# CPS Release Notes, Release 9.1.0

**First Published:** April 29, 2016

**Last Updated:** April 29, 2016

## Contents

This document describes the new features, feature versions and limitations for the Cisco Policy Suite software. Use this document in combination with documents listed in the Obtaining Documentation and Submitting a Service Request, page 12.

This document includes the following sections:



## New and Changed Information

The following sections provide the descriptions of various features that have been added/modified in this release:

### API to Support Additional Hosts Entry

CPS now supports the capability to configure new peer nodes such as PCEF, NTP, NMS, and so on, by modifying the `/etc/hosts` files on all CPS VMs.

To retrieve (GET) the AdditionalHosts configuration from the CPS Cluster Manager VM:

```
GET http://<Cluster Manager IP>:8458/api/system/config/additional-hosts
```

To add or update an AdditionalHosts Entry:

```
PUT http://<Cluster Manager IP>:/api/system/config/additional-hosts
```

The API logs are written in the `/var/log/orchestration-api-server.log` and `/var/log/startupStatus.log` files.

For more information, refer to the *CPS Installation Guide for OpenStack*.

## Support for API Validation

When the orchestration API is used to load configurations to the CPS cluster, the following basic validations are now performed:

- The replica set hosts are in hosts or additionalHosts
- Standard aliases are present (lb01, lb02, and so on)
- Standard VLAN names are present (Internal, Management, and so on)
- Range checking (for example, IPv4/IPv6 IP address syntax validation)
- Cross-referencing of VLANs with hosts

These validations are used when issuing the following API:

POST http://*<Cluster Manager IP>*:8458/api/system/config/

If a validation error is detected, an appropriate message is provided in the API response, and reported in `/var/log/orchestration-api-server.log`.

For more information, refer to the *CPS Installation Guide for OpenStack*.

## Rx Client Configuration Enhancements

New **10.0.0 Early Feature** parameters have been added under Rx Client in Policy Builder to support Mobile Orchestration Gateway. The following are the new parameters:

- Flow Description Source Ip Evaluation: This is a drop-down list. User has the following three options to select from:
  - None: When selected, CPS does not take any action on source IP.
  - Replace Src IP: When selected, CPS replaces flow description source IP with UE framed IP.
  - Replace Src IP if 'any': When selected, CPS replaces the flow description source IP with UE framed IP if source IP is ‘any’.
- Calculate Precedence Avp Value check box: When checked, it enables CPS to send different precedence values for each Rx session for the same Gx session. Default value is unchecked (false).
- Remove Rule On Rule Deactivation check box: When checked, it enables CPS to send different precedence values for each Rx session for the same Gx session. Default value is unchecked (false).
- Authorize Sponsor Data Connectivity check box: When checked, CPS validates the sponsor ID received in AAR request. If the received sponsor ID is unauthorized, CPS returns UNAUTHORIZED_SPONSORED_DATA_CONNECTIVITY (5067) code in AAA. Default value is unchecked (false).

For more information, refer to *Rx Clients* section in *CPS Mobile Configuration Guide* for this release.

## Documentation

The titles of the following CPS guides have been updated for this release:

**Table 1 Guide Name Changes**

| Old Titles | New Titles |
|---|---|
| Cisco Policy Suite Installation Guide | CPS Installation Guide for VMware |
| Cisco Policy Suite Dynamic Orchestration Guide | CPS Installation Guide for OpenStack |

# Installation Notes

## Download ISO Image

Download the 9.1.0 software package (ISO image) from:

https://software.cisco.com/download/release.html?i=!y&mdfid=284883911&softwareid=284979976&release=9.1.0&os=

**Md5sum Details:**

| | |
|---|---|
| 01cd12ec4f989be8b1f6a8630e44ebe9 | CPS_9.1.0_Base.release.tar.gz |
| 061bede8b06769fb2379c8e339acf791 | CPS_9.1.0.release.iso |

## Component Versions

The following table lists the component versions for the CPS 9.1.0 Release:

**Table 2 Component Versions**

| Component | Version |
|---|---|
| ANDSF | 1.2.1.release |
| API router | 1.1.1.release |
| Audit | 1.7.1.release |
| Balance | 4.0.1.release |
| Cisco API | 1.3.1.release |
| Cisco CPAR | 1.3.1.release |
| Control Center | 3.7.1.release |
| Congestion Reference Data | 1.5.1.release |
| Core | 9.1.0.release |
| CSB | 2.0.1.release |
| Custom Reference Data | 3.0.1.release |
| DRA | 1.1.1.release |
| DHCP | 1.7.1.release |
| Diameter2 | 4.0.1.release |
| Fault Management | 1.3.1.release |
| Hotspot | 1.1.0.release |
| ISG Prepaid | 2.1.1.release |
| LDAP | 2.0.1.release |
| Notification | 7.0.1.release |
| Policy Intel | 3.0.1.release |
| POP-3 Authentication | 1.7.1.release |
| RADIUS | 3.6.1.release |

**Table 2 Component Versions**

| Component | Version |
|---|---|
| Recharge Wallet | 1.5.1.release |
| SCE | 2.4.1.release |
| Scheduled Events | 1.6.1.release |
| SPR | 3.0.1.release |
| Unified API | 3.0.1.release |
| Web Services | 1.8.1.release |

# New Installations


- VMware Environment, page 4
- OpenStack Environment, page 4


## VMware Environment

To perform a new installation of CPS 9.1.0 in a VMware environment, refer to *CPS Installation Guide for VMware*.

## OpenStack Environment

To perform a new installation of CPS 9.1.0 in an OpenStack environment, refer to the *CPS Installation Guide for OpenStack*.

# Upgrading an Existing CPS Installation

To upgrade an existing CPS installation, refer to the *CPS Upgrade Guide*.

**Note:** In-service software upgrades to 9.1.0 are supported only from CPS 7.0.5 or higher. If needed, upgrade CPS to 7.0.5 before proceeding.

**Note:** In-service software upgrades to 9.1.0 are supported only for Mobile installations. Other CPS installation types (Wi-Fi, MOG) cannot be upgraded using ISSU.

**Note:** Currently, All-in-One (AIO) upgrades are not supported.

## Post Upgrade Steps

### Re-apply Configuration Changes

After the upgrade is finished, compare your modified configuration files that you backed up earlier with the newly installed versions. Re-apply any modifications to the configuration files.

### Verify Configuration Settings

After the upgrade is finished, verify the following configuration settings.

**Note:** Use the default values listed below unless otherwise instructed by your Cisco Technical Representative.

**Note:** During the upgrade process these configuration files are not overwritten. Only during a new install will these settings be applied.

- **/etc/broadhop/qns.conf**

```
-Dmongo.client.thread.maxWaitTime.balance=1200
-Dmongo.connections.per.host.balance=10
-Dmongo.threads.allowed.to.wait.for.connection.balance=10
-Dmongo.client.thread.maxWaitTime=1200
-Dmongo.connections.per.host=5
-Dmongo.threads.allowed.to.wait.for.connection=10
-Dcom.mongodb.updaterIntervalMS=400
-Dcom.mongodb.updaterConnectTimeoutMS=600
-Dcom.mongodb.updaterSocketTimeoutMS=600
-DdbSocketTimeout.balance=1000
-DdbSocketTimeout=1000
-DdbConnectTimeout.balance=1200
-DdbConnectTimeout=1200
-Dcontrolcenter.disableAndsf=true
-DnodeHeartBeatInterval=9000
-DdbConnectTimeout.balance=1200
-Dstatistics.step.interval=1
-DshardPingLoopLength=3
-DshardPingCycle=200
-DshardPingerTimeoutMs=75
-Ddiameter.default.timeout.ms=2000
-DmaxLockAttempts=3
-DretryMs=3
-DmessageSlaMs=1500
-DmemcacheClientTimeout=200
-Dlocking.disable=true
```

**Note:** The following setting should be present only for GR (multi-cluster) CPS deployments:

```
-DclusterFailureDetectionMS=1000
```

**Note:** In an HA or GR deployment with local chassis redundancy, the following setting should be set to **true**. By default, this is set to false.

```
-Dremote.locking.off
```

- **/etc/broadhop/diameter_endpoint/qns.conf**

```
-Dzmq.send.hwm=1000
-Dzmq.recv.hwm=1000
```

### Reconfigure Service Option

After upgrading from previous release to the current CPS release, Service option configured with Subscriber-Id becomes invalid and customer needs to reconfigure multiple Subscriber Id in SpendingLimitReport under Service Configurations.

