

# Pulse One Appliance Administration Guide

Supporting Pulse One Appliance 2.0.2004.1

Product Release2.0.2004.1Published12 May 2021Document Version1.0

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

#### https://www.pulsesecure.net

© 2021 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 <a href="http://www.pulsesecure.net/support/eula">http://www.pulsesecure.net/support/eula</a>. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

# Contents

PREFACE
Document Conventions1
Text Formatting Conventions1
Command Syntax Conventions1
Notes and Warnings
Requesting Technical Support
Self-Help Online Tools and Resources
Opening a Case with PSGSC
Reporting Documentation Issues
GETTING STARTED WITH PULSE ONE
Overview of Pulse One
Logging Into Pulse One
Understanding Cluster/Node Status Summary
Example: Typical Node Lifecycle10
Changing the User Password11
Adding Pulse One Licenses
Whitelisting IP Addresses for Admin Login12
Whitelisting Countries for Admin Login14
Setting a Session Timeout Threshold17
WORKING WITH THE PULSE ONE DASHBOARD
VIEWING OVERALL SYSTEM HEALTH
Viewing Profiled Devices
VIEWING USER ACTIVITIES
VIEWING UEBA METRICS
VIEWING CLOUD SECURE STATISTICS
Customizing Dashboards and Widgets26
Adding a New Widget
Editing the Dashboard Layout29
Editing Widget Configuration
Controlling Widget Presentation
Exporting Dashboard Information
APPLIANCE MANAGEMENT
Registering an Existing PCS/PPS Appliance
Editing Appliance Information

LAUNCHING THE USER INTERFACE FOR AN APPLIANCE	38
Recognizing Critical Vulnerabilities	39
CONFIGURING AN APPLIANCE TO CONNECT TO PULSE ONE	40
COMPLETING REGISTRATION OF AN APPLIANCE	40
Configuring Log Settings on the Appliance	41
Configuring ActiveSync Handler	43
CREATING AND REGISTERING A PCS APPLIANCE VM ON VSPHERE	
Creating an Appliance Master Template on vSphere	51
CREATING AND REGISTERING A PCS APPLIANCE VM ON AWS	
Identifying the Required Route 53 Zones	
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 UTILIZATION	
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 Groups	
CREATING AN APPLIANCE GROUP	
Adding Appliances to an Appliance Group	
DISTRIBUTING A MASTER CONFIGURATION	
Upgrading Managed Appliances	
UPLOADING AN APPLIANCE SOFTWARE PACKAGE TO PULSE ONE	
Upgrading Software on an Appliance	
Upgrading Software on all Target Appliances in a Group	
Upgrading Software on all Appliances in a Cluster	
Scheduling Upgrade-Related Tasks	
UPLOADING AN ENDPOINT SECURITY ASSESSMENT PLUG-IN PACKAGE	
DOWNLOADING AN ESAP PACKAGE.	
UPLOADING AN ESAP PACKAGE TO PULSE ONE	
UPLOADING ESAP PACKAGES ONTO APPLIANCES AND APPLIANCE GROUPS	
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	115

Editing an Appliance Group	
Deleting an Appliance Group	
VIEWING THE LOGIN ATTEMPTS REPORT.	
VIEWING THE APPLIANCE HEALTH REPORT	
VIEWING THE PROFILED DEVICES REPORT	
VIEWING THE USER ACTIVITIES REPORT.	
VIEWING THE UEBA ANALYTICS REPORTS	
VIEWING LOG AGGREGATION AND ANALYSIS	
Working with Log Queries	
Viewing Services Logs	
USER MANAGEMENT	131
Adding an Admin User	
Editing User Details	
Removing an Admin User	
Resetting a User Password	
Suspending a User.	
ROLE MANAGEMENT	
Adding an Admin Defined Role	
Editing an Admin Role	
Removing an Admin Role	
WORKING WITH PULSE ONE PROPERTIES	
VIEWING PULSE ONE PROPERTIES	
Editing Pulse One Properties	
Understanding Pulse One Properties	
ENTERPRISE CONNECTION PROPERTIES	
Password Properties	
Miscellaneous Properties	
Session Properties	
CONFIGURING ENTERPRISE SSO USING SAML	
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 .	

JABLING ENTERPRISE SSO IN PULSE ONE APPLIANCE	149
DNFIGURING SAML METADATA IN PULSE ONE	149
DDING SAML SP METADATA IN PULSE CONNECT SECURE SERVER	150
JTOMATICALLY CREATING PULSE ONE USERS FOR SAML SSO LOGINS	154
STING SIGN IN WITH ENTERPRISE SSO	156
X: CHECKLIST FOR PREPARING A TARGET APPLIANCE	157

# Preface

•	Document Conventions	1
•	Requesting Technical Support	2
•	Reporting Documentation Issues	3

## **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
{ <b>x</b>   <b>y</b>   <b>z</b> }	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.
bold text	Identifies command names, keywords, and command options.

#### **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/productservice-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/

## **Reporting Documentation Issues**

To report any errors or inaccuracies in Pulse Secure technical documentation, or to make suggestions for future improvement, please send your comments to: techpubs-comments@pulsesecure.net. Include a full description of your issue or suggestion and the document(s) to which it relates.

# Getting Started With Pulse One

•	Overview of Bules One	E
•	Overview of Pulse One	. ว
•	Logging Into Pulse One	. 6
•	Understanding Cluster/Node Status Summary	. 9
•	Changing the User Password	11
•	Adding Pulse One Licenses	12
•	Whitelisting IP Addresses for Admin Login	12
•	Whitelisting Countries for Admin Login	14
•	Setting a Session Timeout Threshold	17

# **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.

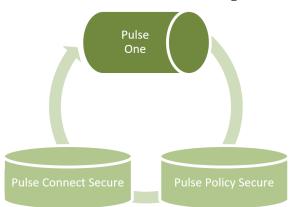


FIGURE 1 Pulse One Unified Management

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. ESAP updates to appliances are also supported.
- **Centralized administration** Collectively administers multiple appliances without logging into them on a box-by-box basis.

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

## Logging Into Pulse One

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

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

- If you are an existing user, enter the user name and password. Click **Sign In** to log in to Pulse One.
- If Enterprise SSO is configured for your user ID, then click **Sign In with Enterprise SSO**. For details about the Enterprise SSO configuration, see **"Enterprise Connection Properties" on page 138**.

Wel	Secure Access	se Secure or the next generation OPUISE C	)ne!	
	Q. Username			
	Password	ign In		
	Forgot password?	Sign In with Enterprise SSO		

FIGURE 2 Pulse One Login Page

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

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

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

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

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

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

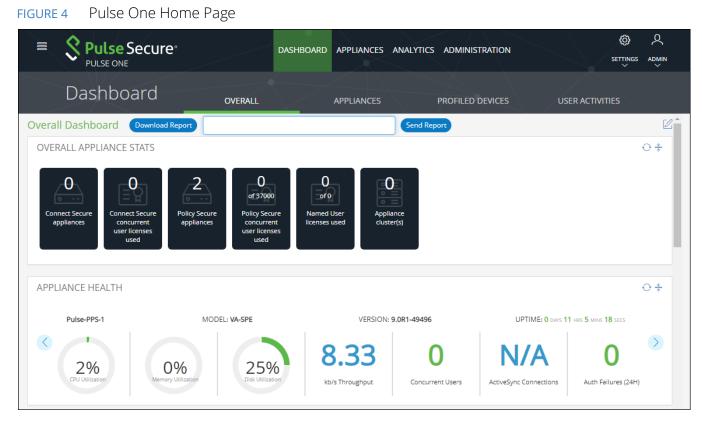
FIGURE 3 Pulse One Welcome Wizard

	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!	
<ul> <li>New dashboard</li> </ul>	widgets are available to add	to your dashboards. These includ	le:
App Visit     Appliance     Go to the new A	Health		>
	•	• • •	
Don't show this to me again			START NOW

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:



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

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

## **Understanding Cluster/Node Status Summary**

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

FIGURE 5 Cluster Status Summary

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

The summary statuses are included:

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

This state indicates that some intervention is required to return the cluster status to Up.

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

Note: After a clustered pair has been formed, the name of the Active node is displayed in brackets.

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

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

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

FIGURE 6 Cluster Status Summary: Unknown

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

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

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

### Example: Typical Node Lifecycle

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

FIGURE 7 Cluster Status Summary: New Node

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

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

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

The following summary status appears:

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

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

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

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

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

FIGURE 9 Cluster Status Summary: Single Node Now Active

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

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

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

FIGURE 10 Cluster Status Summary: Active/Passive Cluster Formed

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

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

After this process completes, the following summary statuses appear:

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

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

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

If either node in an Active/Passive cluster fails:

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

The following summary statuses appear:

FIGURE 12 Cluster Status Summary: After Auto Failover

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

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

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

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

FIGURE 13 Cluster Status Summary: Re-Formed Cluster

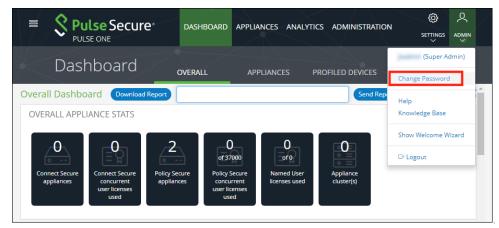
CLUSTER STATUS: • UP NODE STATUS: ACTIVE (BRASS) AUTO FAILOVER: ENABLED

## Changing the User Password

To change the user password:

- 1. Click the **User** icon on the top-right corner of the page.
- 2. From the menu, click Change Password to change your login password.

FIGURE 14 Change Password



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

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

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

# Adding Pulse One Licenses

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

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

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

# Whitelisting IP Addresses for Admin Login

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

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

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

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

To whitelist IP addresses/ranges:

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

The Pulse One Properties page appears.

FIGURE 15 Pulse One Properties
--------------------------------

	ecure	DASHBOARD	APPLIANCES A	AA WORKSPACES	ANALYTICS	ADMINISTRATION		ڑی settings	
Pulse One Properties	Pulse One Properties	Whitelist					Pulse One Properties		
Workspace Properties	Pulse One Proper	ties					Workspace Propertie		llapse All
Apple	Name		Value				Apple CA Certificate Android Enterprise		٢
CA Certificate	Enterprise Connections	s (5)					Enterprise Usage Agr	eement	
Android Enterprise	Password (9)						VPN Cert		
Enterprise Usage Agreement									
VPN Cert	Ession (1)								

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

#### FIGURE 16 Add to Whitelist Page

	CURE DASHBOARD APPLIANCES WORKSPACES ANALYTICS ADMINISTRATION	الله کې
Pulse One Properties	Pulse One Properties Whitelist	
Workspace Properties	IP WHITELIST	$\sim$
LDAP Groups	Add to Whitelist	
Apple	192.186.12.1/11	•
CA Certificate	Please add an ipv4 / ipv6 address in the above text box	
Android Enterprise	IPV4 or IPV6 Address	
Enterprise Usage Agreement	No data to display	
VPN Cert	0 total	
	COUNTRY WHITELIST	<

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

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

#### FIGURE 17 First Whitelist Entry

se One Properties	Whitelist		
WHITELIST			
ld to Whitelist			_
92.186.12.1/11			Ð
ase add an ipv4 / ipv6	address in the	ve text box	
IPV4 or IPV6 Addre	55	۵	
172.22.15.0/24	1	Ê	

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

#### FIGURE 18 Additional Whitelist Entries

d to Whitelist		
2.186.12.1/11		
e add an ipv4 / ipv6 address in the above text box		
IPV4 or IPV6 Address		
172.22.15.0/24	ŧ.	
135.0.0.0/8	Ê	
172.55.0.0/16	Ê	
3 total		

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

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

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

## Whitelisting Countries for Admin Login

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

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

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

Before you can use the country whitelist, you must install the latest location database package. To obtain this file, contact Pulse Secure Technical Support.

Note: For additional information, please refer to Knowledge Base article KB44538.

**Note:** Pulse Secure advises you to always use the latest version of the location database package. The package is updated regularly, and must be replaced every 30 days. The package can be obtained from Pulse Secure Technical Support. If you upload a new package, your current whitelist settings are preserved.

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

To whitelist countries:

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

The **Pulse One Properties** page appears.

FIGURE 19 Pulse One Properties

	ecure <sup>,</sup>	DASHBOARD	APPLIANCES AAA	WORKSPACES AN	IALYTICS	ADMINISTRATION			
Pulse One Properties	Pulse One Properties	Whitelist					Pulse One Properties	5	
Workspace Properties	Pulse One Propert	ies					Workspace Propertie LDAP Groups	25	llapse All
Apple	Name		Value				Apple CA Certificate Android Enterprise		۲
CA Certificate	Enterprise Connections	(5)					Enterprise Usage Ag	reement	
Android Enterprise	Password (9)						VPN Cert		
Enterprise Usage Agreement	+ Misc (4)								
VPN Cert									

- 4. Click the Whitelist tab to view the Add to Whitelist page.
- 5. Click Country Whitelist.

FIGURE 20 Upload Location Database Package

	CUTE DASHBOARD APPLIANCES WORKSPACES ANALYTICS ADMINISTRATION	SETTINGS ADMIN
Pulse One Properties	Pulse One Properties Whitelist	
Workspace Properties	IP WHITELIST	<
LDAP Groups	COUNTRY WHITELIST	$\sim$
Apple		
CA Certificate	Location Database not found.	
Android Enterprise	Please download it from Pulse Support website and upload here in order to use Country Whitelist functionality.	
Enterprise Usage Agreement	SHA256 Hash:	
VPN Cert	Choose File No file chosen	

- 6. Click **Choose File** and locate the required location database package.
- 7. Enter the SHA256 Hash for the selected file.

#### 8. Click Upload.

The page updates to show the uploaded country whitelist.

FIGURE 21	Add to	Whitelist	Page
-----------	--------	-----------	------

😑 🕺 Pulse Se		DASHBOA		WORKSPACES		ADMINISTRATION	ø	ዾ
PULSE ONE		DASIIBOA	RD AFFLIANCES	WORKSPACES	ANALTICS	ADMINISTRATION		
Pulse One Properties	Pulse One Properties	Whitelist						
Workspace Properties	IP WHITELIST							<
LDAP Groups	COUNTRY WHITEL	IST						$\sim$
Apple			Countries			Whitelisted Countries		
CA Certificate			Lountries					
Android Enterprise		Filter				Filter		
		Afghanist	an, AF	A.				
Enterprise Usage Agreement		Albania, A	L					
VPN Cert		Algeria, D	2					
		American	Samoa, AS					
		Andorra, A	D					
		Angola, A	)					
		Anguilla, A	d					
		Antarctica	, AQ					
		Antigua a	nd Barbuda, AG					
		Argentina	AR					
		Armenia,	AM	•				

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

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

FIGURE 22	First Whitelist Entry
-----------	-----------------------

•	Pulse One Properties	Whitelist			
	IP WHITELIST				<
	COUNTRY WHITEL	IST			$\sim$
		Countries		Whitelisted Countries	
		Filter		Filter	_
		Turkmenistan, Twi	*	United Kingdom, GB	1
		Turks and Caicos Islands, TC			1
		Tuvalu, TV			

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

FIGURE 23 Additional Whitelist Entries
--

Countries		Whitelisted Countries
Filter		Filter
Gambia, GM	<b>A</b>	France, FR
Georgia, GE		Germany, DE
Ghana, GH		India, IN
Gibraltar, GI		Italy, IT
Greece, GR		United Kingdom, GB
Greenland, GL		United States, US
Grenada, GD		
Guadeloupe, GP		
Guam, GU		
Guatemala, GT		
Guinea, GN	•	

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

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

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

## Setting a Session Timeout Threshold

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

To set a session timeout threshold:

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

3. Select Pulse One Properties.

The **Pulse One Properties** page appears.

FIGURE 24	Pulse One Properties
-----------	----------------------

= 🞗 Pulse S	ecure <sup>®</sup>	DASHBOARD APPLIAN	ices aaa workspaces	ANALYTICS	ADMINISTRATION		ø	ዶ
PULSE ONE				$\mathbf{X}_{-}$	$\langle \rangle$	$\sim$		
Pulse One Properties	Pulse One Properties Whitelis	it .				Pulse One Properties		
Workspace Properties	Pulse One Properties					Workspace Propertie	s	
LDAP Groups						LDAP Groups Apple		llapse All
Apple	Name	v	/alue			CA Certificate		0
CA Certificate	<ul> <li>Enterprise Connections (5)</li> </ul>					Android Enterprise Enterprise Usage Agr	eement	
Android Enterprise	Password (9)					VPN Cert		
Enterprise Usage Agreement								
VPN Cert								

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

**Note:** The default setting is 20.

6. **Save** the new setting.

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

# Working with the Pulse One Dashboard

•	Viewing Overall System Health	19
•	Viewing Profiled Devices	20
•	Viewing User Activities	21
•	Viewing UEBA Metrics	23
•	Viewing Cloud Secure Statistics	24
•	Customizing Dashboards and Widgets	26
•	Exporting Dashboard Information	33

# **Viewing Overall System Health**

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

FIGURE 25 Overall System Health Dashboard

	DA	SHBOARD APPLIANCES WORKSPA	CES ANALYTICS ADMINIS	TRATION		Q admin
Dashboard	OVERALL PROFILE	D DEVICES USER ACTIVITIE	S CLOUD SECURE			
Overall Dashboard Download Report		Send Report				Z
OVERALL STATS						0 <b>‡</b>
Connect Secure Connect Secure Policy	2 Secure ances Belicy Secure concurrent used Concurrent Remses used Concurrent Remses used	Applance cluster(s)				
APPLIANCE HEALTH						⊖ *
cliff_204	MODEL: PSA5000-V	VERSION: 9.	R4.1-4968	UPTIME: 25 DAYS 22 H	irs <b>3</b> mins <b>49</b> secs	
5% CPU Unitation	0% Memory Utilization	0.31 kb/s Throughput	O Concurrent Users	O ActiveSync Connections	O Auth Failures (24H)	>
CRITICAL EVENTS	⊖ ‡ RESOUR	CE DIAL	⊖ *	LOGINS IN PAST 24 HOURS		⊖ *

This dashboard includes the following widgets by default:

- Overall appliance statistics.
- Appliance health for individual appliances.
- User login activity.
- VPN realm usage.
- Role usage.
- Frequent user logins.

- Logins in the past 24 hours.
- Critical appliance events.
- Resource dial.
- Pulse Connect Secure versions.
- Pulse Policy Secure versions.
- Appliance concurrent users.

