

Pulse One Appliance Administration Guide

Supporting Pulse One Appliance 2.0.1901

Product Release2.0.1901Published15 May 2019Document Version1.1

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

www.pulsesecure.net

© 2019 by 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	
Changing the User Password	8
Adding Pulse One Licenses	9
Whitelisting IP Addresses for Admin Login	9
WORKING WITH PULSE ONE DASHBOARDS1	3
Introduction	3
Viewing Overall System Health1	3
VIEWING METRICS FOR APPLIANCES1	4
Customizing Dashboards and Widgets1	6
Adding a New Widget 1	7
Editing the Dashboard Layout1	8
Editing Widget Configuration2	0
APPLIANCE MANAGEMENT	1
REGISTERING AN EXISTING PCS/PPS APPLIANCE2	
Editing Appliance Information2	
Launching the User Interface for an Appliance	4
Configuring an Appliance to Connect to Pulse One	
Completing Registration of an Appliance2	
Configuring Log Settings on the Appliance	
Configuring ActiveSync Handler2	
CREATING AND REGISTERING A PCS APPLIANCE VM ON VSPHERE	
CREATING AN APPLIANCE MASTER TEMPLATE ON VSPHERE	
Creating and Registering a PCS Appliance VM on AWS4	
Identifying the Required Route 53 Zones4	2

IDENTIFYING THE REQUIRED VPC ID AND SUBNET IDS
IDENTIFYING THE EC2 DEPLOYMENT KEY AND AMI ID
CREATING THE PCS APPLIANCE VM ON AWS
Configuring CPU, Memory and Disk Utilization55
Backing up and Restoring Appliance Configurations
Backing up the Configuration of an Appliance
Deleting the Configuration Backup for an Appliance
Restoring the Configuration of an Appliance
Working with Appliance Groups61
CREATING AN APPLIANCE GROUP61
Adding Appliances to an Appliance Group
DISTRIBUTING A MASTER CONFIGURATION67
Upgrading Managed Appliances71
Uploading an Appliance Software Package to Pulse One
Checking DMI Settings
Upgrading an Appliance
Upgrading All Target Appliances in a Group
Upgrading All Appliances in a Cluster
Scheduling Upgrade-Related Tasks
VIEWING THE ACTIVITIES LOG FOR AN APPLIANCE
VIEWING THE CONFIGURATION CHANGE HISTORY FOR AN APPLIANCE
COMPARING APPLIANCES
Rebooting an Appliance
Removing an Appliance from Pulse One
Preparing a Target Appliance
Preparing an RSA Agent Instance for the Target Appliance
Removing an Appliance from an Appliance Group
Editing an Appliance Group94
Deleting an Appliance Group
VIEWING ANALYTICS AND REPORTS
VIEWING THE LOGIN ATTEMPTS REPORT97
Viewing the Appliance Health Report
VIEWING THE PROFILED DEVICES REPORT
VIEWING THE APPLIANCE ACTIVITIES REPORT
VIEWING THE USER ACTIVITIES REPORT
Viewing Log Aggregation and Analysis
VIEWING APPLIANCE ACTIVITIES
USER MANAGEMENT
Adding an Admin User

Editing User Details	
Removing an Admin User	109
Resetting a User Password	
Suspending a User	
ROLE MANAGEMENT	111
Adding an Admin Defined Role	111
Editing an Admin Role	
Removing an Admin Role	112
WORKING WITH PULSE ONE PROPERTIES	113
VIEWING PULSE ONE PROPERTIES	
Editing Pulse One Properties	
Understanding Pulse One Properties	
ENTERPRISE CONNECTION PROPERTIES	
Password Properties	
Miscellaneous Properties	
CONFIGURING ENTERPRISE SSO USING SAML	117
Overview	
Configuring SAML IDP in Pulse Connect Secure Server	
Automatically Configuring a SAML idP on Pulse One	
Configuring a Metadata Provider in Pulse Connect Secure	
ENABLING ENTERPRISE SSO IN PULSE ONE APPLIANCE	
Configuring SAML Metadata in Pulse One	
Adding SAML SP Metadata in Pulse Connect Secure Server	
AUTOMATICALLY CREATING PULSE ONE USERS FOR SAML SSO LOGINS	
Testing Sign In with Enterprise SSO	132
APPENDIX: CHECKLIST FOR PREPARING A TARGET APPLIANCE	133

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					
italic text	Identifies emphasis					
	Identifies variables					
	Identifies document titles					
Courier Font	Identifies command output					
	Identifies command syntax examples					

Command syntax conventions

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

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

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

Notes and Warnings

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

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

ATTENTION

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

CAUTION

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

Requesting Technical Support

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

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

Self-Help Online Tools and Resources

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

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

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

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

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

Opening a Case with PSGSC

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

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

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

Getting Started With Pulse One

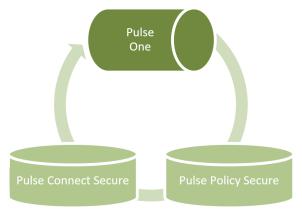
•	Overview of Pulse One	5
•	Logging Into Pulse One	6
•	Changing the User Password	8
•	Adding Pulse One Licenses	9
•	Whitelisting IP Addresses for Admin Login	9

Overview of Pulse One

Pulse One provides unified management of Pulse Connect Secure and Pulse Policy Secure in a single easy-touse 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 114.

IGURE 2	Pulse On	e Login Page				
	K		JISE Secure	5.		
	We	lcome	to Pul	se On	e!	
		Q Username	X /			
		Password	2			
			Sign In			
		Forgot password?	Sign In with Er	iterprise SSO		
	X					

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).

			×
1	2	3	4
Welcome	Manage Appliances	Enable BYOD	Get Started
Pulse One is a centralize Secure or Pulse Policy S		Pulse Secure hardware series, runnin	g either Pulse Connect
	What'	s New!	
 New dashboard 	widgets are available to add	to your dashboards. These includ	le:
 App Visi Appliance Go to the new A 			>
Don't show this to me again			START NOW

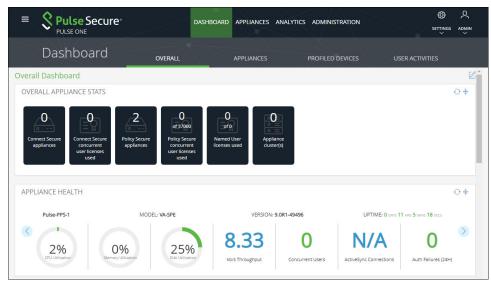
FIGURE 3 Pulse One Welcome Wizard

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:

Pulse One Home Page FIGURE 4



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

Changing the User Password

To change the user password:

FIGURE 5

- 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.

```
Change Password
                                                                                                                       2
                                                                                                               ()
  Pulse Secure<sup>®</sup>
                                            DASHBOARD
                                                          APPLIANCES ANALYTICS ADMINISTRATION
                                                                                                             SETTINGS
                                                                                                                     ADMIN
              PULSE ONE
                                                                                                            (Super Admin)
         Dashboard
                                          OVERALL
                                                              APPLIANCES
                                                                               PROFILED DEVICES
                                                                                                      Change Password
Overall Dashboard
                                                                                                       Help
  OVERALL APPLIANCE STATS
                                                                                                      Knowledge Base
                                                                                                      Show Welcome Wizard
                                        2
         0
                        0
                                                        0
                                                                       0
                                                                                       0
                                                     of 37000
                                                                       of 0
                                                                                                      B Logout
    Connect Secure
                    Connect Secure
                                    Policy Secure
                                                    Policy Secure
                                                                    Named User
                                                                                     Appliance
      appliances
                     concurrent
                                     appliances
                                                     concurrent
                                                                    licenses used
                                                                                     cluster(s)
                     user licenses
                                                     user licenses
                        used
                                                       used
```

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 licenses, access the Command-Line Interface (CLI) and use the following commands:

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

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

Whitelisting IP Addresses for Admin Login

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

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

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

To whitelist IP addresses/ranges:

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

3. Select Pulse One Properties.

The **Pulse One Properties** page appears.

FIGURE 6 Pulse One Properties

= 🞗 Pulse S	ecure	DAS	HBOARD APPLI	ANCES AAA	WORKSPACES	ANALYTICS	ADMINISTRATION		Ø	ዶ
PULSE ONE				\square	$\langle - \rangle$	\mathcal{N}	7			
Pulse One Properties	Pulse One Properties	Whitelist						Pulse One Propertie	5	
Workspace Properties	Pulse One Properties							Workspace Propertie		
LDAP Groups								LDAP Groups Apple		llapse All
Apple	Name			Value				CA Certificate		٢
CA Certificate	⊕ Enterprise Connections (5)							Android Enterprise Enterprise Usage Ag		
Android Enterprise	Password (9)						VPN Cert			
Enterprise Usage Agreement	\pm Misc (4)									
VPN Cert										

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

FIGURE 7 Add to Whitelist Page

	CUTE DASHBOARD APPLIANCES AAA WORKSPACES ANALYTICS ADMINISTRATION	
PULSE ONE Pulse One Properties	Pulse One Properties Whitelist	
Workspace Properties	Add to Whitelist	
LDAP Groups	Please add an ipv4 / ipv6 address in the above text box	
Apple		
CA Certificate	IPV4 or IPV6 Address	
Android Enterprise	No data to display	
Enterprise Usage Agreement	0 total	
VPN Cert		

- 5. Add your first whitelist item:
 - Enter an IP address/range (with CIDR netmask suffix) that includes the IP address from which you are currently logged in.
 - Click the (🖿) icon.

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

FIGURE 8 First Whitelist Entry

Pulse One Properties	Whitelist				
Add to Whitelist					_
					Ð
Please add an ipv4 / ipv6 ad	dress in the a	bove text box			
IPV4 or IPV6 Address			0		
172.22.15.0/24			â		
1 total					
i totai				 	

6. Repeat step 5 to add additional IP addresses/ranges to the whitelist. For example:

FIGURE 9 Additional Whitelist Entries

Pulse One Properties	Whitelist		
dd to Whitelist			
192.186.12.1/11			
ease add an ipv4 / ipv6 aα	ddress in the above text b	ox	
IPV4 or IPV6 Address		۵	
172.22.15.0/24		â	
135.0.0.0/8		â	
172.55.0.0/16		â	
3 total			

7. (Optional) Delete a whitelist entry by clicking its **Delete** ($\widehat{=}$) icon.

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

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

Working with Pulse One Dashboards

•	Introduction	13
•	Viewing Overall System Health	13
•	Viewing Metrics for Appliances	14
•	Customizing Dashboards and Widgets	16

Introduction

Dashboards give the administrator access to health and performance metrics:

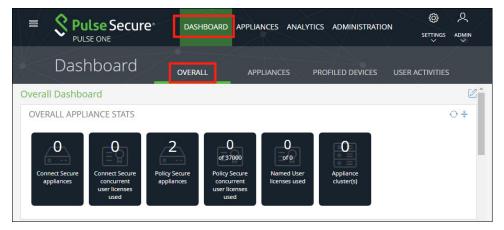
- Pulse One system health, see "Viewing Overall System Health" on page 13.
- Appliances registered on Pulse One, see "Viewing Metrics for Appliances" on page 14.

You can also customize the widgets on the dashboards, see **"Customizing Dashboards and Widgets" on** page 16.

Viewing Overall System Health

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

FIGURE 10 Overall System Health Dashboard



Each widget that can be refreshed by clicking **Reload Widget Content** (^(C)) and collapsed by clicking **Collapse/ Expand Widget** (^{*}).

The administrator can view the following information in separate widgets in the **Overall** tab:

- 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.

Viewing Metrics for Appliances

To view metrics for appliances, select the **Dashboard** tab, and then select the **Appliances** tab:





The administrator can view the following information in separate widgets in the **Appliances** tab:

- The total number of appliances. In this example, 72.
- Individual appliances are displayed as tabs around the central circle.
 - These are sorted into *Pulse Connect Secure* appliances and *Pulse Policy Secure* appliances.
 - The color of the individual tabs indicates the status of the appliance.
 - Hover over any tab to see its name.
- Details for each appliance can be viewed by clicking its tab. This includes:
 - The appliance **Version**.
 - The appliance **Model**. For example: *PSA-300*.
 - Serial Number.
 - Last Config Upload. A timestamp.
 - IF-MAP Federation. Boolean.
 - Using License Server. Boolean.
- Summary metrics are also displayed:
 - The number of Active Sync Connections for the appliances.
 - The number of concurrent users.
 - The number of authorization failures.
 - The throughput of data.
 - CPU utilization.
 - Disk utilization.
 - Memory utilization.

Customizing Dashboards and Widgets

The **Overall Dashboard** and **Workspaces 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:

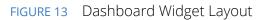
1. Display the required dashboard tab. That is, either the **Overall** tab or the **Workspaces** tab.



	DASHBOARD	APPLIANCES ANAL	YTICS ADMINISTRATION	SETTINGS ADMIN
Dashboard	OVERALL	APPLIANCES	PROFILED DEVICES	USER ACTIVITIES
Overall Dashboard				Z
OVERALL APPLIANCE STATS				↔ *
Connect Secure appliances Connect Secure concurrent user licenses used	Policy Secure appliances	ecure Named User rent licenses used inses		

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

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



	DASHBOARD	APPLIANCES	ANALYTICS	ADMINISTRATION		Q MIN ~
Dashboard	VERALL	APPLIANCE	S PR		R ACTIVITIES	
Overall Dashboard					⊕@v	b0^
OVERALL APPLIANCE STATS					۵ :	×
O APPLIANCE HEALTH					۵	×
OUSER LOGIN ACTIVITY					۵	×
◇ VPN REALM USAGE	ROLE USAC	GE	© ×	◆ FREQUENT USE	ER LOGINS 🔞 🔅	×
↓ LOGINS IN PAST 24 HOURS ×	♦ CRITICAL E	VENTS	© ×	C RESOURCE DIA	L 💿	×

- 3. (Optional) Click **Add New Widget** (⊕) to add a widget to the current layout, see **"Adding a New Widget" on page 17**.
- 4. (Optional) Click **Edit Dashboard** (⁽⁽⁾) to select a new layout, see **"Editing the Dashboard Layout" on** page 18.
- 5. (Optional) Rearrange the current widgets by dragging a widget using its **Change Widget Location** (\bigcirc) handle.
- 6. (Optional) Change the settings for a widget by clicking its **Edit Widget Configuration** (^(©)), see **"Editing Widget Configuration" on page 20**.
- 7. (Optional) Remove a widget by clicking its **Remove Widget** () control.
- 8. (Optional) Click **Undo Changes** (Ω) to reset all unsaved changes and close the layout summary.
- 9. Click **Save Changes** (\checkmark) to save all changes and close the layout summary.

Adding a New Widget

To add a new widget to a dashboard tab:

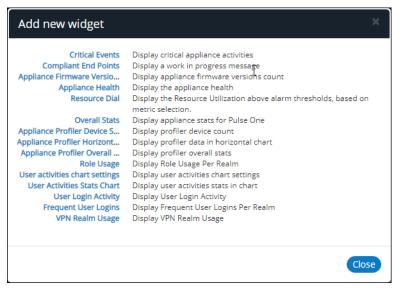
- 1. Display the required dashboard tab. That is, either the **Overall** tab or the **Workspaces** tab.
- 2. Click the **Enable Edit mode** icon (\square) on the top-right of the tab.

A widget layout summary for the dashboard appears.

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

A list of widgets appears.

FIGURE 14 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** (⁽²⁾) control, see **"Editing Widget Configuration" on page 20**.
- 6. (Optional) Click **Undo Changes** (Ω) to reset all unsaved changes and close the layout summary.
- 7. Click **Save Changes** (\checkmark) 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 (\square) on the top-right of the tab.

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

FIGURE 15 Dashboard Widget Layout

E SPulse Secure PULSE ONE	DASHBOARD	APPLIANCES	ANALYTICS	ADMINISTRATION	SETTINGS ADMIN
Dashboard	'ERALL	APPLIANCE	s pr	OFILED DEVICES USER AC	TIVITIES
Overall Dashboard					⊕@⊎റ [^]
OVERALL APPLIANCE STATS					© ×
I APPLIANCE HEALTH					@ ×
USER LOGIN ACTIVITY					@ ×
◇ VPN REALM USAGE	ROLE USAC	GE	@ ×	• FREQUENT USER L	OGINS 🐵 ×
\odot logins in Past 24 hours @ $ imes$	CRITICAL E	VENTS	۵×	CRESOURCE DIAL	۵×

3. Click the **Edit Dashboard** (^(©)) icon and select the required layout from the displayed list.

FIGURE 16 Edit Dashboard Layout

Edit dashboard		×
Title		
Overall Dashboard		
Structure		
Overall Default 2 columns	Rows, 2 columns (12/12/6-6)	12/4-4-4
		Close

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

FIGURE 17 Updated Dashboard Widget Layout

	DASHBOARD APPLI	ANCES ANALYTICS ADMINISTRATION	SETTINGS ADMIN
Dashboard	OVERALL APF	LIANCES PROFILED DEVICES	USER ACTIVITIES
Overall Dashboard			⊕ @ ⊍ ∩
♦ OVERALL APPLIANCE STATS	@×	APPLIANCE HEALTH	@ ×
COGINS IN PAST 24 HOURS	@ ×	CRITICAL EVENTS	@ ×
OUSER LOGIN ACTIVITY	©×	VPN REALM USAGE	@ ×
RESOURCE DIAL	© ×	↔ CONNECT SECURE VERSIONS	@ ×
ROLE USAGE	۰	FREQUENT USER LOGINS	@ ×
	© ×		

- 4. (Optional) Click **Undo Changes** (Ω) to reset all unsaved changes and close the layout summary.
- 5. Click **Save Changes** (\checkmark) 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 (\square) 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 18 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** (Ω) to reset all unsaved changes and close the layout summary.
- 7. Click **Save Changes** (\checkmark) 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
•	Creating and Registering a PCS Appliance VM on vSphere	29
•	Creating and Registering a PCS Appliance VM on AWS	41
•	Configuring CPU, Memory and Disk Utilization	55
•	Backing up and Restoring Appliance Configurations	56
•	Working with Appliance Groups	61
•	Upgrading Managed Appliances	71
•	Viewing the Activities Log for an Appliance	87
•	Viewing the Configuration Change History for an Appliance	88
•	Comparing Appliances	89
•	Rebooting an Appliance	91
•	Removing an Appliance from Pulse One	92
•	Preparing a Target Appliance	93
•	Removing an Appliance from an Appliance Group	93
•	Editing an Appliance Group	94
•	Deleting an Appliance Group	96

Registering an Existing PCS/PPS Appliance

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

Note: This process requires sufficient appliance licensing capacity.