## Additional Notes

The following section contains some additional notes which are necessary for proper installation/working of CPS:

- Session Manager Configuration: After a new deployment, session managers are not automatically configured.
  a. Edit the `/etc/broadhop/mongoConfig.cfg` file to ensure all of the data paths are set to `/var/data` and not `/data`.
  b. Then execute the following command from pcrfclient01 to configure all the replication sets:

```
/var/qps/bin/support/mongo/build_set.sh --all --create
```

- Default gateway in lb01/lb02: After the installation, the default gateway might not be set to the management LAN. If this is the case, change the default gateway to the management LAN gateway.
- CSCuq83478: Diameter haproxy configuration is not correct for IPv6 addresses.

  **Fix:** IPv6 tables need to be turned OFF for IPv6 traffic on lb01, lb02. Management and IPv6 Gx traffic should be on different VLANs in VLAN.csv file at the time of deployment.
- CSCux20675: High message timeouts observed after qnsxx power on

  **Symptom:** High Timeouts observed when qnsxx is brought back into service/recovered after an VM outage.

  **Conditions/Scenario:** Normal HA setup with call model running.

  **Workaround:** Any recovery (blade/VM) should done during off-peak hour when other VMs CPU is < 50%.
- CSCuy23530: Receiving error msg while creating subscriber from SPR API

  **Conditions**: If `clusterPeers` flag is configured in `/etc/broadhop/iomanager01/qns.conf` file OR `/etc/broadhop/iomanager02/qns.conf` file in previous installation of CPS and you are upgrading to 9.1.0.

  **Apply Configuration Change:**

  If `clusterPeers` flag is configured move the flag with same value to `/etc/broadhop/qns.conf` file

  OR

  If `clusterPeers` flag is not configured, add `clusterPeers` entry to `/etc/broadhop/qns.conf` file. Also remove `clusterPeers` entry from `/etc/broadhop/iomanager01/qns.conf` file and `/etc/broadhop/iomanager02/qns.conf` file.

  **Impact if above change is not applied:**

  If `clusterPeers` flag is not moved to new location, cluster broadcast message will not happen.

  **Recommended:** This change is highly recommended to be applied.
- CSCuz43943: Replacing SrcAddress and Port to any is not working

  **Symptom:** PCRF has no option to ignore SOURCE IP in AAR request and send ANY to PGW.

  **Conditions/Scenario:** SOURCE IP is sent in flow description in AAR from the AF.

  **Workaround:** Custom policy needs to be added in AF to replace the SOURCE IP in flows to ANY before sending it to PCRF.
- CSCuz44551: Usage Monitoring key AVP sent in GX RAR when no Usage monitoring needed

  **Problem Description:** Usage Monitoring key AVP is sent out in Gx RAR in case no Usage monitoring is required.

  **Conditions/Scenario:** The Monitoring key AVP is sent even if the usage monitoring is enabled/disabled for sponsored data use case.

  **Workaround:** This issue has no adverse effect as monitoring key without monitoring information in Gx RAR is ignored by PGW.
- CSCuy82522: Incorrect config file on system leads to SSH blocked after upgrade

  **Problem Description:** SSH is blocked on Installer

  **Conditions/Scenario:** The /root/.ssh/config file is modified duing install.sh which blocks ssh

  **Workaround:** The /root/.ssh/config file is modified as below which blocks ssh.

```
[root@C_installer .ssh]# cat /root/.ssh/config
StrictHostKeyChecking=noUserKnownHostsFile=/dev/null
LogLevel=quiet
```

Manually change to:

```
[root@C_installer .ssh]# cat /root/.ssh/config
StrictHostKeyChecking=no
UserKnownHostsFile=/dev/null
LogLevel=quiet
```

- CSCuy82546: custom config file results in HTTPD process unable to start after ISSU

  **Problem Description:** ISSU upgrade fails with errors:

```
http://installer/rpms/quantum/qps/x86_64/repodata/repomd.xml: [Errno 14] PYCURL ERROR 7 - "couldn't
connect to host"
Trying other mirror.
Error: Cannot retrieve repository metadata (repomd.xml) for repository: QPS-Repository. Please
verify its path and try again
You could try using --skip-broken to work around the problem
You could try running: rpm -Va --nofiles --nodigest

Starting httpd: Syntax error on line 1 of /etc/httpd/conf.d/reqtimeout.conf:
Invalid command 'RequestReadTimeout', perhaps misspelled or defined by a module not included in the
server configuration
                                [FAILED]
```