Each widget that can be refreshed by clicking **Reload Widget Content** (<sup>(C)</sup>) and collapsed by clicking **Collapse/ Expand Widget** (<sup>\*</sup>).

Click **Download Report** to create and download a multi-page PDF report that includes each widget that currently displays a populated graph. To send the graph via email, enter an email address and click **Send Report**. See **"Exporting Dashboard Information" on page 33**.

## **Viewing Profiled Devices**

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

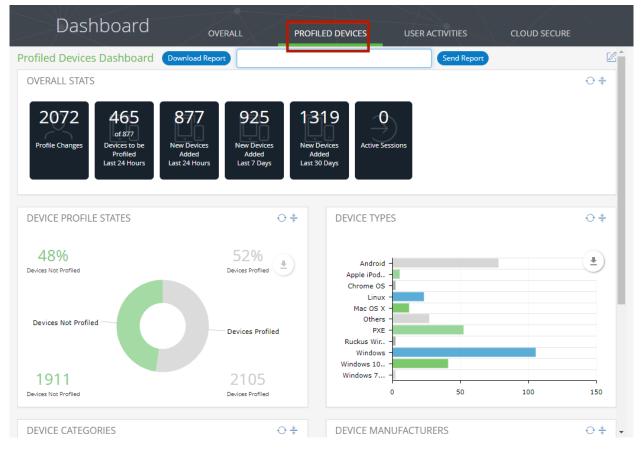


FIGURE 26 Profiled Devices Dashboard

This dashboard includes the following widgets by default:

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

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

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

Click **Download Report** to create and download a multi-page PDF report that includes each widget that currently displays a populated graph. To send the graph via email, enter an email address and click **Send Report**. See **"Exporting Dashboard Information" on page 33**.

For more information on profiled devices, see "Viewing the Profiled Devices Report" on page 122.

## **Viewing User Activities**

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

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

This dashboard includes the following widgets by default:

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

#### FIGURE 27 User Activities Dashboard

Dashboard	LL PROFILED DEVICES USE		CURE
User Activities Dashboard Download Report	Send Report		Ľ
Time Frame: Last 24 Hours Vumber of to	pp users: 5 <b>C</b> Refresh Interval: 5	Minutes Apply Clear	
MAX SESSION LENGTH	AVERAGE SESSION TIME(SECONDS)	COMPLIANCE RESULTS	
AUTH MECHANISM O *	AUTH SUCCESS O *	AUTH FAILURES	⊖ ‡

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

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

Click **Download Report** to create and download a multi-page PDF report that includes each widget that currently displays a populated graph. To send the graph via email, enter an email address and click **Send Report**. See **"Exporting Dashboard Information" on page 33**.

For more information on user activities, see "Viewing the User Activities Report" on page 124.

# **Viewing UEBA Metrics**

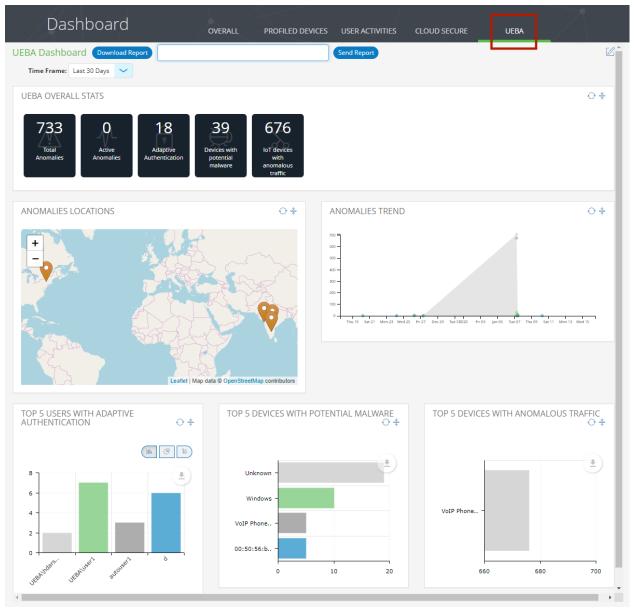
User and Entity Behavior Analytics (UEBA) software analyzes user activity data from logs, network traffic and endpoints. It correlates this data with threat intelligence to identify activities/behaviours that might indicate a malicious presence in your environment.

Pulse One supports the collection and display of UEBA metrics.

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

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

FIGURE 28 UEBA Dashboard



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

The administrator can view the following information:

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

**Note:** You can also view a pair of analytics reports for UEBA, see **"Viewing the UEBA Analytics Reports" on page 125**.

Click **Download Report** to create and download a multi-page PDF report that includes each widget that currently displays a populated graph. To send the graph via email, enter an email address and click **Send Report**. See **"Exporting Dashboard Information" on page 33**.

# **Viewing Cloud Secure Statistics**

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

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

This dashboard includes the following widgets by default:

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

To view metrics for all Cloud Secure appliances:

- 1. Select the **Dashboard** tab, and then select the **Cloud Secure** tab.
- 2. Select the required **Time Frame** for the dashboard. For example, *Last 24 Hours*, *Last 30 Days*.
- 3. Select the required **Refresh Interval** for the dashboard. For example, 5 Mins, 10 Mins, 15 Mins.

4. Click **Apply** to view the filtered statistics. For example:

oud Secure Dashboard Download	Report		Send Report		
Time Frame: Last 30 Days 💙	Refresh Inte	erval: 5 V Minutes Apply	Clear		
TOP 5 SUCCESSFUL SSO APPS	<b>○</b> ‡	TOP 5 FAILED SSO APPS	0 *	SSO DEVICE COMPLIANCE STATS	⊖ ‡
8		3.10 3.05 -			
A pps Count		3.00 - S 2.95 -			
<b>č</b> 2 -		2.90 -			
niccost sheatone		2.85		Not-Assessed	

#### FIGURE 29 Cloud Secure Dashboard

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

Click **Download Report** to create and download a multi-page PDF report that includes each widget that currently displays a populated graph. To send the graph via email, enter an email address and click **Send Report**. See **"Exporting Dashboard Information" on page 33**.

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

## **Customizing Dashboards and Widgets**

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

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

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

#### FIGURE 30 Customizing the Dashboard

	<b>Pulse Secure</b> PULSE ONE		DASHBOARD APPLIANCES ANA	ALYTICS ADMINISTRATION	ې جو settings admin
	Dashboard	OVERALL	PROFILED DEVICES	USER ACTIVITIES	CLOUD SECURE
Over	all Dashboard Download Report		Send Report		Z
	onnect Secure Poli	2 of 1108 Policy Secure concurrent user licenses used	O of 0 Named User licenses used Applance cluster(s)		↔‡
AP	PLIANCE HEALTH				⊖ ‡

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

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

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

Dashboard	OVERA	ALL PROFILED DEVICES	USER A	CTIVITIES CLOUD SECU	JRE
verall Dashboard Download Report		Send Report			⊕ @ ৬
OVERALL APPLIANCE STATS					@ ×
					ô v
APPLIANCE HEALTH					@ ×
APPLIANCE HEALTH     LOGINS IN PAST 24 HOURS	@×	CRITICAL EVENTS	@ ×	♦ RESOURCE DIAL	@ × @ ×

- 3. (Optional) Click **Add New Widget** (⊕) to add a widget to the current layout, see **"Adding a New Widget" on page 28**.
- 4. (Optional) Click **Edit Dashboard** (<sup>(())</sup>) to select a new layout, see **"Editing the Dashboard Layout" on** page 29.
- 5. (Optional) Rearrange the current widgets by dragging a widget using its **Change Widget Location** ( handle.
- 6. (Optional) Change the settings for a widget by clicking its **Edit Widget Configuration** (<sup>@</sup>), see **"Editing Widget Configuration" on page 31**.
- 7. (Optional) Remove a widget by clicking its **Remove Widget** control.
- 8. (Optional) Click **Undo Changes** ( $\Omega$ ) 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

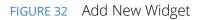
To add a new widget to a dashboard tab:

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



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

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** (<sup>(©)</sup>) control, see **"Editing Widget Configuration" on page 31**.
- 6. (Optional) Click **Undo Changes** ( $\Omega$ ) 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. For example, the **Overall** 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 33 Dashboard Widget Layout

Pulse Secure PULSE ONE	DASHBOARD APPLIANCES ANALYTICS		мім
Dashboard	PROFILED DEVICES	USER ACTIVITIES CLOUD SECURE	
Overall Dashboard Download Report	Send Report	⊕ ĝ	3 ∲ €
◇ OVERALL APPLIANCE STATS		(c	×
<> APPLIANCE HEALTH		¢	×
↔ LOGINS IN PAST 24 HOURS	CRITICAL EVENTS		)×
♦ CONNECT SECURE VERSIONS	OPOLICY SECURE VERSIONS	@ ×	

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

3. Click the **Edit Dashboard** (<sup>(©)</sup>) icon. A display of available layouts appears.

#### FIGURE 34 Edit Dashboard Layout

le Overall Dashboard		
ucture		
Overall Default	······Workspaces-Default······	12/4-4-4
2 columns	Rows, 2 columns (12/12/6-6)	

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

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

FIGURE 35 Updated Dashboard Widget Layout

Pulse Secure PULSE ONE	DASHBOARD APPLIANCES ANALYTICS ADMINISTRATION	
Dashboard	ERALL PROFILED DEVICES USER ACTIVITIES	CLOUD SECURE
Overall Dashboard Download Report	Send Report	⊕⊕⊕Ω
OVERALL APPLIANCE STATS		@ ×
♦ POLICY SECURE VERSIONS	@ ×	
C LOGINS IN PAST 24 HOURS		@×
RESOURCE DIAL	Image: Image	@ ×

- 5. (Optional) Click **Undo Changes**  $(\Omega)$  to reset all unsaved changes and close the layout summary.
- 6. 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. For example, the **Overall** 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** (<sup>@</sup>) control for the widget. For example:

FIGURE 36 Appliance Health Widget

♦ APPLIANCE HEALTH

A dialog appears which displays all configurable options for the widget.

- 5. Make the required changes and click **Apply**.
- 6. (Optional) Click **Undo Changes** ( $\Omega$ ) to reset all unsaved changes and close the layout summary.
- 7. Click **Save Changes** ( $\checkmark$ ) to save all changes and close the layout summary.

# **Controlling Widget Presentation**

You can control individual widgets to control the way that each presents its information:

- "Widgets: Tabular Only" on page 32.
- "Widgets: Mixed Tabular and Graphs" on page 32.
- "Widgets: Graph Only" on page 33.

#### Widgets: Tabular Only

A widget that only includes tabular information appears as follows:

FIGURE 37	Tabular Widget Presentation	
-----------	-----------------------------	--

APPLIANCE CONCURREN	IT USERS	$\odot \frac{1}{2}$
		Export
Appliance Name	Users Count	
test_97	17	
test_94	11	
test_91	9.	
test_92	4	

Click **Export** to save the contents of the table as a Comma Separated Value (CSV) file, see **"Exporting Dashboard Information" on page 33**.

#### Widgets: Mixed Tabular and Graphs

A widget that includes both tabular and graph information appears as follows:

FIGURE 38 Tabular and Graph Widget Presentation



In this widget:

- Click **Graph** (<sup>16</sup>) to switch to a specific line graph view. There may be multiple graphs for a widget.
- Click **Pie Chart** ( ) to switch to a specific line graph view. There may be multiple charts for a widget.
- Click **Table** (<sup>16</sup>) to switch to a specific line graph view. There may be multiple tables for a widget.
- Click Download (<sup>\*)</sup>) to save the contents of the table as a PDF file, see "Exporting Dashboard Information" on page 33.

### Widgets: Graph Only

A widget that only includes graph information appears as follows:

FIGURE 39	Graph Widget Presentation
IIGONE 55	diupri maget i teschadiori



Click **Download** (<sup>(±)</sup>) to save the contents of the table as a PDF file, see **"Exporting Dashboard Information" on page 33**.

# **Exporting Dashboard Information**

There are three ways of exporting graphical information from the **Dashboard**:

• Each tab within the **Dashboard** has a **Download Report** button. Click this button to create and download a multi-page PDF report that includes each widget that currently displays a populated graph.

**Note:** This report does not include tabular widgets or mixed-format widgets that currently display tabular information.

- Each tab within the **Dashboard** has a **Send Report** button. Enter an email address and click this button to create and send the graph via email.
- Most table-only widgets include an **Export** button. Click this button to produce a Comma-Separated Value (CSV) file of the tabular data.
- Most graph widgets include a **Download** (\*) button. Click this button to produce a PDF report that contains the widget.

# Appliance Management

•	Registering an Existing PCS/PPS Appliance
•	Configuring an Appliance to Connect to Pulse One
•	Creating and Registering a PCS Appliance VM on vSphere
•	Creating and Registering a PCS Appliance VM on AWS
•	Configuring CPU, Memory and Disk Utilization
•	Backing up and Restoring Appliance Configurations
•	Working with Appliance Groups    76
•	Upgrading Managed Appliances 87
•	Uploading an Endpoint Security Assessment Plug-In Package
•	Viewing the Activities Log for an Appliance 109
•	Viewing the Configuration Change History for an Appliance
•	Comparing Appliances 111
•	Rebooting an Appliance
•	Removing an Appliance from Pulse One 114
•	Preparing a Target Appliance 115
•	Removing an Appliance from an Appliance Group
•	Editing an Appliance Group 116
•	Deleting an Appliance Group    118

# **Registering an Existing PCS/PPS Appliance**

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

Note: This process requires sufficient appliance licensing capacity.

Note: You can also create and register a virtual PCS appliance for either AWS (see "Creating and Registering a PCS Appliance VM on AWS" on page 56) or vSphere (see "Creating and Registering a PCS Appliance VM on vSphere" on page 44).

To register an existing appliance:

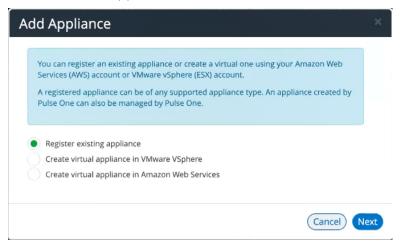
- 1. Log into Pulse One as an administrator.
- 2. Click the **Appliances** menu and then the **Appliances** tab.

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

3. Click Add Appliance.

#### The Add Appliance dialog box appears.

FIGURE 40	Add Appliance
-----------	---------------



4. Select Register existing appliance and click Next.

The Register Appliance dialog appears.

FIGURE 41 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 <b>Pulse Connect Secure</b> and <b>Pulse Policy Secure</b> 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 87**.

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

8. Click Save.

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

FIGURE 42 Re	egistration	Required
--------------	-------------	----------

Registration Required				
0	Use Registration Host : with the following Registration code : to register your appliance.			
	OK			

- 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 40**.

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

### **Editing Appliance Information**

To edit appliance information:

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

The Appliances tab displays all current appliances.

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

FIGURE 43 Edit Appliance Information

Edit Appl	larice		
Name:	Pul	se-Example-PCS-1	
ADDITIC	NAL IN	IFORMATION	$\sim$
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 38**.

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 ( $\frac{1}{2}$ ).
- 4. From the menu options, select Launch Appliance UI.

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

### **Recognizing Critical Vulnerabilities**

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

	ecure <sup>.</sup>			DASHI	BOARD	APPLIANC	es wo	ORKSPACE
Appliance	ces	APPLIANCE	s	COL	NFIG GRC	OUPS		SOFTWA
Appliances + Add Appli	ance Expo	rt 🔶						
Name	Model	Version	△ Last C	onfig	Task Statu	s Pul	se One St	atus ©
😤 test_PCS_8_3R1 (PCS)	VA-SPE	A 8.3R1-55340				• 0	onnected	d ŝ
🖀 test_PCS_8_2R1 (PCS)	VA-SPE	▲ 8.2R1-41240	8min			• 0	onnected	d ŝ
🗥 test_9_0R2_1 (PCS)	PSA-V	⚠ 9.0R2.1-63976	1hr 10m	nin		• 0	onnected	i ŝ
😤 test_PCS_9_0R3_4 (PCS)	PSA-V	9.0R3.4-64054	1hr 13m	nin		• 0	onnected	d ŝ

FIGURE 44 Critical Vulnerability

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

FIGURE 45 Details of a Critical Vulnerability

Appliances + Add Applia	ince Expor	t) 🔿				
Name	Model	Version	△ Last Config	Task Status	Pulse One Status	۲
🙆 test_PCS_8_3R1 (PCS)	VA-SPE	A 8.3R1-55340			Connected	000
🙆 test_PCS_8_2R1 (PCS)		has critical vulnerabilities. ade as soon as possible. Se	e		Connected	000
🙆 test_9_0R2_1 (PCS)	SA44101.		nin		Connected	000
test_PCS_9_0R3_4 (PCS)	PSA-V	9.0R3.4-64054	1hr 13min		Connected	000

To upgrade the software on the appliance, see "Upgrading Software on an Appliance" on page 91.

# 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 40**.
- Configure the appliance to send logs to Pulse One, see "Configuring Log Settings on the Appliance" on page 41.
- Configure the ActiveSync handler on the appliance as required, see **"Configuring ActiveSync Handler" on page 43**.

# **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 35.

4. Click Save Changes.

The Status Information displays the Registration Status in green.

FIGURE 46 Pulse Connect Secure: Pulse One Settings

Status Information

Registration 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 47	Log Events Settings
-----------	---------------------

On L C					Pulse Connec	t Secure	
S Pulse Secure	2 System	Authentication	Administrators	Users	Maintenance	Wizards	••
Log/Monitoring > Events > Log settings							
Log settings							
Events User Access Admin A	ccess Sen	sors Client Logs	SNMP	Statistics	Advanced Setti	ngs	
Log Settings Filters							
Save Changes Reset							
♥ Maximum Log Size							
Max Log Size: 200 MB							
Note: To archive log data, see the Archivi	ing page.						
♥ Select Events to Log							
<ul> <li>Connection Requests</li> <li>Statistics</li> </ul>							
System Status Performa	ance						
Rewrite Reverse	Proxy						
System Errors							
License Protocol Events							
MDM API Trace							
Pulse One Events							
Profiler Events							
HTML5 Access Events							
▼ Syslog Servers							

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

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

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

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

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

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

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

#### 10. Under Syslog Servers:

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

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

- **Type**: Select *TCP*.
- Client Certificate: Select Select Client Cert.
- **Filter**: Select *WELF: WELF*.
- 11. Select the **Advanced Settings** tab and enable **Fault Tolerance** for the Pulse One syslog server.

