

# Pulse Connect Secure

SA/MAG Series to PSA Series and MAG Series to PSA-V Appliance Migration Guide

Release Number9.0R1Published DateFebruary 2019Document Version1.2

Pulse Secure, LLC 2700 Zanker Road, Suite 200 San Jose, CA 95134 https://www.pulsesecure.net

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

Products made or sold by Pulse Secure or components thereof might be covered by one or more of the following patents that are owned by or licensed to Pulse Secure: U.S. Patent Nos. 5,473,599, 5,905,725, 5,909,440, 6,192,051, 6,333,650, 6,359,479, 6,406,312, 6,429,706, 6,459,579, 6,493,347, 6,538,518, 6,538,899, 6,552,918, 6,567,902, 6,578,186, and 6,590,785.

Pulse Secure MAG Series to PSA-V Appliance Migration Guide

Copyright © 2019, Pulse Secure, LLC. All rights reserved. Printed in USA.

# **Revision History**

Release	Document Version	Date	Description
9.0R1	1.2	February 2019	Old GUI screenshots are replaced with new GUI screenshots in section <b>"Migration from SA/MAG to PSA</b> "
9.0R1	1.1	November 2018	Merge the content in single document as most of the content was similar.
			Change in Guide name from "Upgrade" to "Migration".
9.0R1	1.0	July 2018	Also, "upgrade" word references are changed to "migrate" (wherever applicable) inside the document.

# Contents

3
5
5
6
6 19
31
31 31 31 31

# Overview

This document describes guidelines and procedures for successfully migrating older Secure Access and MAG platforms to the new PSA hardware platforms and MAG platforms to the new PSA-V platforms, where source configurations are either as standalone device or as a 2-node/multi-mode cluster configuration.

Binary configurations and selective XML configuration export from old device and import of these configurations to the new device is the recommended way to transfer configuration and settings. Following the steps in this document will ensure successful configuration migration to the next generation PSA devices.

**Note**: IVS migration is not supported directly from Pulse Connect Secure SA devices to the new hardware and should be individually migrated (manually) to become a root IVS which can then later be migrated over to the new hardware devices. This document does not discuss this process.

# Pre-requisite for Migration

Listed below are necessary items for the migration preparation:

 Site assessment: Ensure proper cooling and ventilation; and also ensure network between nodes that are to be clustered are in high bandwidth, low latency LAN type connection (See https://kb.pulsesecure.net/articles/Pulse\_Secure\_Article/KB26035).

**Hardware**: Ensure that hardware components and part are complete (chassis, cables, connectors, and rack mount kits)

**Licenses**: Needed licenses should be procured and ready, and whether you need to configure as license member in an Enterprise Licensing Server environment.

- 2. **Software**: PSA Series devices are delivered with 8.1R4.1 factory build, and PSA-V Series devices are delivered with 9.0R1 factory build, so, determine what software version will be used for the new devices and migrate accordingly. Next generation PSA devices do not support downgrading to previous software versions from its factory default software version or build.
- 3. **Configuration backup**: It is a preferred to backup the system.cfg and user.cfg binary files, along with XML export of Networking Settings immediately prior to migration.

IVS.cfg (if upgrading from SAx500 platform) is not going to be usable for PSA Series as it does not support it, but back it up for any IVS manual conversion (not covered in this document).

4. **Configuration documentation**: Local settings that are mostly kept in system.cfg should be documented, as some of these may need to be manually re-entered to the PSA and PSA-V Series device/s such as cluster configurations.

In A/A cluster, attention should be given to the Network>VPN Tunneling> IP address filter and VPN Tunneling Profile IP pool settings. Also, some of the configurable settings such as SNMP, Log settings, and Syslog can be configured in either cluster mode or individual nodes.



- If converting a cluster, all PSA and PSA-V series devices to be put in cluster should have same version and build of software, and same hardware platforms e.g.; PSA300/PSA3000/PSA5000/PSA7000c/PSA7000f.
- 2. If converting a cluster, ensure to form with same cluster name and port definitions before importing XML, else, import will fail. Examples are external port enabling, cluster name and node names.
- 3. If converting from any platform to PSA7000f or PSA7000c, XML import of networks settings may fail due to network interface differences, ensure to edit XML changing port settings to "**Auto**".
- 4. If converting from a platform that has management port to one without, delete the **<Management-Port>** section from XML before importing XML
- 5. If you are using Active Directory or ACE authentication servers, there may be a need to recreate the AD computer objects for the new PSA and PSA-V series devices, and/or for ACE, to regenerate/re-import the SDCONF.REC file to the devices if authentication fails after import.
- 6. It is assumed during this migration that the replacement PSA Series devices will be installed in the same networks as the SA/MAG devices it is replacing, and PSA-V Series devices will be installed in the same networks as the MAG devices it is replacing.

# Procedure

The below procedure applies to both standalone and cluster migration. The few major steps additional to clustering configurations that may need to be performed are:

- 1. Mapping certificates to ports
- 2. Setting up licensing client if using Enterprise Licensing server
- 3. Checking SNMP settings, checking and setting up of VPN profiles
- 4. Ensuring configs are fully transferred
- 5. Manually adding or correcting discrepancies, if any

# Migration from SA/MAG to PSA

Following are the steps for migration from SA/MAG to PSA:

1. On the existing SA/MAG platform, log in to the standalone device or the primary node of the cluster (where the cluster was first formed) and export its binary configs (**system.cfg** and **user.cfg**), and the XML Network settings configurations.

To export the binary configurations from the PCS device:

- a. In the admin console, select Maintenance > Import/Export > Configuration.
- b. Under **Export**, enter a password if you'd like to password-protect the configuration file.
- c. Click Save Config As to save the file. By default, the filename will be system.cfg.

#### **Figure: Configuration**

System Authentication Administrators Users Maintenance Wizards	Pulse Connect Secure on NODE_3_4
Import/Export > System Configuration	
System Configuration	
Configuration User Accounts XML Import/Export	
♥ Export	
To export system settings to a configuration file, click Save Config As. You can optionally password-protect this file:	
Password for configuration file	
Confirm Password:	
Save Config As	

- d. In the admin console, select Maintenance > Import/Export > User Accounts.
- e. Under **Export**, enter a password if you'd like to password-protect the configuration file.
- f. Click Save Config As to save the file. By default, the filename will be user.cfg.