  **Conditions/Scenario:** The httpd process is unable to start.

  **Workaround:** Check if `/etc/httpd/conf.d/reqtimeout.load` is present.

  If it is, edit /`etc/httpd/conf.d/reqtimeout.conf` and add `Include conf.d/reqtimeout.load` as the first line of the file. For example:

```
[root@installer cluman]# cat /etc/httpd/conf.d/reqtimeout.conf
Include conf.d/reqtimeout.load
RequestReadTimeout header=10-20,minrate=500
RequestReadTimeout body=10,minrate=500
```

- CSCuy82570: CPS 9.0- 2nd attempt to run install.sh script aborts automatically

  **Problem Description:** The install.sh script aborts itself.

  **Conditions/Scenario:** The file `/var/qps/install/current/release-train-7.5.1.tar.gz` modified to `/var/qps/install/current/release-train-9.0.0.tar.gz` during the first failed run of install.sh.

  **Workaround:** Rename the file back to `/var/qps/install/current/release-train-7.5.1.tar.gz` and rerun install.sh.

- By default, pending transaction feature is enabled. If you are not using it, Cisco recommends to disable pending transaction feature post deployment.

  To disable pending transaction, the following parameter can be configured in `/etc/broadhop/qns.conf` file:

```
com.broadhop.diameter.gx.pending_txn.attempts=0
```

  After adding the parameter in `qns.conf` file, restart all VMs.

- If TPS is high, user needs to disable “STA”. To disable STA, user needs to create custom policies. For more information, contact your Contact Technical Representative.

# Limitations and Restrictions

This section covers the following topics:



## Limitations

- If you have a system with the old installer (6.1 or prior), it is mandatory to use the new installer to create VMs and use the new release trains. The latest 9.0.0 release train does not work with the old environment (AIO/HA).
- Solicited Application Reporting

  The following are some restrictions on configuration for the new service options:

  - The pre-configured ADC rule generated by CRD lookup has ADC-Rule-Install AVP definition with support for only three AVPs ADC-Rule-Name, TDF-Application-Identifier, Mute-Notification.
  - For AVPs which are multi-valued, CRD tables are expected to have multiple records - each giving the same output.
  - Comma(,) is not a valid character to be used in values for referenced CRD column in SdToggleConfiguration.
  - AVP Table currently only supports OctetStringAvp value for AVP Data-type.
- During performance testing, it has been found that defining a large number of QoS Group of Rule Definitions for a single sessions results in degraded CPU performance. Testing with 50 QoS Group of Rule Definitions resulted in a 2x increase in CPU consumption. The relationship appears to be a linear relationship to the number of defined QoS Group of Rule Definitions on a service.
- Hour Boundary Enhancement

  Change in cell congestion level when look-ahead rule is already installed:

  If a cell congestion value changes for current hour or any of the look-ahead hours, there will be no change in rule sent for the rules which are already installed.

  No applicability to QoS Rules:

  The look-ahead works for PCC rules only where we have rule activation/deactivation capabilities and can install upcoming changes in advance. However, if the RAN Congestion use case is changed to use the QoS-Info AVP instead of using PCC rules, we need to fall back to the current RAR on the hour boundary implementation for that use case since the standard do not let us install QoS-info changes ahead of time like we can with PCC rules.
- The Cluster Manager's internal (private) network IP address must be assigned to the host name “installer” in the `/etc/hosts` file. If not, backup/restore scripts (env_import.sh, env_export.sh) will have access issues to pcrfclient01/pcrfclient02 VMs.
- The linux VM message.log files repeatedly report errors similar to:

  ```
  vmsvc [warning] [guestinfo] RecordRoutingInfo: Unable to collect IPv4 routing table.
  ```

  This is a known issue affecting ESXi 5.x. Currently, there is no workaround. The `messages.log` file entries are cosmetic and can be safely ignored. For more information, refer to http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2094561

## Common Vulnerabilities and Exposures (CVE)

The following is the list of publicly known Common Vulnerabilities and Exposures (CVE) apply to this version of CPS:

- February 2016 Vulnerabilities:
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160218-glibc
- For NTP:
  - October 2015 Vulnerabilities:
    https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20151021-ntp
  - January 2016 Vulnerabilities:
    https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160127-ntp
- For OpenSSL:
  - December 2015 Vulnerabilities:
    https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20151204-openssl
  - January 2016 Vulnerabilities:
    https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160129-openssl
  - March 2016 Vulnerabilities:
    https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160302-openssl

# CDETS

The following sections lists Open CDETS and Resolved CDETS for Cisco Policy Suite. For your convenience in locating CDETS in Cisco's Bug Toolkit, the caveat titles listed in this section are drawn directly from the Bug Toolkit database. These caveat titles are not intended to be read as complete sentences because the title field length is limited. In the caveat titles, some truncation of wording or punctuation might be necessary to provide the most complete and concise description.

**Note:** If you are a registered cisco.com user, view Bug Toolkit on cisco.com at the following website:

**https://tools.cisco.com/bugsearch**

To become a registered cisco.com user, go to the following website:

https://tools.cisco.com/RPF/register/register.do?exit_url=

## Open CDETS

The following table lists the open CDETS in the CPS 9.1.0 release.

**Table 3 Open CDETS**

| CDETS ID | Headline |
|---|---|
| CSCux38115 | GR A/A sys test: session_cache_ops need to change for shards |
| CSCuy50314 | GT_ST: One site shown relatively higher avg response time for Rx messages |
| CSCuy53225 | Timezone is changing from IST to MST after upgrade |
| CSCuy63114 | Unable to run /var/qps/bin/control/trace.sh |
| CSCuy69067 | mon_db_for_callmodel not monitoring reporting properly |
| CSCuy82102 | Remove IPv6 from STR in case ANGW has only IPv4 address |

**Table 3 Open CDETS**

| CDETS ID | Headline |
|---|---|
| CSCuy82522 | Incorrect config file on system leads to SSH blocked after upgrade |
| CSCuy82546 | custom config file results in HTTPD process unable to start after ISSU |
| CSCuy82570 | 2nd attempt to run install.sh script aborts automatically |
| CSCuy88753 | puppet shows error on qns when firewall is disabled from enabled state |
| CSCuy96208 | CDR's are not generated for Time and Volume usage reported in CCR-T |
| CSCuy97683 | Monitoring Key disabling again in CCR-U even its already disabled |
| CSCuz20128 | Balance Cache Enhancement: Query onetime for Subscriber without balance |
| CSCuz43943 | Replacing SrcAddress and Port to any is not working |
| CSCuz44551 | Usage Monitoring key AVP sent in GX RAR when no Usage monitoring needed |

# Resolved CDETS

The following table lists the resolved/verified CDETS in the CPS 9.1.0 release.

**Table 4 Resolved CDETS**

| CDETS ID | Headline |
|---|---|
| CSCuw75562 | CPS doesn't consider all available peers while retrying on alternate host |
| CSCux50087 | CPS 8.0- A dashboard needs to be saved separately on pcrfclient 01 & 02 |
| CSCux50114 | CPS 8.0- Grafana 503 service not available when pcrfclient01 is booting |
| CSCux85659 | Support configuration of Session-Release-Cause AVP in RAR messages |
| CSCuy02773 | TACACS+ prompt for password multiple time while executing diagnostic.sh |
| CSCuy07668 | Evaluation of qps for OpenSSL January 2016 Vulnerabilities |
| CSCuy18980 | Fix issue with collectd exec scripts |
| CSCuy20663 | Evaluation of Cisco Policy Suite for NTP January 2016 Vulnerabilities |
| CSCuy32665 | Stopping internal interface on standby SM causes 50+ ms lock times |
| CSCuy42128 | cps is retrying message with incorrect destination host name and realm |
| CSCuy51595 | Evaluation of Cisco Policy Suite (CPS) for glibc_feb_2016 vulnerability |
| CSCuy63720 | Sh Retry on CCR-u not working |
| CSCuy64039 | Intermittent AF App Id validation failures after system recovery |
| CSCuy65119 | Updated Override Controls not sent after PNR profile change |
| CSCuy65191 | Error in recovering cluster manager |
| CSCuy70411 | CPS sends SyPrime messages to wrong peers |
| CSCuy72384 | Sh Retry Race Condition Not working, CCR-u before CCR-i retries finishes |
| CSCuy73085 | mongodb.MongoExpirationQuery - Session expiry fail with exception |
| CSCuy73600 | CPS - Gx-RAR not getting generated intermittently. |
| CSCuy77635 | PBJ link should not be displayed in about.sh and CPS Central page |
| CSCuy78687 | Support for non blocking CDR |
| CSCuy78736 | NPE in Rx NDM on Gx RAR timeout (NetLoc/Ran-Nas-Cause feature enabled) |
| CSCuy79618 | Platform: Orch API log can grpw unbounded during error conditions |
| CSCuy80228 | Minor configuration/logging issue for vQoS |
| CSCuy81067 | PCRF sending SGSN_IPV6_ADDRESS value with only Prefix value in Sy-AAR |