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

# **Configuring ActiveSync Handler**

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

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

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

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

The Pulse Workspace Handler screen appears.

FIGURE 48 Pulse Connect Secure: Command Handlers

$\circ$						Pulse Connec	t Secure
S Pulse S	ecure	System ,	Authentication	Administrators	Users	Maintenance	L 🗸 Wizards
Puise One							
Licensing Pulse One	e Security	Certificates	DMI Agent	NCP	Sensors	Client Types	Pulse Collaboration
Virtual Desktops IKE	Ev2 SAML	Mobile	VPN Tunneling	Telemetry	Advanced	I Client Configuration	
Settings Command Handlers							
Pulse Workspace Handler							
Device Role: (none) Clear Active Sync Device Group Lookup Handler Col Select Authentication Server:	Records Delete all	the device records p	cord created for devices ushed from Pulse Works				
Available Auth Servers:	Selected A	Auth Servers:					
	(none) kdd -> Remove	si v	elect only one authentical	ion 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 56**.

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

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

**Note:** During this process, you can optionally use a master appliance template. A master template encapsulates an existing deployed appliance, and enables the re-use of many configuration settings on any appliance that is deployed using the template. To create a master template, see **"Creating an Appliance Master Template on vSphere" on page 51**.

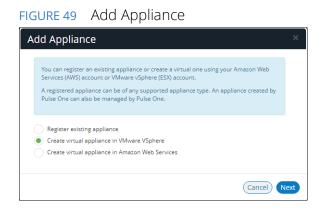
To create and register a PCS appliance as a VM on vSphere:

- 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 50
VSphere Credentials

Sphere Credentials

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

Account:
Add New

Host name:
VSphere host name

Username:
Username

Password:
Password

Cancel
Net

- 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 51 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 52	Appliance	Network	Configu	iration: Serve	ers
-----------	-----------	---------	---------	----------------	-----

Network name fields car	h be looked up from vCenter under Networ	'ks.,
SERVERS		$\sim$
Primary DNS:	8.8.8.8	
Secondary DNS:	8.8.4.4	
NTERNAL 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 53 Appliance Network Configuration: Internal Network Settings

	network configuration for			
Network nam	le fields can be looked up	from vcenter under	Networks,	
SERVERS				<
NTERNAL	NETWORK SETTIN	GS		$\checkmark$
Private Doma	in Name			
invate boint				
nternal FQDI	N:			
nternal Netw	/ork Name:			
P Address:	10.10.10.5	Subnet:	255.255.255.0	
Gateway:	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 54 Appliance Network Configuration: External Network Settings

Network nam	ne fields can be looked up	from vCenter under	Networks.
SERVERS			<
INTERNAL	NETWORK SETTIN	GS	<
FXTERNAI	NETWORK SETTIN	GS	~
Public Domai	n Name:		
External FQD	N:		
External Netw	vork Name:		
IP	64.64.64.5	Subnet:	255,255,255.0
Address:			
Gateway:	64.64.64.1	VLAN:	
MANAGEN	IENT NETWORK SE	TTINGS	.<
MANAGLI			

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 55 Appliance Network Configuration: Management Network Settings

vetwork name fields can be looked	up from vCenter under Networks.	
SERVERS		<
NTERNAL NETWORK SETT	INGS	<
EXTERNAL NETWORK SETT	INGS	<
MANAGEMENT NETWORK	SETTINGS	$\sim$
Aanagement Network		
Name:		
P	Subnet:	
Address:		
Sateway:	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 56 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 51.

#### 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 57 vSphere Appliance Creation In Progress
--

🕄 Recent Tasks			
-			
Task Name	Target	Status	Initiator
Clone virtual machine	pcs_master_template	41 % 🔇	VSPHERE.LOCAL\\
Check new notifications	Solvc.lab.psecure.net	<ul> <li>Completed</li> </ul>	VMware vSphere U

FIGURE 58 vSphere Appliance Creation Complete

🛐 Recent Tasks			
<b>₽</b> .			
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	<ul> <li>Completed</li> </ul>	VSPHERE.LOCAL\\
Clone virtual machine	pcs_master_template	<ul> <li>Completed</li> </ul>	VSPHERE.LOCAL\\
Check new notifications	Solvc.lab.psecure.net	<ul> <li>Completed</li> </ul>	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 59 VSphere Web Client Deploy

vmware vSphere Web Client	†≡	
Navigator	Actions - 192.168.71.11	
Back      Back      Back      Solvc.lab.psecure.net      Solucions-lab	New Virtual Machine ifig New vApp > New Resource Pool Deploy OVF Template	jure Permissi VMs Re
▶ 🛯 192.168.	Connection Maintenance Mode Ion Power Ion	Type mal VMFS 5 mal VMFS 5
	Certificates >	

The **Deploy OVF Template** wizard appears.

FIGURE 60 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 for
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
	Use multiple selection to select all the files associated with an OVF template (.ovf, .vmdk, etc.)

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

FIGURE 61 vSphere Deploy OVF Select Template Files



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

#### FIGURE 62 vSphere Deploy OVF Template Wizard 2

Select template	Select name and location Enter a name for the OVF and select a deployment location.	
Select name and location		
Select a resource	Name pcs_import	
Review details	Filter Browse	
elect storage		
leady to complete	Select a datacenter {0} or {1} folder.	
ady to complete	→  P solv	
	👂 📑 solu	

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 63 vSphere Deploy OVF Template Wizard 3

M Deploy OVF Template						
<ul> <li>Select template</li> <li>Select a resource</li> <li>Select where to run the deployed template.</li> </ul> <ul> <li>Select manual location</li> <li>Select manual location</li> <li>Select manual location</li> <li>Select manual location</li> </ul>						
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	▼ Solu					
6 Select networks	▷					
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 64 VSphere Deploy OVF Template Wizard 5

8	Deploy OVF Template	
<b>*</b>	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 -
	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:

FIC	Deploy OVF Template	Deploy OVF Template Wi	
<b>`</b>	1 Select template 2 Select name and location	Select networks Select a destination network for each source	a network.
~	3 Select a resource	Source Network	Destination Network
~	4 Review details	InternalNetwork	VM Network
~	5 Select storage	ManagementNetwork	VM Network 👻
1	6 Select networks	ExternalNetwork	External Network -
	7 Customize template		
	8 Ready to complete		

FIGURE 65 vSphere Deploy OVF Template Wizard 6

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

FIGURE 66 vSphere Deploy OVF Template Wizard 7

<ul> <li>1 Select template</li> <li>2 Select name and location</li> </ul>	Customize template Customize the deployment p	properties of this software solution.		
3 Select a resource	All properties have valid	values	Show next	Collapse all
4 Review details	valVEConfig	1 setting		4
<ul> <li>5 Select storage</li> <li>6 Select networks</li> <li>7 Customize template</li> <li>8 Ready to complete</li> </ul>	VA IVE Configuration	Please enter the IVE Configuration P Sample values are given below valPAddress=20.20.20; vaNetmask=255.255.255.0; vaGetaway=20.20.20.1; vaDefaultVlan=10; vaPrimaryDNS=10.2.3.45; vaSecondaryDNS=10.2.3.45; vaSecondaryDNS=10.2.3.45; vaNSDomain=jnpr.net; vaWINSServer=TheWINS; vaAdminUsername=admin; vaAdminUsername=admin; vaAdminUsername=admin; vaCommonName=jnpr; vaOrganization=PBU; vaRandomText=Lf3isB3@utt vaManagementIPAddress=10 vaManagementIPAddress=10	rD; fuL; .10.10.10;	text box below

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

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

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

FIGURE 67 vSphere Web	o Client Clone
VMWare <sup>®</sup> vSphere Web Client	ĥ≡
Navigator	🖡 📴 pcs_import 🛛 🛃 👂 📇 🛛 🚳 Actions 🗸
Back	Getting Star Summa Monitor Configure Permissions Snapshots Datastore
Image: Control of the second secon	Actions - pcs_import     Actions - pcs_import     Construct to the result of the
	Clone → Clone to Virtual Machine () Template Clone to Template
	Fault Tolerance     Image: Connect to Template in Library       VM Policies     Image: Connect to Template in Library

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

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

FIGURE 68 VSphere Clone VM to Template Wizard

pcs_import - Clone Virtual Machine To Template     (?)			
1 Edit settings 1a Select a name and folder	Select a name and folder Specify a unique name and target location		
1b Select a compute resource	Enter a name for the template.		
1c Select storage	pcs_master_template		
1d Customize vApp properties	Template names can contain up to 80 characters and they must be unique within each vCenter Serv	ver VM folder.	
Ready to complete	Select a location for the template.		
	Q Search		
	Select a datacenter or VM fol the new template in.	der to 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 69 vSphere Clone VM to Template Wizard 1b

8.	g <sup>ur</sup> pcs_import - Clone Virtual Machine To Template					
	1 Edit settings 1a Select a name and folder	Select a compute resource Select the destination compute resource for this operation				
ľ,	1b Select a compute resource					
	1c Select storage	Q Search				
	1d Customize vApp properties	▼ solu  192.168				
	2 Ready to complete	Select a cluster or host to store this template in.				

22. Select the required compute resource.

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



- 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 71 VSphere Clone VM to Template Wizard 1d

pcs_import - Clone Virtual Machin	ne To Template			(4 (?)
1 Edit settings	Customize vApp propertie Edit the vApp properties	\$		
<ul> <li>1b Select a compute resource</li> </ul>	All properties have valid	values	Show next	Collapse all
1c Select storage	valVEConfig	1 setting		<b>^</b>
<ul> <li>1d Customize vApp properties</li> </ul>	VA IVE Configuration	Please enter the IVE Configuration Parameters in the text box below	v. You can edit or cop	y/paste the
2 Ready to complete		Sample values are given below: valPAddress=20.20.20.20; vaNetmask=255.255.05; vaGateway=20.20.20.1; vaDefault/Van=10; vaPrimaryONS=10.2.3.45; vaSecondaryONS=10.2.3.46; vaDSDomain=ipn:net; vaAdminPassword=P@ssW0rD; vaAdminPassword=P@ssW0rD; vaCommonName=ipn; vaCommonName=ipn; vaRandomText=I.tf3lsB3.dbutfsu :		
		Back	Next 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 44**.

# 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 44.

Perform the following tasks:

- 1. Before you begin, you must locate and record the following information:
  - The required Route 53 zones, see "Identifying the Required Route 53 Zones" on page 57.
  - The required VPC ID and Subnet IDs, see "Identifying the Required VPC ID and Subnet IDs" on page 59.
  - The required EC2 deployment key, see "Identifying the EC2 Deployment Key and AMI ID" on page 61.
- 2. You can then create the appliance, see "Creating the PCS Appliance VM on AWS" on page 64.

### 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 72 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 73 AWS Route 53 Management Console

aws Services	s 🗸 Resource Groups 🗸 🔭			<b>Д</b> •	@ 🔻 Global 🕶	Support 👻
Dashboard	DNS management	Traffic management	Availability monitoring	Domain registrati		
Hosted zones 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. Health checks monitor your applications to healthy resources, and direct DNS queries to healthy resources. Create policy Create health check		A domain is the name, such as example com, that your users use to access your application. Register domain		1
Domains Registered domains Pending requests	Register domain Find and register an available domain, or tran Type a domain name Alerts	efer your existing domains to Route 53.	Check	C	More info Developer Guide FAQs Pricing Forum - DNS and health o Forum - Domain name re	
			<b>∥</b> ≪ No alerts to display ⇒	> >	Request a limit increase	· · · ·
	Resource Status		Last update		Service health	c
					Amazon Route 53 Service is operating AWS service health dash	

#### 5. Select Hosted Zones.

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

FIGURE 74 AWS Route 53 Hosted Zone	S
------------------------------------	---

aws	Services	🗸 Resource Groups 👻 🛠			Å• @ ▾ Global ▾ Support ▾
Dashboard	4	Create Hosted Zone Go to Record	Sets Delete Hosted Zone		<i>C</i> 0
Hosted zones		Q Search all fields	All Types 🔹		$\ \leqslant~~\leqslant~$ 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 Policy records		sip.nu	Public 2	Z22V6N8	
		awste	Public 2	Z354F2J0	
Domains Registered domains		🔵 jakma	Private 2	Z8RZ8UJI	
Pending requests	5	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 75 AWS Public and Private Zones

Domain Name	- Туре	Record Set Count      Com	ment Hosted Zone ID
awstes	Public	2	Z354F2JGVF
nuwav	Public	2	ZSQ2H40W>
sip.nuv	Public	2	Z22V6N8JS2
sko.7-3	Public	2	Z1IHK47TAN
jakmar	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.

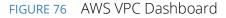
You can then perform any remaining preparations, and then continue to create and register the PCS appliance virtual machine on AWS.

# 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.



aws Servio	ces 🗸 Resource Groups 🗸	*			¢٩	@ 🕶 Ireland 🕶	Support 👻		
VPC Dashboard	Launch VPC Wizard	aunch EC2 Instances			Service Health		Î		
Q Select a VPC	Note: Your Instances will laund	h in the EU (Ireland) re	gion.		Current Status	Details			
	Resources by Reg	ion 2 Refresh R	esources		<ul> <li>Amazon EC2 - EU (Ireland)</li> </ul>	Service is operating normally			
Virtual Private Cloud	You are using the following Ama	You are using the following Amazon VPC resources				View complete service health details			
Your VPCs Subnets	VPCs See all regions +	Ireland 20	Nat Gateways See all regions <del>-</del>	Ireland 2	Account Attributes				
Route Tables					Resource ID length management				
Internet Gateways Egress Only Internet Gateways	Subnets See all regions 🕶	Ireland 53	VPC Peering Connections See all regions +	Ireland <b>O</b>	Additional Information				
DHCP Options Sets	Route Tables	Ireland 33	Network ACLs	Ireland 20	VPC Documentation				
Elastic IPs	See all regions +		See all regions +		All VPC Resources Forums				

5. Select Your VPCs.

A list of available VPCs appears.

FIGURE 77	AWS Available	VPCs
-----------	---------------	------

aws Servie	es 🗸	Resource Groups ~	*						<b>∆•</b> •	✓ Ireland	✤ Support
/PC Dashboard	Crea	te VPC Actions 👻									C 🗘
Filter by VPC: Q Select a VPC	4 Q:	Search VPCs and their	r propert 🗙							« < <b>1</b> t	o 20 of 20 VPC
/irtual Private		Name 🔺	VPC ID -	State -	IPv4 CIDR	IPv6 CIDR v	DHCP options set	Route table -	Network ACL	- Tenancy -	Default VPC
loud		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
nternet 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 78 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 79 AWS SE	elect VPC			
aws Services	• Resource Groups •	*		
VPC Dashboard	Create VPC Actions *			
Filter by VPC:	Q Search VPCs and their p	propert 🗙		
vpc-989d2   itomation	· · · · ·	VPC ID v	State -	IPv4 CIDR
vpc-1b109   -VPC		vpc-989d2	available	10.0.0/16
vpc-0189c   Jck-vpc-5		vpc-1b109	available	10.0.0/16
vpc-ec1da vrouter-vpc vpc-de75c mhoc		vpc-0189c	available	10.5.0.0/16
vpc-de750   mnog vpc-9a838   sudha	үрс	vpc-ec1da	available	10.8.0.0/16
vpc-d3087   jakm	Direct	vpc-de75c	available	10.0.0/24
	100 m m	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 64**). 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 80 AWS Select Public Subnet

Name	<ul> <li>Subnet IE</li> </ul>	) – State	- VPC	Ŧ
private-self-re	g subnet-e8	ea3 availa	ible vpc-ec1da	vrouter-vpc
vrouter-public	subnet-fbf	320 availa	ible vpc-ec1da	vrouter-vpc
4				
Subnet: subnet-fbf32	20a3			
Description	Flow Logs	Route Table	Network ACL	Tags
	Subnet ID su	bnet-fbf32 🖉	1	
	VPC VP	oc-ec1da   vroute	r-vpc	

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

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

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

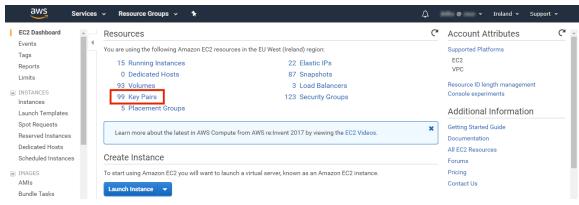
# Identifying the EC2 Deployment Key and AMI ID

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

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

The AWS EC2 Dashboard appears, showing Key Pairs.

#### FIGURE 81 AWS EC2 Dashboard



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

A list of defined key pairs appears.