Note: You can also create and register a virtual PCS appliance for either AWS (see "Creating and Registering a PCS Appliance VM on AWS" on page 41) or vSphere (see "Creating and Registering a PCS Appliance VM on vSphere" on page 29).

To register an existing appliance:

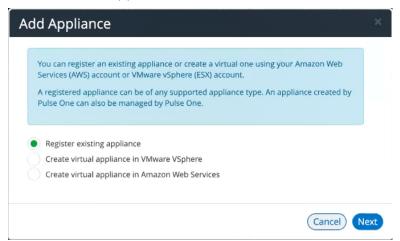
- 1. Log into Pulse One as an administrator.
- 2. Click the **Appliances** menu and then the **Appliances** tab.

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

3. Click Add Appliance.

The Add Appliance dialog box appears.

FIGURE 19	Add Appliance
-----------	---------------



4. Select Register existing appliance and click Next.

The Register Appliance dialog appears.

FIGURE 20 Register New Appliance

Register New Appliance	×
Name:]
ADDITIONAL INFORMATION \sim	
Appliance URL: https://myvpnbox.net	
Pulse One uses Device Management Interface (DMI) to perform software upgrades of registered Pulse Connect Secure and Pulse Policy Secure appliances. DMI is an extension to the NETCONF network management protocol. Click here to learn more about DMI configuration on an appliance.	
IP Address: Port:	
Username:	
Password: Password	
Cancel	Save

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

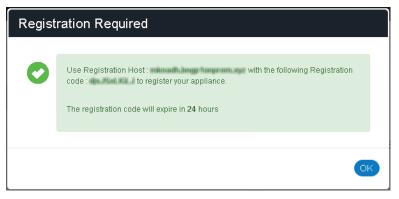
- 6. Enter the management interface address of the appliance as the **Appliance URL**. Typically, this URL will end with "/admin".
- 7. (Optional) If you want the appliance to support Device Management Interface (DMI) software upgrades directly from Pulse One:
 - For **IP Address**, specify the IP Address 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.

Note: You must record this information for when you configure software upgrades. For full details of software upgrades on registered appliances, see **"Upgrading Managed Appliances" on page 71**.

8. Click Save.

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

FIGURE 21 Registration Required



- 9. Record the Registration Host and Registration Code and close the dialog.
- 10. Switch to the appliance application (for example, PCS) and enter the **Registration Host** and a **Registration Code** in the appliance's panel, see **"Configuring an Appliance to Connect to Pulse One" on page 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 22 Edit Appliance Information

Edit Appl	iance	Info	×
Name:	Puls	se-Example-PCS-1	
ADDITIC	NAL IN	FORMATION	\sim
Appliance	URL:	https://myvpnbox.net	
		Cancel	Save

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 24**.

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 ($\stackrel{\circ}{\epsilon}$).
- 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 appliance to send logs to Pulse One, see "Configuring Log Settings on the Appliance" on page 26.
- Configure the ActiveSync handler on the appliance as required, see **"Configuring ActiveSync Handler" on page 27**.

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 23 Pulse Connect Secure: Pulse One Settings

Status Information

Registration Status:
Other Status:

Configuring Log Settings on the Appliance

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

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

FIGURE 24 Log Events Settings

Secure	Pulse Connect Secure		
	aintenance Wizards		
Log/Monitoring > Events > Log settings			
Log settings			
Events User Access Admin Access Sensors Client Logs SNMP Statistics	Advanced Settings		
Log Settings Filters			
Save Changes Reset			
♥ Maximum Log Size			
Max Log Size: 200 MB			
Max Log Size: 200 MB			
Note: To archive log data, see the Archiving page.			
✓ Select Events to Log			
🕾 Osassefan Daswash. 🖉 Olafisfan			
 Connection Requests Statistics System Status Performance 			
Reverse Proxy			
System Errors			
Grossi Eloto Ido Icense Protocol Events			
MDM API Trace			
✓ Pulse One Events			
Profiler Events			
M HTML5 Access Events			

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

Note: To distinguish between different log types (Events, User Access, Admin Access), you must select a different **Facility** for each type.

- **Type**: Select *TCP*.
- Client Certificate: Select Select Client Cert.
- Filter: Select WELF: WELF.

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

Note: To distinguish between different log types (Events, User Access, Admin Access), you must select a different **Facility** for each type.

- **Type**: Select *TCP*.
- Client Certificate: Select Select Client Cert.
- Filter: Select WELF: WELF.

9. Navigate to System > Log/Monitoring > Admin Access > Settings.

10. Under Syslog Servers:

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

Note: To distinguish between different log types (Events, User Access, Admin Access), you must select a different **Facility** for each type.

- **Type**: Select *TCP*.
- Client Certificate: Select Select Client Cert.
- Filter: Select WELF: WELF.

11. Select the **Advanced Settings** tab and enable **Fault Tolerance** for the Pulse One syslog server.

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

Configuring ActiveSync Handler

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

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

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

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

The Pulse Workspace Handler screen appears.

FIGURE 25 Pulse Connect Secure: Command Handlers

0	~					Pulse Connec	t Secure
S Pulse	Secure		Authentication	Administrators	Users	Maintenance	L Wizards
uise One							
Licensing Pulse	One Security	Certificates	DMI Agent	NCP	Sensors	Client Types	Pulse Collaboration
Virtual Desktops	IKEv2 SAML	Mobile	VPN Tunneling	Telemetry	Advance	d Client Configuration	
Settings Command Handle	rs						
Pulse Workspace Handler							
Device Role: (none) Clear Active Sync Dev Group Lookup Handler Select Authentication Serr Available Auth Servers:	rice Records Delete Configuration vera to use for group I	all the device records p	ecord created for devices pushed from Pulse Works				
(none)	Add -> Remove	S	elect only one authenticat	tion server per domain			
Save Changes							

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

Note: To create a user rule, refer to the Pulse Connect Secure Administration Guide available at: **https://** www.pulsesecure.net/techpubs. After you register a PCS appliance, it regularly sends the following information to Pulse One:

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

Note: Hardware-specific PCS XML configuration is not shared during configuration distribution.

- General information. That is, PCS health, statistics (such as CPU, network throughput), licensing details, cluster information and so on. (Sent to On-Prem/Appliance and SaaS/Cloud)
- User sign-in history. That is, logins from both web and the Pulse client. (Sent to On-Prem/Appliance only)
- User and System binary configuration. (Sent to On-Prem/Appliance only)

Creating and Registering a PCS Appliance VM on vSphere

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

Note: You can also create and register a virtual PCS appliance for AWS, see **"Creating and Registering a PCS Appliance VM on AWS" on page 41**.

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

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

Note: During this process, you can optionally use a master appliance template. A master template encapsulates an existing deployed appliance, and enables the re-use of many configuration settings on any appliance that is deployed using the template. To create a master template, see **"Creating an Appliance Master Template on vSphere" on page 36**.

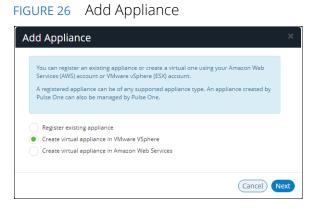
To create and register a PCS appliance as a VM on vSphere:

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

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

3. Click Add Appliance.

The Add Appliance wizard starts.



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

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

FIGURE 27 vSphere Credentials

have Condentials		
	redentials to manage virtual appliances. If you lect them from the list or add new ones to be	
Account:	Add New	~
Host name:	vSphere host name	
Username:	Username	
	Password	
Password:	1 d35W01d	

- 5. You must then specify vCenter credentials. Either:
 - Select Add New for Account, then:
 - For **Account**, select *Add New*.
 - For Hostname, enter the FQDN or IP address of your vCenter host.
 - For Username and Password, enter your vSphere credentials.
 - Select an existing vCenter **Account**.
- 6. Click Next.

The Appliance Configuration panel of the wizard appears.

FIGURE 28 Appliance Configuration

and password to be creat	ed on the virtual appliance.
Appliance Name:	
Company Name:	
License Auth Code:	
Appliance Username:	New-Admin Username:
Password:	New Password:
Confirm Password:	Confirm New Password:

- 7. Enter the **Appliance Name**. This will be the displayed name in the list of appliances and will also be used to automatically populate the **Internal FQDN** and **External FQDN** properties on subsequent wizard panels.
- 8. Specify additional information for the appliance:
 - A Company Name.
 - The **Appliance Username**, **Password** (and **Confirm Password**) for a required user on the appliance. This user will be created after the appliance is created.
 - (Optional) A License Auth Code can be entered if required.

9. Click Next.

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

FIGURE 29	Appliance	Network Configuration: Servers

Network name fields car	be looked up from vCenter under Networ	ks.
SERVERS		\sim
Primary DNS:	8.8.8	
Secondary DNS:	8.8.4.4	
INTERNAL NETWO	RK SETTINGS	<
EXTERNAL NETWO	RK SETTINGS	<
MANAGEMENT NE	TWORK SETTINGS	<

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

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

11. Expand the Internal Network Settings panel.

FIGURE 30 Appliance Network Configuration: Internal Network Settings

	network configuration for			
Network nam	e fields can be looked up	from vCenter under	Networks,	
SERVERS				<
ERVERS				
NTERNAL	NETWORK SETTIN	GS		\checkmark
	_			
rivate Doma	in Name:			
nternal FQDN	d:			
nernari qui				
nternal Netw	ork Name:			
р	10.10.10.5	Subnet:	255,255,255,0	
ddress:	1011011010			
Sateway:	10.10.10.1	VLAN:		
EXTERNAL	NETWORK SETTIN	GS		<
MANAGEN	IENT NETWORK SE	TTINGS		<

12. In the Internal Network Settings:

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

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

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

13. Expand the External Network Settings panel.

FIGURE 31 Appliance Network Configuration: External Network Settings

	network configuration for ie fields can be looked up			
incerior in num	ie neus can be looked ap	non vecner under	THE WORKS.	
SERVERS				<
INTERNAL	NETWORK SETTIN	GS		<
EXTERNAL	NETWORK SETTIN	GS		\sim
Public Domai	n Name:			٦
External FQD	N:			
				_
External Netv	vork Name:			
IP Address:	64.64.64.5	Subnet:	255.255.255.0	
Gateway:	64.64.64.1	VLAN:		
MANAGEN	IENT NETWORK SE	TTINGS		<

14. In the External Network Settings:

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

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

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

FIGURE 32 Appliance Network Configuration: Management Network Settings

Network name fields can be looked	d up from vCenter under Networks.	
SERVERS		<
INTERNAL NETWORK SETT	INGS	<
EXTERNAL NETWORK SET	TINGS	<
MANAGEMENT NETWORK	SETTINGS	\sim
Management Network		
Name:		
P	Subnet:	
Address:		
Gateway:	VLAN:	

16. In the Management Network Settings:

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

The **vSphere Configuration** wizard panel appears.

vSphere Configuration		
Please enter your vSph template with an applia	ere data center information and select a valid appliance ance version >= 9.0R3.	
Data Center:		
Data Store:		
Resource Pool:	Resources	
Appliance Master Template:		

FIGURE 33 vSphere Configuration

- 18. Complete the properties for this panel of the wizard:
 - For **Data Center**, enter your required vSphere data center. Data centers are listed on the **Storage** tab on vSphere.
 - For **Data Store**, enter the required vSphere data store from your selected data center. Data stores are listed under each data center on the **Storage** tab on vSphere.
 - For **Resource Pool**, enter the required vSphere resource pool from your selected data center. Resource pools are listed under each data center on the **Hosts and Clusters** tab on vSphere.
 - (Optional) Enter an Appliance Master Template. Templates are listed under the data center on the VMs and Templates tab on vSphere. For details of how to create an appliance master template, see "Creating an Appliance Master Template on vSphere" on page 36.
- 19. Click Save.

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

20. Click the **Actions** icon ([§]) for the appliance and select **Start Appliance**.

- 21. The status of the new appliance goes through a series of states until it successfully running.
 - Unregistered
 - Creating
 - Starting
 - Started
- 22. (Optional) During the creation of the appliance, you can monitor progress from the vSphere **Recent Tasks** tab.

FIGURE 34	vSphere	Appliance	Creation	In Progress
I I GOILE D I	vopriere	, application	Creation	1111001000

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

FIGURE 35 VSphere Appliance Creation Complete

😨 Recent Tasks			_
P -			
Task Name	Target	Status	Initiator
Relocate virtual machine	-vsphere-applia	✓ Completed	VSPHERE.LOCAL\\
Power On virtual machine	-vsphere-applia	✓ Completed	VSPHERE.LOCAL\\
Reconfigure virtual machine	-vsphere-applia	 Completed 	VSPHERE.LOCAL\\
Clone virtual machine	pcs_master_template	 Completed 	VSPHERE.LOCALII
Check new notifications	Solvc.lab.psecure.net	 Completed 	VMware vSphere U

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

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

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

Creating an Appliance Master Template on vSphere

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

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

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

To create a master appliance template:

- 1. Obtain the Pulse Connect Secure template files from Pulse Secure Support and store the files in an accessible location in your network.
- 2. Log into the vSphere Web Client.
- 3. Right-click and an existing host and click **Deploy OVF Template**. For example:

FIGURE 36 vSphere Web Client Deploy

vmware [®] vSphere Web Client	†≡		
Navigator	I 192.168.71.11 Actions - 192.168.71.11	- 🕞 🔂 🎯 Ac	tions -
	New Virtual Machine New vApp New Resource Pool	, ifigure Pe	ermissi VMs Re
▶ 🛛 192.168.	Connection Maintenance Mode Power	• iormal	Type VMFS 5 VMFS 5
	Certificates	•	

The **Deploy OVF Template** wizard appears.

FIGURE 37 vSphere Deploy OVF Template Wizard 1

1 Select template	Select template
2 Select name and location	Select an OVF template.
3 Select a resource	Enter a URL to download and install the OVF package from the Internet, or browse to a location accessible from the later and the second s
4 Review details	as a local hard drive, a network share, or a CD/DVD drive.
5 Select storage	○ URL
6 Ready to complete	
	Local file
	Browse
	Lise multiple selection to select all the files associated with an OVF template (.ovf, .vmdk, etc.)

- 4. Select the Local file option and click Browse.
- 5. Locate and multi-select the OVF and VMDK template files. For example:

FIGURE 38 vSphere Deploy OVF Select Template Files



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

FIGURE 39 vSphere Deploy OVF Template Wizard 2

1 Select template	Select name and location Enter a name for the OVF and select a deployment location.
2 Select name and location	
3 Select a resource	Name pcs_import
4 Review details	Filter Browse
5 Select storage	Select a datacenter {0} or {1} folder.
6 Ready to complete	

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

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

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

FIGURE 40 vSphere Deploy OVF Template Wizard 3

1 Select template 2 Select name and location	Select a resource Select where to run the deployed template.
3 Select a resource	Filter Browse
4 Review details	Select a host {0} or {1} cluster {0} or {1} resource pool {0} or {1} vapp
5 Select storage	▼
6 Select networks	▶ ■ 192.168.
7 Customize template	
8 Ready to complete	

- 9. Click **Next** to proceed to the next panel of the wizard.
- 10. Review the displayed details and step back through the wizard to correct these if required.
- 11. Click **Next** to proceed to the next panel of the wizard. For example:

FIGURE 41 VSphere Deploy OVF Template Wizard 5

8	Deploy OVF Template						
×	1 Select template 2 Select name and location	Select storage Select location to store the files for the deployed template.					
~	3 Select a resource	Select virtual disk format:	Thin provision	•			
~	4 Review details	VM storage policy:	None	•			
1	5 Select storage	Show datastores from	Storage DRS clusters				
	6 Select networks	Filter					
	7 Customize template						
	8 Ready to complete	Datastores Datastore	Clusters				

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

FIGURE 42 VSphere Deploy OVF Template Wizard 6

1 Select template2 Select name and location	Select networks Select a destination network for each so	urce network.	
3 Select a resource	Source Network	Destination Network	
4 Review details	InternalNetwork	VM Network	
5 Select storage	ManagementNetwork	VM Network	
6 Select networks	ExternalNetwork	External Network	
7 Customize template			

- 13. Select appropriate network interfaces for each of the PCS interfaces.
- 14. Click **Next** to proceed to the next panel of the wizard.

FIGURE 43 vSphere Deploy OVF Template Wizard 7

Contraction OVF Template				(? H
1 Select template2 Select name and location	Customize template Customize the deployment	properties of this software solution.		
✓ 3 Select a resource	All properties have valid	l values	Show next	Collapse all
 4 Review details 	valVEConfig	1 setting		^
✓ 5 Select storage	VA IVE Configuration	Please enter the IVE Configuration	on Parameters in the	text box below
 6 Select networks 7 Customize template 8 Ready to complete 		Sample values are given bo valPAddress=20.20.20.20 vaNetmask=255.255.255. vaGateway=20.20.20.17 vaDefaultVlan=10; vaPrimaryDNS=10.2.3.45 vaSecondaryDNS=10.2.3. vaDNSDomain=jnpr.net; vaWINSServer=TheWINS vaAdminUsername=admii vaAdminPassword=P@ss vaCommonName=jnpr; vaOrganization=PBU; vaRandomText=Lf3IsB3(vaManagementIVatmastr	;; ; ;46; ;; ,∩, W0rD; @uttfuL; ;=10.10.10.10;	
		Back	Next Finish	Cancel

- 15. Make no changes to this wizard page.
- 16. Click **Next** to proceed to the final panel of the wizard.
- 17. Review the displayed details and step back through the wizard to correct these if required.

