



Cisco Policy Suite 18.5.0 Release Notes (1) (Restricted Release)

First Published: November 21, 2018

Last Updated: October 11, 2021

IMPORTANT: CPS 18.5.0 is a Short Term Support (STS) release with availability and use restrictions. Contact your Cisco Account or Support representatives, for more information.

Introduction

This release note identifies new features and enhancements, limitations and restrictions, and open and resolved CDETS in Cisco Policy Suite (CPS) software version 18.5.0. Use this release note in combination with the documentation listed in the Related Documentation section.

This release note includes the following sections:

- New and Changed Feature Information
- Installation Notes
- Limitations and Restrictions
- Open and Resolved CDETS
- Related Documentation
- Obtaining Documentation and Submitting a Service Request

New and Changed Feature Information

This section identifies features that are new or modified in this release.

ANDSF

No new features or changes were introduced in this release.

ATS

Diameter Performance Test Measurement and Reporting

In this release, the following new configuration parameters are included to configure Diameter performance test measurement and reporting:

- `Diameter.Load.Display.Failure.Events=true/false`: This parameter is used to display the Diameter message failover or failback message chart in the Cucumber report. This parameter is included in the `config.properties` file.
- `Diameter.Load.Timeline.Interval=X`: This timer is included in the `timer.properties` file and is used to set the time interval to collect average response time for each interface. The time is specified in minutes. For example, if X is 10, PATS collects average response time every 10 minutes for the entire execution time.

For more information, contact your Cisco Technical Support Representative.

Lattice Functional SubSystem (LFS) Integration with Custom Grammar

PATS supports connections to multiple LFS nodes and execution of APIs to run call flows on different set of network components. LFS is integrated with the PATS.

Supported Versions: site-lfs driver version 18.17.0 and later

Before you use the LFS grammars, configure LFS. In `config.properties` file, specify the following properties:

- To define the LFS endpoint addresses [Mandatory]:

```
LFSInstance01.API.EndpointAddress=http://10.106.183.206:32184/lfs/api/v1.0
```

- To define the LFS endpoints names:

```
LFS.Instance.Names=LFSInstance01
```

PATS provides the following LFS-related grammars:

- Configuring LFS Instance
- Verify Configuration
- Create Node
- Verify Create Node Success Response
- Send Message
- Send Message with Attributes
- Verify Send Message Success Response with Attributes
- Verify Generic Response

New and Changed Feature Information

PATS provides the following asynchronous LFS-related grammars:

- Define Message Filter
- Handle Message in any order
- Handle Message in strict order
- Validate action with ActionID

For more information, contact your Cisco Technical Support Representative.

Support for Asynchronization REST Communication on PATS

In this release, the following new grammars are included to send and validate asynchronous REST call using PATS REST client in PATS Web Service Driver:

- Send Asynchronous REST call using message reference
- Send Asynchronous REST call using attributes
- Send Asynchronous REST call using message reference and attributes
- Validation of the received response

For more information, contact your Cisco Technical Support Representative.

Support for SNMPv3 on PATS

ATS now supports SNMP version 3 test cases.

For more information, contact your Cisco Technical Support Representative.

Behavior Changes

No changes were introduced in this release.

Cisco Ultra eSCEF

Cisco Ultra eSCEF, Release 18.5.0 is qualified for lab testing and for limited controlled live trial purposes only.

Geographic Redundancy

No new features or changes were introduced in this release.

LWR

Support to Store Attributes in LWR

CPS is now enhanced to add multiple attributes in LWR.

For more information, see *CPS LWR Guide*.

Mobile

Convert Attribute from String to Timestamp for Policy Calculations

CPS now converts Sh attribute “vdsThrtlPlcyExpireTs” and stores this in date/timestamp format using custom diameter AVP so that it can be used later for evaluation of Revalidation-Time AVP in Gx RAR. This requires using system generated customer AVPs from the original Sh attribute to store the revalidation time and difference time value.

For more information, see *Setting Up Additional Profile Data* section in *CPS Mobile Configuration Guide*.