FIGURE 82 A	NS EC2 Key Pai	rs	
aws Service	es 🗸 Resource Groups 🗸	*	û @ Ireland ▾ Support ▾
EC2 Dashboard	Create Key Pair Import Key	Pair Delete	▲ 근 ♦ Ø
Tags	Q Filter by attributes or search	by keyword	
Reports Limits	Key pair name	Fingerprint     ·	
<ul> <li>INSTANCES</li> <li>Instances</li> <li>Launch Templates</li> <li>Spot Requests</li> <li>Reserved Instances</li> <li>Dedicated Hosts</li> <li>Scheduled Instances</li> <li>IMAGES</li> <li>AMIs</li> </ul>	abragg achem admin aknox-i apritch ayritch aws-sd aws-sd	5f 10.99.d0.4a.c3.95.e4.4c.49.cd 03.e5.2 0e:1d 4a.36.16.46.72.d5.06.53.10.66.44 b 6d 4e:ed 12.17.22.38.c4.73.2d 52.d5.17.4 14.e4.af.25.84.11:a0.bc.04.5f.41.c6.84.8t 57 ba bc.9d 48.e6 f4.c8.58.c8.5f14ff.af.9 7e:90.12.69.ad.7d.f4.98.ff2.41.55.f02.45 1a.fc.85.8c.ba cc.0d.8d bf.67.45.be.e3.f5 b0.bd 1d.90.ec.bf.2b.24.fa.57.46.a0.b0.fe a1.38.66.29.35.05.84.d0.00.7c.c8.f9.99.7 a1.ec.0dfc.5e.fb2.86.79.e0.b18.48.a9.35	
Bundle Tasks ELASTIC BLOCK STORE	Select a key pair	a notionalisotation action notionalise e e e	

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 83 AWS Select EC2 Key Pair

	Key pair name	Fingerprint	•
	abra	5f:10:99:d0:4a:c3:95:e4:4c:49:cd:03:e5:	
	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:(	
	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	
Key P	Pair: admin	0.0.0	
- [	Key pair name ad	min 42	
	Fingerprint 14	: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:

FIGURE 84 AW	/S EC2 AMIs						
aws Services	s 🗸 Resource Groups 🖌 🛠				, ⊈	kilby @ zeus 🕶	Ireland 🖌 Support 🗸
EC2 Dashboard	Launch Actions V						⊥
Tags	Owned by me 👻 🔍 Filter by tags and	attributes or search by keywor	d			0	<~<~1 to 28 of 28 $~>~> $
Reports Limits	Name - AMI Name	AMI ID 🚽	Source	- Owner	- Visibility	- Status	- Creation Date
	AMLI	ami-02216a6690b4	815181475	815181475	Private	available	August 6, 2018 at 2:03:081
INSTANCES     Instances	jakm	ami-0390cf549bf82	815181475	815181475	Private	available	September 3, 2018 at 2:43
Launch Templates	Jakm	ami-0f8d46a9b20el	815181475	815181475	Private	available	September 4, 2018 at 1:09
Spot Requests	Idarb	ami-a7a25ed0	815181475	815181475	Private	available	March 10, 2014 at 4:42:51
Reserved Instances	sd-bu	ami-08c269c71ae0	815181475	815181475	Private	available	August 31, 2018 at 4:19:56
Dedicated Hosts	Servi	ami-b4ffb1cd	815181475	815181475	Private	available	March 13, 2018 at 11:42:12
Scheduled Instances	Servi	ami-0627430bd6c1	815181475	815181475	Private	available	August 7, 2018 at 3:00:40 F
	Servi	ami-028189c4d8a5	815181475	815181475	Private	available	August 9, 2018 at 3:26:51 F
AMIS	Servi	ami-03ccf2b81763t	815181475	815181475	Private	available	August 30, 2018 at 10:32:0
Bundle Tasks	Servi	ami-4a211b33	815181475	815181475	Private	available	May 30, 2018 at 2:25:14 AN

#### Bundle Tasks

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

FIGURE 85 AW	'S 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
	ldarby-backend2	ami-a7a25ed0	815181475850/I
Image: ami-0390cf549			0.0.0
	AMI ID ami-0390cf54 Owner 81518147585	-	

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

### Creating the PCS Appliance VM on AWS

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

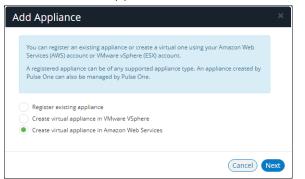
- 1. Log into Pulse One as an administrator.
- 2. Click the **Appliances** menu and then the **Appliances** tab.

The Appliances tab displays all current appliances.

3. Click Add Appliance.

The **Add Appliance** wizard starts.

FIGURE 86 Add Appliance



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

The AWS Credentials panel of the wizard appears.

IGURE 87	AWS Credentials	
		×
AWS Credentials		
	credentials to manage virtual appliances. If you have already entered elect 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 88 Appliance Configuration

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

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

9. Click Next.

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

FIGURE 89	Appliance	Network	Configu	ration: Serve	rs
-----------	-----------	---------	---------	---------------	----

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 90 Appliance Network Configuration: Internal Network Settings

Please enter network configuration for the virtual appliance.	
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 57**.

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

- For the Internal FQDN, complete the FQDN by adding a unique appliance identifier to the 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 91 Appliance Network Configuration: External Network Settings

Please enter network configura	ition for the virtual appliance.	
SERVERS		<
INTERNAL NETWORK SI	ETTINGS	<
EXTERNAL NETWORK S	ETTINGS	$\sim$
Public Domain Name:		
External FQDN:		
MANAGEMENT NETWO	RK 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 57**.

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

 For the External FQDN, complete the FQDN by adding a unique appliance identifier to the 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 92 Appliance Network Configuration: Management Network Settings

Please enter network cor	figuration for the virtual appliance.	
SERVERS		<
INTERNAL NETWO	RK SETTINGS	<
EXTERNAL NETWO	RK SETTINGS	<
MANAGEMENT NET	TWORK SETTINGS	~
Management Domain Name:		
Management FQDN:		

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

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

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

- 17. Click **Next**. The **AWS Configuration** panel of the wizard appears.
  - FIGURE 93 AWS Configuration

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

- 18. Specify the following properties:
  - Amazon Machine Image (AMI) is the AMI ID that you identified in "Identifying the EC2 Deployment Key and AMI ID" on page 61.
  - VPC ID is the value that you identified in "Identifying the Required VPC ID and Subnet IDs" on page 59.
  - **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 59.
  - **Deployment Key** is the key pair that you identified in **"Identifying the EC2 Deployment Key** and AMI ID" on page 61.
- 19. Click Save.

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

FIGURE 94 New Unregistered Appliance

APPLIANCES	CONFIG GROU	PS S	OFTWARES	BACKUP	-RESTORE	SCHEDULED	TASK
Appliances Q se	arch 🗙	+ Add A	opliance Exp	oort 🔁			
Name		Model	Version	Last Config U	Task Status	Pulse One Status	0
C 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.

FIGURE 95 AWS Initializing Appliance

- 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:

		0 11										
EC2 Dashboard	Launch Insta	nce 👻 Connect Acti	ons 👻							4		0
Events												
Tags	Q Filter by ta	ags and attributes or search by ke	yword							1 to 20 o	f 20 🔅	×
Reports	Name	<ul> <li>Instance ID</li> </ul>	Instance Type	Availability Zone ~	Instance State ~	Status Checks ~	Alarm Status	Public	DNS (IPv4)	~   IP	v4 Publi	ic IP
Limits		1908/ Gauduana/	LZ.IIIIGIO	ua-weat-10	- atopped		TRUTTO	002-10-	-sr-ia			-
INSTANCES	sree	i-0f3ecd1c67cea	t2.micro	us-west-1a	stopped		None	a ec2-54	-241-!	54	4.241	
Instances	mob	. i-0fb5a78c74255	t2.small	us-west-1a	running	2/2 checks	None	ac2-54	-215-{	54	4.215	
Launch Templates	aws	i-0779548656d2	t2.xlarge	us-west-1a	stopped		None			54	1.176	1.000
Spot Requests	new-aws	s-ap i-Oedbefcfe213	t2.xlarge	us-west-1a	running	Initializing	None			52	2.52.	
Reserved Instances	Instance: i-	Dedbefcfe2139 (new-aws-	app-PCS) Elas	tic IP: 52.52.111.67								
Dedicated Hosts												

**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 96 Appliance Health

Pulse Secure PULSE ONE	DASHBOARD APPLIANCES	ANALYTICS ADMINISTRATION	SETTINGS ADMIN
Appliances	IPPLIANCES CONFIG GROUPS SOF	TWARE BACKUP-RESTORE SCHEDULED	Q D TASKS SEARCH
Appliances + Add Appliance Export	$\diamond$		2 Appliances
Name Model Version Last	t Config Upload Task Status Pulse One Status 🐵	🖴 Pulse-PPS-1  🔶	Actions -
Pulse-PPS-1 VA-SPE 9.0R1-49496 14hr	r 40min Connected 🕴		
Pulse-PPS-7 VA-SPE 9.0R1-49496 14hr	r 47min Connected	APPLIANCE INFO	<u> </u>
			7.91 b/s Throughput
		CPU Utilization 0%	25% Disk Utilization
		L	

# 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 97	Pulse One Appliances Tab
-----------	--------------------------

E SPulse Secure	DASHBOARD APPLIAN	ICES ANALYTICS	5 ADMINISTRATION		SETTINGS ADMIN
	CONFIG GROUPS	SOFTWARE	BACKUP-RESTORE	SCHEDULED TASKS	G search
Appliances + Add Appliance Export 📀					4 Appliance
Name		Model	Vers Last Config U	Task Status Pulse	e One Status 🛛 💿
Ade_Pulse-106		PSA5000-V	9.0R 5d 18hr 53min	• Co	onnected 🕴
Ade_Pulse-109		PSA7000-V	9.0R 5d 18hr 50min	● Co	onnected 🚦
PPS Pulse-PPS-1		VA-SPE	9.0R 6d 15hr 57min	● Co	onnected 🖁
PPS Pulse-PPS-7		VA-SPE	9.0R 6d 15hr 54min	● Co	onnected 8

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

FIGURE 98 A	ppliance Menu
-------------	---------------

	Pulse Secure		DASHBOARD APPI	IANCES ANALYTICS	5 ADMINISTRATION		SETTINGS ADMIN
	Appliances	APPLIANCES	CONFIG GROUPS	SOFTWARE	BACKUP-RESTORE	SCHEDULED	Q TASKS search
Applia	ANCES + Add Appliance Export	$\Theta$					4 Appliance
Name				Model	Vers Last Config U	Task Status	Pulse One Status 🛛 ©
PES /	Ade_Pulse-106			PSA5000-V	9.0R 5d 18hr 55min		Connected
PCS /	Ade_Pulse-109			P5A7000-V	9.0R 5d 18hr 52min		Reboot Appliance
PP5	Pulse-PPS-1			VA-SPE	9.0R 6d 16hr		Edit Appliance Info Launch Appliance UI
PP5	Pulse-PPS-7			VA-SPE	9.0R 6d 15hr 56min		Remove Appliance Compare Appliances
							Backup Configuration
							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 99 Monitoring a Pending Backup

Appliances + Add Appliance	Export	$\mathbf{O}$					4 App	oliances
Name			Model	Version	Last Config Upload	Task Status	Pulse One Status	۲
PCS 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	000
Pulse-PPS-1			VA-SPE	9.0R1-49496	6d 17hr 25min		Connected	
Pulse-PPS-7			VA-SPE	9.0R1-49496	6d 17hr 22min		Connected	000
<u> </u>					vv () () aaliiii		- connected	•

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

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

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

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

Appliances + Add Appliance Export 🔿					4 Applianc
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
PUISe-PPS-1	VA-SPE	9.0R1-49496	6d 17hr 30min		Edit Appliance Info Launch Appliance UI
PPS Pulse-PPS-7	VA-SPE	9.0R1-49496	6d 17hr 27min		Remove Appliance Compare Appliances
				[	Backup Configuration Upgrade Software Cancel Backup Schedule Task

The cancellation is then confirmed.

FIGURE 100 Canceling a Backup

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 101 Viewing Backup Files

		DASHBOARD APPLIANC	ES ANALYTICS ADMINISTRATION	SETTI	IGS ADMIN
Appliances	APPLIANCES	CONFIG GROUPS	SOFTWARE BACKUP-RESTOR	E SCHEDULED TASKS	Q search
Backup-Restore				1 MB <b>т</b> ₀	tal Backup Size
Appliance Name	Description	Appliance Version	Backup Date	Size	٢
Ade_Pulse-106	test_backup	9.0R3-13030	2019-01-16 13:55:57 +00	000 725.21 KB	000
Ade_Pulse-109	after_clear_config-1	9.0R3-13030	2019-01-16 13:54:35 +00	000 727.01 KB	0

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 102 Viewing Backup Files Before Delete

	Secure	DASHBOARD APPLIA	NCES ANALYTICS ADM	IINISTRATION	борородини Tings admin
Applian		CONFIG GROUPS	SOFTWARE BAC	KUP-RESTORE SCHEDULED TASKS	Q SEARCH
Backup-Restore				1 MB	Total Backup Siz
Appliance Name	Description	Appliance Version	Backup I	Date Size	۵
Ade_Pulse-106	test_backup	9.0R3-13030	2019-01-	16 13:55:57 +0000 725.21 KB	000
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.

- 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 103 Viewing Backup Files
---------------------------------

							SETTIN	
Appliance		CONF	GROUPS	SOFTWARE	BACKUP-RESTORE	SCHEDU	JLED TASKS	Q SEARCH
Backup-Restore							1 MB τα	otal Backup Size
Appliance Name	Description		Appliance Version		Backup Date		Size	٥
Ade_Pulse-106	test_backup		9.0R3-13030		2019-01-16 13:55:57 +0000		725.21 KB	000
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 *pcs-174* is at the top of the list.

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

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

FIGURE 104 Selecting an Appliance

Select Appl	liance to Restore	×
	Ade_Pulse-106	
installed and act • ESAP Packag	sifully 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) op (9.0.3.1494)	
	(Close) Sel	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 105 Monitoring a Configuration Restore for an Appliance

	DASH	IBOARD APPLIANC	ES ANALYTICS ADM	INISTRATION		
Appliances	PLIANCES CON	FIG GROUPS	SOFTWARE BAC	KUP-RESTORE SCHEDUL		Q Earch
Appliances + Add Appliance Export	Э <sub>г</sub>				4 Apr	pliances
Name	Model	Version	Last Config Upload	Task Status	Pulse One Status	۲
PES Ade_Pulse-106	PSA5000-V	9.0R3-13030	5d 20hr 20min	Restore Pending	Connected	040
PCS Ade_Pulse-109	PSA7000-V	9.0R3-13030	5d 20hr 18min		Connected	000
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	8

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 109**.

# 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 76.
- "Adding Appliances to an Appliance Group" on page 81.
- "Distributing a Master Configuration" on page 82.

## 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 106 Create Appliance Group

	ecure	DASHBOARD APPLIANCES	ANALYTICS ADMINIS	TRATION		Q DMIN
Applianc		5 CONFIG GROUPS	SOFTWARE BAC	KUP-RESTORE SCHEE	DULED TASKS	
Appliance Configuration	on Groups 🔿 💽 🖝	eate Appliance Group				
Name	Status	٢				
PPS-9.0R1-Group	Publish Required (i)	2	Please selec	t a group or a	dd one.	
			(			
			(			
			(			

The **Create Appliance Group Wizard** appears.

FIGURE 107 Create Appliance Group Wizard

Creating an appliance group An appliance group will use the base configuration from an applianc appliances in the group. This "master" appliance is used to edit confi You can decide which configuration settings that belong to the group selecting Edit appliance group from the actions menu for the group. You can add appliances to the group and remove them at any time.	figuration settings for the group. p in this wizard. You can edit wh	ich settings are used later by
An appliance group will use the base configuration from an applianc appliances in the group. This "master" appliance is used to edit confi You can decide which configuration settings that belong to the group selecting <b>Edit appliance group</b> from the actions menu for the group.	figuration settings for the group. p in this wizard. You can edit wh	ich settings are used later by
appliances in the group. This "master" appliance is used to edit confi You can decide which configuration settings that belong to the group selecting Edit appliance group from the actions menu for the group.	figuration settings for the group. p in this wizard. You can edit wh	ich settings are used later by
selecting Edit appliance group from the actions menu for the group.		, j
You can add appliances to the group and remove them at any time.	A group cannot be empty and m	nust contain the group master.
Cancel		< Previous Next

4. Click Next.

The Group name and description panel of the wizard appears.

Create Appliance	Group		
Introduction	Group name and description	Group configuration settings	Summary
Group name and de	scription		
Group name:	Group 2		
Description:	Optional short	description of the group	
DMI Information			
Username:	myadmin		
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 87.

### 6. Click **Next**.

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

FIGURE 109 Group Configuration Settings Wizard Panel

Create Appliance G	Group		
Introduction	Group name and description	Group configuration settings	Summary
Group configuration s	ettings		
Select master appliance:	Ade_Pulse-106		~
Master appliance URL:	https://10.64.	/admin	
elect from the list below to define the co	nfiguration settings to be used for the gro	up.	Reset
System			
<ul> <li>Authentication</li> <li>Administrators</li> </ul>			
Users			
Maintenance			
Cancel			< Previous Nex

- 7. In this panel:
  - For **Select master appliance**, select an appliance to be the master appliance.

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

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

https://<ip\_address>/admin

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

#### 8. Click Next.

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

FIGURE 110 Summary Wizard Panel
---------------------------------

Introduction	Group name and description	Group configuration settings	Summary
ummary			
Group name:	pps_group		Edit
Description:			Edit
Username:	100000		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 111	New Appliance Group
------------	---------------------

		DASHBOARD A	APPLIANCES	ANALYTICS	ADMINISTRATION		
Appliances	APPLIANCES	CONFIG GRO	UPS	SOFTWARE	BACKUP-RESTORE	SCHEDULED TASKS	
Appliance Configuration Groups       Name     Status       pps:group     In Sync	Oreate Ap     Oreate Ap     test     Target Appliances					Act	tions 🔻
	+ Add Appliance Status Name	Conf	fig State	Last Cor	ifig Upload		٥

You can now add appliances to the group as target appliances, see **"Adding Appliances to an Appliance Group" on page 81**.

## 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 112 Target Appliances Empty

		DASHBOARD APPLIANCE	ANALYTICS	ADMINISTRATION	
Appliances	APPLIANCES	CONFIG GROUPS	SOFTWARE	BACKUP-RESTORE	SCHEDULED TASKS
Appliance Configuration Groups	Create App	pliance Group			
Name Status	pps-group	( In Sync ) Publish All			Actions -
	Target Appliances	Group Configuration			
	+ Add Appliance				
	Status Name	Config State	Last Confi	ig Upload	۲

5. Click Add Appliance. A dialog appears.

FIGURE 113 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 114 Target Appliances Added

	DASH	IBOARD APPLIANCES AN	NALYTICS ADMINISTRATION	SETTINGS ADMIN
Appliances	APPLIANCES CO	DNFIG GROUPS SC	DFTWARE BACKUP-RESTORE	SCHEDULED TASKS
Appliance Configuration Group	OS 🔶 (🕀 Create Applianc	e Group		
Name         Status            PCS-Group         Publish Required ()         8	Docs	) Publish Required ) Pub	Publish All Publish Selected	Actions •
	+ Add Appliance	Config State	Last Config Upload	٢
	(Pts) Ade_Pr     (Pts) Ade_Pr     (Pts) Ade_Pr	ulse-109 Publish Required		View Changes

## **Distributing a Master Configuration**

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

- "Viewing Configuration Changes" on page 82.
- "Publishing Configuration Changes Manually to Group Members" on page 83.
- "Publishing Configuration Changes to Group Members as a Scheduled Task" on page 85.

