v1/saml/sso? /sp-metadata | 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 76.**
- Move directly to testing the SSO login, see **“Testing Sign In with Enterprise SSO” on page 78.**

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 68](#).

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 70 Metadata Provider

The screenshot displays the Pulse Connect Secure web interface. At the top, the navigation bar includes 'System', 'Authentication' (highlighted with a red box), 'Administrators', 'Users', 'Maintenance', and 'Wizards'. Under 'Authentication', the 'Sign-in SAML' sub-menu is active, and the 'Metadata Provider' option is highlighted with a red box. The configuration form for the SAML Metadata provider is shown below. It includes fields for 'Entity Id' (pre-populated), 'Metadata Validity' (set to 365 days), and a checkbox for 'Do Not Publish IdP in Metadata' (unchecked). The 'Download Metadata' button is highlighted with a red box. At the bottom, there are buttons for 'Save Metadata Provider' and 'Cancel'.

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 68](#).

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 71 Sign In Method

The screenshot shows a web form titled "Add Admin User" with a close button (X) in the top right corner. The form contains the following fields:

- Username:** A text input field containing "po-user1".
- Role:** A dropdown menu showing "Read Only Admin" with a downward arrow.
- Full Name:** A text input field containing "Pulse One User-1".
- Email:** A text input field containing "pouser1@company.com".
- Sign In Method:** A dropdown menu showing "Enterprise SSO" with a downward arrow.

At the bottom right of the form, there are two buttons: "Cancel" (outlined) and "Create" (solid blue).

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

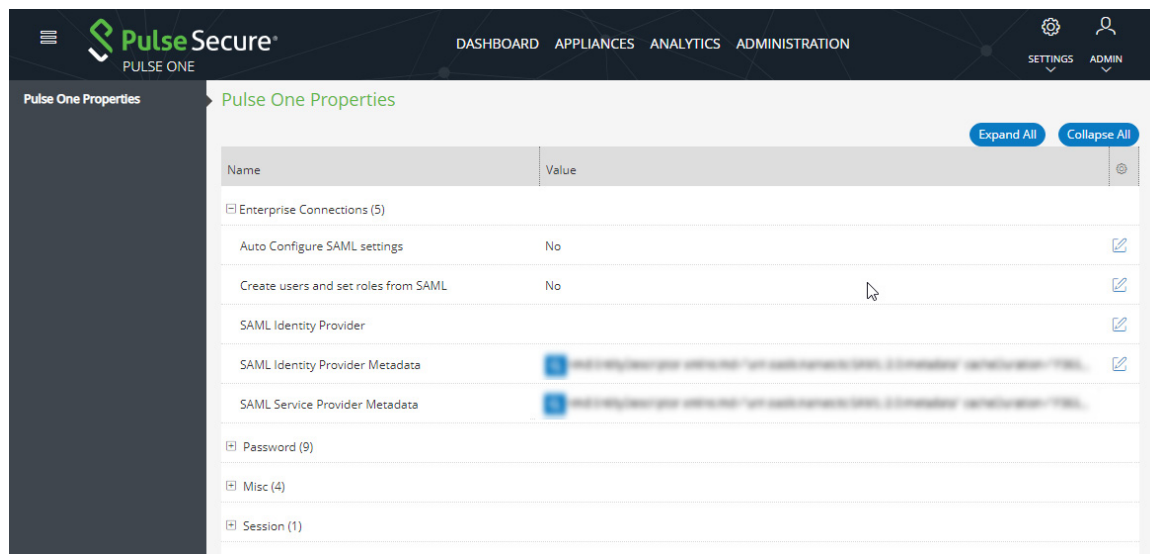
Note: You do not have to perform the process in the section if your appliance is at v8.3r1 or later, and you have already performed auto-configuration of SAML, see [“Automatically Configuring a SAML idP on Pulse One” on page 68](#).

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**.

- 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.
- 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 72 Pulse One Properties



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 68](#).

This section provides the steps to add SAML Service Provider metadata in PCS server.

