CPS Migration and Upgrade Guide, Release 25.1.0

First Published: 2025-04-03

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

Preface

About This Guide

Note The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. While any existing biased terms are being substituted, exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

This document is a part of the Cisco Policy Suite documentation set.

For information about available documentation, see the *CPS Documentation Map* for this release at Cisco.com.

Note The PATS/ATS, ANDSF, and MOG products have reached end of life and are not supported in this release. Any references to these products (specific or implied), their components or functions in this document are coincidental and are not supported. Full details on the end of life for these products are available at: https://www.cisco.com/c/en/us/products/wireless/policy-suite-mobile/eos-eol-notice-listing.html.

Audience

This guide is best used by these readers:

- Network administrators

- Network engineers
- Network operators
- System administrators

This document assumes a general understanding of network architecture, configuration, and operations.

Additional Support

For further documentation and support:

- Contact your Cisco Systems, Inc. technical representative.
- Call the Cisco Systems, Inc. technical support number.
- Write to Cisco Systems, Inc. at support@cisco.com.
- Refer to support matrix at https://www.cisco.com/c/en/us/support/index.html and to other documents related to Cisco Policy Suite.

Conventions (all documentation)

This document uses the following conventions.

Conventions	Indication
bold font	Commands and keywords and user-entered text appear in **bold** font.
italic font	Document titles, new or emphasized terms, and arguments for which you supply values are in *italic* font.
[ ]	Elements in square brackets are optional.
{x | y | z }	Required alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
courier font	Terminal sessions and information the system displays appear in courier font.
< >	Nonprinting characters such as passwords are in angle brackets.

Conventions	Indication
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Note Means reader take note. Notes contain helpful suggestions or references to material not covered in the manual.

Caution Means reader be careful. In this situation, you might perform an action that could result in equipment damage or loss of data.

Warning IMPORTANT SAFETY INSTRUCTIONS.

Means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device.

SAVE THESE INSTRUCTIONS

Note Regulatory: Provided for additional information and to comply with regulatory and customer requirements.

Communications, Services, and Additional Information

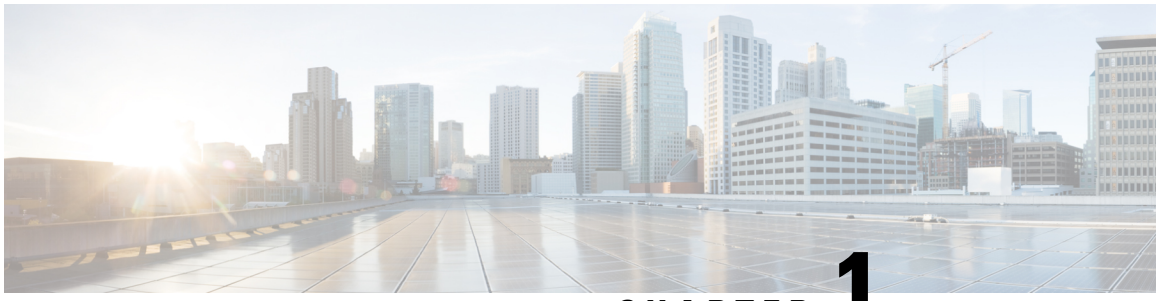
- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business results you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco DevNet.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

Important Notes

Important Any feature or GUI functionality that is not documented may not be supported in this release or may be customer specific, and must not be used without consulting your Cisco Account representative.



CHAPTER 1

Apply Patches to CPS

Apply a Patch

This section describes the general process to apply a patch to CPS.

Patches must be applied during a maintenance window. This section includes instructions for stopping all CPS components before applying the patch and restarting the components after the patch has been applied.

Note Only one patch can be applied to CPS at a time. If you have already applied a patch, you must Undo and then Remove the existing patch before applying the new patch. Refer to Undo a Patch and Remove a Patch for more information. To determine if a patch is currently applied to the system refer to List Applied Patches.

Procedure

Step 1 Run **patch -u** and **patch -r** to remove any applied patches from the Cluster Manager before proceeding. For more information, refer to Undo a Patch and Remove a Patch.