Ignore Case in Sh Attributes for CRD Lookup

CPS now uses Policy Builder configuration option under Sh profile to convert and store lowercase values of Sh code in external-profile. This makes implementation generic and makes CRD table population easier and as per requirement.

For more information, see *Setting Up Additional Profile Data* section in *CPS Mobile Configuration Guide*.

Parse and Prioritize Multiple Service Plans from Comma-delimited Format

CPS now uses attribute code “svcPlan” for splitting comma separated values. Any new attribute which requires similar treatment need code changes.

The following new parameter must be added to the qns.conf file:

- addOnlysvcPlanAsVirtualService

For more information, contact your Cisco Technical Support Representative.

Single Sh Enhancements

In this release, CPS supports multiple XML blobs in Sh interface, which correspond to multiple Gx sessions for a subscriber. Following enhancements have been done to the existing single Sh behavior:

1. SNR with Framed-IP and Service-Indication is sent to HSS for each Gx session.
2. CPS handles PNR with multiple xml blobs and map attributes to the appropriate Gx session to send RARs.

The following new option is added under Sh Parsing Rules in Sh Profile:

- Use Service Indications for Service Data Caching

When this option is enabled, on receiving Sh messages (SNA/PNR) with Sh-User-Data CPS verifies if there is any XML blob with ServiceIndication matching the configured Service-Indication in the PB Domain configuration for that Gx Session. If a match is found, corresponding ServiceData attributes are updated for that session

For more information, see *Setting Up Additional Profile Data* section in *CPS Mobile Configuration Guide*.

Note: In CPS 18.5.0 release, this feature is of demo quality. For more information, contact your Cisco Account representative.

SPR Cache Cleanup by Backup Database

CPS now supports removal of subscriber records located on remote SPR Mongo databases during Gx termination (CCR-T).

When SPR cache cleanup is enabled, CPS writes the subscriber record ID to a sprCleanupQueue that runs on each Policy Server (qns) node when a cross-site remove action occurs. The process MonitorSprCleanupQueue fetches these messages off the queue at configured intervals and writes them to the cleanupSubscriber database maintained on the local hot standby database. Another process, MonitorCleanUpSubscriberDB, fetches the records in a batch from the cleanupSubscriber database and remove these to their respective Remote SPR databases cross-site. In most cases, these records are already deleted. If this action deletes the record, or fails to find the record (previously deleted), the record is then removed from the cleanupSubscriber database. If CPS fails to delete the record because of connectivity, or other blocking issues, the record is retained to be tried again.

The following new statistics have been added:

- subscriberCleanup.addedToQueue: SPR record added to the queue.
- subscriberCleanup.removedFromQueue: SPR record deleted from the queue.
- subscriberCleanup.insert.success/subscriberCleanup.insert.failure: Number of remote subscribers written from queue to subscriberCleanup database on hot standby.
- spr.remote.cleanupDelete.success." + dbAddress/spr.remote.cleanupDelete.failure." + dbAddress: Counter registers when a subscriber is deleted on a remote SPR.

Note: Most transactions do not delete any records as the records have already been removed.

Example: spr.remote.cleanupDelete.success.site1-sessionmgr05:27720

Support for CPS Load Balancer Protection

In this release, CPS supports protecting itself from external signaling storms while still processing as much traffic as it safely can so that it can survive the storm.

For more information, see *Diameter Messages SLA Time and Action on Threshold on LB* in *CPS Mobile Configuration Guide*.

The following new statistics have been added:

- node[x].counters.sla_out_req_busy: Number of outbound Diameter messages responded with Diameter Busy (error code 3004) when the Diameter message have crossed the limit configured in **Message Count Threshold in Diameter Messages SLA Time and Action on Threshold on LB**. The source of the statistics is Policy Director (LB) VM.

New and Changed Feature Information

- `node[x].counters.sla_out_req_drop`: Number of outbound Diameter messages dropped when number of Diameter messages have crossed the limit configured in **Message Count Threshold in Diameter Messages SLA Time and Action on Threshold on LB**. The source of the statistics is Policy Director (LB) VM.
- `node[x].counters.sla_in_req_busy`: Number of inbound Diameter messages responded with Diameter Busy (error code 3004) when number of Diameter messages have crossed the limit configured in **Message Count Threshold in Diameter Messages SLA Time and Action on Threshold on LB**. The source of the statistics is Policy Director (LB) VM.
- `node[x].counters.sla_in_req_drop`: Number of inbound Diameter messages dropped when number of Diameter messages have crossed the limit configured in **Message Count Threshold in Diameter Messages SLA Time and Action on Threshold on LB**. The source of the statistics is Policy Director (LB) VM.