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

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

Navigator	📱 🔂 pcs_import 🛛 🛃 🕨 💷 🤅	🔄 📇 🔯 Actions 🗸
A Back	Getting Star Summa Monit	tor Configure Permissions Snapshots Datastore
↓	Actions - pcs_import	Cother (64-bit)
▼	Power Guest OS	ility: ESX/ESXi 4.0 and later (VM version 7)
pcs_import	Snapshots	Fools: Not running, not installed More info
	Open Console	10:
	Migrate Clone	© 2001 102.188.71.11 ▶ ∰ Clone to Virtual Machine ©
	Template	Clone to Template
	Fault Tolerance	Clone to Template in Library
	VM Policies	,

FIGURE 44 VSphere Web Client Clone

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

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

FIGURE 45 vSphere Clone VM to Template Wizard

B ^C pcs_import - Clone Virtual Machine To Template					
1 Edit settings	Select a name and folder Specify a unique name and target location				
1a Select a name a					
1b Select a compute					
1c Select storage	pcs_master_template				
1d Customize vApp	operties Template names can contain up to 80 characters and they must be unique within each vCenter Server VM f	folder.			
2 Ready to complete	Select a location for the template.				
	Q Search				
	Select a datacenter or VM folder to o the new template in.	create			

- 20. Specify a name and select a location for the required template.
- 21. Click **Next** to proceed to the next panel of the wizard. For example:

FIGURE 46 VSphere Clone VM to Template Wizard 1b

 1 Edit settings 1a Select a name and folder 	Select a compute resource Select the destination compute resource for this operation
1b Select a compute resource 1c Select storage 1d Customize vApp properties 2 Ready to complete	Q Search Image: Search Image: Search Image: Search Image: Search Image: Search Search </th

22. Select the required compute resource.

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

FIGURE 47 vSphere Clone VM to Template Wizard 1c



- 24. Set Select virtual disk format to Same format as source.
- 25. Click **Next** to proceed to the next panel of the wizard. For example:

FIGURE 48 VSphere Clone VM to Template Wizard 1d

^C pcs_import - Clone Virtual Machir	ne To Template			(?)
1 Edit settings	Customize vApp properties	15		
 1a Select a name and folder 1b Select a compute resource 	All properties have valid	l values	Show next	Collapse all
✓ 1c Select storage	valVEConfig	1 setting		
 1d Customize vApp properties 2 Ready to complete 	VA IVE Configuration	Please enter the IVE Configuration Parameters in the text box below. Y Sample values are given below: valPAdness=20 20.20.20; vaNetmask=255.255.255.0; vaSetautVlan=10; vaPrimaryDNS=10.2.3.46; vaSetautVlan=10; 0.2.3.46; vaSetautVlSSetautPlanet vaVINSServer=TheVINS; vaAdminUservame=admin; vaAdminUservame=admin; vaAdminUservame=admin; vaAdminUservame=admin; vaAdminUservame=admin; vaAdminUservame=admin; vaAdminUservame=admin; vaAdminUservame=admin; vaAdminUservame=admin; vaAdminUservame=admin; vaCommonName=jnp; vaCommonName=jnp;	fou can edit or coρ	yy/paste the v
		Back	xt Finish	Cancel

- 26. Click **Next** to proceed to the final panel of the wizard.
- 27. Review the displayed details and step back through the wizard to correct these if required.
- 28. Click **Finish** to complete the wizard and create the master appliance template.

After you have a master appliance template, you can optionally use it on the **vSphere Configuration** page of the **Add Appliance Wizard**, see **"Creating and Registering a PCS Appliance VM on vSphere" on page 29**.

Creating and Registering a PCS Appliance VM on AWS

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

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

Note: You can also create and register a Virtual Machine appliance for vSphere, see **"Creating and Registering** a PCS Appliance VM on vSphere" on page 29.

Perform the following tasks:

- 1. Before you begin, you must locate and record the following information:
 - The required Route 53 zones, see "Identifying the Required Route 53 Zones" on page 42.
 - The required VPC ID and Subnet IDs, see "Identifying the Required VPC ID and Subnet IDs" on page 44.
 - The required EC2 deployment key, see "Identifying the EC2 Deployment Key and AMI ID" on page 46.
- 2. You can then create the appliance, see "Creating the PCS Appliance VM on AWS" on page 49.

Identifying the Required Route 53 Zones

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

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

FIGURE 49 AWS Selecting Region



- 3. On the AWS top bar, click **Services** and then locate the **Network & Content Delivery** options.
- 4. Under Network & Content Delivery, select Route 53.

The AWS Route 53 Management Console appears.

FIGURE 50 AWS Route 53 Management Console

aws se	ervices	🗸 Resource Groups 🗸 🔭			∆ •	0 •	Global 👻	Support 👻
Dashboard Hosted zones	•	DNS management	Traffic management	Availability monitoring	I	Domain reg	istration	
Health checks Traffic flow Traffic policies Policy records		5 Hosted zones Ø	A visual tool that lets you easily create policies for multiple endpoints in complex configurations. Create policy	Health checks monitor your applications and web resources, and direct DNS queries to healthy resources. Create health check	example	in is the name, s a.com, that your your application Register d	users use to	
Domains Registered domains Pending requests	nains Register domain stered domains Find and register an available domain, or transfer your existing domains to Route 53.				C		uide and health ch	
		Resource	Status	≪ ≪ No alerts to display ≫ Last update	>1	Request a lir Service he	nit increase	e
						Service	n Route 53 e is operating health dashb	· · ·

5. Select Hosted Zones.

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

FIGURE 51 AWS Route 53 Hosted Zones

aws Service	s 🗸 Resource Groups 🗸 🛠			Å• @ ▾ Global ▾ Support ▾
Dashboard 🚽	Create Hosted Zone Go to Recor	d Sets Delete Hosted Zone		20
Hosted zones	Q Search all fields	All Types		$\ \ll \ \ \ll \ $ Displaying 1 to 5 out of 5 Hosted Zones $\ \gg \ \ \gg \ $
Health checks	Domain Name	✓ Type ✓ Record Set Count ✓	Comment Hosted Zone ID	
Traffic flow	sko.7	Public 2	Z1IHK47T	
Traffic policies	ip.nu sip.nu	Public 2	Z22V6N8	
Policy records	awste	Public 2	Z354F2J0	
Domains	jakma	Private 2	Z8RZ8UJI	
Registered domains Pending requests	nuwa	Public 2	ZSQ2H40	

In the domain name list:

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

For example:

FIGURE 52 AWS Public and Private Zones

D	omain Name	- Туре	Record Set Count	Comment Hosted Zone ID
a	wstes	Public	2	Z354F2JGVF
n	uwave	Public	2	ZSQ2H40W>
Si Si	ip.nuv	Public	2	Z22V6N8JS2
s	ko.7-8	Public	2	Z1IHK47TAN
🔵 ja	akmar	Private	2	Z8RZ8UJIPG

- 6. Select the required Public zone and record its Domain Name.
- 7. Locate the required Private zone and record its Domain Name.

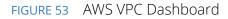
You can then perform any remaining preparations, and then continue to create and register the PCS appliance virtual machine on AWS.

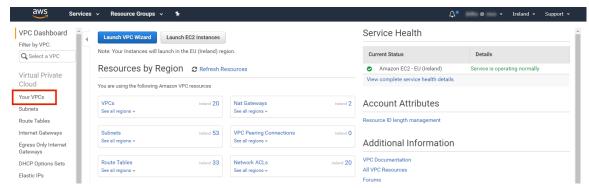
Identifying the Required VPC ID and Subnet IDs

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

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

The AWS VPC Dashboard appears.





5. Select Your VPCs.

A list of available VPCs appears.

FIGURE 54 AWS Available VPCs

VPC Dashboard	Create VPC Actions *									C 🗘
C Select a VPC	Q Search VPCs and their	propert X							« < 1 to	o 20 of 20 VPC
Virtual Private	Name •	VPC ID -	State -	IPv4 CIDR	IPv6 CIDR ~	DHCP options set	Route table -	Network ACL ~	Tenancy -	Default VPC
Cloud	Dev VF	vpc-2763	available	10.0.0/16		dopt-b90afdd1 dhcp-option	rtb-2563	acl-2663	Default	No
our VPCs	Jordan	vpc-20de	available	10.0.0/16		dopt-b90afdd1 dhcp-option	rtb-26de	acl-27de	Default	No
ubnets	PEvan:	vpc-e9bd	available	10.0.0/16	2a05:d018:a1b:1900::/56	dopt-b90afdd1 dhcp-option	rtb-9e62	acl-6172	Default	No
	SD-Aut	vpc-989d	available	10.0.0/16		dopt-b90afdd1 dhcp-option	rtb-54ec	acl-2511	Default	No
oute Tables	achern	vpc-42e4	available	2 CIDRs	2a05:d018:cfb:ec00::/56	dopt-b90afdd1 dhcp-option	rtb-311b	acl-6ef2	Default	No
iternet Gateways	aknox-	vpc-9990	available	10.0.0/16	2a05:d018:838:1800::/56	dopt-b90afdd1 dhcp-option	rtb-c92e	acl-d533	Default	No

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

FIGURE 55 AWS VPC ID

-vpc-5	vpc-0189	available	10.5.0.0/16
vrouter-vpc	vpc-ec1d	available	10.8.0.0/16
-vpc	vpc-9a83	available	10.0.0.0/16

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

FIGURE 56 AWS Select VPC

aws	Services 🗸	Resource G	roups 🗸	*		
VPC Dashboard Filter by VPC:		te VPC Ac	tions v	ropert 🗙		
vpc-989d2	Itomation		•	VPC ID	State	IPv4 CIDR
vpc-1b109	-VPC			vpc-989d2	available	10.0.0.0/16
vpc-0189c	Jck-vpc-5			vpc-1b109	available	10.0.0/16
vpc-ec1da vrou vpc-de75c mho	uter-vpc			vpc-0189c	available	10.5.0.0/16
vpc-9a838 sudh			/pc	vpc-ec1da	available	10.8.0.0/16
vpc-d3087 jakr	n		Direct	vpc-de75c	available	10.0.0/24
·····				vpc-9a838	available	10.0.0/16

8. Click Subnets.

A list of all subnets in the selected VPC appears.

This list must include three different subnets that are in the same **Availability Zone**. Each will be used for one of the standard PCS interfaces in a later procedure (see **"Creating the PCS Appliance VM on AWS" on page 49**). The interfaces requirements are:

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

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

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

FIGURE 57 AWS Select Public Subnet

private-self-re	g :	subnet-e	Bea3	avai	able	vpc-ec1da	vrouter-vpc	
vrouter-public	:	subnet-fb	f320	avai	able	vpc-ec1da	vrouter-vpc	
							_	
hnot: subset-fbf3	20-3						000	
bnet: subnet-fbf32	20a3						000	
bnet: subnet-fbf32	20a3 Flow	Logs	Route	e Table	Ne	etwork ACL	Tags	

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

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

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

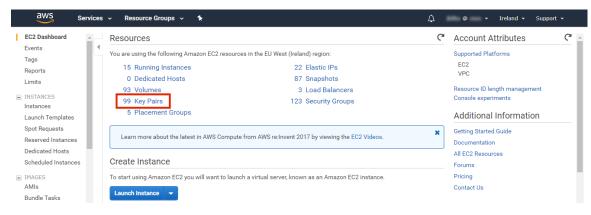
Identifying the EC2 Deployment Key and AMI ID

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

- 1. Login to the AWS Management Console.
- 2. On the AWS top bar, select the required Region.
- 3. On the AWS top bar, click **Services** and then locate the **Compute** options.
- 4. Under Compute, select EC2.

The AWS EC2 Dashboard appears, showing Key Pairs.

FIGURE 58 AWS EC2 Dashboard



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

A list of defined key pairs appears.

aws Servic	es 👻 Resource Groups 🗸	*			ф @	Ireland 👻	Support 👻	
EC2 Dashboard	Create Key Pair Import Key	Pair Delete				Δ	⊕ ♥	•
Tags	Q Filter by attributes or search	by keyword			0	< < 1 to 5	i0 of 100 >	×
Reports Limits	Key pair name	Fingerprint		-				
INSTANCES	abragg	5f:10:99:d0:4a:c3:95:e4:4c:49:cd:03:e5	2					-
Instances	abragg	0e:1d:4a:36:16:46:72:d5:06:53:f0:66:44	lib					
Launch Templates	achem	6d:4e:ed:12:17:22:38:c4:73:2d:52:d5:f7	14					
Spot Requests	admin	14:e4:af:25:84:11:a0:bc:04:5f:41:c6:84	8t					
Reserved Instances	aknox-l	57:ba:bc:9d:48:e6:f4:c8:58:c8:5f:f4:ff.at	9					
Dedicated Hosts	apritcha	7e:90:12:69:ad:7d:f4:98:ff:24:15:5f:02:4	15:					
Scheduled Instances	apritcha	1a:fc:85:8c:ba:cc:0d:8d:bf:67:45:be:e3:	f5					
	aws-sd	b0:bd:1d:90:ec:bf:2b:24:fa:57:46:a0:b0	fe					
IMAGES AMIs	aws-sd	a1:38:66:29:35:05:84:d0:00:7c:c8:f9:99	:7					
AMIS Bundle Tasks	aws-sd	a1:ec:0d:fc:5e:fb:e8:67:9e:0b:18:48:a9	3!					
	Select a key pair							
STORE								

FIGURE 59 AWS EC2 Key Pairs

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

FIGURE 60 AWS Select EC2 Key Pair

abra	5f:10:99:d0:4a:c3:95:e4:4c:49:cd:03:e5:	0.0.47
abra	0e:1d:4a:36:16:46:72:d5:06:53:f0:66:44	-
ache	6d:4e:ed:12:17:22:38:c4:73:2d:52:d5:f7	
admin	14:e4:af:25:84:11:a0:bc:04:5f:41:c6:84:{	1000
akno	57:ba:bc:9d:48:e6:f4:c8:58:c8:5f:f4:ff:af:	
aprit	7e:90:12:69:ad:7d:f4:98:ff:24:15:5f:02:4	
air: admin		Q (
Key pair name a	dmin <i>අ</i>	٦
Fingerprint 1	4:e4:af:25:84:11:a0:bc:04:5f:41:c6:84:8b:9d:a3:	

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

A list of defined AMIs appears. For example:

EC2 Dashboard	es v Resource Groups v 🛧				û jki	by @ zeus ▪	Ireland → Support →
Events Tags	Owned by me V O Filter by tags and a	attributes or search by keyword	4			0	<pre></pre>
Reports Limits	Name - AMI Name	AMI ID +	1	Owner -	Visibility	- Status	Creation Date
	AML	ami-02216a6690b4	815181475	815181475	Private	available	August 6, 2018 at 2:03:0
INSTANCES Instances	jakm	ami-0390cf549bf82	815181475	815181475	Private	available	September 3, 2018 at 2:
Launch Templates	Jakm	ami-0f8d46a9b20el	815181475	815181475	Private	available	September 4, 2018 at 1:
	Idarb	ami-a7a25ed0	815181475	815181475	Private	available	March 10, 2014 at 4:42:
Spot Requests Reserved Instances	sd-bi	ami-08c269c71ae0	815181475	815181475	Private	available	August 31, 2018 at 4:19
Dedicated Hosts	Servi	ami-b4ffb1cd	815181475	815181475	Private	available	March 13, 2018 at 11:42
Scheduled Instances	Servi	ami-0627430bd6c1	815181475	815181475	Private	available	August 7, 2018 at 3:00:4
Scheduled Instances	Servi	ami-028189c4d8a5	815181475	815181475	Private	available	August 9, 2018 at 3:26:5
IMAGES	Servi	ami-03ccf2b81763t	815181475	815181475	Private	available	August 30, 2018 at 10:3
AMIs Bundle Tasks	Servi	ami-4a211b33	815181475	815181475	Private	available	May 30, 2018 at 2:25:14

FIGURE 61 AWS EC2 AMIs

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

FIGURE 62 AWS EC2 AMIs Name - AMI Name AMI ID - Source AMI builder ami-02216a6690b446543 815181475850/. jakman-image-from-... ami-0390cf549bf823210 815181475850/j... Jakman-Splunk Ent... ami-0f8d46a9b20eb2144 815181475850/J. ami-a7a25ed0 815181475850/1. Idarby-backend2 Image: ami-0390cf549bf823210 Permissions Details Tags AMLID ami-0390cf549bf823210 🖉 815181475850 Owner

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

Creating the PCS Appliance VM on AWS

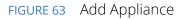
After you have identified all required information (see **"Creating and Registering a PCS Appliance VM on AWS" on page 41**), you can start the process to create and register a PCS appliance as a VM on AWS:

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

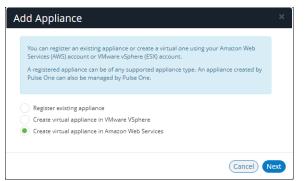
The **Appliances** tab displays all current appliances.

3. Click Add Appliance.

The Add Appliance wizard starts.



EICLIPE 61 AWS Cradentials



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

The AWS Credentials panel of the wizard appears.

		3
WS Credentials		
	redentials to manage virtual appliances. If you have already entered lect them from the list or add new ones to be used for this appliance.	
Account:	Add New 🗸	
Access Key:	AWS Access Key	
Secret Key:	AWS Secret	
	Cancel	

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

6. Click Next.

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

FIGURE 65 Appliance Configuration

	e name, company name, license code, and an admin username ed on the virtual appliance.
Appliance Name:	L.
Company Name:	
icense Auth Code:	
Appliance Username:	New Admin Username:
Password;	New Password:
Confirm Password:	Confirm New Password:

- 7. Enter the **Appliance Name**. This will be the displayed name in the list of appliances and will also be used to automatically populate the **Internal FQDN** and **External FQDN** properties on subsequent wizard panels.
- 8. Specify additional information for the appliance:
 - A Company Name.
 - (Optional) A License Auth Code can be recorded if required.
 - The **Appliance Username**, **Password** (and **Confirm Password**) for a required user on the appliance. This user will be created after the appliance is created.

9. Click **Next**.

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

FIGURE 66	Appliance	Network	Configu	iration: S	Servers
-----------	-----------	---------	---------	------------	---------

Please enter network co	nfiguration for the virtual appliance.	
SERVERS		~
Primary DNS:	8.8.8.8	
Secondary DNS:	8.8.4.4	
INTERNAL NETWO	RK SETTINGS	<
EXTERNAL NETWO	RK SETTINGS	<
MANAGEMENT NE	TWORK SETTINGS	<

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

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

11. Expand the Internal Network Settings panel.

FIGURE 67 Appliance Network Configuration: Internal Network Settings

Please enter network configuration for the virtual app	oliance.
SERVERS	<
INTERNAL NETWORK SETTINGS	\sim
Hosted Zone:	
Internal FQDN:	
EXTERNAL NETWORK SETTINGS	<
MANAGEMENT NETWORK SETTINGS	<

12. In the Internal Network Settings:

• For the **Hosted Zone**, enter the internal domain name (internal Route 53 hosted zone) for your appliance. See **"Identifying the Required Route 53 Zones" on page 42**.