Step 2 Download the latest patch file from a location provided by your Cisco representative to the Cluster Manager VM.

Step 3 Log in to the Cluster Manager as a root user.

Step 4 Download the patch file to the Cluster Manager VM. For example:

```
wget http://siteaddress/xxx.tar.gz
```

where,

`siteaddress` is the link to the website from where you can download the patch file.

`xxx.tar.gz` is the name of the patch file.

Step 5 Run the **patch -a** command to apply the patch:

```
/var/qps/install/current/scripts/patch/patch -a filename.tar.gz
```

where *filename* is the path and filename of the downloaded patch file.

For example:

```
/var/qps/install/current/scripts/patch/patch -a /tmp/CPS701_1234.tar.gz
```

Step 6 Run the following command to restore the Policy Builder configurations.

```
/var/qps/install/current/scripts/setup/restorePolicyRepositories.sh
```

Step 7 Run **build_all.sh** script to create updated CPS packages. This builds updated VM images on the Cluster Manager with the new patch applied.

```
/var/qps/install/current/scripts/build_all.sh
```

Step 8 Update the VMs with the new software using **reinit.sh** script. This triggers each CPS VM to download and install the updated VM images from the Cluster Manager:

```
/var/qps/install/current/scripts/upgrade/reinit.sh
```

Step 9 Refer to section Rolling Restart of CPS VMs QNS Process (Odd Sides) , on page 2 and Rolling Restart of CPS VMs QNS Process (Even Sides), on page 3 for further steps.

Step 10 Run **about.sh** to verify that the component is updated:

```
about.sh
```

What to do next

After applying a patch in HA deployment, run the following command from Cluster Manager:

```
puppet apply --logdest=/var/log/cluman/puppet-custom-run.log
--modulepath=/opt/cluman/puppet/modules --config=/opt/cluman/puppet/puppet.conf
/opt/cluman/puppet/nodes/node_repo.pp
```

Note Manually enter `puppet apply` command in your system.

After applying the `puppet apply` command, run the following command from Cluster Manager to update the `/etc/httpd/conf/httpd.conf` file on all VMs:

```
/var/qps/install/current/scripts/modules/update_httpd_conf.py
```

Rolling Restart of CPS VMs QNS Process (Odd Sides)

Important The commands mentioned in the steps must be entered manually.

Procedure

Step 1 Stop Policy Server (qns) process:

```
for vmName in `hosts.sh | sort | sed -n 'p;n'`; do echo $vmName; ssh $vmName "service monit stop";
ssh $vmName "service qns stop"; echo; done
```

Step 2 Verify whether the Policy Server (qns) process has stopped:

```
for vmName in `hosts.sh | sort | sed -n 'p;n'`; do echo $vmName; ssh $vmName "service qns status";
echo; done
```

Step 3 Start Policy Server (qns) process:

```
for vmName in `hosts.sh | sort | sed -n 'p;n'`; do echo $vmName; ssh $vmName "service qns start";
ssh $vmName "service monit start"; echo; done
```

Step 4 Verify that the Policy Server (qns) process has started:

```
for vmName in `hosts.sh | sort | sed -n 'p;n'`; do echo $vmName; ssh $vmName "service qns status";
echo; done
```

Step 5 Verify the CPS health status using the `diagnostics.sh` script.

Rolling Restart of CPS VMs QNS Process (Even Sides)

Important The commands mentioned in the steps must be entered manually.

Procedure

Step 1 Stop Policy Server (qns) process:

```
for vmName in `hosts.sh | sort | sed -n 'n;p'`; do echo $vmName; ssh $vmName "service monit stop";
ssh $vmName "service qns stop"; echo; done
```

Step 2 Verify whether the Policy Server (qns) process has stopped:

```
for vmName in `hosts.sh | sort | sed -n 'n;p'`; do echo $vmName; ssh $vmName "service qns status";
echo; done
```

Step 3 Start Policy Server (qns) process:

```
for vmName in `hosts.sh | sort | sed -n 'n;p'`; do echo $vmName; ssh $vmName "service qns start";
ssh $vmName "service monit start"; echo; done
```

Step 4 Verify that the Policy Server (qns) process has started:

```
for vmName in `hosts.sh | sort | sed -n 'n;p'`; do echo $vmName; ssh $vmName "service qns status";
echo; done
```

Step 5 Verify the CPS health status using the `diagnostics.sh` script.