Support for qns Flags Validation

CPS is now enhanced to support the following two flags in qns file:

- `disable.force.crd.cache.build.after.publish`
- `enable.crd.schema.cache.synchronization`

For more information, contact your Cisco Technical Support Representative.

Support for Stale Session Parameters

CPS now supports the following Gx Offline Stale Session Clean up configuration parameters:

- `admin.primary.host`
- `admin.secondary.host`
- `admin.port`
- `memcache.host`
- `tps.per.shards`
- `mongo.query.batch.size`
- `factor.count.audit.log`
- `session.count.threshold`
- `session.threshold.timer`
- `session.cache.update.timer`
- `number.of.shards`
- `logback.configurationFile`

For more information, see *Gx Offline Stale Session Clean Up* section in *CPS Mobile Configuration Guide*.

The following commands are supported in `prfclient` to clean up built stale sessions:

- `monit stop stale-session-cleaner-helper`
- `monit restart stale-session-cleaner-helper`

Support to Mask Java Warmup

CPS now supports masking java warm up issues to avoid using any workarounds. The following parameters must be configured:

- `qns.node.warmup`
- `number.warmup.calls`
- `warmup.time.threshold`
- `qns.node.warmup.hostname.substrin`

For more information, contact your Cisco Technical Support Representative.

MOG

No new features or changes were introduced in this release.

Operations

Support for CPS Auto Healing in Case of Endpoint Heart Beat Failures

As part of this feature, Auto Healing and Auto Correction support is added in CPS when heart beating between Load Balancer (LB) and QNS VMs fails.

For more information, see *Support for CPS Auto Healing in Case of Endpoint Heart Beat Failures* section in *CPS Operations Guide*.

Support for Graphite Database Authentication

CPS now allows users to configure credentials (users and passwords) for Graphite database access in VMware and OpenStack environments.

Before upgrade/migration or after fresh installation, you need to configure at least one Graphite/Grafana user. The Graphite data source in grafana needs to be updated to use configured user credentials before upgrade/migration or after fresh installation. For more information on updating graphite data source, see *Configuring Graphite User Credentials in Grafana* in *CPS Operations Guide*.

For more information, see the following sections in CPS Operations Guide:

- *Add User*
- *Delete User*
- *Accessing Graphite DB Using CLI*

- *Configuring Graphite User Credentials in Grafana*
- *Accessing Graphite Database Using CLI*

Support to Detect Endpoint Failure

CPS now supports KPIs to enable monitoring system health based on IPC messaging statistics. Adding KPI's to monitor the following:

1. Number of request messages sent to qns from lb and number of response messages received at lb from qns.
2. Time spent in IPC queue by the message.

These KPIs are used to monitor the health of the system.

API Additions or Changes

No changes were introduced in this release.

MIB Additions or Changes

No changes were introduced in this release.

KPI Additions or Changes

No changes were introduced in this release.

Log Additions or Changes

No changes were introduced in this release.

SNMP Alarm Additions or Changes

In this release, the following changes have been done:

- Severity level changed from **critical** to **info** for HA Failover and GR Failover alarms.
- Additional message text added for SPR_DB_ALARM:

For error: 6101:Remote SPR DB:Primary member is down

For clear: 6101:Remote SPR DB:Cleared alarm for remote spr db primary

Support to Mask Java Warmup

In this release, CPS now sends an error alarm (DiameterQnsWarmupError) when the warmup feature is enabled and there is a problem in retrieving Policy Server (qns) node number, site ID. Also the alarm is generated when there is an exception while parsing the warmup dictionaries or scenario file.

You can monitor the critical files only on Cluster Manager.