#### **Figure: User Accounts**

System Authentication Administrators Users Maintenance Wizards	Pulse Connect Secure on NODE_3_4
Import/Export > User Configuration	
User Configuration	
Configuration User Accounts XML Import/Export	
* Export	
Export user settings to a configuration file. You can optionally password-protect this file:	
Password for configuration file:	
Confirm Password:	
Save Config As	

#### To export the XML Network Configuration:

- a. In the admin console, select Maintenance > Import/Export > Export XML.
- b. Under Export, expand System Settings and select **Network > All.**
- c. Click **Export** and save the XML file.

#### Figure: XML Import/Export

💲 Pulse	Secure	System	Authentication	Administrators	Users
Import/Export > Export XML					
Export XML					
Configuration	User Accounts XM	L Import/Export			
Export Export Universal	Import				
✓ Schema Files					
Download the Scher	na files				
✓ Select Settings and Ex	port				
Expand All S	elect All Export	+	•		
System Settings     Select All System	selection made em Settings				
Status All   None	<ul> <li>System date and</li> <li>Cockpit page</li> <li>Dashboard Settin</li> <li>Cloud Secure Das</li> <li>Devices</li> </ul>	time gs shboard Settir	ıgs		
Configuration All   None	<ul> <li>Licenses</li> <li>DMI Agent</li> <li>NCP</li> <li>Sensors</li> <li>Client Types</li> <li>Certificates</li> <li>Pulse Collaboration</li> <li>Virtual Desktops</li> <li>User Record Synone</li> <li>IKEv2</li> <li>SAML</li> <li>Mobile</li> <li>VPN Tunneling A</li> </ul>	on chronization CL Limit Enfo	rcement Option		
Security Network All   None	<ul> <li>Security</li> <li>Overview</li> <li>Internal Port</li> <li>External Port</li> <li>Management Port</li> <li>VLANs</li> <li>Hosts</li> <li>Hosts</li> </ul>	t			

- 2. Make notes of all the local settings for both nodes (if not yet done during preparation stage): IP information, clustering, virtual ports, VLANs, hosts, routes, DNS settings, SNMP (if configured), Syslog.
- 3. Shut down old SA/MAG cluster or standalone devices.
- 4. Configure the new PSA devices with same internal/external/management ports IPs with same IP addresses as the old SA devices and the proper DNS settings. Do not configure any other settings at

this time.

5. Apply the proper licenses for the new PSA devices. If the SA/MAG is a member of an Enterprise License Server, you have to manually recreate the client and re-establish connection to the license server later **at the end of migration**.

**()** Note: If upgrading a non-clustered SA/MAG device, proceed to Step-11.

6. In the new PSA device (first device), manually create a new cluster **with same name and settings** with **same node names** as the old SA/MAG cluster.

Figure: Create New Cluster

💲 Pu	<mark>lse</mark> Secur	e <sub>System</sub>	Authentication	Administrators	Users	Maintenance	Wizards
Clustering > Create	New Cluster						
Create New Cl	uster						
Join	Create						
-	DOA 2000						
Type:	PSA-3000						
Cluster Name:	GEC_CLUSTER	lame of the cluster to cr lust be alphanumeric, "-	eate. .", or "_"; must start with a I	etter and have a maximum	of 19 character	s.	
Cluster Password	•••••	hared secret among the lust be at least 6 charad	e nodes in the cluster. cters long				
Confirm Passwor		hared secret among the lust match the passwor	e nodes in the cluster. d you typed in the previous	line			
Member Name:	GEC1 ×	lame of this node in the lust be alphanumeric, "-	cluster ", or "_"; must start with a I	etter and have a maximum	of 19 character	S.	
Create Cluster	▲						

#### Figure: Confirm Create Cluster

<b>Secure Secure</b>	System	Authentication	Administrators	Users	Maintenance	Wizards
▲ Confirm Create Cluster						
Are you sure you want to create a new clust	er GEC_CLU	JSTER ?				
Please click <b>Create</b> to create a new cluster Click <b>Cancel</b> if you do not want to create a o Create Cancel	and add this cluster.	appliance with memb	er name GEC1 to the	cluster.		

- 7. Add the second device to the cluster in the primary node cluster configuration and save the settings.
  - a. Click Add Members to add a member.

#### **Figure: Clustering Status**

ŜР	ul	se Secure	System Authentication	Administrators	Users	Maintenance	Wizar	ds	Pulse Connect Secure on GEC1	••
Clustering > C	luster S	latus								
Cluster Sta	tus									
Status	F	roperties								
Cluster Nam	e: GEC	_CLUSTER								
Type:	PSA	-3000								
Configuration	Activ	re/Active								
Add Memb	ers	Enable Disable I	Remove							
10	• re	cords per page							Search:	
		Member Name	Internal Address	Exte	rnal Address	; <u> </u>	Status	Notes	Sync Rank Update	
	•	GEC1	10.209.69.44/22				٩	Leader	0	
									← Previous 1	$Next \rightarrow$

b. Enter member node name and IP and check netmask and gateway, then click Add.

#### Figure: Add Cluster Member

\$F	Pulse Secure	System Authentication Adr	ninistrators Users Maintenance Wi	zards	Pulse Connect Secure on GEC1	1~
Clustering >	Cluster Add					
Cluster Ad	dd					
Cluster: GE	C_CLUSTER					
Delete					X	
	Node Name	Internal IPv4 address	Internal IPv4 Netmask	Internal IPv4 Gateway		
	GEC2	10.209.69.44	255.255.252.0	10.209.71.254	Add	
Note: after t nodes willer Save Cha	the changes are saved, you must click e completely overwritten during the journers Cancel	"Network" on the left panel to check and ensure ining process.	the network settings for all new nodes are fully configu	red prior to their joining. Keep in mind that	at the entire state currently on the	ne new

c. Click on Save Changes.