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

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

FIGURE 68 Appliance Network Configuration: External Network Settings

Please enter network configuration for the virtual appli	ance.
SERVERS	<
INTERNAL NETWORK SETTINGS	<
EXTERNAL NETWORK SETTINGS	\sim
Public Domain Name:	
External FQDN:	
MANAGEMENT NETWORK SETTINGS	<

- 14. In the External Network Settings:
 - For the **Public Domain Name**, enter the external domain name (external Route 53 hosted zone) for your appliance. See **"Identifying the Required Route 53 Zones" on page 42**.

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

 For the External FQDN, complete the FQDN by adding a unique appliance identifier to the lefthand side of the external domain name in this field. Typically, you will specify the Appliance Name you specified in the Appliance Configuration dialog, and the external Hosted Zone is a suffix. 15. Expand the Management Network Settings panel.

FIGURE 69 Appliance Network Configuration: Management Network Settings

Please enter network conf	guration for the virtual appliance.	
SERVERS		<
INTERNAL NETWOR	K SETTINGS	<
EXTERNAL NETWOR	K SETTINGS	<
MANAGEMENT NET	WORK SETTINGS	\sim
Management Domain Name:		
Management FQDN:		

- 16. In the Management Network Settings:
 - For Management Domain Name, enter a name for the AWS network.

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

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

- 17. Click Next. The AWS Configuration panel of the wizard appears.
 - FIGURE 70 AWS Configuration

9.0R3.	entials and select a valid AMI with an applia nets should be part of the same availability	
Amazon Machine Image (AMI):	ami-123456	
VPC ID:	vpc-123456	
Region:	US West (N. California)	~
Private Subnet Id:	Public Subnet Id:	sub-123456
Management Subnet ID:	sub-123456	
Key Pair Name:	abcdef	

- 18. Specify the following properties:
 - Amazon Machine Image (AMI) is the AMI ID that you identified in "Identifying the EC2 Deployment Key and AMI ID" on page 46.
 - VPC ID is the value that you identified in "Identifying the Required VPC ID and Subnet IDs" on page 44.
 - **Region** is automatically populated from your chosen region.
 - **Private Subnet ID**, **Public Subnet ID**, and **Management Subnet ID** are the three subnet IDs that you identified in "Identifying the Required VPC ID and Subnet IDs" on page 44.
 - **Deployment Key** is the key pair that you identified in **"Identifying the EC2 Deployment Key** and AMI ID" on page 46.
- 19. Click Save.

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

FIGURE 71 New Unregistered Appliance

APPLIANCES	CONFIG GROUP	PS S	OFTWARES	BACKUP	-RESTORE	SCHEDULED	TASK
Appliances Q Sea	arch 🗙	+ Add Ap	opliance Exp	oort 🔁			
Name		Model	Version	Last Config U	Task Status	Pulse One Status	۲
🛆 new-aws-app		AWS				Unregistered	

20. Click the **Actions** icon ([‡]) for the appliance and select **Start Appliance**.

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

- Unregistered
- Creating
- Starting
- Started
- 22. Wait until the appliance is created.
- 23. Go to the **EC2 Dashboard** in AWS and view **Instances**.
- 24. The new appliance is listed and reports a **Status Check** of Initializing. For example:

FIGURE 72 AWS Initializing Appliance

EC2 Dashboard Events	↓ La	unch Instance	Connect Actio	ons ¥						Δ	0 I	• 6
Tags	C	Filter by tags and a	attributes or search by key	word							20 of 20	> >
Reports	1	Name -	Instance ID ~	Instance Type	Availability Zone -	Instance State ~	Status Checks ~	Alarm Status	Pul	blic DNS (IPv4)	IPv4 Pu	blic IP
Limits			1-001 0000000401	12.11IGIO	ua-weat-10	- atopped		NUND	004	-10-01-12	10.01.	-
INSTANCES		sree	i-0f3ecd1c67cea	t2.micro	us-west-1a	stopped		None	ec2	-54-241-	54.241	-
Instances		mob .	i-0fb5a78c74255	t2.small	us-west-1a	running	2/2 checks	None	a ec2	-54-215-	54.215	
Launch Templates		aws	i-0779548656d2	t2.xlarge	us-west-1a	stopped		None			54.176	
Spot Requests		new-aws-ap	i-0edbefcfe213	t2.xlarge	us-west-1a	running	Initializing	None			52.52.	
Reserved Instances Dedicated Hosts	In	stance: i-0edbefc	fe2139 (new-aws-a	app-PCS) Elasti	c IP: 52.52.111.67							86

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

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

Configuring CPU, Memory and Disk Utilization

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

The panel shows the following status:

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

To view the health of an appliance:

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

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

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

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

FIGURE 73 Appliance Health

	DASH	IBOARD APPLIANCES	ANALYTICS ADM	IINISTRATION	SETTINGS ADMIN
Appliances	APPLIANCES CONFI	G GROUPS SC	DFTWARE BA	ACKUP-RESTORE SCHED	Q DULED TASKS SEARCH
Appliances + Add Appliance Export	\mathbf{O}				2 Appliances
Name Model Version	Last Config Upload Task Status	s Pulse One Status 🐵	🖨 Pulse-F	PPS-1 🔿	Actions -
Pulse-PPS-1 VA-SPE 9.0R1-49496	14hr 40min	Connected			
Pulse-PPS-7 VA-SPE 9.0R1-49496	14hr 47min	Connected	APPLIANC	EINFO	<u> </u>
			0 将 Concurrent U	-	7.91 C kb/s Throughput
			CPU Utilizati		25% Disk Utilization

Backing up and Restoring Appliance Configurations

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

Each appliance can have a single configuration backup only.

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

Backing up the Configuration of an Appliance

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

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

FIGURE 74	Pulse One Appliances 1	īab
-----------	------------------------	-----

E SPulse Secure	DASHBOARD APPLIA	NCES ANALYTICS	S ADMIN	NISTRATION			Q DMIN Ƴ
Appliances Appliances	CONFIG GROUPS	SOFTWARE	ВАСК	UP-RESTORE	SCHEDULE		Q ARCH
Appliances + Add Appliance Export						4 App	oliances
Name		Model	Vers l	Last Config U	Task Status	Pulse One Status	٢
Ade_Pulse-106		PSA5000-V	9.0R 5	5d 18hr 53min		Connected	000
Ade_Pulse-109		PSA7000-V	9.0R 5	5d 18hr 50min		Connected	
Pulse-PPS-1		VA-SPE	9.0R 6	öd 15hr 57min		Connected	0.00
Pulse-PPS-7		VA-SPE	9.0R 6	5d 15hr 54min		Connected	000

3. Locate the appliance that you want to backup and click its **Actions** icon ([‡]).

FIGURE 75 Appliance Menu

101	Pulse Secure		DASHBOARD A	APPLIANCES	ANALYTICS	ADM	IINISTRATION		SETTINGS AL	Q DMIN V
	Appliances	APPLIANCES	CONFIG GROUP	s so	FTWARE	BAC	CKUP-RESTORE	SCHEDULED		Q ARCH
Applia	Ances + Add Appliance Export	Θ							4 App	oliances
Name					Model	Vers	Last Config U	Task Status	Pulse One Status	۲
PES .	Ade_Pulse-106				PSA5000-V	9.0R	5d 18hr 55min		Connected	000
PES	Ade_Pulse-109				PSA7000-V	9.0R	5d 18hr 52min		Reboot Appliance	
PPS	Pulse-PPS-1				VA-SPE	9.0R	6d 16hr		Edit Appliance Inf Launch Appliance	
PPS	Pulse-PPS-7				VA-SPE	9.0R	6d 15hr 56min		Remove Appliance Compare Applian	
									Backup Configura	
									Upgrade Software Schedule Task	

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

4. Click Backup Configuration.

The **Backup Appliance** dialog appears.

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

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

FIGURE 76 Monitoring a Pending Backup

Appliances + Add Appliance Export					4 App	liance
Name	Model	Version	Last Config Upload	Task Status	Pulse One Status	٢
Ade_Pulse-106	PSA5000-V	9.0R3-13030	5d 20hr 20min	Backup Pending	Connected	000
Ade_Pulse-109	PSA7000-V	9.0R3-13030	5d 20hr 18min		Connected	040
PPS Pulse-PPS-1	VA-SPE	9.0R1-49496	6d 17hr 25min		Connected	000
Pulse-PPS-7	VA-SPE	9.0R1-49496	6d 17hr 22min		Connected	0.00

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

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

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

To do this, click the **Actions** icon ([§]) for the appliance, and then click **Cancel Backup**.

Appliances + Add Appliance Export					4 Appliances
Name	Model	Version	Last Config Upload	Task Status	Pulse One Status 🛛 💿
Ade_Pulse-106	PSA5000-V	9.0R3-13030	5d 20hr 25min	Backup In Progress Cancellable	Connected 🕴
Ade_Pulse-109	PSA7000-V	9.0R3-13030	5d 20hr 23min		Reboot Appliance
PP5 Pulse-PPS-1	VA-SPE	9.0R1-49496	6d 17hr 30min		Edit Appliance Info Launch Appliance UI
Pulse-PPS-7	VA-SPE	9.0R1-49496	6d 17hr 27min		Remove Appliance Compare Appliances
					Backup Configuration
					Upgrade Software
				L	Cancel Backup
1					Schedule Task

The cancellation is then confirmed.

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

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

```
FIGURE 78 Viewing Backup Files
```

■ Pulse Secu PULSE ONE		DASHBOARD APPLIANCI	S ANALYTIC	5 ADMINISTRATION			
Appliances	APPLIANCES	CONFIG GROUPS	SOFTWARE	BACKUP-RESTORE	SCHEDULED	TASKS	Q search
Backup-Restore					1	MB Total I	Backup Size
Appliance Name	Description	Appliance Version		Backup Date	Size		۲
Ade_Pulse-106	test_backup	9.0R3-13030		2019-01-16 13:55:57 +0000	725.	21 KB	8
Ade_Pulse-109	after_clear_config-1	9.0R3-13030		2019-01-16 13:54:35 +0000	727.	01 KB	000

In this example:

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

Deleting the Configuration Backup for an Appliance

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

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

FIGURE 79 Viewing Backup Files Before Delete

	cure*	DASHBOARD APPLIA	NCES ANALYTICS	5 ADMINISTRATION		
Appliance	S APPLIANCES	CONFIG GROUPS	SOFTWARE	BACKUP-RESTORE	SCHEDULED TASKS	Q SEARCH
Backup-Restore					1 MB Total	Backup Siz
Appliance Name	Description	Appliance Version		Backup Date	Size	۵
Ade_Pulse-106	test_backup	9.0R3-13030		2019-01-16 13:55:57 +0000	725.21 KB	000
	after_clear_config-1	9.0R3-13030		2019-01-16 13:54:35 +0000	727.01 KB	

In this example, the configuration backup for Ade_Pulse-106 is at the top of the list.

- 3. Locate the configuration backup that you want to delete.
- 4. Click the **Actions** icon ([§]) for the appliance, and then click **Delete Configuration**.

A confirmation dialog appears.

5. Confirm the deletion.

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

Restoring the Configuration of an Appliance

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

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

FIGURE 80 Viewing Backup Files

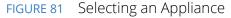
E SPULSE Sect	ure*	DASHBOARD APPLIANC	ES ANALYTICS	ADMINISTRATION		
Appliances	APPLIANCES	CONFIG GROUPS	SOFTWARE	BACKUP-RESTORE	SCHEDULED TASKS	Q SEARCH
Backup-Restore					1 MB Tota	al Backup Size
Appliance Name	Description	Appliance Version	В	lackup Date	Size	٥
Ade_Pulse-106	test_backup	9.0R3-13030	2	019-01-16 13:55:57 +0000	725.21 KB	032
Ade Pulse-109	after clear config-1	9.0R3-13030	2	019-01-16 13:54:35 +0000	727.01 KB	00

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

3. Locate the configuration backup that you want to restore.

4. Click the **Actions** icon (¹) for the appliance, and then click **Restore Configuration**.

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



Select Appliance to Restore					
	Ade_Pulse-106				
installed and act • ESAP Packa	ssfully restore this backup, please make sure that following packages are tivated on the "target" appliance by using it's admin UI: ge (3.2.7) top (9.0.3.1494)				
	(Close) Set	ect			

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

5. Select the required appliance and click Select.

The configuration restore for the selected appliance is scheduled.

6. Click the **Appliances** tab.

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

FIGURE 82 Monitoring a Configuration Restore for an Appliance

	DASHBOARD APPLI	ANCES ANALYTICS ADMINIST		
Appliances	NCES CONFIG GROUPS	SOFTWARE BACKUP	RESTORE SCHEDULED TASKS	Q SEARCH
Appliances + Add Appliance Export			4	Appliances
Name	Model Version	Last Config Upload Tas	k Status Pulse One Statu	s ©
PC5 Ade_Pulse-106	PSA5000-V 9.0R3-13030	5d 20hr 20min Re	store Pending Connected	
Ade_Pulse-109	PSA7000-V 9.0R3-13030	5d 20hr 18min	Connected	000
Pulse-PPS-1	VA-SPE 9.0R1-49496	6d 17hr 25min	Connected	000
Pulse-PPS-7	VA-SPE 9.0R1-49496	6d 17hr 22min	Connected	ę

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

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

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

- 7. (Optional) While the **Task Status** for a selected appliance is *Restore Pending*, you can cancel the restore process. To do this, click the **Actions** icon ([§]) for the appliance, and then click **Cancel Restore**.
- 8. (Optional) View the activities for an appliance to see the results of backup and restore operations, see **"Viewing the Activities Log for an Appliance" on page 87**.

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 61.
- "Adding Appliances to an Appliance Group" on page 65.
- "Distributing a Master Configuration" on page 67.

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 83 Create Appliance Group

	DASHBOARD APPLIANCES	ANALYTICS ADMINIS	TRATION	SETTINGS ADMIN	
Appliances Appliances	S CONFIG GROUPS	SOFTWARE BAC	KUP-RESTORE	SCHEDULED TASKS	
Appliance Configuration Groups 🕘	eate Appliance Group				
Name Status	۵				
PPS-9.0R1-Group Publish Required (i)	2	Please selec	t a group	or add one.	
)	

The Create Appliance Group Wizard appears.

FIGURE 84 Create Appliance Group Wizard

Create Appliance	Group		
Introduction	Group name and description	Group configuration settings	Summary
Creating an applianc	e group		
	e base configuration from an applia master" appliance is used to edit co		nfiguration to all the other
	ation settings that belong to the gro from the actions menu for the grou		ch settings are used later by
You can add appliances to the g	group and remove them at any time	e. A group cannot be empty and m	ust contain the group master.
Cancel			< Previous Next

4. Click Next.

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

FIGURE 85 Group Name and Description Wizard Panel

Create Appliance	Group			
Introduction	Group name and d	lescription	Group configuration settings	Summary
Group name and des	scription			
Group name:	Gro	oup 2		
Description:	Ор	itional short c	lescription of the group	
DMI Information				10
Username:	my	vadmin		
Password:				
Port:				
Cancel				< Previous 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.

For full details of appliance upgrades, see "Upgrading Managed Appliances" on page 71.

6. Click Next.

The Group configuration settings panel of the wizard appears.

FIGURE 86 Group Configuration Settings Wizard Panel

Create Appliance C	Group		
Introduction	Group name and description	Group configuration settings	Summary
iroup configuration s	ettings		
Select master appliance:	Ade_Pulse-106		~
Master appliance URL:	https://10.64.	/admin	
ect from the list below to define the co	nfiguration settings to be used for the gro	oup.	Rese
 System Authentication 			
Authentication Administrators			
Users			
Maintenance			
Cancel			< Previous Ne

- 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 configuration settings that must be shared between all group members in the bottom list.

8. Click Next.

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

FIGURE 87 Summary Wizard Panel

Introduction	Group name and description	Group configuration settings	Summary
ummary			
Group name:	pps_group		Edit
Description:			Edit
Username:	10000		Edit
Password:			Edit
Port:			Edit
Master appliance:	Ade_Pulse-106		Edit
Master appliance URL:	https://10.64	/admin	Edit
Group config settings:	99		Edit

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

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

FIGURE 88	New Appliance Group
-----------	---------------------

E SPULSE Secure		DASHBOARD AP	PPLIANCES ANALYTICS	ADMINISTRATION	SETTINGS ADMIN
Appliances	APPLIANCES	CONFIG GROUF	PS SOFTWARE	BACKUP-RESTORE	SCHEDULED TASKS
Appliance Configuration Groups Name Status pps-group In Sync		ppliance Group			Actions •
	+ Add Appliance Status Name	Config	State Last Co	nfig Upload	٥

You can now add appliances to the group as target appliances, see **"Adding Appliances to an Appliance Group" on page 65**.

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 89 Target Appliances Empty

		DASHBOARD APPLIANCES	ANALYTICS AD	PMINISTRATION		
Appliances	APPLIANCES	CONFIG GROUPS	SOFTWARE	BACKUP-RESTORE	SCHEDULED TASKS	
Appliance Configuration Groups	🕀 🕀 Create App	pliance Group				
Name Status	pps-group	(In Sync) Publish All			Ac	tions -
	Target Appliances	Group Configuration				
	+ Add Appliance					
	Status Name	Config State	Last Config	Upload		۲

5. Click Add Appliance. A dialog appears.

FIGURE 90 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 91 Target Appliances Added

	Pulse Secure [®]		DASHBOARD APPLIA	NCES ANALYTICS	ADMINISTRATION		
Арј	pliances	APPLIANCES	CONFIG GROUPS	SOFTWARE	BACKUP-RESTORE	SCHEDULED TASKS	
Appliance Co	onfiguration Groups	Create Ap	opliance Group				
Name Status PCS-Group Publish Required ① 2	PCS-Group (① Publish Required) Publish All Publish Selected Actions • Docs Target Appliances Group Configuration						
		+ Add Appliance	e Confi	g State	Last Config Upload		٢
		• •	Ade_Pulse-109 Publi	sh Required 🕕	5d 21hr 2min	View Changes	ŝ
		• •	Ade_Pulse-106 Public	sh Required 🛈	5d 21hr 12min	View Changes	000

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 67.
- "Publishing Configuration Changes Manually to Group Members" on page 67.
- "Publishing Configuration Changes to Group Members as a Scheduled Task" on page 70.

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.