For more information, see the following sections:

- *Application Notifications* in CPS SNMP, Alarms, and Clearing Procedures Guide
- *Testing Traps Generated by CPS* in CPS Troubleshooting Guide

Statistics Additions or Changes

SPR Cache Cleanup by Backup Database

The following new statistics have been added:

- `subscriberCleanup.addedToQueue`: SPR record added to the queue.
- `subscriberCleanup.removedFromQueue`: SPR record deleted from the queue.
- `subscriberCleanup.insert.success/subscriberCleanup.insert.failure`: Number of remote subscribers written from queue to subscriberCleanup database on hot standby.
- `spr.remote.cleanupDelete.success." + dbAddress/spr.remote.cleanupDelete.failure." + dbAddress`: Counter registers when a subscriber is deleted on a remote SPR.

Note: Most transactions do not delete any records as the records have already been removed.

Example: `spr.remote.cleanupDelete.success.site1-sessionmgr05:27720`

Support for CPS Load Balancer Protection

The following new statistics have been added:

- `node[x].counters.sla_out_req_busy`: Number of outbound Diameter messages responded with Diameter Busy (error code 3004) when the Diameter message have crossed the limit configured in **Message Count Threshold in Diameter Messages SLA Time and Action on Threshold on LB**. The source of the statistics is Policy Director (LB) VM.
- `node[x].counters.sla_out_req_drop`: Number of outbound Diameter messages dropped when number of Diameter messages have crossed the limit configured in **Message Count Threshold in Diameter Messages SLA Time and Action on Threshold on LB**. The source of the statistics is Policy Director (LB) VM.
- `node[x].counters.sla_in_req_busy`: Number of inbound Diameter messages responded with Diameter Busy (error code 3004) when number of Diameter messages have crossed the limit configured in **Message Count Threshold in Diameter Messages SLA Time and Action on Threshold on LB**. The source of the statistics is Policy Director (LB) VM.
- `node[x].counters.sla_in_req_drop`: Number of inbound Diameter messages dropped when number of Diameter messages have crossed the limit configured in **Message Count Threshold in Diameter Messages SLA Time and Action on Threshold on LB**. The source of the statistics is Policy Director (LB) VM.

Performance Improvement

No new features or changes were introduced in this release.

Platform

Support for Clearing Stale Component Alarms

Before 18.5.0 release, CPS sometimes used to display stale component alarms while executing

`diagnostics.sh -get_active_alarm` which gave false system status to the user.

In 18.5.0 release, support for clearing stale alarms has been added and CPS no longer displays stale component alarms.

Note: The system generates the clear notification for all the resource monitored by snmpd on each VM so lot of clear notification gets generated on the system based on the deployment architecture. This lowers the performance of snmptrapd application on the system during upgrade/re-initialization of the system.

For more information, see *Active Alarms* section in *CPS SNMP, Alarms, and Clearing Procedures Guide*.

Policy Reporting

No new features or changes were introduced in this release.

Product Security

CentOS 7.5 Security Enhancements/Kernel Upgrade

In this release, CentOS has been updated to 7.5. With CentOS 7.5, kernel has been upgraded to 3.10.0-862.14.4.el7.x86_64. Also, all the packages have been upgraded to be compatible with CentOS 7.5.

For service related issues, you can use `journalctl` to get systemctl logs.

The following tables lists 46 vulnerabilities that have been fixed as a part of this feature:

Table 1 - CVEs

| CVE | Name |
|----------------|--|
| CVE-2016-2183 | CentOS 7 : python (CESA-2018:2123) |
| CVE-2017-10268 | CentOS 7 : mariadb (CESA-2018:2439) |
| CVE-2017-10378 | CentOS 7 : mariadb (CESA-2018:2439) |
| CVE-2017-10379 | CentOS 7 : mariadb (CESA-2018:2439) |
| CVE-2017-10384 | CentOS 7 : mariadb (CESA-2018:2439) |
| CVE-2017-10384 | CentOS 7 : mariadb (CESA-2018:2439) |
| CVE-2017-11368 | CentOS 7 : krb5 (CESA-2018:0666) |
| CVE-2017-11600 | CentOS 7 : kernel (CESA-2018:1965) (Spectre) |
| CVE-2017-11671 | CentOS 7 : gcc (CESA-2018:0849) |