#### **Figure: Save Changes**

\$ F	Pulse Secure	System Authentication Admin	istrators Users Maintenance Wiz	ards	Pulse Connect Secure on GEC1	••
Clustering >	Cluster Add					
Cluster Ad	dd					
Cluster: GE	C_CLUSTER					
Delete					/	
	Node Name	Internal IPv4 address	Internal IPv4 Netmask	Internal IPv4 Gateway		
	GEC2	10.209.69.44	255.255.252.0	10.209.71.254	Add	
Note: after the nodes will be Save Cha	he changes are saved, you must click perimpletely overwritten during the jo anges Cancel	"Network" on the left panel to check and ensure the ining process.	e network settings for all new nodes are fully configure	d prior to their joining. Keep in mind tha	t the entire state currently on th	ie new

d. Check cluster **status**, it should go **transitioning** for short period, then first node becomes enabled and status should be **Leader**, the second node remains **Enabled**, **Unreachable** until it

#### joins the cluster.

#### **Figure: Clustering Status**

Ŝ F	<b>v</b> u	<mark>lse</mark> Secure	System Authenticatio	on Administrators	Users	Maintena	nce Wizards	Pulse Connect Secure on GEC1	••
Clustering >	Cluste	r Status							
Cluster S	tatus								
Status		Properties							
Cluster Nar	me:	GEC_CLUSTER							
Type:		PSA-3000							
Configurati	on:	Active/Passive							
Internal VIF	on G	EC1:							
		IPv4: 10.209.69.55							
		IPv6: not defined							
Add Men	nbers	Enable Disable	Remove Fail-Over VIP						
10	•	records per page						Search:	
		Member Name	Internal Address	External Address		Status	Notes	Sync Rank Update	
	*	GEC1	10.209.69.45/22			۹	Leader	0	
		GEC2	10.209.69.44/22			۰	Enabled, Unreachable	0	
								← Previous 1	Next $\rightarrow$

- 8. If the XML config is exported from an **Active/Passive** Cluster, following needs to be done prior to XML Import:
  - a. Configure External Port for the Cluster Members (if external ports are configured in cluster)
  - b. Go to Clustering > Cluster Properties page on the IVE. Change the Cluster Type from Active/Active to Active/Passive and add the cluster VIP address/es (the example here does not use external port).

💲 Pu	lse Secure	System	Authentication	Administrators	Users	Maintenance	Wizards
Clustering > Cluster	Properties						
Cluster Proper	ties						
Status	Properties						
Type: Cluster Name: Cluster Password:	PSA-3000 GEC_CLUSTER						
Confirm Password	t: ••••••						
This is a high	h-availability failover mode, in which	h one node is a	active while the other is	held as backup.			
Internal VIP:							
External VIP	IPv4: 10.209.69.55 × IP IPv4: IPv4: IF	0v6:					
Active/Active This mode reader	e configuration equires an external load-balancer.						

### Figure: Active/Passive Configuration

c. Save the cluster configuration settings.

### **Figure: Advanced Settings**

✓ Advanced Setting	✓ Advanced Settings					
Enable Advanc	ed Settings					
Save Changes	Delete Cluster					

d. Change confirmation will appear confirming change from **Active/Active** to **Active/Passive**.

Figure:	Change	Confirr	nation
---------	--------	---------	--------

Clustering > Cluster Properties								
Cluster Properties								
Status								
	•							
info: Internal(IPv4) VIP changed to     10.209.69.55								
() info: Cluster Pai mode								
Туре:	PSA-3000							
Cluster Name:	GEC_CLUSTER							
Cluster Password:	•••••							
Confirm Password:	•••••							

9. Log in to the second MAG device and join this node to the cluster by **Clustering > Join Cluster**.

Figure: Join Existing Cluster

Clustering > Join Existing Cl	uster
Join Existing Cluster	
Join Create	
l r	
Cluster Name:	GEC_CLUSTER Name of the cluster to join
Cluster Password:	••••••
Existing Member Address	10.209.69.45 Internal IP address of any existing cluster member
Join Cluster	<u>_</u>

In confirmation page, click **Join**.

#### Figure: Confirm Join Cluster

Pulse Secure	System	Authentication	Administrators	Users	Maintenance	Wizards			
▲ Confirm Join Cluster									
This node will next contact the cluster member '10.209.69.45' and ask to join the cluster GEC_CLUSTER. If this succeeds, the node will join as member of the cluster. WARNING: This host's entire state will be overwritten with the current cluster configuration, including bookmarks, IP address, netmask etc.									
Please click <b>Join</b> to join the cluster.									
Join Cancel									

After successful join, admin session will be forced off the secondary node that just joined.

10. Log in to primary node and check cluster status and it should stabilize in a few minutes.

\$ P	uls	e Secure	System Aut	hentication	Administrators	Users	Maintenan	ce Wiza	rds	Pulse Connect Secure on GEC2
Clustering > Clu	uster Statu	3								
Cluster Stat	tus									
Status	Prop	erties								
Cluster Name	e:	GEC_CLUSTER								
Туре:		PSA-3000								
Configuration	c .	Active/Passive								
Internal VIP o	on GEC1:									
		IPv4: 10.209.69.55								
		IPv6: not defined								
Add Memb	ers	Enable Disable R	temove Fail-C	Over VIP						
10 .	- record	is per page								Search:
		Member Name	Interna	al Address	Extern	al Address		Status	Notes	Sync Rank Update
	G	EC1	10.209.69.45/22					٩	Leader	0
	* G	EC2	10.209.69.44/22					٩	Enabled	0

Figure: Clustering Status

- 11. In the standalone environment or primary node of the new cluster, do the XML Import of Networking Settings. All networking settings would get imported, including the following:
  - Internal Virtual Ports
  - External Virtual Ports
  - Management Ports
  - VLANs
  - Static Routes
  - Port settings

Go to **Maintenance > Import/Export** and, select **Import XML**, then browse for the XML network settings file, then click **Import**.