#### **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.

	DASHBOAR	RD APPLIANCES ANALYTICS ADMINI	STRATION	SETTINGS ADMIN
Appliances	APPLIANCES CONFIG	GROUPS SOFTWARE B	ACKUP-RESTORE	SCHEDULED TASKS
opliance Configuration Group	S 🔶 (	P		
ame Status CS-Group Publish Required (i)	PCS-Group ( (i) Pub Docs	lish Required ) Publish All Publish S		Actions -
PS-9.0R1-Group In Sync	Target Appliances Group	Configuration		
ps-group In Sync 🕴	+ Add Appliance			
	Configuration Chang			Close Changes 8
	Modification Summary	Ade_Pulse-109	Group Config	uration
	Log > Events (modified) Log > User (modified) Log > Admin (modified)	Previous Configuration  12 <node>locslhost2</node> 13 <syslog-servers> 14 <syslog-server></syslog-server></syslog-servers>	13 <sy< td=""><td>n  Ade&gt;locslhost2 slog-servers&gt; syslog-server&gt;</td></sy<>	n  Ade>locslhost2 slog-servers> syslog-server>

### FIGURE 115 View Configuration Changes

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

### Publishing Configuration Changes Manually to Group Members

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

**Note:** Publishing to a group can also be performed as a scheduled task for groups. See **"Publishing Configuration Changes to Group Members as a Scheduled Task" on page 85**.

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 116 Publish All

Pulse Secure PULSE ONE		DASHBOARD APPLIANCE	ANALYTICS A	DMINISTRATION		
Appliances	APPLIANCES	CONFIG GROUPS	SOFTWARE	BACKUP-RESTORE	SCHEDULED TASKS	
Appliance Configuration Groups	Create Appl	liance Group				
Name         Status            PCS-Group         Publish Required (1)         5	PCS-Group	( (i) Publish Required )	Publish All Pu		Ac	tions 🔻
	Target Appliances	Group Configuration				
	+ Add Appliance					
	Status Name	Config Sta	te Last	Config Upload		٢
	Ad	de_Pulse-109 Publish Re	quired (i) 5d 2	2hr 29min	View Changes	000

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 117 Configuration Change in Member Appliance

	Pulse Secure	DASHBOAR	D APPLIANCES ANALYTICS ADMIN	ISTRATION	
Ар	pliances	APPLIANCES CONFIG	GROUPS SOFTWARE E	BACKUP-RESTORE	SCHEDULED TASKS
Appliance Co	nfiguration Groups	Create Appliance Group			
Name	Status	Status Name	Config State Last Config	g Upload	۲
PCS-Group	Publish Required 🕕 🕴	PPS Pulse-PPS-7			
PPS-9.0R1-Group	Configuration E Mismatch (1)	PP5 Pulse-PPS-7	Configuration Mismatch 6d 19hr 38	imin	(Close Changes)
pps-group	In Sync 8	Configuration Change	Keep Non-compliant Apply Group G	Config Context Size	5
		Modification Summary	Pulse-PPS-7	Group Config	guration
		MAC Addr Realms (Guest	Previous Configuration	New Configurati	on A
		Wired modified)	13 <device-check- interval&gt;60<th></th><th>ice-check- /device-check-</th></device-check- 		ice-check- /device-check-
			14 <device- server&gt;None 15 <directory-server>Guest Wired Authenticationserver&gt;</directory-server></device- 	15 <dir< td=""><td>ice- /device-server&gt; ectory-server&gt;Same rectory-server&gt;</td></dir<>	ice- /device-server> ectory-server>Same rectory-server>
			16 <dynamic-policy></dynamic-policy>	16 <dyn< th=""><th>amic-policy&gt;</th></dyn<>	amic-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 118 Configuration Mismatch

ontro	olled settings(s) t	hat have been changed on the appliance hbirdi-SA-1_38.101. This has caused hbirdi-SA	A-1_38.101 to be out of
	Appliance Co	nfiguration Group Configuration	
	Base Text	New Text	*
	1	<pre>1 sconfiguration multise"http://wnl.jouniper.new/iw-aw/i.107" multises.set=http://www.di.org/2001/2015Chema-instance" iveData="2335" saData="2224"&gt; 2 «dmin=roides 3 «dmin=roides 3 «dmin=roides 4 «dmin=roides 5 «dmin=roides 6 «canage=dmin=realms&gt; 6 «downard=rome=admin=realms&gt;falsedmin=roides 8 «alion=adis=/data=/data=&gt;falsefalsefalse 10 «decenve=adis=rome=admin=realms&gt;false «generalise/malle&gt; 12 «generalise(rome=align=false)/authentication= 12 «generalise(rome=align=false)/authentication= 13 «calon=adis=false=/acients&gt;false<td></td></pre>	
		14	
	. A	Appliance Co	Base Text     New Text     Configuration xmlns="http://xml.juniper.met/ive=ss/8.127"     xdimiarizationspr//xml.yd.exp/2001/XDLSchema-instance"     vebter=7187 schema=7224"     deamin=relamin     configuration     configura

#### 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 83**.

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 (<sup>§</sup>) for the appliance group you want to upgrade, and then click **Schedule Task**.

The **Create Task** dialog appears.

FIGURE 119	Create Publish Configuration Task	
------------	-----------------------------------	--

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

- 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 120 Scheduled Publish Configuration Task

Filter by:	Task Type:	Select Task Type	~	Apply Clear				
Task Type		Task Status	Schedul	ed Time	Appliance / Group	Comments	0	
Publish confi	guration	Success	20 <mark>18-10</mark>	-31 11:11:00 +0530	pcs-26-27	publish-group-26-27	2	Û

- 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 upgrade operations are supported. You can:

 Upload one or more appliance system software packages on Pulse One, see "Uploading an Appliance Software Package to Pulse One" on page 88.

**Note:** You must ensure that each appliance has its DMI enabled and configured correctly, see **"Checking DMI Settings" on page 90**.

 Upload one or more ESAP packages on Pulse One, see "Uploading an Endpoint Security Assessment Plug-In Package" on page 103.

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

- Upgrade a single appliance, see "Upgrading Software on an Appliance" on page 91.
- Upgrade all appliances in an appliance group, see "Upgrading Software on all Target Appliances in a Group" on page 93.
- Upgrade both appliances in a cluster, see "Upgrading Software on all Appliances in a Cluster" on page 95.
- 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 96.

## 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 121	Available Software
------------	--------------------

	<b>lse Secu</b>	re®	DASHBOARD	PPLIANCES ANALYTICS ADMI	NISTRATION		
Appl	iances	APPL	JANCES CONFIG GROU	JPS SOFTWARE	BACKUP-RESTORE SC	CHEDULED TASKS	
Available Softw			CS software) can be stored on Pul:	se One. **	<u>Downlo</u>	ad Appliance Softv	vare <sup>"Ľ</sup>
Туре	Version	Description	File Name	MD5 Hash	Created	Size	٢
Pulse Policy Secure	9.0R3	pps-90r3	package-51582,1.pkg	33ccf56b7843fed7f2688238236fc3bb	2018-10-23 11:55:48 +0530	1006.46 MB	
Fulse Folicy Secure	0.0000000	199-1-1-1-1-					

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.



Upload Softwa	are		×
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 123 Appliance Software Package Added

Available Softw	are + Add So	oftware			Download	l Appliance Soft	tware <sup>"L</sup>
** Only 3 software vers	sions of each type	(i.e. 3 PPS and 3 P	CS software) can be stored on Pul	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	Ш
Pulse Connect Secure	9.0R1	pcs-90r1	pcs_package_90r1_debug-6395	31ac7d82bc53e374a7f03e01fd85e595	2018-10-23 15:17:46 +0530	868.66 MB	10
Pulse Connect Secure	9.0R3-12402	pcs-90r3	pcs_90r3_debug_package-b124	6fdc23ba0424e7f75e70d7feb2032894	2018-10-23 12:11:56 +0530	936.52 MB	III

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**

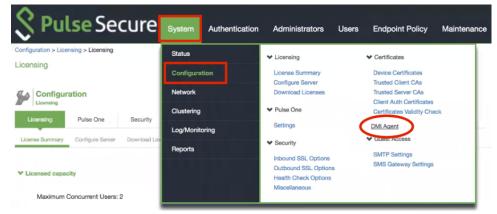
Before you can upgrade an appliance from Pulse One, you must ensure that the appliance has Device Management Interface (DMI) enabled and configured correctly.

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 124 Accessing Pulse Policy Secure DMI Agent Settings



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

FIGURE 125 Pulse Policy Secure DMI Agent Settings

Configuration > DMI Agent	
DMI Agent	
Configuration OM 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 a	nd configure Pulse Secure devices
Enter settings to enable the DMI Agent on this device and facilitate connection to a DMI-enabled management application.	
✓ Inbound connection status	
Connection State: Listening	
Number of Active Connections: 0	
✓ Outbound connection status	
Connection State: Disconnected Last Connection Time: Connected Server: Admin User Logged In:	
♥ DMI connections	
Inbound: 🕑 Enabled	
Outbound: Enabled	

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

FIGURE 126 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 35**. Specifically, you need the choice of whether to perform DMI over the internal port or the management port.

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

### Upgrading Software on an Appliance

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

**Note:** Alternatively, you can schedule one or more upgrade processes for a later time, see **"Scheduling Upgrade-Related Tasks" on page 96**.

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 88**.

**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 127 Available Appliances

	/	DASHBOARD APPLIANC	CES ANALYTICS	ADMINISTRATION	G SETTI	IGS ADMIN
Appliances	APPLIANCES	CONFIG GROUPS	SOFTWARE	BACKUP-RESTORE	SCHEDULED TASKS	Q SEARCH
Appliances + Add Appliance Export	$\Theta$					4 Appliances
Name			Model	Vers Last Config U T	Task Status Pulse One	Status ©
Ade_Pulse-106			PSA5000-V	9.0R 5d 18hr 53min	Connect	ted 🚦
PCS Ade_Pulse-109			PSA7000-V	9.0R 5d 18hr 50min	Connect	ted 🖇
Pulse-PPS-1			VA-SPE	9.0R 6d 15hr 57min	Connect	ted 🖁
Pulse-PPS-7			VA-SPE	9.0R 6d 15hr 54min	Connect	ted 🚦

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	re	х
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		
		upgrade

FIGURE 128 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 129 Up	ograde Pending
---------------	----------------

Appliances	+ Add Appliance	Export	$\Theta$			
Name	Model	Version	Last Config U	Task Status	Pulse One Status	0
PP5 pps-31	VA-SPE	5.4R3-45254	1hr 35min	Software upgrade Pending	Connected	ш
PP5 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 130 Appliance Rebooting

Appliances	+ Add Appliance	Export	$\Theta$	
Name	Model	Version	Last Config U Task Status	Pulse One Status
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 Software on all Target Appliances in a Group

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

The target appliances in the group are upgraded automatically.

**Note:** Alternatively, you can schedule one or more upgrade tasks for the master appliance at a later time, see **"Scheduling a Full Upgrade of an Appliance Group" on page 101**.

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 131 Available Appliance Groups

E Pulse Secure PULSE ONE	DASHBOARD APPLIANCES ANALYTICS ADMINISTRATION	Q admin
Appliances Appliances	CONFIG GROUPS SOFTWARE BACKUP-RESTORE SCHEDULED TASKS	
Appliance Configuration Groups 📀 💮 Greate	Appliance Group	
Name         Status         Image: Constraint of the state of the st	PCS-Group (① Publish Required ) Publish All Publish All Publish Science Action	ins <b>v</b>
	+ Add Appliance       StatusName     Config State       Last Config Upload	٢
	Ade_Pulse-109 Publish Required i 5d 23hr 45min View Changes	000
	Ade_Pulse-110 Publish Required      5d 23hr 44min     View Changes	000
	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 132 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 Software on all Appliances in a Cluster

Upgrading all appliances in a cluster is similar to the upgrade of a single appliance, see **"Upgrading Software on an Appliance" on page 91**.

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 96**.

# 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 97.
- "Scheduling a Full Upgrade from the Appliances Tab" on page 99.
- "Scheduling a Full Upgrade of an Appliance Group" on page 101.

### 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 133	Scheduled	Tasks

■ <b>Pulse Secure</b> *	DASHBO	ARD APPLIANCES	ANALYTICS ADMIN	ISTRATION		
Appliances	APPLIANCES CONF	G GROUPS	SOFTWARE I	BACKUP-RESTORE	SCHEDULED TASKS	_
Scheduled Tasks Create Task						
Filter by: Task Type: Select Task Type	Apply Clear					
Task Type Task Status	Target Version	Scheduled Time	Appliance / Group	Comments	۲	
No data to display						
0 total						_

3. Click Create Task.

The **Create Task** dialog appears.

FIGURE 134	Create	Task
------------	--------	------

Create Task		X
Choose Appliance or Group	Appliance Group	
Task Type:	Select Task Type 🗸	
Scheduled Time:	Jan 17, 2019	
Comments:		
	Cancel	ave

- 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 135 Scheduled S	Staging Task Added
------------------------	--------------------

Pulse Secure PULSE ONE	DASHBOA	RD APPLIANCES ANALYTICS	ADMINISTRATION	SETTINGS ADMIN
Appliances	APPLIANCES CONFIG	GROUPS SOFTWARE	BACKUP-RESTORE	SCHEDULED TASKS
Scheduled Tasks Create Task Filter by: Task Type: Select Task Type	Apply Clear			
Task Type Task Status	Target Version Scher	duled Time Applian	ce / Group Comments	٥
Stage a software package	2018-	0-24 00:00:00 +0530 pps-36	stage-pps	G. B
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 136 Scheduled Install Task Added
---

Pulse Secure PULSE ONE	2* D	ASHBOARD APPLIANCES	ANALYTICS ADM	INISTRATION		
Appliances	APPLIANCES	CONFIG GROUPS	SOFTWARE	BACKUP-RESTORE	SCHEDULED TASKS	
Scheduled Tasks Create Task						
Filter by: Task Type: Select Task Typ	le Apply	Clear	1			1
Task Type Task Status	Target Version	Scheduled Time	Appliance / Grou	up Comments	۲	
Stage a software package		2018-10-24 00:00:00 +0530	pps-36	stage-pps	ß	•
Install a staged package		2018-10-24 04:00:00 +0530	pps-39	install	C.	0
2 total						

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

#### Scheduling a Full Upgrade from the Appliances Tab

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

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

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

FIGURE 137 List of Appliances

E SPULSE Secure	DASHBOARD APPLIANC	ES ANALYTIC	5 ADMINISTRATION		
	CONFIG GROUPS	SOFTWARE	BACKUP-RESTORE	SCHEDULED TASKS	SEARCH
Appliances + Add Appliance Export 🕂					4 Appliances
Name		Model	Vers Last Config U 1	Task Status Pulse One S	Status 🔘
Ade_Pulse-106		PSA5000-V	9.0R 5d 18hr 53min	Connecte	ed å
Ade_Pulse-109		PSA7000-V	9.0R 5d 18hr 50min	Connected	ed 🕴
Pulse-PPS-1		VA-SPE	9.0R 6d 15hr 57min	Connecte	ed 🖁
Pulse-PPS-7		VA-SPE	9.0R 6d 15hr 54min	Connected	ed ê

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 138 Cr	eate Task
---------------	-----------

Create Task		
Schedule task for pps-36		
Task Type:	Select Task Type	•
Target Version:	Select Target Version	-
Scheduled Time:	Oct 24, 2018	
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 139 Scheduled Staging Task Added

Pulse Secure PULSE ONE	DASH	HBOARD APPLIANCES	ANALYTICS ADMIN	ISTRATION		
Appliances	APPLIANCES CO	ONFIG GROUPS	SOFTWARE	BACKUP-RESTORE	SCHEDULED TASKS	
Scheduled Tasks Create Task Filter by: Task Type: Select Task Type	- Apply Clea	ar				
Task Type Task Status	Target Version	Scheduled Time	Appliance / Group	Comments	۵	
Stage a software package		2018-10-24 00:00:00 +0530	pps-36	stage-pps	Ø	۵
1 total						

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

The **Create Task** dialog appears.

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

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

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

#### Scheduling a Full Upgrade of an Appliance Group

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

**Note:** Before you upgrade a group, you can optionally publish any configuration changes from the master appliance to all group members. This can be performed as a separate scheduled task. You can also choose to publish a configuration to a group at any other time, see **"Distributing a Master Configuration" on page 82**.

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

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

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

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

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

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

The **Create Task** dialog appears.

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

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

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

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

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

The **Create Task** dialog appears.

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

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

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

#### 9. Click Save.

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

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

## Uploading an Endpoint Security Assessment Plug-In Package

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

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

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

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

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

- Download the required ESAP package to local storage, see "Downloading an ESAP Package" on page 104.
- Upload the ESAP package to Pulse One, see "Uploading an ESAP Package to Pulse One" on page 104.
- Upload (and optionally activate) the ESAP package to individual appliances or appliance groups, see "Uploading ESAP Packages onto Appliances and Appliance Groups" on page 105.

#### Downloading an ESAP Package

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

1. Open the following page:

#### https://support.pulsesecure.net

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

After you have downloaded the ESAP package, you can upload it to Pulse One, see **"Uploading an ESAP Package to Pulse One" on page 104**.

#### Uploading an ESAP Package to Pulse One

The process of uploading an ESAP package to Pulse One is similar to the upload of system software to Pulse One, see **"Uploading an Appliance Software Package to Pulse One" on page 88**.

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

To upload an ESAP package to Pulse One:

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

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

3. Click Add Software.

The **Upload Software** dialog appears.

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

Note: The upload may take several minutes.

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

FIGURE 140 Appliance Software Package Added

Appli	ances	APPLIANCES	CONFIG GROUPS	SOFTWARE	BACKUP-RESTC	RE SCHEDU	ED TASKS	
Available Softwa	re + Add Software					Downlo	ad Appliance So	oftware 🖓
** Only 3 software version	ons of each type (i.e. 3 PP	S and 3 PCS software) can be stored	on Pulse One. **					
Туре	Version	Description	File Name	MD5 Hash		Ireated	Size	٢
ESAP Package	3.4.5	ESAP 3.4.5	ESAP3.4.5_dbg.pkg	30ed5c1ec13bbaf8	248d7eb146cd9c1c	019-10-01 10:23:35 +0530	39.27 MB	ŧ
ESAP Package	3.4.6	ESAP 3.4.6	ESAP3.4.6_dbg.pkg	eec297901756b02	953a3b41b1391c31 2	019-10-01 10:53:25 +0530	39.69 MB	444

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

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

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

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

After you have uploaded the ESAP package to Pulse One, you can upload (and optionally activate) individual appliances and appliance groups, see **"Uploading ESAP Packages onto Appliances and Appliance Groups" on page 105**.

#### Uploading ESAP Packages onto Appliances and Appliance Groups

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

- Upload (and optionally activate) ESAP on a single appliance, see **"Uploading an ESAP Package onto an Appliance" on page 106**.
- Upload (and optionally activate) on all appliances in an appliance group, see **"Uploading an ESAP Package onto all Target Appliances in a Group" on page 107**.
- Upload (and optionally activate) ESAP on both appliances in a cluster, see "Uploading an ESAP Package onto all Appliances in a Cluster" on page 108.