Pulse Secure PULSE ONE	DASHBOARD	APPLIANCES ANALYTIC	CS ADMINISTRATION	SETTINGS ADMIN
Appliances	APPLIANCES CONFIG G	ROUPS SOFTWAR	RE BACKUP-RESTORE	SCHEDULED TASKS
Appliance Configuration Groups	Create Appliance Group)		
Name Status PCS-Group Publish Required (1) 1	PCS-Group ((i) Publis		Publish Selected	Actions >
PPS-9.0R1-Group In Sync		nfiguration		
pps-group In Sync 🕴	Status Name Status Name Ade_Pulse-109	Config State	Last Config Upload	Close Changes
(Configuration Changes	5	Apply Group Config Context Siz	e 5
	Modification Summary Log > Events (modified) Log > Log (modified) Log > Admin (modified)	Ade_Pulse-109 Previous Configuration 12 <node>local 13 <rr></rr> 4 <rr></rr> 4 <rr></rr> 14 <rr></rr> 5 <client. 16 <client. 16 <client. 16 <client. 16 <client. 16 <client. 16 <client. 16 <client. 17 <client. 18 <client. 19 <client. 19 <client. 19 <client. 10 <client.< td=""><td>rers> 13 rrer> 14 cert>Select 15 rt> Cert(cation- 16 typs>top 17 one19</td><td>ation <pre>cnode>localhost2</pre>/node> <syslog-servers> <syslog-servers> <sliett-retselect c="" nt-act=""> <communication- <fscilityocall<="" communication-="" pre=""></communication-></sliett-retselect></syslog-servers></syslog-servers></td></client.<></client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </client. </node>	rers> 13 rrer> 14 cert>Select 15 rt> Cert(cation- 16 typs>top 17 one19	ation <pre>cnode>localhost2</pre> /node> <syslog-servers> <syslog-servers> <sliett-retselect c="" nt-act=""> <communication- <fscilityocall<="" communication-="" pre=""></communication-></sliett-retselect></syslog-servers></syslog-servers>

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 70**.

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 93 Publish All

Pulse Secure PULSE ONE	DAS	SHBOARD APPLIANCES	ANALYTICS ADM	INISTRATION		
Appliances	APPLIANCES		SOFTWARE	BACKUP-RESTORE	SCHEDULED TASKS	
Appliance Configuration Groups	Create Appliar	nce Group				
Name Status PCS-Group Publish Required ① \$	PCS-Group ((Docs	i) Publish Required)	Publish All Publis		Ac	ions •
	Target Appliances	Group Configuration				
	+ Add Appliance					
	Status Name	Config State	Last Cor	nfig Upload		۲
	Ade_	Pulse-109 Publish Requ	ired 🛈 5d 22hr	29min	View Changes	8

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 94 Configuration Change in Member Appliance

	Pulse Secure	DASHBOAR	D APPLIANCES ANALYTICS ADMINIS	STRATION	SETTINGS ADMIN
Ар	pliances	APPLIANCES CONFIG	GROUPS SOFTWARE B	ACKUP-RESTORE S	CHEDULED TASKS
Appliance Co	nfiguration Groups	Create Appliance Group			
Name	Status	Status Name	Config State Last Config	Upload	٥
PCS-Group	Publish Required 🕕 🕴	\sim			
PPS-9.0R1-Group	Configuration 8 Mismatch (1)	PP5 Pulse-PPS-7	Configuration Mismatch 6d 19hr 38n	nin	Close Changes
pps-group	In Sync ž	Configuration Change	Keep Non-compliant Apply Group Co	onfig Context Size 5	
		Modification Summary	Pulse-PPS-7	Group Configur	ation
		MAC Addr Realms (Guest	Previous Configuration	New Configuration	A
		Wired modified)	13 <device-check- interval>60<td></td><td>e-check-</td></device-check- 		e-check-
	•		14 <device- server>None 15 <directory-server>Quest Wired Authenticationserver></directory-server></device- 	14 <device server>None15 <direct as above<td>- evice-server> tory-server>Same</td></direct </device 	- evice-server> tory-server>Same
			16 <dynamic-policy></dynamic-policy>	16 <dynam:< td=""><td>ic-policy≻ ↓</td></dynam:<>	ic-policy≻ ↓

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

- 5. You can either:
 - Retain the changes by clicking Keep Non-compliant, OR
 - Apply the group configuration by clicking **Apply Group Config**.

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

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

FIGURE 95 Configuration Mismatch

Compliance Problem				
The following setting(s) are group of compliance.	contro	olled settings(s) that	t have been changed on the appliance hbirdi-SA-1_38.101. This has caused hbirdi-SA-1_38.101 to be	e out of
Modification Summary		Appliance Confi	figuration Group Configuration	
Auth Roles: Admin (Vanishing Act added)		Base Text	New Text	
Auf Relate: Admini Hamman Test Rela edded) Auf Relate: Administrators modifiel Auf Relate: Administrators modifiel System Security (modified) Diolose: Transmissi Comestion Politiss (modified) Auft Relate: User (Outload Angentere User Role modified) Auft Relate: User (National Test Relate: 2 added) Auft Relate: User (National Relate: 3 added) Auft Relate: Admini (Chassis 550 modified)			1 configuration multime"http://will.junipri.ne///wess/8/127" public surf program. Surg/2001/2015/bene-instance" 2 cadminerates) 4 cadminerates) 4 cadminerates) 5 cadminerates) 6 cadaqge-adminerates) 6 cadaqge-adminerates) 7 cadaces>demy-all//access) 8 calculorates/markets/allow- add-renor-admineratings 9 catalorates/anstales/ 9 cadalorates/anstales/ 9 cadalorates/ 9	Î
	1	-	14	-
Context Size 5		Side by side	Inline Cancel Keep Non-compliant Apply Group	Config

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 67**.

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 96 Create Publish Configuration Task

Create Task			×
Choose Appliance or Group	Appliance Group		
	pps-group	~	
Task Type:	Select Task Type	~	
Scheduled Time:	Select Task Type Stage a software package Install a staged package		
Comments:	Publish configuration		
		Cancel S	

- 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 97 Scheduled Publish Configuration Task

ilter by:	Task Type:	Select Task Type	Apply Clear			
Task Type		Task Status	Scheduled Time	Appliance / Group	Comments	0
Publish con	figuration	Success	2018-10-31 11:11:00 +0530	pcs-26-27	publish-group-26-27	12 1

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

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

Upgrading Managed Appliances

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

- Upload one or more appliance software packages on Pulse One, see "Uploading an Appliance Software Package to Pulse One" on page 71.
- You must ensure that each appliance has its DMI enabled and configured correctly, see "Checking DMI Settings" on page 73.
- Upgrade a single appliance, see "Upgrading an Appliance" on page 75.
- Upgrade all appliances in an appliance group, see "Upgrading All Target Appliances in a Group" on page 77.
- Upgrade both appliances in a cluster, see "Upgrading All Appliances in a Cluster" on page 79.
- Schedule the upgrade of an appliance in two stages:
 - First, schedule the upload of an image to a staging area on an appliance.
 - Second, schedule the installation of a staged software package on an appliance.

For details, see "Scheduling Upgrade-Related Tasks" on page 79.

Uploading an Appliance Software Package to Pulse One

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

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

To upload an appliance software package:

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

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

FIGURE 98 Available Software

	lse Secu	re⁺	DASHBOARD A	PPLIANCES ANALYTICS ADM	IINISTRATION		
Appl	iances	APPL	LIANCES CONFIG GROU	JPS SOFTWARE	BACKUP-RESTORE SCH	IEDULED TASKS	
Available Software			C5 software) can be stored on Pul-	se One. **	Download	d Appliance Soft	ware ^{"L}
			CS software) can be stored on Puls	se One. ** MD5 Hash	<u>Download</u> Created	<u>d Appliance Soft</u>	ware »
* Only 3 software vers	ions of each type	(i.e. 3 PPS and 3 P					

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

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

4. Click Add Software.

The Upload Software dialog appears.

re
r

Upload Softwa	re		×
Software Type:	Pulse Policy Secure	~	
Version:	e.g. 9.0R1, 5.4R1, 5.4R3-HF2		
Description:			
MD5 Hash:			
Select Software:	Choose File No file chosen		
	Cancel	Uplo	ad

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

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

• Enter the MD5 Hash value for the software package.

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

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

6. Click Upload.

The upload may take several minutes.

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

FIGURE 100 Appliance Software Package Added

Available Softw	are + Add So	oftware			Download	Appliance Sof	<u>tware</u> _≯ □
** Only 3 software ver	sions of each type	(i.e. 3 PPS and 3 P	CS software) can be stored on Puls	se One. **			
Туре	Version	Description	File Name	MD5 Hash	Created	Size	٥
Pulse Policy Secure	9.0R3	pps-90r3	package-51582.1.pkg	33ccf56b7843fed7f2688238236fc3bb	2018-10-23 11:55:48 +0530	1006.46 MB	
Pulse Connect Secure	9.0R1	pcs-90r1	pcs_package_90r1_debug-6395	31ac7d82bc53e374a7f03e01fd85e595	2018-10-23 15:17:46 +0530	868.66 MB	ш
Pulse Connect Secure	9.0R3-12402	pcs-90r3	pcs_90r3_debug_package-b124	6fdc23ba0424e7f75e70d7feb2032894	2018-10-23 12:11:56 +0530	936.52 MB	ш

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

To do this, click the **Actions** icon ([‡]) for the software package, and then click **Edit Software**.

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

To do this, click the **Actions** icon ([§]) for the software package, and then click **Delete Software**.

You can now perform one or more appliance software upgrades.

Checking DMI Settings

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

To check DMI settings:

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

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

FIGURE 101 Accessing Pulse Policy Secure DMI Agent Settings

Status	✓ Licensing	✓ Certificates
Configuration	License Summary Configure Server	Device Certificates Trusted Client CAs
Network	Download Licenses	Trusted Server CAs Client Auth Certificates
Clustering	✓ Pulse One	Certificates Validity Check
Log/Monitoring	 ✓ Security 	DMI Agent
Reports	Inbound SSL Options Outbound SSL Options Health Check Options Miscellaneous	SMTP Settings SMS Gateway Settings
	Configuration Network Clustering	Configuration License Summary Configure Server Network Download Licenses Clustering Y Pulse One Log/Monitoring Settings Reports Inbound SSL Options Cutbound SSL Options Health Check Options

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

FIGURE 102 Pulse Policy Secure DMI Agent Settings

Configuration > DMI Agent	
DMI Agent	
Configuration DMI Agent	
Licensing Pulse One	Security Certificates DMI Agent Guest Access
Device Management Interface (DMI)	is an extension to the NETCONF network management protocol. It allows DMI-enabled management applications to connect with and configure Pulse Secure devices.
Enter settings to enable the DMI Ag	ent on this device and facilitate connection to a DMI-enabled management application.
V Inbound connection status	
Connection State:	Listening
Number of Active Connections:	0
V Outbound connection status	
Connection State:	Disconnected
Last Connection Time:	
Connected Server: Admin User Logged In:	
❤ DMI connections	
Inbound:	Enabled
Outbound:	Enabled

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

FIGURE 103 Pulse Policy Secure DMI Agent Settings

✤ DMI connections	
Inbound:	Enabled
Outbound:	Enabled

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

To do this, you need the DMI settings that you used when you registered the appliance, see **"Registering an Existing PCS/PPS Appliance" on page 21**. Specifically, you need the choice of whether to perform DMI over the internal port or the management port.

- For the **Accept connections on** setting, select the required interface type. That is, either the *Internal Port* or the *Management Port*.
- The **TCP port** number. The default is *830*.
- 6. The DMI settings on the appliance are now configured correctly for software upgrades from Pulse One.

Upgrading an Appliance

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

Note: Alternatively, you can schedule one or more upgrade processes for a later time, see **"Scheduling Upgrade-Related Tasks" on page 79**.

Before you can perform an immediate software upgrade on an appliance, you must upload the required appliance software package, see **"Uploading an Appliance Software Package to Pulse One" on page 71**.

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

To perform a software upgrade for an appliance:

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

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

FIGURE 104 Available Appliances

	DASHBOARD APPLIANCES	5 ANALYTIC	s administration		
Appliances Appliances	CONFIG GROUPS S	OFTWARE	BACKUP-RESTORE	SCHEDULED TASKS	Q SEARCH
Appliances + Add Appliance Export					4 Appliances
Name		Model	Vers Last Config U	Task Status Pulse	one Status 💿
Ade_Pulse-106		PSA5000-V	9.0R 5d 18hr 53min	• Co	nnected 🚦
PLS Ade_Pulse-109		PSA7000-V	9.0R 5d 18hr 50min	● Co	nnected
Pulse-PPS-1		VA-SPE	9.0R 6d 15hr 57min	Co	nnected
PPS Pulse-PPS-7		VA-SPE	9.0R 6d 15hr 54min	● Co	nnected §

3. Click the **Actions** icon ([‡]) for the appliance you want to upgrade, and then click **Upgrade Software**.

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

Upgrade Softwa	ire	×
Appliance Name:	Pulse-PPS-1	
Select Software:	9.0R3 (Pulse Policy Secure)	~
Version: 9.0R3 Description: pps-90r3		
Size: 1006.46 MB Type: Pulse Policy Secure		
	Clos	se) Upgrade

FIGURE 105 Upgrade Software

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

Full details for the selected package are displayed.

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

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

FIGURE 106 Upgrade Pending

Appliances	+ Add Appliar	Export	\bigcirc			
Name	Model	Version	Last Config U	Task Status	Pulse One Status	0
PPS pps-31	VA-SPE	5.4R3-45254	1hr 35min	Software upgrade Pending	Connected	
PPS pps-32	VA-SPE	5.4R3-45254	1hr 33min		Connected	
PP5 pps-33	VA-SPE	5.4R3-45254	1hr 33min		Connected	

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

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

Note: All appliance configuration is preserved during this process.

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

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

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

FIGURE 107	Appliance Rebooting
------------	---------------------

Appliances	+ Add Appliance	Export	Θ		
Name	Model	Version	Last Config U Task Status	Pulse One Status	۲
PPS pps-31	VA-SPE	5.4R3-45254	Unknown 🚯	O Not Connected	
PPS pps-32	VA-SPE	5.4R3-45254	1hr 44min	Connected	
PPS pps-33	VA-SPE	5.4R3-45254	1hr 44min	Connected	

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

Upgrading All Target Appliances in a Group

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

The target appliances in the group are upgraded automatically.

Note: Alternatively, you can schedule one or more upgrade tasks for the master appliance at a later time, see **"Scheduling a Full Upgrade of an Appliance Group" on page 85**.

To upgrade all members of an appliance group:

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

The Appliance Configuration Groups tab lists all appliance groups on Pulse One. For example:

FIGURE 108 Available Appliance Groups

■ SPulse Secure PULSE ONE	DASHBOARD APPLIANCES ANALYTICS ADMINISTRATION	
Appliances Appliances	CONFIG GROUPS SOFTWARE BACKUP-RESTORE SCHEDULED TASKS	
Appliance Configuration Groups 🕀 🛞 Create /	Appliance Group	
Name Status © PCS-Group Publish Required ① E	PCS-Group (① Publish Required) (Publish All (Publish Selected Docs Group Configuration 4 Add Appliances Group Configuration	tions
	StatusName Config State Last Config Upload	۲
	Ade_Pulse-109 Publish Required ① 5d 23hr 45min View Changes	000
	Ade_Pulse-110 Publish Required ① 5d 23hr 44min View Changes	222
	Ade_Pulse-111 Publish Required () 5d 23hr 43min (View Changes	000

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

The Upgrade Software dialog appears. For example:

FIGURE 109 Appliance Group Upgrade Software

Upgrade Softwa	re	×
Appliance Name:	PCS-Group	
Select Software:	9.0R3	~
Version: 9.0R3 Description: pps-90r3 Size: 1006.46 MB Type: Pulse Policy Secure		
		Close Upgrade

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

Full details for the selected package are displayed.

- 5. To start the upgrade, click **Upgrade**.
- 6. Click the **Appliances** tab.

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

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

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

Note: All appliance configuration is preserved during this process.

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

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

- After the software package upload to an appliance is complete, the appliance reboots to complete the upgrade, and the connection between Pulse One and the appliance is lost.
- After the appliance reboots, the upgrade of the appliance is complete, but it may take several minutes to reconnect to the appliance from Pulse One.

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

Upgrading All Appliances in a Cluster

Upgrading all appliances in a cluster is similar to the upgrade of a single appliance, see **"Upgrading an Appliance" on page 75**.

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

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

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

Note: Alternatively, you can schedule the upgrade processes for a later time, see **"Scheduling Upgrade-Related Tasks" on page 79**.

Scheduling Upgrade-Related Tasks

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

There are three types of scheduled task:

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

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

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

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

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

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

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

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

The scheduling of tasks is supported for:

- Single appliances.
- Appliance groups. You schedule the tasks against the group, and all group members will automatically perform the designated task.

- Appliance clusters:
 - For *Active/Active* clusters, you can only schedule tasks for the *Leader node*. After both the upload and the installation tasks are complete, all other nodes upgrade automatically.
 - For *Active/Passive* clusters, you can only upgrade the Passive node. After both the upload and the installation tasks are complete, the Active node upgrades automatically.

You can initiate appliance upgrades using scheduled tasks as follows:

- "Scheduling a Full Upgrade from the Scheduled Tasks Tab" on page 80.
- "Scheduling a Full Upgrade from the Appliances Tab" on page 83.
- "Scheduling a Full Upgrade of an Appliance Group" on page 85.

Scheduling a Full Upgrade from the Scheduled Tasks Tab

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

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

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

FIGURE 110 Scheduled Tasks

	Se Secure [®]	D	ASHBOARD APPLIANCES	ANALYTICS ADM	IINISTRATION		
Applia	ances	APPLIANCES	CONFIG GROUPS	SOFTWARE	BACKUP-RESTORE	SCHEDULED TASKS	
Scheduled Tasks Filter by: Task Type:	Create Task	- Apply C	Clear				
Task Type No data to display	Task Status	Target Version	Scheduled Time	Appliance / Gro	up Comments	0	
0 total							_

3. Click Create Task.

The **Create Task** dialog appears.