| CVE | Name |
|----------------|---|
| CVE-2017-13215 | CentOS 7 : kernel (CESA-2018:2384) (Foreshadow) |
| CVE-2017-16939 | CentOS 7 : kernel (CESA-2018:1318) |
| CVE-2017-3636 | CentOS 7 : mariadb (CESA-2018:2439) |
| CVE-2017-3641 | CentOS 7 : mariadb (CESA-2018:2439) |
| CVE-2017-3651 | CentOS 7 : mariadb (CESA-2018:2439) |
| CVE-2017-3653 | CentOS 7 : mariadb (CESA-2018:2439) |
| CVE-2017-3736 | CentOS 7 : openssl (CESA-2018:0998) |
| CVE-2017-3737 | CentOS 7 : openssl (CESA-2018:0998) |
| CVE-2017-3738 | CentOS 7 : openssl (CESA-2018:0998) |
| CVE-2017-7562 | CentOS 7 : krb5 (CESA-2018:0666) |
| CVE-2018-1063 | CentOS 7 : policycoreutils (CESA-2018:0913) |
| CVE-2018-10675 | CentOS 7 : kernel (CESA-2018:2384) (Foreshadow) |
| CVE-2018-1068 | CentOS 7 : kernel (CESA-2018:1318) |
| CVE-2018-1087 | CentOS 7 : kernel (CESA-2018:1318) |
| CVE-2018-1091 | CentOS 7 : kernel (CESA-2018:1318) |
| CVE-2018-10915 | CentOS 7 : postgresql (CESA-2018:2557) |
| CVE-2018-2562 | CentOS 7 : mariadb (CESA-2018:2439) |
| CVE-2018-2622 | CentOS 7 : mariadb (CESA-2018:2439) |
| CVE-2018-2640 | CentOS 7 : mariadb (CESA-2018:2439) |
| CVE-2018-2665 | CentOS 7 : mariadb (CESA-2018:2439) |
| CVE-2018-2668 | CentOS 7 : mariadb (CESA-2018:2439) |
| CVE-2018-2755 | CentOS 7 : mariadb (CESA-2018:2439) |
| CVE-2018-2761 | CentOS 7 : mariadb (CESA-2018:2439) |
| CVE-2018-2767 | CentOS 7 : mariadb (CESA-2018:2439) |
| CVE-2018-2771 | CentOS 7 : mariadb (CESA-2018:2439) |
| CVE-2018-2781 | CentOS 7 : mariadb (CESA-2018:2439) |
| CVE-2018-2813 | CentOS 7 : mariadb (CESA-2018:2439) |
| CVE-2018-2817 | CentOS 7 : mariadb (CESA-2018:2439) |
| CVE-2018-2819 | CentOS 7 : mariadb (CESA-2018:2439) |
| CVE-2018-3620 | CentOS 7 : kernel (CESA-2018:2384) (Foreshadow) |
| CVE-2018-3639 | CentOS 7 : kernel (CESA-2018:1629) (Spectre) |

| CVE | Name |
|---------------|---|
| CVE-2018-3646 | CentOS 7 : kernel (CESA-2018:2384) (Foreshadow) |
| CVE-2018-3693 | CentOS 7 : kernel (CESA-2018:2384) (Foreshadow) |
| CVE-2018-5390 | CentOS 7 : kernel (CESA-2018:2384) (Foreshadow) |
| CVE-2018-5740 | CentOS 7 : bind (CESA-2018:2570) |
| CVE-2018-7566 | CentOS 7 : kernel (CESA-2018:2384) (Foreshadow) |
| CVE-2018-8897 | CentOS 7 : kernel (CESA-2018:1318) |

Security Enhancements

This section lists enhancements introduced to support Cisco Product Security Requirements and the Product Security Baseline (PSB). For more information about Cisco Product Security Requirements, refer to: <https://www.cisco.com/c/en/us/about/security-center/security-programs/secure-development-lifecycle/sdl-process.html>

Security Enhancements for CPS Platform

CPS now supports the following platform security requirements:

- Analysis controlled space protections. The following controlled spaces can be identified in CPS:
 - Platform scripts/puppet code
 - Virtual machines (VM)
 - Web access – grafana, control center, policy builder, HAProxy stats access, cluman API access
 - Diameter access
- Provides log indications of attack or abuse
- Utilization of offering-internal identifiers
- Provides log unrestricted access to controlled space
- Provides log startup, shutdown, and other status changes
- Prevents program or command injection

For more information, contact your Cisco Technical Support Representative.