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

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

#### Uploading an ESAP Package onto an Appliance

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

Before you can perform an ESAP upload to an appliance, you must upload the required ESAP package onto Pulse One, see **"Uploading an ESAP Package to Pulse One" on page 104**.

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

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

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

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

3. Click the Actions icon for the required appliance, and then click Upload ESAP Package.

The Upload ESAP Package dialog appears.

4. For Select Software, choose the required ESAP package.

Full details for the selected package are displayed.

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

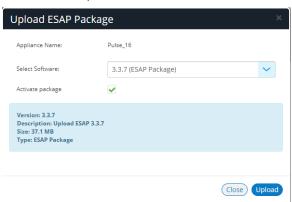


FIGURE 141 Upload Software

**Note:** If you do not select the **Activate package** check box, the package is uploaded but not activated. You can activate it later in the UI for the appliance. Please refer to the specific appliance product documentation for details of this procedure. 6. To start the upload/activation, click **Upload**.

. . . . . . .

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

Appliances (+ Add Appliance) Export							
Name	Model	Vers	Last Config U	Task Status	Pulse One Statu		
🖀 10_204_58_149 (PCS)	PSA3000-V	9.1R	3hr 51min	ESAP Upload Pending	Connected		
🛱 10_204_58_178 (PCS)	PSA3000-V	9.1R	3hr 39min		Connected		

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

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

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

#### Uploading an ESAP Package onto all Target Appliances in a Group

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

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

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

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

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

3. Click the **Actions** button for the required appliance group, and then click **Upload ESAP Package**.

The Upload ESAP Package dialog appears.

4. For **Select Software**, choose the required ESAP package for the upload.

Full details for the selected package are displayed.

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

#### FIGURE 143 Upload Software

Upload ESAP Pa	ckage		×
Appliance Name:	Pulse_16		
Select Software:	3.3.7 (ESAP Package)		~
Activate package			
Version: 3.3.7 Description: Upload ESAF Size: 37.1 MB Type: ESAP Package	9 3.3.7		
		Close Up	bload

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

- 6. To start the upload/activation, click **Upload**.
- 7. Click the **Appliances** tab.

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

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

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

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

#### Uploading an ESAP Package onto all Appliances in a Cluster

Uploading (and optionally activating) an ESAP package on all appliances in a cluster is similar to the ESAP upload of a single appliance, see **"Uploading an ESAP Package onto an Appliance" on page 106**.

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

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

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

In both cases, no reboot is required.

## Viewing the Activities Log for an Appliance

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

To view the activities log for an appliance:

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

The Appliances tab displays all current appliances.

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

For example:

FIGURE 144 Activities Details

Pulse Secure* PULSE ONE	DASHBOARD APPLIANCE	S ANALYT	TICS ADMINISTRATION	
Appliances Appliances	CONFIG GROUPS	SOFTWARE	BACKUP-RESTORE SC	Q, HEDULED TASKS SEARCH
Appliances + Add Appliance Export				4 Appliances
Name Model Last Config U Task Stat	us Pulse One Status 💿	<i>⊢</i> ,	Ade_Pulse-106 🔿	Actions -
C5 Ade_Pulse +SA5000-V 9 6d 42min	Connected 🕴		PLIANCE INFO	
PC5 Ade_Pulse PSA7000-V 9 6d 40min	Connected 🕴			
Pulse-PPS-1 VA-SPE 9 6d 21hr 47min	Connected 🕴	AC	TIVITIES	
Pulse-PPS-7 VA-SPE 9 6d 21hr 44min	Connected			Export
		Time	Activity	
		2019-0	01-16 13:58:42 ① Successfully u	ploaded backu
		2019-0	01-16 13:58:41 🕕 Successfully u	ploaded backu
		2019-0	01-16 13:58:41 ① Created backu	p file
		2019-0	01-16 13:57:42 ① Successfully u	ploaded backu
		2019-0	01-16 13:57:41 ① Successfully u	ploaded backu
		2019-0	01-16 13:57:41 ① Created backu	ip file
		2019-0	01-16 13:56:09 🕕 Task 358193ae	e-cd01-4556-89 Q

# 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 145 View Configuration Changes

Pulse Secure PULSE ONE	DASHBOARD APPLIA	NCES	ANALYTICS ADMINISTRATION	
Appliances Appliances	CONFIG GROUPS	SOF	-TWARE BACKUP-RESTORE SCHEL	Q DULED TASKS SEARCH
Appliances + Add Appliance Export				4 Appliances
Name Model Last Config U Task Sta	tus Pulse One Status	0	🖴 Ade_Pulse-109  🔶	Actions -
PLS Ade_Pulse PSA5000-V 9 6d 42min	Connected	000	APPLIANCE INFO	
PL5 Ade_Pulse PSA7000-V 9 6d 40min	Connected	88		
Pulse-PPS-1 VA-SPE 9 6d 21hr 47min	Connected	000	ACTIVITIES	<
Pulse-PPS-7 VA-SPE 9 6d 21hr 44min	Connected	000	CONFIGURATION HISTORY	$\sim$
			2019-01-10 17:31:45 +0000	Y
			Dashboard Settings (added)	€
			Status Settings (added)	€
		►	Oate and Time (added)	€
			Licensing Info (added)	⊕,
			Licensing Settings (added)	<b>⊕</b> ,
			Pulse One (added)	<b>⊕</b> ,
			SSL Options (added)	<b>⊕</b> ,
			Ø Health Check (added)	<b>⊕</b> ,
			Security Options (added)	€
			Device Certs (pulsesecure.net added)	€
			Auto-Import (added)	€

## **Comparing Appliances**

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

To compare two appliances:

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

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

- 3. Select the source appliance that you want to compare and click its **Actions** icon ( $\square$ ).
- 4. On the drop-down menu, click **Compare Appliances**.

FIGURE 146 Compare Appliances

Pulse Secure PULSE ONE	DASHBOARD APPLIANCES ANALYTICS ADMINISTRATION	SETTINGS ADMIN
	CONFIG GROUPS SOFTWARE BACKUP-RESTORE SCHEDULED	Q TASKS search
Appliances + Add Appliance Export		4 Appliances
Name Model Last Config U Task Sta	atus Pulse One Status 🐵 🗁 Ade_Pulse-109 🔶	Actions -
PLS Ade_Pulse PSA5000-V 9 6d 44min	Connected	
PLS Ade_Pulse PSA7000-V 9 6d 42min	Connected	<
Pulse-PPS-1 VA-SPE 9 6d 21hr 49min	Reboot Appliance	<
Pulse-PPS-7 VA-SPE 9 6d 21hr 46min	Edit Appliance Info Launch Appliance UI CONFIGURATION HISTORY	<
	Remove Appliance Compare Appliances Backup Configuration Upgrade Software Schedule Task	

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:

Appliance Configuration Com	parison	×
Differences Licensing Info (modified) Pulse One (modified) Device Certs (* p1qa.com added) Network (Vorview (modified) Internal Port (modified) Log > Events (modified) Log > Events (modified) Log > Admin (modified) Log > Admin (modified)	Ade_Pulse-109  Previous Configuration  revious Configuration  reviou	Ade_Pulse-106 New Configuration  record and a set of the set of th
Context Size 5		Close

FIGURE 147 Appliance Configuration Comparison

### **Rebooting an Appliance**

Rebooting an appliance is necessary when the services on the appliance must be restarted, or when there are other issues with an appliance that must be resolved.

After the reboot, the appliance will connect back to the network and Pulse One will indicate the status of the appliance in the dashboard.

To reboot an appliance:

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

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

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

4. On the drop-down menu, click **Reboot Appliance**.

00	S Pulse	Secure	•		DA	SHBOARD APPLIA	NCES A	NALYTICS AL	DMINISTRATION				
	Applian	ces		APPLIANCES	CONFI	G GROUPS	SOFT	WARE	BACKUP-RESTO	RE S	CHEDULED TASKS		Q
Appli	ances + Add App	liance Ex	port	$\mathbf{O}$								4	Appliances
Name		Model	Ver	Last Config U	Task Status	Pulse One Status	٢	🖨 Ade_P	ulse-109 🔿			Actie	ons 🗸
PES	Ade_Pulse-106	PSA5000-V	9.0R	6d 17hr 45min		Connected	000						
PES	Ade_Pulse-109	PSA7000-V	9.0R	6d 17hr 42min		Connected	000	APPLIANO	E INFO				$\sim$
PP5	Pulse-PPS-1	VA-SPE	9.0R	7d 14hr 50min		Reboot Appliance		2 🕾	0,	ዾ	7.54 🛆		
PP5	Pulse-PPS-7	VA-SPE	9.0R	7d 14hr 47min		Edit Appliance Info Launch Appliance l		Concurrent l	Jsers Auth Failu	ıres (24H)	kb/s Throughput		
						Remove Appliance Compare Appliance							
						Backup Configurati Upgrade Software Schedule Task		3% CPU Utilizat		% Utilization	26% Disk Utilization		

### FIGURE 148 Reboot Appliance

The **Reboot Appliance** confirmation dialog appears.

5. Ensure that you have selected the correct appliance and click **Yes**.

The selected appliance reboots.

## Removing an Appliance from Pulse One

If you no longer want to use an appliance with Pulse One, or want to re-provision it, you can remove the appliance.

To remove an appliance:

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

The Appliances tab displays all current appliances.

- 3. Select the appliance that you want to remove and click its **Actions** icon ( <sup>‡</sup> ).
- 4. Click **Remove Appliance to remove the appliance from Pulse One.**

100	S Pulse PULSE ONE	Secure			DA	SHBOARD APPLIA	NCES 4	ANALYTICS AD	MINISTRATION			
	Applian	ices		APPLIANCES	CONF	IG GROUPS	SOFT	TWARE	BACKUP-RESTORE	SCHEDULED TASKS		Q search
Appli	ances + Add App	bliance Ex	port	$\Theta$							4	Appliances
Name		Model	Ver	Last Config U	Task Status	Pulse One Status	٢	🖨 Ade_Pu	ılse-109 🕂		Actio	ons 🗸
PES	Ade_Pulse-106	PSA5000-V	9.0R	6d 17hr 45min		Connected	8					
PC5	Ade_Pulse-109	PSA7000-V	9.0R	6d 17hr 42min		Connected	000	APPLIANC	E INFO			~
PPS	Pulse-PPS-1	VA-SPE	9.0R	7d 14hr 50min		Reboot Appliance		2 将	0 ዶ	7.54 🛆		
PPS	Pulse-PPS-7	VA-SPE	9.0R	7d 14hr 47min		Edit Appliance Info		Concurrent L	sers Auth Failures (24H	) kb/s Throughput		
						Remove Appliance Compare Appliance Backup Configurat Upgrade Software Schedule Task	es	3% CPU Utilizati		26% Disk Utilization		

FIGURE 149 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 157**.

## 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 ( $\frac{1}{2}$ ) for the appliance you want to remove.

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

#### FIGURE 150 Remove from Group

= \$	Pulse Secu	re		DASHBOARD A	APPLIANCES	ANALYTICS	ADMINISTRATION		
A	ppliances	/	APPLIANCES	CONFIG GRC	DUPS	SOFTWARE	BACKUP-RESTORE	SCHEDULED TASKS	
Appliance	Configuration Gr	oups	Create	Appliance Group					
Name	Status		PCS-Grou	ID ((i) Publis	h Required )	Publish All	Publish Selected	Act	tions
PCS-Group	Publish Required (i)	000	Docs		, ritequireu ,				
PPS-9.0R1-Group	Mismatch Ignored 🕗	000	Target Applianc	es Group Cor	nfiguration				
pps-group	In Sync	000	+ Add Appliance						
			Status Nan	ne	Config State	I	ast Config Upload		٥
			• •	Ade_Pulse-109	Publish Requ	uired 🛈 🛛	5d 17hr 48min	View Changes	0
		4						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 151 Edit Group Configuration

III	S Pulse Secure	DASHBOARD APPLIANCES ANALYTICS ADMINISTRATION		Q admin
	Appliances	APPLIANCES CONFIG GROUPS SOFTWARE BACKUP-RESTORE SCHEDU	LED TASKS	
Applia	nce Configuration Group	S 🔶 (🖲 Create Appliance Group		
Name PCS-Group PPS-9.0R1-G pps-group	Status Publish Required () 3 Edit group configuration Delete group Schedule Task Upgrade Software	PCS-Group ( Publish Required )       Publish All       Publish Selected         Docs       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.	Act	ions -
		Config History (changes to be published)		
		2019-01-10 17:29:11 +0000		
		Dashboard Settings (added)		æ,
		Status Settings (added)		æ,
	•	Date and Time (added)		<del>Q</del>
		SSL Options (added)		æ,

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

FIGURE 152 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:	Justrin.	
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 (  $\frac{1}{2}$  ).

	S Pulse Secure	* D.	ASHBOARD APPLIANCES	ANALYTICS AI	DMINISTRATION	
	Appliances	APPLIANCES	CONFIG GROUPS	SOFTWARE	BACKUP-RESTORE	SCHEDULED TASKS
Applia	nce Configuration Grou	DS 🕂 🕀 Create	Appliance Group			
Name PCS-Group	Status Publish Required (1) 2	PPS-9.0R1-	Group (⑦ Mismatcl	n Ignored ) Put		Actions -
PPS-9.0R1-G	Froup Mismatch Ignored	Target Appliances	Group Configuration			
pps-group	Delete group Schedule Task Upgrade Software	Status Name	Config State	Last Config U	Jpload	٢
	opgrade solutione	PPS PL	Ise-PPS-7 Mismatch Ig	nored 🕐 🛛 7d 15h	nr 3min	View Changes

FIGURE 153 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	119
•	Viewing the Appliance Health Report	120
•	Viewing the Profiled Devices Report	122
•	Viewing the Appliance Activities Report	121
•	Viewing the User Activities Report	124
•	Viewing the UEBA Analytics Reports	125
•	Viewing Log Aggregation and Analysis	126
•	Viewing Services Logs	128
•	Viewing Appliance Activities	129

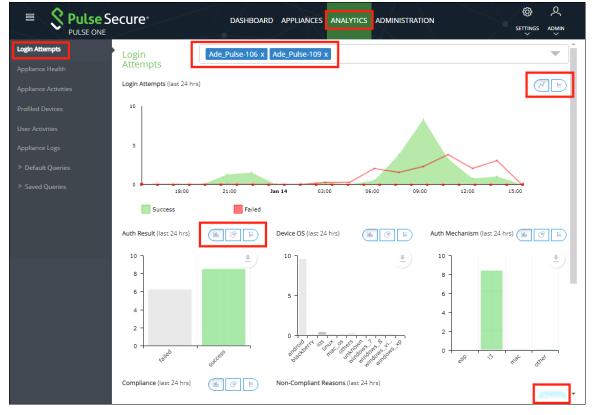
## Viewing the Login Attempts Report

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.





- 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:

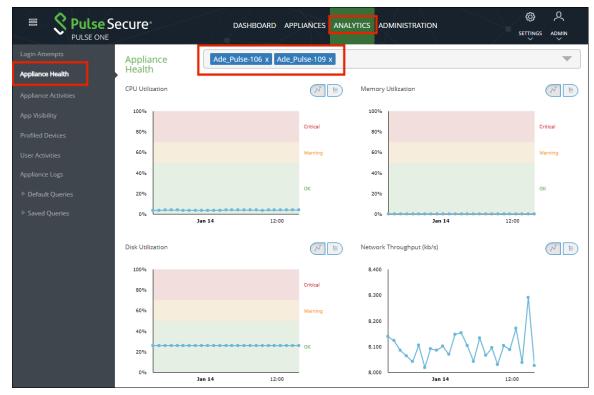
- 1. Select the **Analytics** menu.
- 2. Select Appliance Health.
- 3. From the Appliance Health drop-down, select one or more appliances for the report.

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 155 Appliance Health Report



# Viewing the Appliance Activities Report

To view the **Appliance Activities** report:

- 1. Select the **Analytics** menu.
- 2. Select Appliance Activities.

3. From the **Appliance Activities** drop-down, select the required filter (*Critical, Alert, Notice,* and so on) for the report.



E Pulse S PULSE ONE	ecure	DASHBOARD	APPLIANCES ANALYTICS	ADMINISTRATION	
Login Attempts	Appliance Activities	Critical 🗸	Export		<u>^</u>
Appliance Health	13 12 10	Critical Informational			1
Appliance Activities Profiled Devices	11 D 82 7 66 4 4 19 1	Alert Notice Warning			
User Activities	Men 17 Wed 19	Error Emergency Debug	Thu 27 Set 29 Mon 31 2019	Thu 03 Sat 05 Mon 07 Wed	09 Fri 11 Jan 13
Appliance Logs	2019-01-13T21:07:39Z	Ci Virtual Appliance li	censed with 4 CPU cores, but on	ly provisioned with 2 CPU core(s)	Ade Pulse-106
♥ Default Queries Compliance Failure	2019-01-13T21:04:18Z			ly provisioned with 2 CPU core(s)	Ade_Pulse-109
, Compliance Failure Per User Compliance Success	2019-01-13T20:45:56Z	O Virtual Appliance li	censed with 8 CPU cores, but on	ly provisioned with 2 CPU core(s)	Pulse-PPS-1
Compliance Success Per U	2019-01-13T20:08:51Z	් Virtual Appliance li	censed with 8 CPU cores, but on	ly provisioned with 2 CPU core(s)	Pulse-PPS-7
Login Failure Login Failure Per User	2019-01-12T21:07:18Z	් Virtual Appliance li	censed with 4 CPU cores, but on	ly provisioned with 2 CPU core(s)	Ade_Pulse-106
Login Success Login Success Per User	2019-01-12T21:03:56Z	් Virtual Appliance li	censed with 8 CPU cores, but on	ly provisioned with 2 CPU core(s)	Ade_Pulse-109
Logout	2019-01-12T20:45:33Z	් Virtual Appliance li	censed with 8 CPU cores, but on	ly provisioned with 2 CPU core(s)	Pulse-PPS-1
Logout Per User ▼ Saved Oueries	2019-01-12T20:08:23Z	O <sup>r</sup> Virtual Appliance lie	censed with 8 CPU cores, but on	ly provisioned with 2 CPU core(s)	Pulse-PPS-7
Surce quenes	2019-01-11T21:06:58Z	Ö Virtual Appliance li	censed with 4 CPU cores, but on	ly provisioned with 2 CPU core(s)	Ade_Pulse-106

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

## Viewing the Profiled Devices Report

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

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

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

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

For details about registering the Pulse Policy Secure appliance, see **"Registering an Existing PCS/PPS Appliance" on page 35**.