Create Task		×
Choose Appliance or Group	Appliance Group	
Task Type:	Select Task Type	•
Scheduled Time:	Jan 17, 2019)
Comments:		
	Cancel	Save

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

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

FIGURE 112 Scheduled Staging Task Added

E SPULSE Secure	DASH	HBOARD APPLIANCES	ANALYTICS ADMI	NISTRATION		
Appliances	APPLIANCES CO	ONFIG GROUPS	SOFTWARE	BACKUP-RESTORE	SCHEDULED TASKS	
Scheduled Tasks Create Task Filter by: Task Type: Select Task Type	Apply Clea	D				
Task Type Task Status	Target Version	Scheduled Time	Appliance / Grou	p Comments	٥	
Stage a software package		2018-10-24 00:00:00 +0530	pps-36	stage-pps	Ø	•
1 total						

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

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

8. Click Save.

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

FIGURE 113 Scheduled Install Task Added

	Secure [®]	Dŕ	ASHBOARD APPLIANCES	ANALYTICS ADMIN	IISTRATION		
Applia	inces	APPLIANCES	CONFIG GROUPS	SOFTWARE	BACKUP-RESTORE	SCHEDULED TASKS	
	Select Task Type		Iear		I		
Task Type Stage a software package	Task Status	Target Version	Scheduled Time 2018-10-24 00:00:00 +0530	Appliance / Group	stage-pps	© 7	0
-			2018-10-24 04:00:00 +0530	pps-39	install	12	÷

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

Scheduling a Full Upgrade from the Appliances Tab

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

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

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

FIGURE 114 List of Appliances

■ SPulse Secure PULSE ONE	DASHBOARD APPLIANCES ANALYT	ICS ADMINISTRATION	SETTINGS ADMIN
Appliances	CONFIG GROUPS SOFTWARE	BACKUP-RESTORE S	Q SCHEDULED TASKS SEARCH
Appliances + Add Appliance Export			4 Appliances
Name	Model	Vers Last Config U Ta	sk Status 🛛 Pulse One Status 🐵
Ade_Pulse-106	PSA5000	V 9.0R 5d 18hr 53min	Connected
PLS Ade_Pulse-109	PSA7000	V 9.0R 5d 18hr 50min	Connected
PPS Pulse-PPS-1	VA-SPE	9.0R 6d 15hr 57min	Connected
Pulse-PPS-7	VA-SPE	9.0R 6d 15hr 54min	Connected

3. Click the **Actions** icon ([‡]) for the appliance you want to upgrade, and then click **Schedule Task**.

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

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

The **Create Task** dialog appears.

FIGURE 115 Create Task

Create Task		3
Schedule task for pps-36		
Task Type:	Select Task Type	
Target Version:	Select Target Version 🗸	
Scheduled Time:	Oct 24, 2018 🛗 12 00 AM	
Comments:		
	Cancel	

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

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

FIGURE 116 Scheduled Staging Task Added

	e Secure [®]	DASI	HBOARD AP	PPLIANCES AN	ALYTICS ADI	MINISTRATION		Q admin
Applia	nces	PPLIANCES CO	ONFIG GROUI	PS SO	FTWARE	BACKUP-RESTORE	SCHEDULED TASKS	
Scheduled Tasks		Apply Clea	ar					
Task Type	Task Status	Target Version	Scheduled Tin	ne	Appliance / Gr	roup Comments	٥	
Stage a software package			2018-10-24 00:0	10:00 +0530	pps-36	stage-pps	œ	•
1 total								

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

The **Create Task** dialog appears.

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

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

- 9. (Optional) You can edit the details for a scheduled task by clicking the **Edit** icon (\square) for the task.
- 10. (Optional) You can cancel a scheduled task by clicking the **Delete** icon for the task.

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

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

Scheduling a Full Upgrade of an Appliance Group

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

Note: Before you upgrade a group, you can optionally publish any configuration changes from the master appliance to all group members. This can be performed as a separate scheduled task. You can also choose to publish a configuration to a group at any other time, see **"" on page 66**.

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

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

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

- 3. (Optional) If there are unpublished configuration changes for the group, you can choose to publish the configuration changes to all target appliances before performing other scheduled tasks. To do this:
 - Click the **Actions** icon ([§]) for the appliance group you want to upgrade, and then click **Schedule Task**. The **Create Task** dialog appears.
 - In the **Create Task** dialog, for **Task Type**, select *Publish configuration*.
 - For **Scheduled Time**, select the start time for the task.
 - (Optional) Add **Comments** as required. These appear on the **Scheduled Tasks** list.
 - Click Save.

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

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

The **Create Task** dialog appears.

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

Note: If you scheduled a *Publish configuration* task for this group, you must leave sufficient time for that task to complete.

- (Optional) Add **Comments** as required. These appear on the **Scheduled Tasks** list.
- 6. Click Save.

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

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

The **Create Task** dialog appears.

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

Note: Ensure that you leave sufficient time for the *Stage a software package* task to complete.

- (Optional) Add **Comments** as required. These appear on the **Scheduled Tasks** list.
- 9. Click Save.

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

- 10. (Optional) You can edit the details for a scheduled task by clicking the **Edit** icon (\square) for the task.
- 11. (Optional) You can cancel a scheduled task by clicking the **Delete** icon for the task.

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

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

Viewing the Activities Log for an Appliance

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

To view the activities log for an appliance:

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

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

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

4. In the panel on the right, expand **Activities** to display details of all activities. For example:

000		I lse Se se one	cui	re*	DASHBOARD APPL	IANCES	ANALYTICS	ADMINISTRATION	· · · ·	
	Арр	liance	es	APPLIANCES	CONFIG GROUPS	SO	FTWARE	BACKUP-RESTORE SCHEDU		Q ARCH
Appliar	nces +	Add Applianc	e	Export					4 App	pliance
Name		Model		Last Config U Task Status	Pulse One Status	٢	🖨 Ade_	_Pulse-106 🔿	Actions	•
PES Ad	de_Pulse	SA5000-V	9	6d 42min	Connected	000		NCE INFO		<
PCS Ac	de_Pulse	PSA7000-V	9	6d 40min	Connected	000				<u> </u>
PPS PL	ulse-PPS-1	VA-SPE	9	6d 21hr 47min	Connected	000	ACTIVIT	IES		~
PPS PL	ulse-PPS-7	VA-SPE	9	6d 21hr 44min	Connected	000	_		Expo	ort
							Time	Activity		
							2019-01-16	13:58:42 ① Successfully uploade	ed backu 🝳	Î
						4	2019-01-16	13:58:41 ① Successfully uploade	ed backu 🝳	4
							2019-01-16	13:58:41 ① Created backup file	٩	
							2019-01-16	13:57:42 ① Successfully uploade	ed backu 🝳	
							2019-01-16	13:57:41 ① Successfully uploade	ed backu 🝳	
							2019-01-16	13:57:41 ① Created backup file	٩	
							2019-01-16	13:56:09 ① Task 358193ae-cd01	-4556-89 🔍	

Viewing the Configuration Change History for an Appliance

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

To view the configuration changes history:

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

The Appliances tab displays all current appliances.

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

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

FIGURE 118 View Configuration Changes

E SPulse Sec	cure [®] ^D	ASHBOARD APPLI	ANCES	ANALYTICS	ADMINISTRATION	چ settings admin	I
Appliance	S APPLIANCES C	ONFIG GROUPS	SO	FTWARE	BACKUP-RESTORE	SCHEDULED TASKS SEARCH	ł
Appliances + Add Appliance	Export					4 Applian	ices
Name Model	Last Config U Task Status	Pulse One Status	۲	🗁 Ade	_Pulse-109 🔿	Actions -	Î
Ade_Pulse PSA5000-V	9 6d 42min	Connected	000				5
Ade_Pulse PSA7000-V	9 6d 40min	Connected	000	APPLIA	NCE INFO	<	
PPS Pulse-PPS-1 VA-SPE	9 6d 21hr 47min	Connected	000	ACTIVI	TIES	<	
PPS Pulse-PPS-7 VA-SPE	9 6d 21hr 44min	Connected	000	CONFIG	GURATION HISTORY	\sim	
				2019-01-10	17:31:45 +0000		Y
				② Dash	board Settings (added)	R	
				Statu	s Settings (added)	θ	
			•	Ø Date	and Time (added)	e,	
				licen	sing Info (added)	e,	
				licen	sing Settings (added)	Q	
				Ø Pulse	One (added)	θ	
				🚳 SSL C	ptions (added)	e,	
				Ø Healt	h Check (added)	e,	
				Secur	ity Options (added)	Q	
				Ø Devic	e Certs (pulsesecure.net	added) 🔍	
				lo Auto-	Import (added)	C	L .

Comparing Appliances

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

To compare two appliances:

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

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

3. Select the source appliance that you want to compare and click its **Actions** icon (\square).

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

FIGURE 119 Compare Appliances

	JISE SE	cure		DASHBOARD	APPLIANCE	5 ANALY	TICS ADMINISTRATION		C C C C C C C C C C C C C C C C C C C
Арр	liance	s	APPLIANCES	CONFIG GF	ROUPS	oftware	BACKUP-RESTORE	SCHEDULED TASKS	Q
Appliances +	Add Appliance	Export	\mathbf{O}						4 Appliances
Name	Model	Last Con	nfig U Task Sta	itus Pulse One	Status 🔘	<u></u>	Ade_Pulse-109 🔿		Actions -
Ade_Pulse	PSA5000-V	9 6d 44mir	n	Connec	ted 🖁				
Ade_Pulse	PSA7000-V	9 6d 42mir	n	Connect	ted 🔋	AP	PLIANCE INFO		<
PPS Pulse-PPS-1	VA-SPE	9 6d 21hr	49min	Reboot Ap	ppliance	AC	TIVITIES		<
PP5 Pulse-PPS-7	VA-SPE	9 6d 21hr	46min	Edit Appli Launch Aj	ance Info ppliance Ul	СС	NFIGURATION HISTOR	Y	<
					Appliances onfiguration Software	•			

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

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

6. Select a setting. For example, *Pulse One (Modified)*.

In the **Results** pane, the **Base** text and **New** text highlight the differences in the two appliances for that setting. For example:

FIGURE 120 Appliance Configuration Comparison

Appliance Configuration Co	nparison	×
Differences Licensing Info (modified) Puise One (modified) Device Certs (* p1qa.com added) Network Overwiew (modified) Internal Port (modified) External Port (modified) Log > Verst (modified) Log > User (modified) Log > Admin (modified)	Ade_Pulse-109 Previous Configuration	Ade_Pulse-106 New Configuration Rew Configuration Configuration
Context Size 5		Close

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 ($\frac{1}{2}$).
- 4. On the drop-down menu, click **Reboot Appliance**.

FIGURE 121 Reboot Appliance

100	S Pulse	Secure			DA	SHBOARD AP	PLIANCES	ANALYTICS	ADMINIS	TRATION			Q admin
	Applian	ces		APPLIANCES	CONF	IG GROUPS	sc	IFTWARE	BACH	KUP-RESTORE	SCHEDULED TASKS		Q search
Appli	ances + Add App	liance Ex	port	Θ								4.	Appliances
Name		Model	Ver	Last Config U	Task Status	Pulse One Stat	us ©	🖨 Ade	_Pulse-1	109 🕂		Actio	ons 🗸
PLS	Ade_Pulse-106	PSA5000-V	9.0R	6d 17hr 45min		Connected	ê			•			
PLS	Ade_Pulse-109	PSA7000-V	9.0R	6d 17hr 42min		Connected	000	APPLIA	NCE INF	0			~
PP5	Pulse-PPS-1	VA-SPE	9.0R	7d 14hr 50min		Reboot Applia		2	ዯ	0 씨	7.54 🔿		
PP5	Pulse-PPS-7	VA-SPE	9.0R	7d 14hr 47min		Edit Appliance Launch Applia		Concurre	ent Users	Auth Failures (24H)	kb/s Throughput		
						Remove Applia Compare Appl			•				
						Backup Config Upgrade Softw Schedule Task	vare		% tilization	0% Memory Utilization	26% Disk Utilization		

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.**

	S Pulse PULSE ONE	Secure			DA	SHBOARD APPLIA	NCES	ANALYTICS ADMINI	STRATION			
	Applian	ces		APPLIANCES		IG GROUPS	SOF	TWARE BAC	KUP-RESTORE	SCHEDULED TASKS		Q SEARCH
Appli	ances + Add App	liance Ex	port	\mathbf{O}							4	Appliance
Name		Model	Ver	Last Config U	Task Status	Pulse One Status	٢	Ade_Pulse-	109 🕂		Actio	ons 🗸
PES	Ade_Pulse-106	PSA5000-V	9.0R	6d 17hr 45min		Connected	ê					
PES	Ade_Pulse-109	PSA7000-V	9.0R	6d 17hr 42min		Connected	000	APPLIANCE IN	=0			~
PP5	Pulse-PPS-1	VA-SPE	9.0R	7d 14hr 50min		Reboot Appliance		2 🔊	0 ዶ	7.54 🗅		
PP5	Pulse-PPS-7	VA-SPE	9.0R	7d 14hr 47min		Edit Appliance Info Launch Appliance U	Л	Concurrent Users	Auth Failures (24H)	kb/s Throughput		
						Remove Appliance Compare Appliance						
						Backup Configurati Upgrade Software Schedule Task		3% CPU Utilization	0% Memory Utilization	26% Disk Utilization		

FIGURE 122 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 133**.

Removing an Appliance from an Appliance Group

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

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

To remove an appliance from the group:

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

A list of configuration groups is displayed.

- 3. Select the group from which the appliance needs to be removed.
- 4. Select the Target Appliances tab.
- 5. Click the **Actions** icon ([‡]) for the appliance you want to remove.

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

FIGURE 123 Remove from Group

= \$	Pulse Secur	′e∗		DASHBOARD	APPLIANCES	ANALYTICS	ADMINISTRATION		
A	ppliances	/	APPLIANCES	CONFIG GR	OUPS	SOFTWARE	BACKUP-RESTORE	SCHEDULED TASKS	5
Appliance	Configuration Gro	oups	Create	e Appliance Group					
Name	Status		PCS-Grou	D ((i) Publi	sh Required)	Publish All	Publish Selected	Ac	tions -
PCS-Group	Publish Required (i)	904	Docs		sintequired)				
PPS-9.0R1-Group	Mismatch Ignored 🕐	000	Target Appliance	es Group Co	onfiguration				
pps-group	In Sync	000	+ Add Appliance						
			Status Nan	ne	Config State		Last Config Upload		۵
			• •	Ade_Pulse-109	Publish Requ	uired 🛈	6d 17hr 48min	View Changes	000
								Remove from gro	pup

An alert message confirms the removal of the appliance from the group.

Editing an Appliance Group

This section details the steps to modify an appliance group.

To edit an appliance group:

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

A list of configuration groups is displayed.

3. Select the group that you want to modify and click its **Actions** ($\frac{1}{2}$) icon.

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

FIGURE 124 Edit Group Configuration

BB	S Pulse Secure PULSE ONE	DASHBOARD APPLIANCES ANALYTICS ADMINISTRATION		
\geq	Appliances	APPLIANCES CONFIG GROUPS SOFTWARE BACKUP-RESTORE SCHEDULE	D TASKS	
Applian	ce Configuration Group	5 😯 (🖲 Create Appliance Group		
Name PCS-Group PPS-9.0R1-Gro pps-group	Status Publish Required ① 2 Edit group configuration 2 Delete group 3 Schedule Task 4 Upgrade Software 3	PCS-Group (① Publish Required) Publish All Publish Selected Docs Target Appliances Group Configuration Master appliance: Ade_Pulse-106 (In Sync) Edit master appliance configuration You can review changes to the master appliance that are part of the current groups publish configuration here. Config History (changes to be published)	Act	ians •
		2019-01-10 17:29:11 +0000		
		Dashboard Settings (added)		θ.
	4	Status Settings (added)		æ,
	Þ	Date and Time (added)		æ,
		SSL Options (added)		⊕,

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

FIGURE 125 Edit Appliance Group Wizard

Edit Appliance Group		
Group name and description	Group configuration settings	Summary
Group name and description		
Group name:	PCS-Group	
Description:	Docs	
DMI Information		
Username:	jeadmin.	
Password:	Password	
Port:	830	
Cancel		< Previous Next >

- 5. Work through the wizard, making the required changes to the group name, master appliance, and configuration settings.
- 6. Click Finish.

Deleting an Appliance Group

This section details the steps to delete an appliance group.

Note: The appliances within the appliance group are not deleted when you the delete the group, and can be viewed as normal in the **Appliances** tab.

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

A list of all configuration groups is displayed.

3. Click the group that you want to delete and click its **Actions** icon ($\frac{1}{2}$).

000	S Pulse Secure PULSE ONE	D.	ASHBOARD APPLIANCES	ANALYTICS A	DMINISTRATION	وک کې settings admin
\geq	Appliances	APPLIANCES	CONFIG GROUPS	SOFTWARE	BACKUP-RESTORE	SCHEDULED TASKS
Appliar	nce Configuration Grou	ps 🔿 🕀 Create.	Appliance Group			
Name PCS-Group	Status	PPS-9.0R1-	Group (⑦ Mismatcl	n Ignored) 🖓		Actions •
PPS-9.0R1-G	roup Mismatch Ignored	Target Appliances	Group Configuration			
pps-group	Delete group Schedule Task Upgrade Software	Status Name	Config State	Last Config L	J pload hr 3min	(View Changes)

FIGURE 126 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	97
•	Viewing the Appliance Health Report	98
•	Viewing the Profiled Devices Report	99
•	Viewing the Appliance Activities Report	101
•	Viewing the User Activities Report	102
•	Viewing Log Aggregation and Analysis	103
•	Viewing Appliance Activities	104

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 127 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:

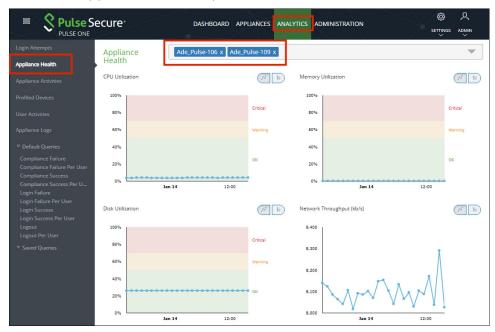
- 1. Select the **Analytics** menu.
- 2. Select **Appliance Health**.
- 3. From the **Appliance Health** drop-down, select one or more appliances for the report.

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 128 Appliance Health Report



Viewing the Profiled Devices Report

Pulse Secure Profiler dynamically identifies and classifies both managed and unmanaged endpoint devices, enabling control of access to networks and resources based on the type of the device.

The **Profiled Devices** report in Pulse One displays the list of devices that are discovered in the network.

To view profiled devices in Pulse One reports, a Pulse Policy Secure appliance must be registered in Pulse One and this Pulse Policy Secure appliance should have the Local Profiler Authentication server configured.

For details about configuring Local Profiler Authentication server in the Pulse Policy Secure appliance, refer to *Pulse Secure Profiler Deployment Guide*.

For details about registering the Pulse Policy Secure appliance, see **"Registering an Existing PCS/PPS Appliance" on page 21**.