#### Figure: Import XML

<b>Pulse Secure</b> System Authentication Administrators Users Maintenance Wizards	Pulse Connect Secure on NODE_3_4	1*
Import/Export > Import XML		
Import XML		
Configuration User Accounts XML ImportExport		
Export Export Universal Import		
♥ Schema Files		
Download the Schema files		
✓ Import		
To import data, select a valid XML data file, then click Import. During the import process, all members of a cluster are disabled and all end-user sessions are terminated. After the import pro automatically enabled but users must sign-in again. Note: XML import doesn't support modifying Clustering Properties. Please use binary import option #1 for that instead.	cess completes, the cluster men	nbers are
* XML data file: Browse No file chosen		ľ
Import		

If it errors out with interface issues like upgrading to PSA7000f or PSA7000c, edit XML as follows before import: (Set link-speed to "auto")

<internal-port>

<node>SSLVPN-NODEX</node>

<settings>

<ip-address>10.10.10.n</ip-address>

<netmask>255.255.255.224</netmask>

<default-gateway>10.10.10.1</default-gateway>

k-speed>auto</link-speed>

<arp-ping-timeout>5</arp-ping-timeout>

<mtu>1500</mtu>

</settings>

<virtual-ports>

</virtual-ports>

<arp-cache>

</arp-cache>

<routes>

</routes>

</internal-port>

### Figure: Import Progress

O D L C	Pulse Connect Secure								
VILSE SECURE System Authentication Administrators Users Maintenance Wizards	<b>۲</b> *								
Import/Export > Import XML									
Import XML									
Configuration User Accounts Administrative Network XML Import/Export									
Export Export Universal Import									
Import in progress     Please wait for import to complete before payingtion to other admin pages									
✓ Schema Files									
Download the Schema files									
♥ Import									
To import data, select a valid XML data file, then click Import.									
* XML data file: Browse ive-export (5) xml									
Import									

#### **Figure: Detailed Information**

oort/Export						
Configuration	User Accounts	Administrative Network	XML Import/Export			
port Export Unive	ersal Import					
Info: Import comp	leted. Some services	may be restarted.				

**Note**: If the Source device has Management Port (e.g. MAG-SM360), and the Destination IVE does not have Management Port (e.g. PSA300), the XML import would fail with the following error:

### Figure: Error Message

	Pulse Connect Secure	
Verse Secure System Authentication Administrators Users Maintenance Wizards	2 IUUU B	•
Import/Export		
Configuration User Accounts Administrative Network XML Import/Export		
Export Export Universal Import		
© Error : Import failed: XML import failed		
Detailed Information:		
Fatal error in XML file at line: 52, column: 39 Message: Expected end of tag 'log' Framework: Encountered a validation error in the XML file Failure		
OK		

To work-around this issue, remove the Management Port settings (highlighted below) from the XML and then retry the XML Import.

#### Figure: Management Port Settings

<management-port></management-port>	
<node>localhost2</node>	
<settings></settings>	
<is-enabled>disabled</is-enabled>	
<jp_address></jp_address>	
<netmask></netmask>	
<default-gateway></default-gateway>	
<enable-ipv6>disabled</enable-ipv6>	
<ipv6-address></ipv6-address>	
<ipv6-prefix-length>64</ipv6-prefix-length>	
<ipv6-default-gateway></ipv6-default-gateway>	
<li>k-speed&gt;auto</li>	
<arp-ping-timeout>5</arp-ping-timeout>	
< <u>mtu&gt;1500</u>	
<arp-cache></arp-cache>	
<ndp-cache></ndp-cache>	
<routes></routes>	
<ipv6-routes></ipv6-routes>	
<network-connect></network-connect>	
<nc-base-jp>10.200.200</nc-base-jp>	
<network-ip-filter></network-ip-filter>	
<node>localhost2</node>	
< <u>OC-IP-TUTErs&gt;</u>	
< <u>oc-ip-tilter</u> >	
<pre> </pre>	

12. In the standalone environment or primary node of the new cluster, import the system.cfg (this is the same process in a standalone mode migrate).

Note: This export process is the same for upgrading a standalone device.

#### To import the system configurations on the PSA device:

- a. In the admin console, select Maintenance > Import/Export > Configuration.
- b. Specify whether you want to import the Secure Access Service certificate.

**Note**: The certificate is not imported unless you select the **Import Device Certificate(s)**? check box.

- c. Select **Import everything except network settings and licenses** This option imports all configuration settings except the network, cluster and license settings.
- d. Browse to the configuration file, which is named **system.cfg** by default.
- e. Enter the password you specified for the file. If you did not specify a password before exporting the file, then leave this field blank.

#### f. Click Import Config.

Figure: System.cfg

💲 Pulse	Secure	System	Authentication	Administrators	Users	Maintenance	Wizards
Import/Export > System Conf	iguration						
System Configuration Configuration	User Accounts XM	L Import/Export	t				
✓ Export							
To export system se	ettings to a configuration f	ile, click Save	Config As. You can o	ptionally password-prot	ect this file:		
Password for config Confirm Password:	uration file:		]				
Save Config As.							
✓ Import							
To import system se Options:	ettings from a configuratio Import Device Certif Note: Checking this wil	n file, select t ficate(s)? I overwrite the ex	he configuration file ar	d which settings to brir	ng in, and clic	k Import Config. All ı	members in the
Other Import Option	ıs: Import everything (e	except Device	Certificate(s))	_			
	Import everything but Preserves the IP address Note: Use this setien et Note: Use this setien et	ut the IP address, netmask, def	ess ault gateway, VIPs, ARPs description file in from	and routes of the network in	terfaces on this	device.	
	<ul> <li>Import everything ex Leaves everything in Ne Note: Always use this of Import only Device</li> </ul>	xcept network etwork Settings, o option if configura Certificate(s)	settings, cluster settin Clustering Properties, Lice tion file was exported from	ngs and licenses nsing sections and Onboard a node that is part of a clus	ling Profile UUII ter.	D unchanged.	
	Imports the Device Cert Note: You must check t	tificate(s) only. the Import Device	e Certificate(s) checkbox a	ibove.			
Config File:	Browse No file ch	hosen 🔶					
Password:		Use this	if the configuration file was	password-protected			
Import Config							

System settings and certificates are imported.