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.

E S Pulses	Secure	DASHBOARD	APPLIANCES	ANALYTICS	5 ADMINISTRA	πιον		MIN
	Profiled Devi	ices						
	Filter	Collector T	ype: Any	<b>~</b>	Apply Clear		Ехро	æ
Appliance Activities	Applian M	MAC A IP	Host Na	OS	Ca Manuf	. First Seen	Last Seen	
Profiled Devices	pps-171 6	8:f7:2 10	Shahee	Wi V	Vi LCFC(	2017-11-2	2017-11-2	-
	pps-171 8	c:70:5	KAJAL	Wi V	Vi Intel C	2017-11-2	2017-11-2	Ε
	pps-171 0	0:50:5 10	appserver	Wi V	Vi VMwa	2017-12-0	2017-12-0	
	pps-171 0	c:o4:7 10		PXE N	le Super	2017-11-2	2017-11-2	
▷ Default Queries	pps-171 0	c:o4:7 10		PXE N	le Super	2017-11-2	2017-11-2	
Saved Queries	pps-171 0	0:50:5 10	gpratee	Wi V	Vi VMwa	2017-11-2	2017-11-2	Ŧ
	20 🗸 Re	cords per page Total recor	de: 179	F	irst Previous 1	2 3 4 5	Next	
	Device Details			L	ast			
	DHCP Details	SNMP Details	NMAP Details	User Agent	History W	MI Details		
	Classified C	Classified OS	Request	Combinat	Message Type	Options	Vendor	
	Network Boo	PXE	10.204	3547929	3	1,2,3,4,5,6,11,1	PXECIi	

FIGURE 157 Profiled Devices

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

# Viewing the User Activities Report

Pulse One administrators can aggregate user activities information as consolidated reports in Pulse One.

**Note:** Displayed information is based on data from registered appliances with version 9.0R1 or above.

This report provides the aggregated view of list of all users and their last login activities, compliance status, session length, appliance names, login success and failures.

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

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

To view the **User Activities** report:

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

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

## Viewing the UEBA Analytics Reports

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

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

Pulse One supports the following analytics reports:

• The Behavioral Analytics (User Anomalies) report.

To view this report, click the **Analytics** tab, and then click the **User Anomalies** report. For example:

#### FIGURE 158 Behavioral Analytics User Anomalies Report

	ecure		DASHBOARI	D APPLIANCES ANALYTICS		TION			ې admin
Login Attempts	Behavioral Analytics (	User Anomalies)							Â
Appliance Health	Time Frame: Last 30 Days	Vsername:	Recent IP Ad	dress: Re	ecent MAC Addre	55:	Recent Location:	Apply Clear	- 1
Appliance Activities	Username	Anomalies Count	Recent Appliance	Recent Anomaly Detection T	Status	Recent IP Address	Recent MAC Address	Recent Location	
App Visibility	UEBA\hdarshan	2	darshan	2019-12-24 04:57:23 +0000	Active	172.21.8.58	a0: 6b	Unknown	0
Profiled Devices	UEBA\user1	7	darshan	2019-12-27 07:12:33 +0000	Active	172.21.8.95	8c: :31	Bangalore	0
User Activities	autouser1	3	darshan	2020-01-07 06:23:36 +0000	Active	10.204.90.222	00: :0f	Mumbai	0
<ul> <li>Behavioral Analytics</li> <li>User Anomalies</li> </ul>	d	6	darshan	2020-01-10 06:42:26 +0000	Active	10.96.202.9	00: :33	Delhi	0
Device Anomalies									
Appliance Logs									- 1

• The Behavioral Analytics (Device Anomalies) report.

To view this report, click the **Analytics** tab, and then click the **User Anomalies** report. For example:

FIGURE 159 Behavioral Analytics Device Anomalies Report

= S Pulse S	ecure	$\pi$	DASHBOARD APPLI	ANCES ANALYTICS	ADMINISTRATION				© ♀ settings admin ♡
Login Attempts	Behavioral Analy	tics (Device Anomalies)							
Appliance Health	Time Frame: Last 30	Days 💙 MAC Address:	Device Category:	R	ecent IP Address:	Recent	Location:	Apply (	llear
Appliance Activities	MAC Address	Device Category	Recent Appliance	Anomalies Count	Recent Anomaly Detection T	Status	Recent IP Address	Recent Location	
App Visibility	00: :0f	VoIP Phones/Adapters	darshan	681	2020-01-07 06:23:36 +0000	Active	10.96.	Unknown	Ø
Profiled Devices	Unknown	Unknown	darshan	19	2020-01-07 09:30:07 +0000	Active	10.96.	Bangalore	Ø
User Activities	00: 54	Unknown	darshan	8	2020-01-07 09:50:59 +0000	Active	10.96	Unknown	0
♥ Behavioral Analytics	a0: 0c	Windows	darshan	7	2020-01-07 06:23:36 +0000	Cleared	172.21.	Hyderabad	Ø
Device Anomalies Appliance Logs									

**Note:** You can also view a dashboard of graphs and maps for UEBA anomalies, see "Viewing UEBA Metrics" on page 23.

# Viewing Log Aggregation and Analysis

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

Note: To view logs output by Pulse One, see "Viewing Services Logs" on page 128.

#### FIGURE 160 Appliance Logs

	cure			DASI	HBOARD APPLIANC	ES ANALY	YTICS ADMINISTRATION
Login Attempts	Applia	nce Lo	gS Save Q	uery			
Appliance Health	Match	n ALL					From Dec 18, 2018 11:48:31 to Jan 17, 2019 11:48:31
Appliance Activities	Qs	earch					
App Visibility	Count		Select Field		Group	Select F	Field - Search
Profiled Devices	By:		, ciccer reid		By:	beleeer	
User Activities	Priority	Facility	Time	Source	User	Event ID	Message
Appliance Logs							
♥ Default Queries	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 Failure Per Compliance Failure Per	Major	local0	2019-01-17 11:48:07 +0000	10.64.26.47	System () []	SYS31126	Error generating data for chart cloud_secure_auth_result
Compliance Success Per Login Failure	Major	local0		10.64.26.47	System () []	SYS31126	Error generating data for chart cloud_secure_compliance
Login Failure Per User Login Success			11:48:07 +0000				
Login Success Per User	Major	local0	2019-01-17	10.64.26.47	System () []	SYS31126	Error generating data for chart cloud_secure_os_type
Logout Logout Per User			+0000				
♥ Pulse One ♥ Services Logs All	Major	local0	2019-01-17 11:48:07 +0000	10.64.26.47	System () []	SYS31126	Error generating data for chart cloud_secure_os_version
▼ Saved Queries							

The system provides a set of **Appliance Logs > Managed Appliances > Default Queries** in the navigation pane.

To view logs from any of the default queries, expand **Appliance Logs > Default Queries** and click on the required query.

The Administrator can also customize the queries and save them for future use. These customized queries are then listed below **Saved Queries**, see **"Working with Log Queries" on page 127**.

#### Working with Log Queries

The **Appliance Logs > Default Queries** page supports filtering using a string token. Type the token in the search bar or double-clicking a string in the logs details. The view is then filtered to display all messages with the token that is being searched for. Users can enter multiple tokens separated by space.

This customized query can then be saved using **Save As**.

To view logs from a customized query, expand **Saved Queries** and click on the required query. For example:

FI	GURE 161 Save Qu	Jery								
	♥ Managed Appliances Compliance Failure Compliance Failure Per Compliance Success	Prior	Facility	Time	Source	User	Event ID	Message		
Compliance Success Compliance Success Per Login Failure	Save	Save Query X								
	Login Failure Per User Login Success Login Success Per User Logout	Name	2:	mySav	edQuery					
							(	Cancel Save		
	All <sup>♥</sup> Saved Queries mySavedQuery	Major	local0	2019-01- 14 17:27:56 +0000	10.64.26.47	System () []	SYS31126	Error generating dat	ta foi	

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

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

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

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

# Viewing Services Logs

The logs generated by Pulse One can be viewed in **Appliance Logs > Default Queries > Pulse One > Services Logs**. These log entries fall into two categories:

- Services logs generated by Pulse One.
- Unitycom logs generated by Pulse One.

**Note:** To view logs output by appliances that are registered on Pulse One, see **"Viewing Log Aggregation and Analysis" on page 126**.

#### FIGURE 162 Services Logs

🔳 🤶 Pulse S	ecure <sup>*</sup>	DASHBOARD APPLIAN	CES WORKSPACES ANALYTICS	ADMINISTRATION	<u>م</u> ک
PULSE ONE					
Login Attempts	Appliance Logs All Sav	e As			
Appliance Health	Match ALL		From	Sep 11, 2019 13:39:00 to Oct 11, 2	2019 13:39:00
Appliance Activities	Q uno_pws-api_1 × IN	FO × Search			
App Visibility					
Profiled Devices	Time	Application Name	Message		
User Activities	2019-10-11 12:39:38.000	docker/uno_pws-api_1		1 12:39:38,320 INFO [pws.api.sa.app] Author cure_CloudSecureMappingApi', 'POST') with >,	
opliance Logs	2019-10-11 12:39:32.000	docker/uno_pws-api_1		1 12:39:32,462 INFO [pws.api.sa.app] Author cure_CloudSecureMappingApi', 'POST') with >,	
<sup> </sup>	2019-10-11 12:39:28.000	docker/uno_pws-api_1	docker/uno_pws-api_1 2019-10-1 Starting new HTTP connection (1):	1 12:39:28,343 INFO [requests.packages.urllil log_indexer	o3.connectionpool]
Compliance Failure Compliance Failure Per Compliance Success	2019-10-11 12:39:28.000	docker/uno_pws-api_1	docker/ <mark>uno_pws-api_1</mark> 2019-10-1 Starting new HTTP connection (1):	1 12:39:28,578 INFO [requests.packages.urlli elasticsearch	o3.connectionpool]
, Compliance Success Per Login Failure	2019-10-11 12:39:28.000	docker/uno_pws-api_1	docker/ <mark>uno_pws-api_1</mark> 2019-10-1 stats.pws_api_sa_stats_StatsApi', 'F	1 12:39:28,550 INFO [pws.api.sa.app] Author POST') with >, >]> as	zing ('sa-
Login Failure Per User Login Success Login Success Per User Logout	2019-10-11 12:39:28.000	docker/uno_pws-api_1		1 12:39:28,340 <mark>INFO</mark> [pws.api.logsearch.app] ogSearchQueryApi', 'POST') with > as ], permis	
Logout Per User ▼ Pulse One	2019-10-11 12:39:28.000	docker/uno_pws-api_1	docker/ <mark>uno_pws-api_1</mark> 2019-10-1 Starting new HTTP connection (1):	1 12:39:28,556 INFO [requests.packages.urlli elasticsearch	o3.connectionpool]
♥ Services Logs All	2019-10-11 12:39:28.000	docker/uno_pws-api_1	docker/uno_pws-api_1 2019-10-1	1 12:39:28,464 INFO [pws.api.sa.app] Author	zing ('sa- 🗸
♥ Saved Queries	Rows per page: 50	·		First Previous 1	2 3 4 5 Next

The system provides **Default Queries > Pulse One > Services Logs** in the navigation pane.

To view logs from any of the default queries, expand **Service Logs > Default Queries** and click on the required query.

The Administrator can also create custom queries and save them for future use. These customized queries are then listed below **Saved Queries**, see **"Working with Log Queries" on page 127**.

## **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.

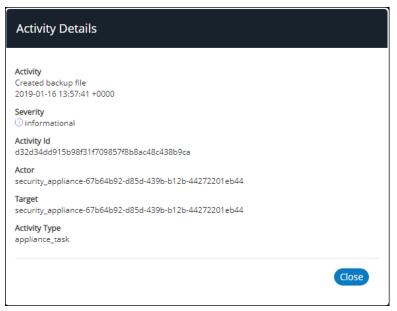
#### FIGURE 163 Filter Activities

E SPulse Se PULSE ONE	cure	ASHBOARD APPLIANCES ANALYTICS ADMINISTRA	TION SETTINGS ADMIN
User Management	Activities		
Role Management	Q Search	×	⑦ ♣ * ▲ ♂ ⑨ ♣ ♥ Export
Appliance Activities	Time	Activity	Appliance
	2019-01-09 20:17:44 +0000	① Rendering new configuration.	Pulse-PPS-7
	2019-01-09 20:15:39 +0000	① Pending configuration has been created.	Pulse-PPS-7
	2019-01-09 20:15:38 +0000	① Rendering new configuration.	Pulse-PPS-7
	2019-01-09 20:13:44 +0000	① 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	$\vec{O}^{\rm S}$ Virtual Appliance licensed with 8 CPU cores, but only provision	on 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 164 Activity Details



# User Management

•	Adding an Admin User	131
•	Editing User Details	132
•	Removing an Admin User	133
•	Resetting a User Password	133
•	Suspending a User	134

## Adding an Admin User

To add an admin user:

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

A list of existing admin users is displayed.

3. Click Add User to add an admin user.

The Add Admin User window appears.

GURE 165 Add A	Admin User	
Add Admin User		
Username:	po-user1	
Role	Read Only Admin	~
Full Name:	Pulse One User-1	
Email:	pouser1@company.com	
Sign In Method:	Enterprise SSO	~
		(Cancel) Cre

**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 166 Edit User Details

E SPULSE SO	ecure	DASHBOARD APPLIANCE	S ANALYTICS ADMIN	IISTRATION	SETTINGS ADMIN
User Management	Admin Users Q Search	× Add Us	er Delete User	>	2 Total Admin users
Role Management Appliance Activities	User Role admin Super Admin	P	ulse One User-1	ify Group Activities 🛛 Edit Re	set 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	
				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 167 Reset Login

E SPULSE SO	ecure dashe	OARD APPLIANCES ANALYTICS A	
User Management	Admin Users Q Search	X Add User Delete User	2 Total Admin users
Role Management	User Role	Pulse One User	
Appliance Activities	admin Super Admin		Verify Group Activities 🖉 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 Pulse S PULSE ONE	ecure		DASHBOARD APPLI	ANCES	ANALYTICS	ADMINISTRATION	ی settings admin
User Management	Admin Us	ers Q Search	× (	dd User	Delete User	$\Theta$	2 Total Admin users
Role Management	User	Role		Pu	lse One User	r-1	
Appliance Activities	admin	Super Admin				Verify Group Activities	Edit Reset login Suspend User
	Pulse One	Read Only Admin			Username:	po-user1	
					Full Name:	Pulse One User-1	
					Email:	pouser1@exampl	le.com
					Role:	Read Only Admin	
					Sign In Method:	Enterprise SSO	
				•	Status:	Unlocked	

FIGURE 168 Suspend User

# Role Management

•	Adding an Admin Defined Role	135
•	Editing an Admin Role	136
•	Removing an Admin Role	136

## 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 169 Create New Role

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

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 170 Modify Role

■ <b>Pulse Se</b> PULSE ONE	ecure <sup>®</sup> D	ASHBOARD APPLIAN	ICES ANALYTICS ADMINISTRATION	
User Management	Role Management Add Role	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	el

## 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	137
•	Editing Pulse One Properties	137
•	Understanding Pulse One Properties	138

### **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 171 Pulse One Properties

	CUIC DASHBOARD APPLIANCES ANA WORKSPACES ANALYTICS ADMINISTRATIO	N	© SETTINGS	
Pulse One Properties	Pulse One Properties Whitelist	Pulse One Properties	5	
Workspace Properties	Pulse One Properties	Workspace Propertie	15	
LDAP Groups		LDAP Groups Apple		llapse All
Apple	Name Value	CA Certificate		۲
CA Certificate	⊞ Enterprise Connections (5)	Android Enterprise Enterprise Usage Agreement		
Android Enterprise	Password (9)	VPN Cert		
Enterprise Usage Agreement				
VPN Cert	⊕ Session (1)			

# **Editing Pulse One Properties**

To edit a Pulse One property:

- 1. View Pulse One properties, see Viewing Pulse One Properties<XREF>.
- 2. Click the **Edit** ( $\square$  button corresponding to the field you want to edit.
- 3. Change the value and then click **Save**. For example:

#### FIGURE 172 Edit Properties

🗧 🤇 Pulse Se		@ / Q
PULSE ONE	Edit Property	
Pulse One Properties		_
	Auto Configure SAML settings:   Ves  No	Expand All Collapse All
	Cancel	) Save
	Auto Configure SAML settings Yes	

## **Understanding Pulse One Properties**

All Pulse One properties are described in the following sections:

- "Enterprise Connection Properties" on page 138
- "Password Properties" on page 138
- "Miscellaneous Properties" on page 139
- "Session Properties" on page 139

#### **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 154**.

- **SAML Identity Provider** The Pulse Connect Secure appliance that is configured for Pulse One server SAML auto-provisioning.
- **SAML Identity Provider Metadata** Required metadata for the SAML identity provider.
- **SAML Service Provider Metadata** Required metadata for the SAML service provider.

#### **Password Properties**

The **Password** settings are described below:

- Console Minimum Password Length The minimum length of a console password.
- **Console Password Expiration Days** The number of days after which an Administrator must change their console password.
- **Console Password Require Lowercase** Boolean. If *True*, the console password must contain at least one lowercase letter.
- **Console Password Require Number** Boolean. If *True*, the console password must contain at least one number.
- **Console Password Require Special** Boolean. If *True*, the console password must contain at least one special character.

- **Console Password Require Uppercase** Boolean. If *True*, the console password must contain at least one uppercase letter.
- **Console Password Reset Timeout Hours** The number of hours a console password reset email link is valid.
- **Domain Allowed Password Attempts** The number of login attempts until a console account is locked.
- Welcome Timeout Hours The number of hours a registration token in a welcome email is valid.

#### **Miscellaneous Properties**

The miscellaneous (Misc) settings are described below:

- Created On The date on which the management console was created.
- Locale The console language code.
- Page Footer The footer information that will be displayed at the bottom of the admin console.
- **Server Version** The current Management Server version that will be displayed at the bottom of the admin console.

Note: You cannot edit the Created On and Server Version properties.

#### **Session Properties**

The Session properties are described below:

• Session idle timeout (minutes) – The timeout for an idle session. After this timeout is reached, the user is logged out automatically. The default is 20.