To view **Profiled Devices** report:

1. Select Analytics > Profiled Devices.

The **Profiled Devices** page appears. This includes a table of devices and a **Device Details** area.

- 2. (Optional) Type a text entry (such as an IP address, a MAC address or a manufacturer name) into the **Filter** field and click **Apply**. The table updates to show entries that match that string.
- 3. (Optional) Select a **Collector Type** to filter the table based on the selected type and click **Apply**. The table updates to show entries that match that type: *DHCP, SNMP, NMAP, SSH, WMI, MDM, TRAP, USER AGENT*.
- 4. (Optional) Select the required number of **Records per page**. The default is 20.
- Select a device in the table to update the Device Detail category tabs at the bottom of the page: DHCP Details, SNMP Details, NMAP Details, User Agent, History, WMI Details, MDM Details and SSH Details.

Note: Some devices will not populate the **Device Details** tabs. These devices have been imported into a PPS appliance from another PPS appliance using the PPS GUI. See the *Pulse Policy Secure* documentation for details.

6. Click **Export** to download the details in a .csv format file.

FIGURE 129 Profiled Devices

😑 🞗 Pulse S	ecure	DASHB		PLIANCES	ANALYT	ICS AD	MINISTRAT		Ø	ዶ
PULSE ONE									SETTINGS A	
	Profiled De	evices								
	Filter	C	ollector Type:	Any	~	Apply	Clear		Ex	port
	Applian	MAC A	IP	Host Na	os	Са	Manuf	First Seen	Last Seen	
Profiled Devices	pps-171	68:f7:2	10	Shahee	Wi	Wi	LCFC(2017-11-2	2017-11-2	-
	pps-171	8c:70:5		KAJAL	Wi	Wi	Intel C	2017-11-2	2017-11-2	Ξ
	pps-171	00:50:5	10	appserver	Wi	Wi	VMwa	2017-12-0	2017-12-0	
	pps-171	0c:o4:7	10		PXE	Ne	Super	2017-11-2	2017-11-2]
	pps-171	0c:o4:7	10		PXE	Ne	Super	2017-11-2	2017-11-2	
	pps-171	00:50:5	10	gpratee	Wi	Wi	VMwa	2017-11-2	2017-11-2	-
	20 🗸	Records per page	Total records: 175			First P	revious 1	2 3 4 5	Next	
	Device Details Last									
Login Failure Per User DHCP Details SNMP Details NMAP Details User Agent History WMI Details WMI Details										
	Classified C	. Classifi	ed OS Re	equest	Combinat	. Mes	sage Type	Options	Vendor .	
	Network Boo.	. PXE	1	0.204	3547929	3		1,2,3,4,5,6,11,1.	PXECII.	

The above table is populated as endpoints join the network. It might take a few hours (to several days) for all the endpoints to be profiled.

Viewing the 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 130 Appliance Activities

	ecure®	DASHBOARD	APPLIANCES ANALYTICS	ADMINISTRATION	© A settings admin
Login Attempts	Appliance Activities	Critical ~	Export		<u>^</u>
Appliance Health	13 12 10	Informational			
Appliance Activities		Alert Notice			
Profiled Devices	0 Mon 17 Wed 19	Warning Error Emergency	Thu 27 Sat 29 Mon 31 2019	Thu 03 Sat 05 Men 07 Wed 09	Fri 11 jan 13
User Activities	Time	Debug			Target
Appliance Logs	2019-01-13T21:07:39Z	ा Virtual Appliance li	censed with 4 CPU cores, but or	ly provisioned with 2 CPU core(s)	Ade_Pulse-106
♥ Default Queries	2019-01-13T21:04:18Z	Ö Virtual Appliance li	censed with 8 CPU cores, but or	ly provisioned with 2 CPU core(s)	Ade_Pulse-109
Compliance Failure Compliance Failure Per User	2019-01-13T20:45:56Z	O Virtual Appliance li	censed with 8 CPU cores, but or	ly provisioned with 2 CPU core(s)	Pulse-PPS-1
Compliance Success Compliance Success Per U	2019-01-13T20:08:51Z	O Virtual Appliance lie	censed with 8 CPU cores, but or	ly provisioned with 2 CPU core(s)	Pulse-PPS-7
Login Failure Login Failure Per User	2019-01-12T21:07:18Z	O Virtual Appliance li	censed with 4 CPU cores, but or	nly provisioned with 2 CPU core(s)	Ade_Pulse-106
Login Success Login Success Per User	2019-01-12T21:03:56Z	O Virtual Appliance li	censed with 8 CPU cores, but or	nly provisioned with 2 CPU core(s)	Ade_Pulse-109
Logout	2019-01-12T20:45:33Z	O Virtual Appliance li	censed with 8 CPU cores, but or	nly provisioned with 2 CPU core(s)	Pulse-PPS-1
Logout Per User ▽ Saved Queries	2019-01-12T20:08:23Z	O' Virtual Appliance li	censed with 8 CPU cores, but or	nly provisioned with 2 CPU core(s)	Pulse-PPS-7
· Javed Quenes	2019-01-11T21:06:58Z	Ö Virtual Appliance lie	censed with 4 CPU cores, but or	nly provisioned with 2 CPU core(s)	Ade_Pulse-106

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

Viewing the User Activities Report

Pulse One administrators can aggregate user activities information as consolidated reports in Pulse One. This report provides the aggregated view of list of all users and their last login activities, compliance status, session length, appliance names, login success and failures.

- **Users Summary** table information of all the users such as username, last login time, last login IP and their session lengths. This list can be filtered by date range, username and realm.
- Selected User Sign-in Activities table information of selected user's authentication results, timestamps, authentication type, authentication mechanism, compliance information. The user details can be filtered by mac address, realm, compliance results, authentication mechanism and authentication results.

Note: PCS/PPS appliances with versions 9.0R1 or above must be registered with Pulse One to view user activity reports.

To view the **User Activities** report:

- 1. Select Analytics > User Activities.
- 2. Click a user to view the sessions details of that user in the Activities table.
- 3. Use the **View** drop-down to change the number of rows to be displayed.
- 4. Use the **Columns** drop-down to customize the columns to be displayed.
- 5. Use the filters to narrow down the search results.
- 6. Use the **Export** button to save the report in the .csv format.

If the device from which user performed sign-in was profiled by any registered PPS/Profiler in Pulse One, a hyperlink will be shown in MAC Address column. Upon clicking, it will take that device's profiler report.

Viewing Log Aggregation and Analysis

The syslog forwarded from the configured PCS/PPS appliances can be viewed in **Appliance Logs**. Here, users have a consolidated view of logs generated by every PPS/PCS appliance that is configured to forward syslogs to the Pulse One server.

FIGURE 131 Appliance Logs

	ecure			DA	SHBOARD APPLIA		LYTICS ADMINISTRATION
Login Attempts	Applia	nce Lo	gS Save Q	luery			1
Appliance Health	Match	ALL		_			From Dec 18, 2018 11:48:31 to Jan 17, 2019 11:48:31
Appliance Activities	Qs	earch					
Profiled Devices							tield Search
User Activities	Count By:	- 3	Select Field -	-	Group By:	Select F	
Appliance Logs							
♥ Default Queries	Priority	Facility	Time	Source	User	Event ID	Message
Compliance Failure Compliance Failure Per User Compliance Success	Major	local0	2019-01-17 11:48:07 +0000	10.64.26.47	System () []	SYS31126	Error generating data for chart cloud_secure_device_platform
Compliance Success Per U Login Failure Login Failure Per User	Major	local0	2019-01-17 11:48:07 +0000	10.64.26.47	System () []	SYS31126	Error generating data for chart cloud_secure_auth_result
Login Success Login Success Per User Logout Logout Per User	Major	local0	2019-01-17 11:48:07 +0000	10.64.26.47	System () []	SYS31126	Error generating data for chart cloud_secure_compliance
© Saved Queries mySavedQuery	Major	local0	2019-01-17 11:48:07 +0000	10.64.26.47	System () []	SYS31126	Error generating data for chart cloud_secure_os_type
	Major	local0	2019-01-17 11:48:07 +0000	10.64.26.47	System () []	SYS31126	Error generating data for chart cloud_secure_os_version

The system provides a set of **Default Queries** below the Appliance Logs menu in the navigation pane. Administrator can also customize the queries and save them for future use. These customized queries are listed below **Saved Queries**.

The **Appliance Logs** page allows searching by a string token by typing in the token in the search bar or doubleclicking a string in the logs details. The view is then filtered to display all messages with the token that is being searched for. Users can enter multiple tokens separated by space.

This customized query can then be saved using the **Save Query** feature.

Appliance Logs © Default Queries	Prior	Facility	Time	Source	User	Event ID	Message
Compliance Failure Compliance Failure Per User	Save	e Que	ry				ж
Compliance Success Compliance Success Per U Login Failure Login Failure Per User Login Success	Nam	e:	mySav	edQuery			
						(Cancel Save
Logout Per User Saved Queries mySavedQuery	Major	local0	2019-01- 14 17:27:56 +0000	10.64.26.47	System () []	SYS31126	Error generating data for

To view logs from any of the system default queries, expand **Default Queries** and click on the query.

To view logs from the customized queries, expand **Saved Queries** and click on the query.

It is also possible to filter the logs by timestamp. This can be done by choosing a **From date** and **To date** in the date fields on the top-right corner of the panel.

Users can also choose to filter search results by **Match All** (which will display search results that have all specified tokens) or **Match Any** (which will display search results that include any of the specified tokens).

The number of search results to be displayed on the screen can be 50, 100, 250, 500 by making a choice on the bottom left corner of the screen. Finally, the search results can span over multiple pages and navigated using the buttons on the bottom right corner of the screen.

Note: Only the saved queries can be deleted using the **Delete Query** feature.

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 133 Filter Activities

	ecure [®]	DASHBOARD APPLIANCES ANALYTICS ADMINISTRATIO	
User Management	Activities		
Role Management	Search	×)
Appliance Activities	Time	Activity	Appliance
	2019-01-09 20:17:44 +0000	 Rendering new configuration. 	Pulse-PPS-7 Q *
	2019-01-09 20:15:39 +0000	① Pending configuration has been created.	Pulse-PP5-7
	2019-01-09 20:15:38 +0000	① Rendering new configuration.	Pulse-PP5-7
	2019-01-09 20:13:44 +0000	\bigcirc Pending configuration has been created.	Pulse-PPS-7
	2019-01-09 20:13:43 +0000	① Rendering new configuration.	Pulse-PPS-7
	2019-01-09 20:07:00 +0000	\ddot{C} Virtual Appliance licensed with 8 CPU cores, but only provision	. Pulse-PPS-7

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

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

FIGURE 134 Activity Details

Activity Details	
Activity Created backup file 2019-01-16 13:57:41 +0000	
Severity informational 	
Activity Id d32d34dd915b98f31f709857f8b8ac48c438b9ca	
Actor security_appliance-67b64b92-d85d-439b-b12b-44272201eb44	
Target security_appliance-67b64b92-d85d-439b-b12b-44272201eb44	
Activity Type appliance_task	
Close	

User Management

•	Adding an Admin User	107
•	Editing User Details	108
•	Removing an Admin User	109
•	Resetting a User Password	109
•	Suspending a User	110

Adding an Admin User

To add an admin user:

1. Select the **Administration** tab.

FIGURE 135 Add Admin User

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.

Jsername:	po-user1	
Role	Read Only Admin	~
Full Name:	Pulse One User-1	
Email:	pouser1@company.com	
5ign In Method:	Enterprise SSO	~

Note: If Role is set to **Read Only Admin**, then the user will not be given the permissions to create/ update/ delete functions.

- 4. In the Add Admin User window, enter the **Username**, **Full Name** and **Email** for the user.
- 5. Select a **Role** from the drop-down list:
 - *Super Admin* This role has full access to the admin console. Super admin can create other admins.
 - *Read Only Admin* This role has read-only access to the entire system. Read-only admin can view dashboard and report, perform search function, and run pre-defined queries.

- 6. Select a Sign in Method. Either:
 - Select **Enterprise SSO** if the same user ID exists on both Pulse One (Service Provider) and the Pulse Connect Secure (Identity Provider), OR
 - Select Local Authentication.
- 7. Click **Create**. The new user is displayed in the list of users.

Editing User Details

To modify a user's details:

- 1. Select the **Administration** tab.
- 2. Select User Management.

A list of existing admin users is displayed.

- 3. Select the user from the list.
- 4. In the user details panel click the **Edit** icon and make the required changes.

5. Click Update.

FIGURE 136 Edit User Details

E SPULSE SO	ecure	DASHBOARD APPLIAN	ICES ANALYTICS ADMI	INISTRATION	SETTINGS ADMIN
User Management	Admin Users Q Search	Add	User Delete User	Э	2 Total Admin users
Role Management	User Role		Pulse One User-1		
Appliance Activities	admin Super Admin			rrify Group Activities 🛛 Edit Rese	t login Suspend User
	Pulse One Read Only Admir		Username:	po-user1	
			Full Name:	Pulse One User-1	
			Email:	pouser1@example.com	
			Role:	Read Only Admin	~
			Sign In Method:	Enterprise SSO	~
		•	Status:	Unlocked	
				Cancel Update	

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 137 Reset Login

E SPULSE SE	ecure	D	ASHBOARD	APPLIANCES	ANALYTICS	ADMINISTRATION	SETTINGS ADMIN
User Management	Admin User	'S Search	×	Add User	Delete User	Θ	2 Total Admin users
Role Management	User	Role		Pu	se One Use		
Appliance Activities	admin	Super Admin				Verify Group Activities	Z Edit Reset login Suspend User
	Pulse One	Read Only Admin			Username:	po-user1	
					Full Name:	Pulse One User-1	
					Email:	pouser1@example.	com
					Role:	Read Only Admin	
					Sign In Method:	Enterprise SSO	
				*	Status:	Unlocked	

Suspending a User

To suspend an admin user:

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

The user will be locked and will not be able to log in.

The Forgot Password option in the Login page will not send email to reset the password.

3. (Optional) To unlock the suspended user, select the user and click **Reset Login**. This will send a mail to the user with a set new password link.

E S Pulse S	ecure		DASHBOARD APPLIA	NCES ANALYTICS	ADMINISTRATION	BETTINGS ADMIN
User Management	Admin U	Sers Search	×	ld User Delete Us	er) 🕂	2 Total Admin users
	User	Role		Pulse One Us	ser-1	
Appliance Activities	admin	Super Admin			Verify Group Activities	Zedit Reset login Suspend User
	Pulse One	Read Only Admin		Username:	po-user1	
				Full Name:	Pulse One User-1	
				Email:	pouser1@examp	le.com
				Role:	Read Only Admin	
				Sign In Metho	d: Enterprise SSO	
				Status:	Unlocked	

FIGURE 138 Suspend User

Role Management

•	Adding an Admin Defined Role	111
•	Editing an Admin Role	112
•	Removing an Admin Role	112

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 139 Create New Role

Create New Role							
Role Name:	PO User1 Role						
Role Assignment							
Dashboard Settings		Read Only None	~				
Service Accounts		None	~				
Appliances		Delete	\sim				
Users		Delete	\sim				
▶ Roles		Read Only	~				
		Cancel	Create				

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 140 Modify Role

E S Pulse Se Pulse ONE	ecure	DASHBOARD APPLIAN	NCES ANALYTICS ADMINISTRATION	SETTINGS ADMIN
User Management	Role Management Add Role	e Delete Role		
Role Management	System Defined Roles	3 Roles	SysAdminRole	
Appliance Activities	Read Only Admin			
	Super Admin		Role Assignment	
	Workspace User		Dashboard	Read Only 🖌
			Settings	Read Only 💙
	Admin Defined Roles	1 Roles	Service Accounts	Read Only 🗸
	SysAdminRole	Duplicate	▶ Appliances	Read Only 💙
			Users	None 🗸
			▶ Roles	None 🗸
		4	Save	ancel

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	113
•	Editing Pulse One Properties	113
•	Understanding Pulse One Properties	114

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 141 Pulse One Properties

	ecure Dashboard appliances and workspaces analytics administration		ڑ SETTINGS	Q admin ♀
Pulse One Properties	Pulse One Properties Whitelist	Pulse One Properties		
Workspace Properties	Pulse One Properties	Workspace Propertie	s	
LDAP Groups		LDAP Groups Apple		llapse All
Apple	Name Value	CA Certificate		۲
CA Certificate	Enterprise Connections (5)	Android Enterprise Enterprise Usage Agr	eement	
Android Enterprise	E Password (9)	VPN Cert		
Enterprise Usage Agreement	• Misc (4)			
VPN Cert				

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** (\square button corresponding to the field you want to edit.
- 3. Change the value and then click **Save**. For example:

FIGURE 142 Edit Properties

Pulse Se Pulse One Pulse One Properties	Edit Property	SETTINGS ADMIN
ruse one rioperaes	Auto Configure SAML settings: Yes No	Expand All Collapse All
	(iancel Save
	Auto Configure SAML settings Yes	Ľ

Understanding Pulse One Properties

All Pulse One properties are described in the following sections:

- "Enterprise Connection Properties" on page 114
- "Password Properties" on page 114
- "Miscellaneous Properties" on page 115

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 130**.

- **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.

Configuring Enterprise SSO Using SAML

٠	Overview	117
•	Configuring SAML idP in Pulse Connect Secure Server	118
•	Automatically Configuring a SAML idP on Pulse One	122
•	Configuring a Metadata Provider in Pulse Connect Secure	124
•	Enabling Enterprise SSO in Pulse One Appliance	125
	Configuring SAML Metadata in Pulse One	
•	Adding SAML SP Metadata in Pulse Connect Secure Server	126
	Automatically Creating Pulse One Users for SAML SSO Logins	
	Testing Sign In with Enterprise SSO	

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 143 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 118.
- "Automatically Configuring a SAML idP on Pulse One" on page 122.
- (Optional) "Automatically Creating Pulse One Users for SAML SSO Logins" on page 130.
- "Testing Sign In with Enterprise SSO" on page 132.

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 118.
- "Configuring a Metadata Provider in Pulse Connect Secure" on page 124.
- "Enabling Enterprise SSO in Pulse One Appliance" on page 125.
- "Configuring SAML Metadata in Pulse One" on page 125.
- "Adding SAML SP Metadata in Pulse Connect Secure Server" on page 126.
- (Optional) "Automatically Creating Pulse One Users for SAML SSO Logins" on page 130.
- "Testing Sign In with Enterprise SSO" on page 132.