13. Next, in the same primary node, import the user.cfg binary file.

*Note*: This export process is the same for upgrading a standalone device.

#### To import the system configurations on the PSA device:

- a. In the admin console, select **Maintenance** > **Import/Export** > **User Accounts**.
- b. Browse to the configuration file, which is named **user.cfg** by default.
- c. Enter the password you specified for the file. If you did not specify a password before exporting the file, then leave this field blank.
- d. Click Import Config.

#### Figure: user.cfg

System Authentication Administrators Users Maintenance Wizards	Pulse Connect Secure on NODE_3_4	<b>1</b> Y
Import/Export > User Configuration		
User Configuration		
Configuration User Accounts XML Import Export		
♥ Export		
Export user settings to a configuration file. You can optionally password-protect this file:		
Password for configuration file		
Save Config As		
♥ Import		
Import user settings by selecting the configuration file and clicking Import Config. Import User Accounts will invalidate all existing End-User and Administrators sessions.		
Browse No file chosen		
Password. Use this if the configuration file was password-protected		
Import Config		

- 14. After importing XML, system and user.cfg files, check and/or modify/add remaining local settings and other settings such as:
  - a. Network > Overview settings (set in cluster or individual nodes)
  - b. Network > Routes (for internal, external and other ports)
  - c. Network > Hosts (set in cluster or individual nodes)
  - Network > Internal Port/ External Port>Virtual Ports (if clustered, set this up in cluster "Entire Cluster")
  - e. Network > VLANs (if clustered, set this up in cluster "Entire Cluster")
  - f. **Network > VPN Tunneling** (set in cluster or individual nodes)
  - g. Log/Monitoring > SNMP (set in cluster or individual nodes)
  - h. Configuration>Certificates>Device Certificates (and its ports bindings)
  - i. Resource Policies>VPN Tunneling>Connection Profiles (if configured)
  - j. Auth Servers > ACE Auth server, if used (check the node secret file status)

**Configuration > Licensing -** License client-server settings (if used as license client in Enterprise Licensing Server environment), proper licenses installed

- 15. Check cluster status (if clustered) and test operation by logging in to the cluster VIPs (or the standalone PSA device IP). Test the authentication using AD, ACE, etc., and all other functionalities enabled, such as NC or Pulse.
- 16. This completes the SA/PSA to PSA hardware platform migration.

## Migration from MAG to PSA-V

Following are the steps for migration from MAG to PSA-V:

 On the existing SA/MAG platform, log in to the standalone device or the primary node of the cluster (where the cluster was first formed) and export its binary configs (system.cfg and user.cfg), and the XML Network settings configurations.

#### To export the binary configurations from the PCS device:

- a. In the admin console, select Maintenance > Import/Export > Configuration.
- b. Under **Export**, enter a password if you'd like to password-protect the configuration file.
- c. Click Save Config As to save the file. By default, the filename will be system.cfg.

#### Figure: Configuration

System Authentication Administrators Users Maintenance Wizards	Pulse Connect Secure on NODE_3_4
ImportExport > System Configuration	
System Configuration	
Configuration User Accounts XML Import/Export	
▼ Export	
To export system settings to a configuration file, click Save Config As. You can optionally password-protect this file:	
Password for configuration file	
Confirm Password:	
Save Config As	

- d. In the admin console, select Maintenance > Import/Export > User Accounts.
- e. Under **Export**, enter a password if you would like to password-protect the configuration file.
- f. Click Save Config As to save the file. By default, the filename will be user.cfg.

#### Figure: Save Config As – user.cfg

Secure Secure Secure	stem Authentication Administrators	Users Maintenance Wizards	Pulse Connect Secure on NODE_3_4
Import/Export > User Configuration			
User Configuration			
Configuration User Accounts XML Impo	ort/Export		
✓ Export			
Export user settings to a configuration file. You can	optionally password-protect this file:		
Password for configuration file:			
Confirm Password:			
Save Config As			

#### To export the XML Network Configuration:

- a. In the admin console, select **Maintenance** > **Import/Export** > **Export XML**.
- b. Under Export, expand System Settings and select Network > All.
- c. Click **Export** and save the XML file.

💲 Puls	e Secure System Authentication Administrators Users	5
Import/Export > Export XI	ИL	
Export XML		
Configuration	User Accounts XML Import/Export	
Export Export Univer	sal Import	
✤ Schema Files		
Download the Sc	hema files	
<ul> <li>Select Settings and</li> </ul>	Export	
Expand All	Select All Export	
Select All Sy	rstem Settings	
Status All   None	<ul> <li>System date and time</li> <li>Cockpit page</li> <li>Dashboard Settings</li> <li>Cloud Secure Dashboard Settings</li> <li>Devices</li> </ul>	
Configuration All   None	<ul> <li>Licenses</li> <li>DMI Agent</li> <li>NCP</li> <li>Sensors</li> <li>Client Types</li> <li>Certificates</li> <li>Pulse Collaboration</li> <li>Virtual Desktops</li> <li>User Record Synchronization</li> <li>IKEv2</li> <li>SAML</li> <li>Mobile</li> </ul>	
Security Network All   None	<ul> <li>VEN Turnleing ACE Link Enforcement Option</li> <li>Security</li> <li>Overview</li> <li>Internal Port</li> <li>External Port</li> <li>Management Port</li> <li>VLANs</li> </ul>	
	<ul> <li>✓ Hosts</li> <li>✓ VPN Tunneling</li> </ul>	

#### Figure: XML Import/Export

- 2. Make notes of all the local settings for both nodes (if not yet done during preparation stage): IP information, clustering, virtual ports, VLANs, hosts, routes, DNS settings, SNMP (if configured), Syslog.
- 3. Shut down old MAG cluster or standalone devices.
- 4. Configure the new PSA-V devices with same internal/external/management ports IPs with same IP addresses as the old MAG devices and the proper DNS settings. Do not configure any other settings

at this time.