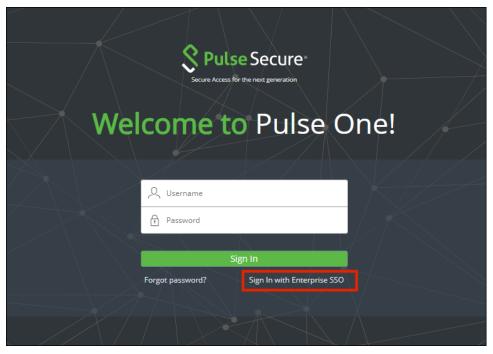
# Configuring Enterprise SSO Using SAML

•	Overview	141
•	Configuring SAML idP in Pulse Connect Secure Server	142
•	Automatically Configuring a SAML idP on Pulse One	146
•	Configuring a Metadata Provider in Pulse Connect Secure	148
•	Enabling Enterprise SSO in Pulse One Appliance	149
•	Configuring SAML Metadata in Pulse One	149
•	Adding SAML SP Metadata in Pulse Connect Secure Server	150
•	Automatically Creating Pulse One Users for SAML SSO Logins	154
•	Testing Sign In with Enterprise SSO	156

### 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 173 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 142.
- "Automatically Configuring a SAML idP on Pulse One" on page 146.
- (Optional) "Automatically Creating Pulse One Users for SAML SSO Logins" on page 154.
- "Testing Sign In with Enterprise SSO" on page 156.

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 142.
- "Configuring a Metadata Provider in Pulse Connect Secure" on page 148.
- "Enabling Enterprise SSO in Pulse One Appliance" on page 149.
- "Configuring SAML Metadata in Pulse One" on page 149.
- "Adding SAML SP Metadata in Pulse Connect Secure Server" on page 150.
- (Optional) "Automatically Creating Pulse One Users for SAML SSO Logins" on page 154.
- "Testing Sign In with Enterprise SSO" on page 156.

## 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 35**.

**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 174	SAML	Settings
------------	------	----------

Secure		Administrators	Users	Pulse Connect		1.4
System A	uthentication	Administrators	Users	Maintenance	Wizards	
SAML> Settings						
♥ Metadata Server Configuration						
Timeout value for metadata fetch request 300 seconds	1 - 600. Specifies th	ne time in seconds to wait	for response of	SAML metadata fetch re	quest.	
Validity of uploaded/downloaded metadata file: 0 days		the time in days after whic force any validity on the pe			cpires. O means the	at Connect
Host FQDN for SAML:	The FQDN used for	rgenerating URLs for SAN	IL services.			
Alternate Host FQDN for SAML:	The FQDN used for	rgenerating SA's Single Si	gn-On Service	URL when Pulse(NC) Se	ession 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.

<	<b>Pulse Secu</b>	ro				Puise Con		
v	FuiseSecu	System Auth	entication Administr	ators Users	Maintenance	Wizards		-
nfigu	ration > Certificates > Device Certificate							
evic	e Certificate							
		curity Certificates	DMI Agent NCP	Sensors	Client Types	Pulse Collaboration	Virtual Desktops	
IKE	Ev2 SAML Mobile	VPN Tunneling Tel	demetry Advanced Clie	ent Configuration				
evic	e Certificates Trusted Client CAs Tru	usted Server CAs Code-signing C	Certificates Client Auth Certific	ates Certificates Validi	tv Check			
_								
	records per page					Searc	sh:	
		Issued by	X	/alid Dates		Searc Used by	sh:	
10	✓ records per page	Issued by posqalab-CA	4	/alid Dates Aug 30 06:06:04 2017 GI 2019 GMT	MT to Aug 30 08:06:04	Used by	dh:	
10	records per page Certificate issued to		CA A	Aug 30 06:06:04 2017 GI	-	Used by <internal port=""></internal>	1	
10	records per page Certificate issued to     records net	posqalab-CA	CA A	Aug 30 06:06:04 2017 Gi 2019 GMT vlay 2 15:18:09 2016 GM	IT to Apr 9 17:22:15 20	Used by <internal port=""></internal>	1	
10	records per page Certificate issued to     * secure net     * fast sequeerserv.com	progelab-CA EnterpriseSub2-C		Aug 30 06:06:04 2017 Gi 2019 GMT May 2 15:18:09 2016 GM GMT <b>A</b> Det 30 08:53:19 2017 GN	IT to Apr 9 17:22:15 20	Used by <internal port=""> 18 VP1, <external port<="" td=""><td>1</td><td></td></external></internal>	1	
10	records per page Certificate issued to      * psecure.net      * test.sequoertserv.com      10.30.	pagalab-CA EnterpriseSub2-C EXCHSRVCA	DA A C	Aug 30 06:06:04 2017 GI 2019 GMT May 2 15:18:09 2016 GM SMT Dot 30 08:53:19 2017 GM 2019 GMT Dot 30 09:02:41 2017 GM	IT to Apr 9 17:22:15 20 AT to Oct 30 08:53:19 AT to Oct 30 09:02:41	Used by <internal port=""> 18 VP1, <external port<="" td=""><td>1</td><td></td></external></internal>	1	

FIGURE 175 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 176 Basic Identity Provider Configuration

<u>.</u>	~					Puise Co	nnect Secure	
S Puls	e Secu		A	Administrators			14/id-	1
		System	Authentication	Administrators	Users	Maintenance	Wizards	
igning In								
Sign-in Policies	Sign-in Pages	Sign-in Notificatio	ons Sign-in SAML					
Metadata Provider	entity Provider		•					
l Basic Identity Prov	vider (idP) Configura	ation (Rublished in M	letadata)					
✓ Basic Identity Pro	vider (idP) Configura	ation (Published in M	letadata)					
, i			letadata)					
✓ Basic Identity Prov Protocol Binding to us Post			letadata)					
Protocol Binding to us			letadata)					
Protocol Binding to us		•	<b>ietadata)</b> r signing SAML messages se	nt by this IdP				
Protocol Binding to uz Post Ø Artifact	• for SAML Response	Certificate to use fo     Certificate to use fo	·		by the Peer Se	arvice Provider (SP). This	certificate is used by t	he peer SP to
Protocol Binding to us Post Artifact Signing Certificate:	e for SAML Response	Certificate to use fo     Certificate to use fo     encrypt the data in t	r signing SAML messages se r decrypting the encrypted da the SAML messages	ta in SAML messages sent				
Protocol Binding to us Post Artifact Signing Certificate: Decryption Certificate:	e for SAML Response pulsesecure.net No Encryption	Certificate to use fo     Certificate to use fo     encrypt the data in 1     If enabled, the user     disabled in Peer SP	r signing SAML messages se r decrypting the encrypted da the SAML messages 's existing NC (Pulse) session 'configuration.	ta 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 Reuse Existing N	e for SAML Response pulsesecure.net No Encryption C (Pulse) Session	Certificate to use fo Certificate to use fo encrypt the data in 1 If enabled, the user disabled in Peers P If both options are s	r signing SAML messages se r decrypting the encrypted da the SAML messages 's existing NC (Pulse) session - configuration. selected, the priority is given to	it any will be used in the S "Reuse Existing NC (Puls	P-initiated SSC			
Protocol Binding to use Post Artifact Signing Certificate: Decryption Certificate: Other Configurations Reuse Existing N Accept unsigned.	for SAML Response     pulsesecure.net     No Encryption     C (Pulse) Session AuthnRequest	<ul> <li>Certificate to use fo</li> <li>Certificate to use fo</li> <li>encrypt the data in the user disabled in Peer SP</li> <li>If both options are so Individual SPs can</li> </ul>	r signing SAML messages se r decrypting the encrypted da the SAML messages 's existing NC (Pulse) session 'configuration.	if any will be used in the S "Reuse Existing NC (Puls thnRequest.	P-initiated SSC e) Session".	) scenario, instead of aut	henticating the user ag	ain. Can be
Protocol Binding to us Post Artifact Signing Certificate: Decryption Certificate: Other Configurations Reuse Existing N	for SAML Response     pulsesecure.net     No Encryption     C (Pulse) Session AuthnRequest	Certificate to use fo Certificate to use fo encrypt the data in 1 If enabled, the user disabled in Peer SP If both options are s Individual SPs can If enabled, SAML as assertion.	r signing SAML messages se r decrypting the encrypted da the SAML messages 's existing NC (Putse) session 'configuration. relected, the priority is given to choose to accept unsigned At	ta in SAML messages sent if any will be used in the S p "Reuse Existing NC (Puls othnRequest. ong with signing the SAML	P-initiated SSC e) Session". response by de	) scenario, instead of aut afault.Individual SPs can	henticating the user ag	ain. 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:** If the PCS server is already configured as a SAML identity provider, make sure that POST binding is enabled and the **Accept Unsigned AuthnRequest** option is selected.

- Select a Signing Certificate from the list.
- For **Decryption Certificate**, select No Encryption.
- Clear the Reuse Existing NC (Pulse) Session check box.
- Select the Accept Unsigned AuthnRequest check box.

For more details, refer to the "Configuring Sign-in SAML Identity Provider Settings" section in the *Pulse Connect Secure Administration Guide*.

9. Click **Save Changes** to save the Identity Provider configuration.

## Automatically Configuring a SAML idP on Pulse One

**Note:** This section is only applicable if your PCS appliance is at v8.3r1 or later. If your PCS is at an earlier release, you must perform a number of manual processes, see **"Overview" on page 141**.

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 35.
- Configured the SAML idP on Pulse Connect Secure, see "Configuring SAML idP in Pulse Connect Secure Server" on page 142.

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 177 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:

Yes No Ade_45_84_SAML
Yes
Value

FIGURE 178 Pulse One Properties Configure Auto SAML

After this process is complete, auto-configuration of the SAML idP will be performed.

 (Optional) To confirm the auto-configuration of the SAML idP, log into Pulse Connect Secure and access the System > Configuration > SAML settings page. There will now be a Metadata Name called *AutoConfigured*. For example:

FIGURE 179 Pulse Connect Secure SAML Auto-configuration

$\diamond$	Dulas						Pulse Connect Secu	re
0	Pulses	ECUTE System Authen	tication Administrators Us	ers N	Naintenance Wizar	ds		1~
	Configuration SAML							
Lic	ensing Pulse One	e Security Certificates Mobile VPN Tunneling Telemo	DMI Agent NCP Sensors	C	Client Types Pulse C	ollaboration Virtual Desktops L	Jser Record Synchronization	
Vew	Metadata Provider	Delete Refresh Settings						
10	<ul> <li>records per p</li> </ul>	age					Search:	
۵	Metadata Name	Entity Ids		Roles	Valid Till	Status	Metadata Location	Download
		No. 10 common service and the local service of the	10 - 10 - 17 - 18 - 18 - 18 - 18 - 18 - 18 - 18	SP	2038-01-18 19:14:07		Local	•
	AutoConfigured	https:// /api/v1/sa realm= /sp-metad		SP	2038-01-18 19:14:07		Local	

The auto-configuration of the SAML idP is complete.

You can then either:

- Continue with an optional activity "Automatically Creating Pulse One Users for SAML SSO Logins" on page 154.
- Move directly to testing the SSO login, see "Testing Sign In with Enterprise SSO" on page 156.

## 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 146**.

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 180 Metadata Provider

0	~					Puise Conne	ct Secure	
S Pulse	Secur	°e <sub>System</sub>	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 146**.

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 181 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 146**.

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.

00	S Pulse S PULSE ONE	ecure	DASHBOARD	APPLIANCES	ANALYTICS	ADMINISTRATION		s		
Pulse One	Properties	Pulse One Properties								
		Name		Value				Expand Al		llapse All
		Enterprise Connections (5)								
		Auto Configure SAML settings		No						Z
		Create users and set roles from SAML		No			6			Z
		SAML Identity Provider								Z
		SAML Identity Provider Metadata		🖸 mili mijim	er pro entre n	e 'et sen teres		-	e-785	Z
		SAML Service Provider Metadata		Constitution (1997)	e pa nice	é 've selenenes	(mm, ) ) menuters'	***	e-1185.	
		Password (9)								
		+ Misc (4)								
		+ Session (1)								

#### FIGURE 182 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 146**.

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 183 Metadata Provider Location Configuration

0	~		F F F F F F F F			Pu	ise Connect Secur	9
S Pulse	Secure	System	Authentication	Administrators	Users	Maintenance	Wizards	1~
<sub>SAML&gt;</sub> New Metadata Pr	ovider		-					
Name:	Label to reference m	etadata provider.						
♥ Metadata Provider I	Location Configuration							
Location: Upload Metadata File: V Metadata Provider 1	Local      Remote     Browse     No file     chosen     Current File:     None  Verification Configuration	Secure from the cor	a vrovider. In case of Loca ti ured download url.	l, metadata file needs to be	uploaded by a	dmin. In case of Remote	: Location, metadata file is f	etched by Connect
Accept Unsigned N	letadata	If checked Conn	ect 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 184 Service Provider

✓ Metadata Provider Filter Configuration

Roles:	📄 Identity Provider 🖉 Service Provider 📄 Policy Decision P	ointRoles which Connect Secure looks for in the metadata file.
		List of entity ids to be imported. (one per line). If left empty all entity ids in the file are imported.
Entity Ids to import:		
Rayo Changes	an est	

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

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

FIGURE 185	SAML Identity Provider			
♥ Configuration				
	viders' 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 186 New Peer Service Provider

0					Pulse Conne	ct Secure	
S Pulse Secure							<b>.</b>
Sy	/stem	Authentication	Administrators	Users	Maintenance	Wizards	
Signing In > New Peer Service Provider							
New Peer Service Provider							
*Configuration Mode: O Manual 🖲 Metadata <sub>if metadata</sub>	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 187 Customize IdP Behavior

✓ Customize IdP	Behavlor	
🗹 Override [	Default Configuration	
Reuse Exist	ting 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	in boun oppons are selected, the phongy is given to reduce Existing NC (Puise) Session .
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	O Sha-256	
Relay State:		RelayState' sent to SP in IdP-inifiated SSO scenario. If left blank, the (URL) identifier of the resource being accessed is sent as RelayState'.
* Session Lifetime	e 🔵 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:	<ul> <li>Ignore Re-Authentication for User</li> </ul>	session.
Uzer Identity		
_ Subject Name Format:	DN T	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	ute Statements	If checked, Attribute statements will be sent for the SP.
Use IdP De	fined Attributes	
Customize	IdP 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 154.
- Move directly to testing the SSO login, see **"Testing Sign In with Enterprise SSO" on page 156**.

## 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 188 PCS User Roles

User Roles > Pulse One: SAML Role1 > General > Overview		
General Web Files SAM Telnet		Virtual Deskt
* Name: Description:	Pulse One: SAML Role1	

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 189 Attribute Statement Configuration

Attribute Statement Configura	tion			
Attributes to be sent in SA	ML Attribute Statements can	be configured as name-value p	airs and/or to be fetch	ed from a Directory s
Name-Value based configu	ration, here values can be sys	stem variables available in SSC	) parameter fields:	
Delete 🕇 🖡				
Attribute Name	Friendly Name	Attribute Value	Value Type	
			Single-Valued ᅌ	Add
roles				
TOICS		<role sep=","></role>	Multi-Valued	

6. Log into Pulse One.

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

FIGURE 190 Pulse One Properties Enterprise Connections

	ecure Dashboard	APPLIANCES	ANALYTICS	ADMINISTRATION		
Pulse One Properties	<ul> <li>Pulse One Properties</li> </ul>				Expand	ollapse All
	Name	Value			Expand	©
	Enterprise Connections (3)					
	Auto Configure SAML settings	Yes	_			Z
	Create users and set roles from SAML	Yes				Z
	SAML Identity Provider					Z
	Password (9)					
	⊕ Misc (4)					
	🗄 Session (1)					

- 10. Select the Administration menu, and then click Role Management.
- 11. Ensure that there is an admin-defined role whose name was referenced in step 3. For example:

FIGURE 191 Pulse One Admin Defined Roles

	ecure dashboard appliances analytics administration	EETTINGS ADMIN
User Management	Role Management Add Role Delete Role	
Role Management	System Defined Roles	3 Roles
Appliance Activities	Read Only Admin Super Admin Workspace User	
	Admin Defined Roles	1 Roles
	SAML Role1	Duplicate

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 192 Pulse One Properties

$ \longrightarrow $	Pul	se Secure	
$\langle \rangle $		for the next generation	
We	lcome t	o Pulse One	
	Q. Username		
- XX	Password		
		Sign In	
	Forgot password?	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 193 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: [/users/ resource-policies/web-policies/ptp[application=ptp_policy_2,parent- type=none]] Please specify the IVE hostname on the Network Settings page under Network Identify.	Configure a valid hostname under System > Network > Overview.
Policies > Secure Email	Network > Overview	Import of configuration from Pulse One returned an Error: [/users/ resource-profiles/mobile/secure-mail-profiles/secure-mail- profile[virtual-hostname=myhost.myco.com]] Please specify the IVE hostname on the Network Settings page under Network Identify	Configure a valid hostname under System > Network > Overview.
Security	Network Settings > Internal Port > Virtual Port	Import of configuration from Pulse One returned an Error: [/system/ configuration/security/ssl-options] Virtual port number virtual_internal is not a valid Virtual Port	
	Network Settings > External Port > Virtual Port	Import of configuration from Pulse One returned an Error: [/system/ configuration/security/ssl-options] Virtual port number virtual_external is not a valid Virtual Port	
SAML Auth-Server	System > Configuration > SAML > Settings		Configure a valid "Host FQDN for SAML" on the System > Configuration > SAML > Settings page.

Block Type (which is distributed) (Names as in Pulse One Console)	Requires Preparation of (which is not distributed) (Names as in Appliances Menu	Sample Log Messages	How to Prepare the Target Appliance
Signing in > Sign-in SAML	System > Configuration > SAML > Settings	Import of configuration from Pulse One returned an Error:[/ authentication/signin/saml/identity-provider/sp-default- configuration/source-id] Modification of this attribute is not allowed.	Configure a valid "Host FQDN for SAML" on the System > Configuration > SAML > Settings page.
(PPS) Policies > Enforcer > Access	Policies > Enforcer > Connection	Import of configuration from Pulse One returned an Error: Failed to resolve path references. Import of configuration from Pulse One returned an Error:[/uac/infranet-enforcer/resource-access-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 <sup>nd</sup> Request Policy'.	Configure the appropriate 'RADIUS Request Attributes Policy' under Endpoint Policy > Network Access > Radius Attributes.