- Navigate to **System > Configuration > SAML**.
- Click **New Metadata Provider**.
- 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 73 Metadata Provider Location Configuration

SAML >

New Metadata Provider

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 74 Service Provider

▼ **Metadata Provider Filter Configuration**

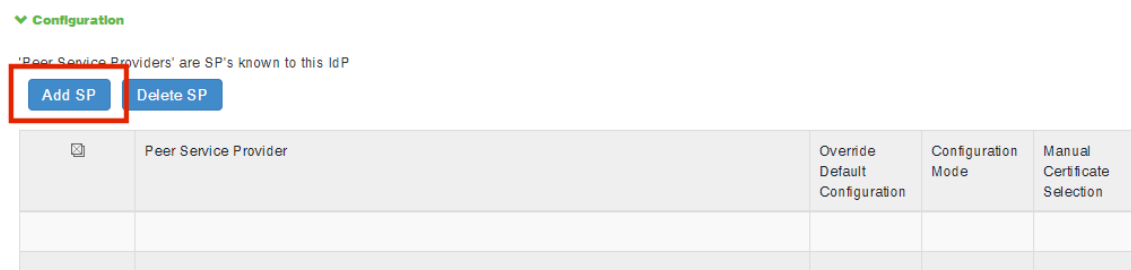
Roles: ☐ Identity Provider ☒ Service Provider ☐ Policy Decision Point Roles which Connect Secure looks for in the metadata file.

Entity ids to import:

7. Click **Save Changes**.8. Navigate to **Authentication > Signing In > Sign-In SAML > Identity Provider**.

- In the **Configuration** section, click **Add SP**.

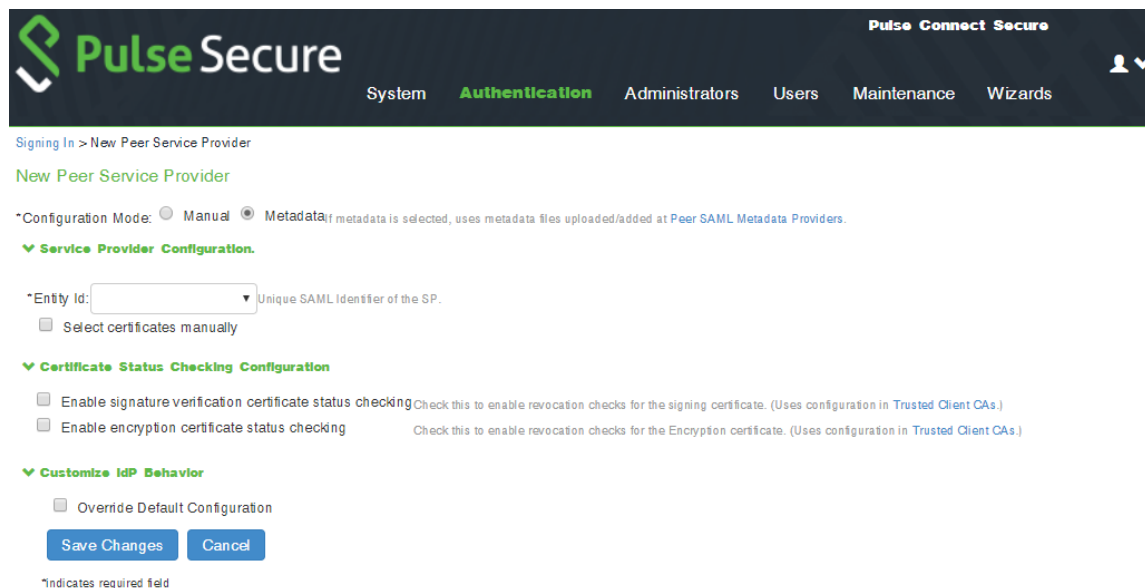
FIGURE 75 SAML Identity Provider



The **New Peer Service Provider** page appears.

- 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 76 New Peer Service Provider



- In the **Customize IdP Behavior** section, select the **Override Default Configuration** check box.
- Clear the **Reuse Existing NC (Pulse) Session** check box.

13. Select the **Accept unsigned AuthnRequest** check box.

FIGURE 77 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.
Algorithm that needs to be used for generating signature for SAML assertion and response

*Signature Algorithm: ☐ Sha-1 ☒ Sha-256

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: 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: Format of 'NameIdentifier' field in generated Assertion.

* Subject Name: 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 76.**
- Move directly to testing the SSO login, see **"Testing Sign In with Enterprise SSO" on page 78.**

Automatically Creating Pulse One Users for SAML SSO Logins

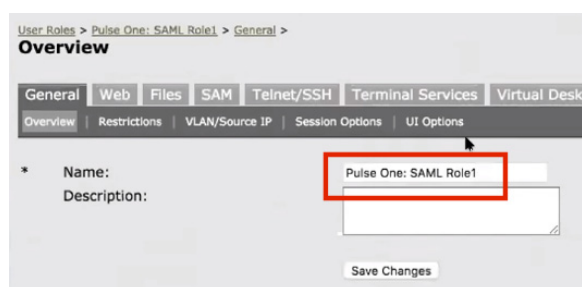
Note: This section is optional for all PCS appliance versions.