**Table 4 Resolved CDETS**

| CDETS ID | Headline |
|---|---|
| CSCuy81135 | PCRF including IMS default bearer values in GX-RAR for an AUDIO call |
| CSCuy82196 | Firewall rules are enabled even when firewallState is set to “disabled” |
| CSCuy82683 | CPS 9.0- DiameterMessageDealer-Error decoding message exception seen |
| CSCuy84851 | on qns/session VMs mongoauth iptable rules getting deleted alternatively |
| CSCuy86619 | Installation guide have no information about multiple Cert in DER format |
| CSCuy87721 | CPS-9.0 ISSU upgrade was failed due to missing package on CM VM |
| CSCuy88082 | Called Station Id AVP not picked upon receiving CCR-U |
| CSCuy88129 | LDAP: Existing dedicated bearer is not deleted after MIND revalidation |
| CSCuy88992 | Override control missing in CCA-U message during Session sync |
| CSCuy90491 | Consolidated Syslog is not failing over to pcrfclient02 |
| CSCuy92886 | GR: Stale Sessions are not getting deleted in MOG-GR setup |
| CSCuz01165 | max wait time fix |
| CSCuz01902 | pcrf feature changes |
| CSCuz03453 | Hit Not Found errors when trying to export service configuration |
| CSCuz06602 | puppet error on arbiter installation on third site |
| CSCuz07864 | CPS 9.0 - puppet error during patch installation |
| CSCuz09298 | Some config.csv values missing from Orch API yaml config |
| CSCuz11301 | Platform: Whisper logs taking up 20+GB of space during error conditions |
| CSCuz13043 | ISSU: During ISSU after VM reboot pcrfclient puppet fails at grafana |
| CSCuz18955 | mongo_stat.sh does not terminate when collectd does |
| CSCuz20128 | Balance Cache Enhancement: Query onetime for Subscriber without balance |
| CSCuz21008 | CPS9.0- Upon LDAP timeout/down during refresh installed rulebase removed |
| CSCuz28044 | Monitoring Key 3e8 not being set correctly in CCA-i |
| CSCuz29693 | CPS is not binding Rx session with Gx session when IMSI_APN set |
| CSCuz40494 | OpenStack Cluster4 - Stability Test - qns restart |

# Related Documentation

This section contains information about the documentation available for Cisco Policy Suite.

## Release-Specific Documents

Refer to the following documents for better understanding of the Cisco Policy Suite.

- *CPS Backup and Restore Guide*
- *CPS Geographic Redundancy Guide*
- *CPS Installation Guide for VMware*
- *CPS Installation Guide for OpenStack*
- *CPS Mobile Configuration Guide*

- *CPS Operations Guide*
- *CPS Policy Reporting Guide*
- *CPS Release Notes*
- *CPS Troubleshooting Guide*
- *CPS Upgrade Guide*
- *CPS Wi-Fi Configuration Guide*
- *CPS_MOG SNMP and Alarms Guide*

The documents can be downloaded from the following links:

- Common Guides: http://www.cisco.com/c/en/us/support/wireless/quantum-policy-suite-bng/products-installation-and-configuration-guides-list.html
- Mobile Configuration Guide: http://www.cisco.com/c/en/us/support/wireless/quantum-policy-suite-mobile/products-installation-and-configuration-guides-list.html
- Wi-Fi Configuration Guide: http://www.cisco.com/c/en/us/support/wireless/quantum-policy-suite-wi-fi/products-installation-and-configuration-guides-list.html

# Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation*.

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the What's New in Cisco Product Documentation RSS feed. The RSS feeds are a free service.



This document is to be used in conjunction with the documents listed in the Obtaining Documentation and Submitting a Service Request, page 12 section.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.