5. Apply the proper licenses for the new PSA-V devices. If the MAG is a member of an Enterprise License Server, you have to manually recreate the client and re-establish connection to the license server later at the end of migration.

Note: If upgrading a non-clustered MAG device, proceed to step-10.

- 6. Now, admin must install the core licenses. Without core licenses, the clustering option is not enabled and admin cannot create a cluster in a PSA-V. From 8.3R3 and later releases, core licenses can be downloaded from PCLS. Refer to the License Configuration for VA-SPE/PSA-V Appliances **Deployment Guide** for detailed steps. If admin is deploying 8.3R1 and then upgrading to 8.3Rx, core license is not needed.
- 7. In the new PSA-V device (first device), manually create a new cluster with same name and settings with **same node names** as the old MAG cluster.

💲 Pu	<mark>lse</mark> Secu	re System	Authentication	Administrators	Users	Maintenance	Wizards
Clustering > Create	New Cluster						
Create New Cl	uster						
Join	Create						
Type:	MAG-SM160						
Cluster Name:	GEC_CLUSTER	Name of the cluster to Must be a phanumeri	o create. c, "-", or "_"; must start with	a letter and have a maxim	um of 19 chara	cters.	
Cluster Password:		Shared secret among Must be at least 6 ch	the nodes in the cluster. aracters long				
Confirm Password	Confirm Password: Shared secret among the nodes in the cluster. Must mat h the password you typed in the previous line						
Member Name:	GEC1	Name of this node in Must be a phanumeri	the cluster c, "-", or "_"; must start with	a letter and have a maxim	um of 19 chara	cters.	
Create Cluster	-						

Figure: Create

Figure: Confirm Create Cluster

Secure Secure	System	Authentication	Administrators	Users	Maintenance	Wizards	
▲ Confirm Create Cluster							
Are you sure you want to create a new clust	Are you sure you want to create a new cluster GEC_CLUSTER ?						
Please click <b>Create</b> to create a new cluster and add this appliance with member name <i>GEC1</i> to the cluster. Click <b>Cancel</b> if you do not want to create a cluster.							
Create							

8. Add the second device to the cluster in the primary node cluster configuration and save the settings.

a. Add a member by clicking **Add Members**.

#### **Figure: Add Members**

Secure Secure	System Authentication	Administrators Users Maint	tenance Wizar	ds	Pulse Connect Secure on GEC1
Clustering > Cluster Status					
Cluster Status					
Status Properties					
Cluster Name: GEC_CLUSTER					
Type: MAG-SM160					
Configuration: Active/Active					
Add Members Enable Disable	Remove				
10 records per page					Search:
Member Name	Internal Address	External Address	Status	Notes	Sync Rank Update
GEC1	10.209.113.37/20		٩	Leader	0
* Indicates the node you are currently using					← Previous 1 Next -

b. Enter member node name and IP and check netmask and gateway, then click Add.

#### Figure: Mode Name

\$ P	Pulse Secure	System Authentication A	Administrators Users Maintenance Wiza	Pulse Connect on GEC1 ards	Secure
Clustering > 0	Cluster Add				
Cluster Ac	dd				
Cluster: GE	C_CLUSTER				
Delete					
	Node Name	Internal IPv4 address	Internal IPv4 Netmask	Internal IPv4 Gateway	
	GEC2	172.22.149.1 x	255.255.240.0	10.209.127.254	Add
					Ŷ
Note: after the nodes will be Save Character	he changes are saved, you must click " e completely overwritten during the join anges Cancel	"Network" on the left panel to check and ens ning process.	sure the network settings for all new nodes are fully configure	id prior to their joining. Keep in mind that the entire state or	urrently on the new

c. Click on Save Changes.

#### **Figure: Save Changes**

\$ P	<b>ulse</b> Secure	System Authentication Adr	ministrators Users Maintena	ance Wizards	Pulse Connect Secure on GEC1
Clustering > C	Cluster Add	,			
Cluster Ad	bt				
Cluster: GEC	_CLUSTER				
	Node Name	Internal IPv4 address	Internal IPv4 Netmask	Internal IPv4 Gateway	
					Add
	GEC2	172.22.149.1	255.255.255.0	172.22.149.1	( = )
Note: after th nodes will be Save Cha	e changes are saved, you must click "h s completely overwritten during the joini anges Cancel	Network" on the left panel to check and ensure ing process.	e the network settings for all new nodes are	e fully configured prior to their joining. Kee	p in mind that the entire state currently on the

d. Check cluster **status**, it should go **transitioning** for short period, then first node becomes enabled and status should be **Leader**, the second node remains **Enabled**, **Unreachable** until it joins the cluster.

#### **Figure: Status**

$\sim$	<b>o</b> u	<mark>lse</mark> Secure	System	Authentication	Administrators	Users	Maintena	ince Wizards	Pulse Connect Secure on GEC1	•
Clustering >	Cluster	Status								
Cluster S	tatus									
Status		Properties								
Cluster Na	me: Gl	EC_CLUSTER								
Туре:	M	AG-SM160								
Configurat	ion: Ad	ctive/Active								
Add Me		Enable Disable	Remove							
10	•	records per page							Search:	
		Member Name	Internal A	ddress	External Address		Status	Notes	Sync Rank Update	
	*	GEC1	10.209.113.37/20				۰	Leader	0	
		GEC2	172.22.149.1/24				۰	Enabled, Unreachable	0	
									← Previous 1	Next -

- 9. If the XML config is exported from an **Active/Passive** Cluster, following needs to be done prior to XML Import:
  - a. Configure External Port for the Cluster Members (if external ports are configured in cluster)
  - b. Go to Clustering > Cluster Properties page on the IVE. Change the Cluster Type from Active/Active to Active/Passive and add the cluster VIP address/es (the example here does not use external port).