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:

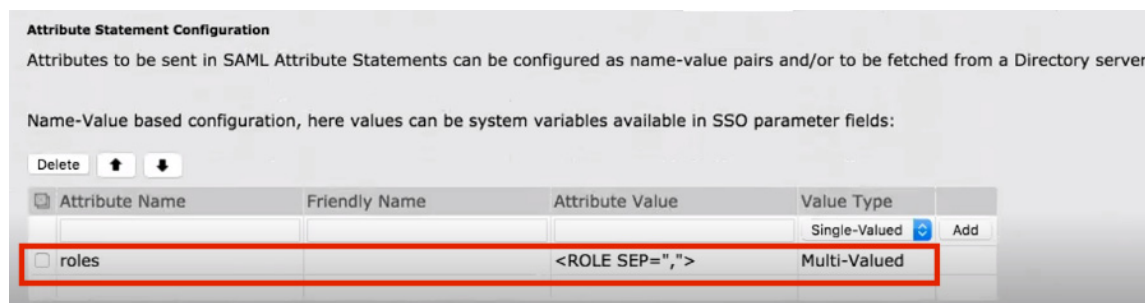
FIGURE 78 PCS User Roles



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:

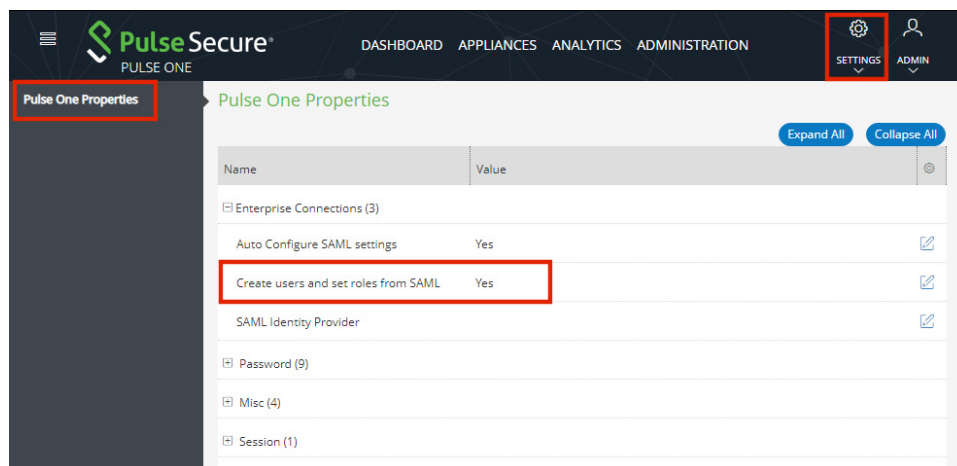
FIGURE 79 Attribute Statement Configuration



6. Log into Pulse One.

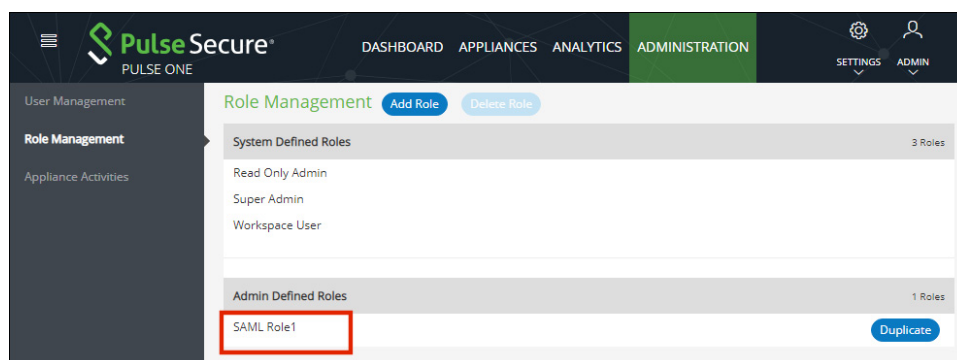
7. Click the **Settings** icon on top-right-corner of the page.
8. Select **Pulse One Properties**.
9. Under **Enterprise Connections**, ensure that the **Create users and roles from SAML** property is set to Yes.

FIGURE 80 Pulse One Properties Enterprise Connections



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 81 Pulse One Admin Defined Roles



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 82 Pulse One Properties



You are navigated to the Pulse Connect Secure login page.

2. Enter your Username and Password, and click **Sign In**.

FIGURE 83 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=PMDRootCA]/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/realms[name=TestRealm1]/authentication-policy/radius-request-attributes-policies/selected-policies] Invalid reference: no 'RADIUS Request Attributes Policy' object found with identifier '2 nd Request Policy'. | Configure the appropriate 'RADIUS Request Attributes Policy' under Endpoint Policy > Network Access > Radius Attributes. |