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 144	SAML	Settings
------------	------	----------

S Pulse Secure	Puise Connect Secure
	Authentication Administrators Users Maintenance Wizards
SAML> Settings Y Metadata Server Configuration	
Timeout value for metadata fetch request. 300 seconds	1 - 600. Specifies the time in seconds to wait for response of SAML metadata fetch request.
Validity of uploaded/downloaded metadata file: 0 days	0 - 9999. Specifies the time in days after which downloaded/uploaded metadata file expires. O means that Connect Secure doesnot 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.

5. Navigate to **System > Configuration > Certificates > Device Certificate**, create a new CSR, and import certificate and keys. Skip this step if the PCS external interface / internal interface (whichever is chosen) already provides a certificate that matches the host's Fully Qualified Domain Name.

Certificates > Device Certificate	System Authentication Ad	ministrators Users Maintenance W	/izards
- Certificates > Device Certificate			
tificate			
Pulse One Security SAML Mobile VP	Certificates DMI Agent IN Tunneling Telemetry Adva		Ise Collaboration Virtual Desktops
	na sua denomina de antes de la composición de la composicinde la composición de la composición de la c		
ares musted cirent CAs musted Sen	Ver CA's Code-signing Cerencates Chent Au	of Genericates Genericates Valurity Greek	
ficate issued to	Issued by	Valid Dates	Used by
psecure.net	posqalab-CA	Aug 30 06:06:04 2017 GMT to Aug 30 06:06:04 2019 GMT	<internal port=""></internal>
test.saqacertserv.com	EnterpriseSub2-CA	May 2 15:18:09 2016 GMT to Apr 9 17:22:15 2018 GMT 🛦	VP1, <external port=""></external>
0.30.	EXCHSRVCA	Oct 30 08:53:19 2017 GMT to Oct 30 08:53:19 2019 GMT	ext-AS-VP
	EXCHSRVCA	Oct 30 09:02:41 2017 GMT to Oct 30 09:02:41	
0.209.	Enteriorit	2019 GMT	
	SAML Mobile VP ates Trusted Client CAs Trusted Sen vice Certificate(s) If you don't have a cert ficate & Key. Delete records per page icate issued to secure.net est sagapertserv.com	SAML Mobile VPN Tunneling Telemetry Adva ates Trusted Client CAs Trusted Server CAs Code-signing Certificates Client Au vice Certificate(s) If you don't have a certificate yet, you can create a CSR and import the foote & Key. Delete Delete records per page issued by secure net progalab-CA est sagapertserv.com EnterpriseSub2-CA	SAML Mobile VPN Tunneling Telemetry Advanced Client Configuration ates Trusted Client CAs Trusted Server CAs Code signing Certificates Client Auth Certificates Valid Dates icate issued to Issued by Valid Dates Aug 30 06.06.04 2017 GMT to Aug 30 06.06.04 2017 GMT to Aug 30 06.06.04 2019 GMT Certificates Certi

FIGURE 145 Import Certificate and Keys

6. Navigate to Authentication > Signing In > Sign In SAML > Identity Provider.

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

FIGURE 146 Basic Identity Provider Configuration

	~					Puise Co	nnect Secure	
S Puls	e Secui	re _{System}	Authentication	Administrators	Users	Maintenance	Wizards	1
igning In								
Sign-in Policies	Sign-in Pages	Sign-in Notification	ns Sign-in SAML					
Metadata Provider	lentity Provider		•					
	vider (IdP) Configura	tion (Published in Me	stadata)					
Protocol Binding to us Post Artifact	te for SAML Response	•		at hu this IdP				
Protocol Binding to us	pulsesecure.net	Certificate to use for Certificate to use for	signing SAML messages ser decrypting the encrypted dat		by the Peer Se	arvice Provider (SP). This	s certificate is used by t	the peer SP to
Protocol Binding to us Post Artifact Signing Certificate: Decryption Certificate Other Configurations	pulsesecure.net	▼ Certificate to use for ▼ Certificate to use for ■ Certificate to use for encrypt the data in the If enabled, the user's disabled in Peer SP	signing SAML messages see decrypting the encrypted dat he SAML messages s existing NC (Pulse) session configuration.	a in SAML messages sent if any will be used in the S	P-initiated SSC			
Protocol Binding to us Post Artifact Signing Certificate: Decryption Certificate Other Configurations	pulsesecure.net No Encryption	Cerfficate to use for Cerfficate to use for encrypt the data in the If enabled, the user' disabled in Peer SP If both options are se	signing SAML messages ser decrypting the encrypted dat he SAML messages s existing NC (Pulse) session	if any will be used in the S "Reuse Existing NC (Puls	P-initiated SSC			
Protocol Binding to us Post Artifact Signing Certificate: Decryption Certificate Other Configurations Reuse Existing N	pulsesecure.net No Encryption IC (Pulse) Session AuthnRequest	Certificate to use for Certificate to use for encrypt the data in th If enabled, the user' disabled in Peer SP If both options are ss Individual SPs can c If enabled, SAML as	signing SAML messages set decrypting the encrypted dat he SAML messages s existing NC (Pulse) session configuration. elected, the priority is given to	ia in SAML messages sent if any will be used in the S "Reuse Existing NC (Puls thnRequest.	P-initiated SSC e) Session".) scenario, instead of aut	thenticating the user ag	jain. Can be
Protocol Binding to us Post Artifact Signing Certificate: Decryption Certificate Other Configurations Reuse Existing N Accept unsigned	pulsesecure.net No Encryption IC (Pulse) Session AuthnRequest	Cerfficate to use for Cerfficate to use for Cerfficate to use for disabled in Peer SP If both options are set Individual SPs can c If enabled, SAML as assertion.	signing SAML messages see decrypting the encrypted dat he SAML messages s existing NC (Pulse) session configuration. dected, the priority is given to hoose to accept unsigned Au	in SAML messages sent if any will be used in the S o "Reuse Existing NC (Puls thn Request. ong with signing the SAML	P-initiated SSC e) Session". response by de) scenario, instead of aut afault.Individual SPs can	thenticating the user ag	jain. Can be

- 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: Only the **Post** protocol is supported in this release. **Artifact** is not supported.

- 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 117**.

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 118.

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 147 Pulse One Properties Enterprise Connections

Pulse One Properties	
Name	Value
🗆 Enterprise Connections (5)	
Auto Configure SAML settings	No
Create users and set roles from SAML	No
SAML Identity Provider	
SAML Identity Provider Metadata	
SAML Service Provider Metadata	
Password (9)	
⊞ Misc (4)	

5. Set the Auto Configure SAML Properties property to Yes.

Note: When you set **Auto Configure SAML Properties** to *Yes*, the **SAML Identity Provider Metadata** and the **SAML Service Provider Metadata** properties are removed. These are not required when auto-configuration is enabled.

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

ulse 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
E Password (9)	
∃ Misc (4)	

FIGURE 148 Pulse One Properties Configure Auto SAML

Once 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*.

FIGURE 149 Pulse Connect Secure SAML Auto-configuration

	~						Pulse Connect Secur	
S Put	se Secure	System Authentication	Administrators U	sers N	Maintenance Wiza	ards		1
	tion							
Licensing	Pulse One Security	Certificates DMI Agent Tunneling Telemetry	NCP Sensor	rs C	Client Types Pulse	Collaboration Virtual Des	User Record Synchronization	
New Metadata Pi	ovider Delete Refres	n Settings						
New Metadata Pr 10 - rec	ovider Delete Refres	Settings					Search:	
	ords per page	n Settings		Roles	Valid Till	Status	Search: Metadata Location	Download
10 • rec	ords per page	n Settings		Roles	Valid Till 2038-01-18 19:14:07	Status		Download +

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 130.
- Move directly to testing the SSO login, see "Testing Sign In with Enterprise SSO" on page 132.

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 122**.

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 150 Metadata Provider

Pulse Connect Secure								
S Pulse	Secur	°e _{System}	Authentication	Administrators	Users	Maintenance	Wizards	1.
Signing In								
Sign-in Policies	Sign-in Pages	Sign-in Notification	s Sign-in SAML					
Metadata Provider Ident	ity Provider							
This is configuration of Pul	lse Connect Secure	(SA) SAML Metadata	provider.					
*Entity Id:			Unique SAML identifier	of the Connect Secure. By	default uses ho	ost name configured at S.	AML Settings.	
*Metadata Validity:	365 days		1 - 9999. Specifies the I	maximum duration for which	h a peer SAML	entity can cache the Cor	nect Secure metad	ata file.
Do Not Publish IdP in Download Metadata Save Metadata Provi			Prevents the Connect S	ecure metadata file to be p	ublished at the	location specified by the	Entity Id.	

Enabling Enterprise SSO in Pulse One Appliance

Note: You do not have to perform the process in the section if your appliance is at v8.3r1 or later, and you have already performed auto-configuration of SAML, see **"Automatically Configuring a SAML idP on Pulse One" on page 122**.

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 151 Sign In Method

Username:	po-user1	
Role	Read Only Admin	~
Full Name:	Pulse One User-1	
Email:	pouser1@company.com	
Sign In Method:	Enterprise SSO	~

Note: To use Enterprise SSO login, the same user identity (username) must exist on both Pulse One (Service Provider) and the Identity Provider (Pulse Connect Secure).

Configuring SAML Metadata in Pulse One

Note: You do not have to perform the process in the section if your appliance is at v8.3r1 or later, and you have already performed auto-configuration of SAML, see **"Automatically Configuring a SAML idP on Pulse One" on page 122**.

To configure metadata in Pulse One:

- 1. In the Pulse One admin console, click the settings icon on top-right-corner of the page and select **Pulse One Properties**.
- 2. Click the **Edit** icon corresponding to **SAML Identity Provider** and select the Pulse Connect Secure appliance that you are setting up as the Identity Provider.
- 3. Click the Edit icon corresponding to SAML Identity Provider Metadata.

- 4. Copy the contents of the metadata file that you downloaded from Pulse Connect Secure, paste it into the **Edit Property** window, and click **Save**. The **SAML Service Provider Metadata** will automatically be populated.
- 5. Click **SAML Service Provider Metadata**, copy the metadata content, paste it into a file such as *saml-metadata-pws.xml* and save the file to your computer. This file will be used when configuring Pulse Connect Secure later.

	se Secure de	DASHBOARD APPLIANCES A	ANALYTICS ADMINISTRATION	Settings admin
Pulse One Properties	Pulse One Properties			Expand All Collapse All
	Name	Value		0
	Enterprise Connections (5)			
	Auto Configure SAML settings	No		Z
	Create users and set roles from SAML	No	2	Z
	SAML Identity Provider			
	SAML Identity Provider Metadata	and institutions	per antiscindi "art andictorinectic Stati, 2.2 mm	
	SAML Service Provider Metadata	and instructions	yor attinued for automatic line, 20mm	aley' achicyator-1981,
	⊕ Password (9)			

FIGURE 152 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 122**.

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

- 1. Navigate to System > Configuration > SAML.
- 2. Click New Metadata Provider.
- 3. Enter a Name for the metadata provider.

- 4. Under Metadata Provider Location Configuration:
 - For Location, select Local.
 - For **Upload Metadata File**, click **Browse** and select the SP metadata file *saml-metadata-pws.xml* that you saved on your computer in the previous process.

FIGURE 153 Metadata Provider Location Configuration

0	~					Pu	ise Connect Secur	•
S Pulse	Secure	System	Authentication	Administrators	Users	Maintenance	Wizards	1~
^{SAML>} New Metadata Pr	ovider		-					
Name:	Label to reference me	etadata provider.						
Ƴ Metadata Provider I	Location Configuration							
Location:	🖲 Local 🔵 Remote	Location of metada	ta provider. In case of Loca	l, metadata file needs to be	uploaded by a	dmin. In case of Remote	Location, metadata file is f	etched by Connect
Upload Metadata File:	Browse No file chosen Current File: None	occure none die co						
♥ Metadata Provider V	Verification Configuration	n	4					
Accept Unsigned N	letadata	If checked Conr	iect Secure accepts unsign	ed 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 154 Service Provider

✓ Metadata Provider Filter Configuration

Roles:	📄 Identity Provider 🗹 Service Provider 📄 Policy Decision F	PointRoles which Connect Secure looks for in the metadata file. List of enfly ids to be imported. (one per line). If left empty all enfly ids in the file are imported.
Entity Ids to import:		
Save Changes Ca	ancel	

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

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

FIGURE 155	SAML Identity Provider					
♥ Configuration	✓ Configuration					
	vviders' are SP's known to this IdP Delete SP					
	Peer Service Provider	Override Default Configuration	Configuration Mode	Manual Certificate Selection		

The New Peer Service Provider page appears.

10. In the **Service Provider Configuration** and **Certificate Status Checking Configuration** sections, make the necessary service provider specific settings. For more details, refer to the "Configuring Sign-in SAML Identity Provider Settings" section in the *Pulse Connect Secure Administration Guide*.

FIGURE 156 New Peer Service Provider

Pulse Connect Secure							
S Pulse Secure							.
Sy	/stem	Authentication	Administrators	Users	Maintenance	Wizards	
Signing In > New Peer Service Provider							
New Peer Service Provider							
*Configuration Mode: O Manual 🖲 Metadata _{if metadata}	is selected	, uses metadata files uploade	ed/added at Peer SAML Me	adata Provider	'S.		
♥ Service Provider Configuration.							
*Entity Id: Unique SAML Identifier	of the SP.						
Select certificates manually							
♥ Certificate Status Checking Configuration							
Enable signature verification certificate status chec	king Check	this to enable revocation che	ecks for the signing certificat	e. (Uses config	juration in Trusted Client	CAs.)	
Enable encryption certificate status checking		this to enable revocation che					
← Customize IdP Behavior							
Override Default Configuration							
Save Changes Cancel							
"indicates required field							

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

13. Select the Accept unsigned AuthnRequest check box.

FIGURE 157 Customize IdP Behavior

✓ Customize IdP	Behavior	
🖉 Override 🛙	Default Configuration	
Reuse Exist	ing 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 unsi	gned AuthnRequest	n uun upnuns are selected, me phung is given tui neuse Existing inc (Fuise) sessiun .
Sign SAML.	Assertion	If enabled, SAML assertion will also be signed along with signing the SAML response by default.
*Signature	Sha-1	Algorithm that needs to be used for generating signature for SAML assertion and response
Algorithm	🔘 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	Suggested maximum duration of the session at the SP created due to SAML SSO.
	Role Based	
	Customize	
* SignIn Policy:	No SP-initiated SSO 🔻	The SignIn Policy used by this IdP to authenticate the user in SP-initiated SSO scenario.
* Force	Reject Authn Request	SA behavior if SP sends an authentication request with ForceAuthn set to true for a user with valid browser session. Prevails over
Authentication	 Re-Authenticate User 	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
Behavior:	Ignore Re-Authentication for User	
User Identity		
_ Subject Name Format:	DN •	Format of 'Nameldentifier' field in generated Assertion.
* Subject Name:	uid= <username></username>	Template for generating user's identity as sent in 'Nameldentifier' field.
Attribute Statem	ent Configuration	
🗹 Send Attribu	ite Statements	If checked, Attribute statements will be sent for the SP.
Use IdP Def	fined Attributes	
🔵 Customize I	dP Defined Attributes	
Save Chang		

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 130.
- Move directly to testing the SSO login, see "Testing Sign In with Enterprise SSO" on page 132.

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 admindefined role. For example:

FIGURE 158 PCS User Roles

User Roles > Pulse One: SAML Role1 > General Overview	[>	
General Web Files SAM Tel Overview Restrictions VLAN/Source IP	net/SSH Terminal Services	Virtual Desk
* Name: Description:	Pulse One: SAML Role1	
	Save Changes	

In this example, there must be a role called SAML Role1 on Pulse One.

- 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 159 Attribute Statement Configuration

Attribute Statement Configurat	tion			
Attributes to be sent in SA	ML Attribute Statements can I	be configured as name-value p	airs and/or to be fetche	ed from a Directory ser
Name-Value based configu	uration here values can be sw	stem variables available in SSO) parameter fields:	
vame-value based configu	iration, here values can be sy	stem variables available in SSC	parameter neids:	
Delete				
Attribute Name	Friendly Name	Attribute Value	Value Type	
			Single-Valued 📀	Add
roles		<role sep=","></role>	Single-Valued ᅌ	Add

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 160 Pulse One Properties Enterprise Connections

	e Secure' dashboar	RD APPLIANCES ANALYT	ICS ADMINISTRATION		MIN
Pulse One Properties	Pulse One Properties		Ex	band All Collaps	se All
	Name	Value			0
	Enterprise Connections (3)				
	Auto Configure SAML settings	Yes			Z
	Create users and set roles from SAN	IL Yes			
	SAML Identity Provider				Z
	+ Password (9)				
	⊞ Misc (4)				

- 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 161 Pulse One Admin Defined Roles

CUTE DASHBOARD APPLIANCES ANALYTICS ADMINISTRATION	
Role Management Add Role Delete Role	
System Defined Roles	3 Roles
Read Only Admin Super Admin Workspace User	
Admin Defined Roles SAML Role1	1 Roles Duplicate
	Role Management Add Role Delete Role System Defined Roles Read Only Admin Super Admin Workspace User

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 162 Pulse One Properties

		se Secure*		
We	lcome t	o Pulse O	ne!	
	Q Username			
	Forgot password?	Sign In Sign In with Enterprise SSO		

You are navigated to the Pulse Connect Secure login page.

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

FIGURE 163 Pulse Connect Secure Login Page

Secure Secure		
Welcome Pulse C	to onnect Secure	
Username Password		Please sign in to begin your secure session.
	Sign In	

 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: resource-policies/web-policies/ptp[application=ptp_policy_ 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=PP5_PCS_Combo]/connections/connection [name=L2_Connection_WIRED]/trusted-servers/trusted- server[dn=ANY,ca=PMDRoorCA]/ca] Invalid reference: no 'Trusted Server CA' object found with identifier 'PMDRootCA'.	Configure the appropriate Trusted Server CA' under System > Configuration > Certificates > Trusted Server Cas, by importing the Trusted Server CA'.
(PPS) Auth > Realms > Users	Endpoint Policy > Network Access > Radius Attributes	Import of configuration from Pulse One returned an Error:[/users/ user-realms/realm[name=TestRealm1]/authentication-policy/radius- request-attributes-policies/selected-policies] Invalid reference: no 'RADIUS Request Attributes Policy' object found with identifier '2 nd Request Policy'.	Configure the appropriate 'RADIUS Request Attributes Policy' under Endpoint Policy > Network Access > Radius Attributes.