#### **Figure: Cluster Properties**

💲 Pul	<mark>se</mark> Secure	System	Authentication	Administrators	Users	Maintenance	Wizards	Pulse Connect Secure on GEC1
Clustering > Cluster Pr	operties							
Cluster Propertie	S							
Status F	Properties							
Tupo: M	AG \$M160							
Cluster Name:	GEC_CLUSTER							
Cluster Password:								
Confirm Password:								
Configuration Se	ttings							
This is a high-a	vailability failover mode, in whic	h one node is ac	tive while the other is	held as backup.				
Internal VIP:								
IP	v4: 172.22.149.99	IPv6:						
External VIP:								
IP	v4:	IPv6:						

c. Save the cluster configuration settings.

### Figure: Advanced Settings

✓ Advanced Settings					
Enable Advanced Settings					
Save Changes	Delete Cluster				
<u>^</u>					

d. Change confirmation will appear confirming change from **Active/Active** to **Active/Passive**.

💲 Puls	e Secure	System	Authentication	Administrators	Users	Maintenance	Wizards	Pulse Connect Secure on cl62
Clustering > Cluster Pro	perties							
Cluster Properties	i							
Status Pr	operties							
<b>9</b> info: Cluster Pair	switched to Active/Passive mo	ode 🗶	]					
Туре:	PSA-5000		-					
Cluster Name:	pcs-cl							
Cluster Password:								
Confirm Password:								
✓ Configuration Sett	ings							
Active/Passive c	configuration							
This is a high-av	ailability failover mode, in whic	ch one node is	active while the other is	held as backup.				
Internal VIP:								
IPv	4: 10.209.127.237	IPv6: fc00:1	111:5678:5678::ad1:7fed					
External VIP:								
IPv	4: 10.30.127.237	IPv6: fc00:7	777:5678:5678::ad1:7fed					

#### **Figure: Confirmation Change**

10. Log in to the second PSA-V device and join this node to the cluster by **Clustering > Join Cluster**.

### Figure: Join Existing Cluster

Clustering > Join Existing Clus	ter						
Join Existing Cluster	Join Existing Cluster						
Join Create							
Cluster Name:	cluster-1	Name of the cluster to join					
Cluster Password:							
Existing Member Address: 10.209.113.30		Internal IP address of any existing cluster member					
Join Cluster							

In confirmation page, click **Join**.

#### Figure: Confirm Join Cluster

Q Dullas Comme	Pulse Connect Secure
VILSE SECURE System Authentication Administrators Users Maintenance Wizards	
▲ Confirm Join Cluster	
This node will next contact the cluster member '10.209.113.30' and ask to join the cluster <i>Cluster-1</i> . If this succeeds, the node will join as member of the cluster. WARNING: This host's entire state will be overwritten with the current cluster configuration, including bookmarks, IP address, netmask etc.	
Please click <b>Join</b> to join the cluster. Click <b>Cancel</b> to return to the previous page.	
Join Cancel	

After successful join, admin session will be forced off the secondary node that just joined.

11. Log in to primary node and check cluster status and it should stabilize in a few minutes.

#### Figure: Cluster Status

\$P	Pul	<mark>se</mark> Secure	System Authentication	Administrators Users Maint	enance Wiza	ards	Pulse Connect Secure on cl62
Clustering > 0	Cluster S	tatus					
Cluster St	atus						
Status	F	Properties					
Cluster Nan	ne: pcs-	cl					
Type:	PSA	-5000					
Configuratio	on: Acti	ve/Active					
Add Mem	ibers	Enable Disable F	Remove				
10	• re	cords per page					Search:
		Member Name	Internal Address	External Address	Status	Notes	Sync Rank Update
	*	cl62	10.209.113.62/20	10.30.113.62/16	٥	Enabled	0
		cl92	10.209.113.92/20	10.30.113.92/16	٥	Leader	0
← Previous     1 Next →							

- 12. In the primary node of the new cluster, do the XML Import of Networking Settings. All networking settings would get imported, including the following:
  - Internal Virtual Ports
  - External Virtual Ports
  - Management Ports
  - VLANs
  - Static Routes
  - Port settings
  - a. Go to **Maintenance > Import/Export, select Import XML**, then browse for the XML network settings file, then click Import.

#### Figure: XML Import/Export

System Authentication Administrators Users Maintenance Wizards	Pulse Connect Secure on NODE_3_4
Import/Export > Import XML	
Import XML	
Configuration User Accounts XML Import/Export	
Export Export Universal Import	
✓ Schema Files	
Download the Schema files	
✓ Import	
To import data, select a valid XML data file, then click Import. During the import process, all members of a cluster are disabled and all end-user sessions are terminated. After the import pro automatically enabled but users must sign-in again. Note: XML import doesn't support modifying Clustering Properties. Please use binary import option #1 for that instead.	cess completes, the cluster members are
* XML data file: Browse No file chosen	
Import	

- 13. Now assign VLANs (if any):
  - a. Go to **System > Traffic Segregation > Default Network**.
  - b. Move the interfaces from the **Available Interfaces** to **Selected Interfaces**.
  - c. Click on Save Changes.

#### Figure: Traffic Segregation

S Pulse Secur	' <b>e</b> System Aut	hentication Administrators	Users Maintenance	Wizards	Pulse Connect Secure Default Network T Go on DFS_VA_NODE_115_17
Traffic Segregation > Traffic Segregation - Default	Network				
Traffic Segregation - Default Network					
✓ Settings Interfaces: Available (none)	Add -> Remove	Selected Interfaces: "Internal Port QA-VLAN-74 (ID 74) Default	default Interface denoted by *		

- 14. In the primary node of the new cluster, do the same XML Import process for Logs and SNMP settings, by importing the Logs and Settings XML done in step 1.2.c. All log settings would get imported, including the following:
  - Events
  - User Access
  - Admin Access
  - Sensors
  - Log Filters
  - SNMP

15. In the primary node of the new cluster, import the **system.cfg** (this is the same process in a standalone mode migrate).

*Note*: This export process is the same for upgrading a standalone device.

#### To import the system configurations on the PSA device:

- a. In the admin console, select Maintenance > Import/Export > Configuration.
- b. Specify whether you want to import the Secure Access Service certificate. Note: The certificate is not imported unless you select the **Import Device Certificate(s)**? check box.
- c. Select **Import everything except network settings and licenses** This option imports all configuration settings except the network, cluster and license settings.
- d. Browse to the configuration file, which is named **system.cfg** by default.
- e. Enter the password you specified for the file. If you did not specify a password before exporting the file, then leave this field blank.
- f. Click Import Config.