Undo a Patch

The following steps disables the currently applied CPS patch, and reverts the system to the base software version. For example, if a patch 7.5.0.xx is installed on the system, this command reverts the software to the base version 7.5.0.

Note If you have custom plug-ins installed in your system, refer to CPS Installations using Custom Plug-in before executing the `patch -u` command.

To undo the applied patch, execute the following command on the Cluster Manager:

```
/var/qps/install/current/scripts/patch/patch -u
```

After undoing the applied patch execute the following commands in Cluster Manager to re-build the CPS system and push the changes to VMs:

```
/var/qps/install/current/scripts/build_all.sh
```

```
/var/qps/install/current/scripts/upgrade/reinit.sh
```

After undoing a patch, qns processes need to be restarted. Refer to Rolling Restart of CPS VMs QNS Process (Odd Sides) , on page 2 and Rolling Restart of CPS VMs QNS Process (Even Sides), on page 3 for further steps.

Remove a Patch

Execute the following command on the Cluster Manager to completely remove a patch and all related items from the Cluster Manager. This deletes the patch file from the `/var/qps/.tmp/patches` directory of the Cluster Manager:

```
/var/qps/install/current/scripts/patch/patch -r patch_name
```

where, *patch_name* is the name of patch you want to remove.

Example,

/var/qps/install/current/scripts/patch/patch -r Patch_1_11.9.9

Note Currently, CPS supports only one patch at a time. You must remove any existing patches before applying a new patch.

After removing a patch, qns processes need to be restarted. Refer to Rolling Restart of CPS VMs QNS Process (Odd Sides) , on page 2 and Rolling Restart of CPS VMs QNS Process (Even Sides), on page 3 for further steps.

List Applied Patches

Execute the following command on Cluster Manager to list the applied patches installed in the system:

```
/var/qps/install/current/scripts/patch/patch -l
```

The `about.sh` command also displays if any patch is applied on the current CPS system or not.

CPS Installations using Custom Plug-in

CPS provides several methods to patch baseline release functionality. One method utilizes the “repositories” configuration file to specify the location of additional software on the CPS Cluster Manger. As such, the current patch utilities aide in removing all repositories. However, CPS Custom plug-in software also uses the “repositories” configuration file to specify the location of custom software. Therefore an additional manual step is required to reconfigure CPS custom plug-in code after patches are removed.

Procedure

Step 1 From the CPS Cluster Manager, undo the patches:

Note
While the patch utility logs that it is removing the repositories configuration file, it actually renames it, at the same path location, as “repositories.back”.

```
/var/qps/install/current/scripts/patch/patch -u
```

The following messages show the progress of the `patch -u` command:

```
undo the patches
copy puppets from /var/qps/patches backup to /var/qps/install/current/puppet
copy scripts from /var/qps/patches backup to /var/qps/install/current/scripts
remove /etc/broadhop/repositories
patch undone successfully, please run build_all.sh and reinit.sh to push the changes to VMs
```

Step 2 For CPS installations utilizing custom plug-ins, the following step is required before software upgrade.

a. From the CPS Cluster Manager, restore the “repositories” configuration file, without patch references.

Copy the repositories backup to the original location:

```
cp /etc/broadhop/repositories.back /etc/broadhop/repositories
```

b. Remove references to software patch locations, and leave references to custom plugin code:

In the example below, leave the first line (`file:///var/qps/.tmp/plugin1`) as it is, and remove the second line (`file:///var/qps/.tmp/patch1`) before continuing with the software upgrade process.

```
file:///var/qps/.tmp/plugin1
```

```
file:///var/qps/.tmp/patch1
```