Web Security Enhancements

CPS now supports the following web security requirements:

- Implementation of the HTTP Strict Transport Security mechanism in PB2, PB and CC interfaces.
- While using session ID to keep an authentication state and track user progress within a web application, the application should treat the session ID as untrusted data, sanitize and validate it before use.

For more information, contact your Cisco Technical Support Representative.

UDC

UDC Optimization

The following new parameter is supported in UDC:

- `udc.wait.for.response`

For more information, contact your Cisco Technical Support Representative.

UI Enhancements

No new features or changes were introduced in this release.

vDRA

Note: In CPS 18.5.0 release, vDRA is not supported. For more information, contact Cisco Technical Representative.

Installation Notes

Download ISO Image

Download the 18.5.0 software package (ISO image) from:

<https://software.cisco.com/download/home/284883882/type/284979976/release/18.5.0>

Md5sum Details

ccad9ec8cb7a9e80b8de2c2be9d6e5de CPS_18.5.0_Base.qcow2.release.tar.gz

1b4e9d40e1da9ca16293800c28962670 CPS_18.5.0_Base.vmdk.release.tar.gz

735a0de5b12f212a3ad050deee8a706a CPS_18.5.0.release.iso

Component Versions

The following table lists the component version details for this release.

Table 2 Component Versions

| Component | Version |
|------------|----------------|
| ANDSF | 18.5.0.release |
| API router | 18.5.0.release |
| Audit | 18.5.0.release |
| Balance | 18.5.0.release |

| Component | Version |
|---------------------------|----------------|
| CALEA | 18.5.0.release |
| Cisco API | 18.5.0.release |
| Cisco CPAR | 18.5.0.release |
| Congestion Reference Data | 18.5.0.release |
| Control Center | 18.5.0.release |
| Core | 18.5.0.release |
| CSB | 18.5.0.release |
| Custom Reference Data | 18.5.0.release |
| DHCP | 18.5.0.release |
| Diameter2 | 18.5.0.release |
| DRA | 18.5.0.release |
| Entitlement | 18.5.0.release |
| Fault Management | 18.5.0.release |
| IPAM | 18.5.0.release |
| ISG Prepaid | 18.5.0.release |
| LDAP | 18.5.0.release |
| LDAP Server | 18.5.0.release |
| LWR | 18.5.0.release |
| Microservices Enablement | 18.5.0.release |
| Notification | 18.5.0.release |
| PCF | 18.5.0.release |
| Policy Intel | 18.5.0.release |
| POP-3 Authentication | 18.5.0.release |
| Recharge Wallet | 18.5.0.release |
| SCE | 18.5.0.release |
| SCEF | 18.5.0.release |
| Scheduled Events | 18.5.0.release |
| SPR | 18.5.0.release |
| TIM AVP | 18.5.0.release |
| UDC | 18.5.0.release |
| UDSC Interface | 18.5.0.release |

| Component | Version |
|-------------|----------------|
| Unified API | 18.5.0.release |

New Installations

- VMware Environment
- OpenStack Environment

VMware Environment

To perform a new installation of CPS 18.5.0 in a VMware environment, see the *CPS Installation Guide for VMware, Release 18.5.0*.

After installation is complete, you need to configure at least one Graphite/Grafana user. The Graphite data source in grafana needs to be updated to use configured user credentials after fresh installation. For more information on updating graphite data source, see *Configuring Graphite User Credentials in Grafana* in CPS Operations Guide.

OpenStack Environment

To perform a new installation of CPS 18.5.0 in an OpenStack environment, see the *CPS Installation Guide for OpenStack, Release 18.5.0*.