#### **Figure: Configuration**

💲 Pulse	Secure	System	Authentication	Administrators	Users	Maintenance	Wizards
Import/Export > System Config	uration						
System Configuration							
Configuration	ser Accounts XM	/IL Import/Export					
✓ Export							
To export system set	tings to a configuration	file, click Save	Config As. You can op	otionally password-prot	ect this file:		
Password for configur	ration file:						
Save Config As							
✓ Import To import system set Options:	tings from a configurati Import Device Cert Note: Checking this w	on file_select th ificate(s)? ill overwrite the exis	sting Device Certificate(s).	d which settings to brir	ng in, and clio	ck Import Config. All i	members in the
Other Import Options:	<ul> <li>Import everything (</li> <li>Import everything (</li> <li>Import everything (</li> <li>Preserves the IP address of the option</li> <li>Import everything of Leaves everything in Note: Always use this</li> <li>Import only Device Imports the Device Ce Note: You must check</li> </ul>	except Device ( out the IP addresses, netmask, defa sony if the experted except network s vetwork Settings, C option if configurat of Certificate(s) only. the Import Device	Certificate(s)) ss util gateway, VIPs, ARPs a configuration file is from a settings, cluster settin clustering Properties, Licen ion file was exported from Certificate(s) checkbox a	nd routes of the network in <del>standalone node.</del> gs and licenses sing sections and Onboarc a node that is part of a clus bove.	terfaces on this ling Profile UUII ter.	: device. D unchanged.	
Config File: Password:	Browse No file o	Use this if	the configuration file was p	password-protected			
Import Config							

- g. System settings and certificates are imported.
- 16. Next, in the same primary node, import the user.cfg binary file.

🕖 Note: This export process is the same for upgrading a standalone device.

#### To import the system configurations on the PSA device:

- a. In the admin console, select Maintenance > Import/Export > User Accounts.
- b. Browse to the configuration file, which is named **user.cfg** by default.
- c. Enter the password you specified for the file. If you did not specify a password before exporting the file, then leave this field blank.
- d. Click Import Config.

#### Figure: User Accounts

<b>Pulse Secure</b> System Authentication Administrators Users Maintenance Wizards	Pulse Connect Secure on NODE_3_4	1.
Import/Export > User Configuration		
User Configuration		
Configuration User Accounts XML Import Export		
♥ Export		
Export user settings to a configuration file. You can optionally password-protect this file:		
Password for configuration file.		
Confirm Password:		
Save Config As		
♥ Import		
Import user settings by selecting the configuration file and clicking Import Config. Import User Accounts will invalidate all existing End-User and Administrators sessions.		
Browse No file chosen		
Password. Use this if the configuration file was password-protected		
Import Config		

- 17. Next, import the **All roles** XML configuration file. This step restores all the roles restriction settings for Virtual Ports.
- 18. After importing the 2 XML files and the system and user.cfg files, check and/or modify/add remaining local settings and other settings as necessary if not restored, such as:
  - a. Network > Overview settings (set in cluster or individual nodes)
  - b. Network > Routes (for internal, external and other ports)
  - c. Network > Hosts (set in cluster or individual nodes)
  - Metwork > Internal Port/ External Port>Virtual Ports (if clustered, set this up in cluster "Entire Cluster")
  - e. Network > VLANs (if clustered, set this up in cluster "Entire Cluster")
  - f. Network > VPN Tunneling (set in cluster or individual nodes)
  - g. Log/Monitoring > SNMP (set in cluster or individual nodes)
  - h. Log/Monitoring > Events/Admin Access/User Access > Settings (set in cluster or individual nodes if different)
  - i. Configuration>Certificates>Device Certificates (and its ports bindings)
  - j. Resource Policies>VPN Tunneling>Connection Profiles (if configured)
  - k. Auth Servers > ACE Auth server, if used (check the node secret file status)

- I. **Configuration > Licensing** License client-server settings (if used as license client in Enterprise Licensing Server environment), proper licenses installed
- 19. Check cluster status (if clustered) and test operation by logging in to the cluster VIPs (or the standalone PSA device IP). Test the authentication using AD, ACE, etc., and all other functionalities enabled, such as NC or Pulse.
- 20. This completes the MAG to PSA-V platform migration.

# References

# **PSA Hardware Guides**

https://www.pulsesecure.net/download/techpubs/current/502/pulseappliances/psa/p sa7000HardwareGuide.pdf

https://www.pulsesecure.net/download/techpubs/current/501/pulseappliances/psa/psa5000HardwareGuide.pdf

https://www.pulsesecure.net/download/techpubs/current/500/pulseappliances/psa/p sa3000HardwareGuide.pdf

https://www.pulsesecure.net/download/techpubs/current/499/pulseappliances/psa/psa300HardwareGuide.pdf

# Pulse Connect Secure Administration Guide

https://docs.pulsesecure.net/WebHelp/PCS/9.0R1/Home.htm

https://www.pulsesecure.net/download/techpubs/current/1219/pulse-connect-secure/pcs/9.0rx/ps-pcs-sa-9.0r1-admin-guide.pdf

# KB discussing supported network type for clustering

https://kb.pulsesecure.net/articles/Pulse\_Secure\_Article/KB26035

# **PSA-related KBs**

https://kb.pulsesecure.net/articles/Pulse\_Secure\_Article/KB40034/?q=kb40034&l=en\_US&fs=Sear ch&pn=1&atype=

https://kb.pulsesecure.net/articles/Pulse\_Secure\_Article/KB40035/?q=kb40034&l=en\_US&fs=Sear ch&pn=1&atype=

- 8.3R3 PCS and 5.4R3 PPS Service Provider Virtual Appliance Deployment Guide
- 8.3R3 PCS and 5.4R3 PPS License Configuration for VA-SPE/PSA-V Appliances: On-Premise and Cloud