After installation is complete, you need to configure at least one Graphite/Grafana user. The Graphite data source in grafana needs to be updated to use configured user credentials after fresh installation. For more information on updating graphite data source, see *Configuring Graphite User Credentials in Grafana* in CPS Operations Guide.

Migrate an Existing CPS Installation

To migrate an existing CPS installation, see the *CPS Migration and Upgrade Guide, Release 18.5.0*. CPS migration is supported from CPS 14.0.0 to CPS 18.5.0.

Before migration, you need to configure at least one Graphite/Grafana user. The Graphite data source in grafana needs to be updated to use configured user credentials before upgrade/migration or after fresh installation. For more information on updating graphite data source, see *Configuring Graphite User Credentials in Grafana* in CPS Operations Guide.

Upgrade an Existing CPS Installation

To upgrade an existing CPS installation, see the *CPS Migration and Upgrade Guide, Release 18.5.0*. CPS upgrade is supported from CPS 18.3.0 and CPS 18.4.0 to CPS 18.5.0.

Before upgrade, you need to configure at least one Graphite/Grafana user. The Graphite data source in grafana needs to be updated to use configured user credentials before upgrade/migration or after fresh installation. For more information on updating graphite data source, see *Configuring Graphite User Credentials in Grafana* in CPS Operations Guide.

Post Migration/Upgrade Steps

Re-Apply Configuration Changes

After the migration/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 migration/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 migration/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, it is set to false.

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

- /etc/broadhop/diameter_endpoint/qns.conf
 - o -Dzmq.send.hwm=1000
 - o -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 you need to reconfigure multiple Subscriber Id in SpendingLimitReport under Service Configurations.

Verify logback.xml Configuration

Make sure the following line exists in the logback.xml file being used. If not, then add the line:

```
<property scope="context" name="HOSTNAME" value="${HOSTNAME}" />
```

To ensure logback.xml file changes are reflected at runtime, the scanPeriod must be explicitly specified:

```
<configuration scan="true" scanPeriod="1 minute">
```

Note: In case scanPeriod is missing from already deployed logback.xml file, the application needs to be restarted for the updated scanPeriod configuration to be applicable.

After completing the updates in logback.xml, execute the following command to copy the file to all the VMs:

```
SSHUSER_PREFERROOT=true copytoall.sh /etc/broadhop/logback.xml /etc/broadhop/logback.xml
```

Additional Notes

This section provides additional notes 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 pcrclient01 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

- 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.

- Add support to disable syncing carbon database and bulk stats files (ISSM)

Add the following flags in `/var/install.cfg` file:

```
SKIP_BLKSTATS
```

```
SKIP_CARBONDB
```

Example to disable syncing:

```
SKIP_BLKSTATS=1
```

```
SKIP_CARBONDB=1
```

- Add the following parameters in `/var/install.cfg` file to skip installation type selection and initialization steps during ISSU/ISSM:

```
INSTALL_TYPE
```

```
INITIALIZE_ENVIRONMENT
```

Example:

```
INSTALL_TYPE=mobile
```

```
INITIALIZE_ENVIRONMENT=yes
```

Primary Member is Isolated from all Arbiters

Issue: If the primary database member gets isolated from all the arbiters then diagnostics output displays incorrect states.

Solution: If a member is shown in an unknown state, it is likely that the member is not accessible from one of other members, most likely an arbiter. In that case, you must go to that member and check its connectivity with other members. Also, you can login to mongo on that member and check its actual status.

CSCvn06270: PB publishing time is high in B if compare with A Cluster

Issue: It takes longer time to publish the Policy Builder configuration in HA clusters.

Condition: SVN source and destination repositories are on different hosts/clusters rather than on the same host/cluster.

Solution: This is SNV server behavior and not CPS issue. If you are publishing on same host then use `svn copy` command and if host is different than use `svn import` command. As mentioned in the SVN docs, copy is faster than import.

For example, if you are logged in using <http://lbvip02/repos/configuration> and publishing to <http://lbvip02/repos/run> then both the hosts are same (lbvip02) and you can use `svn copy` command.

Limitations and Restrictions

But if you are logged in using <http://lbvip02/repos/configuration> and publishing to http://<different_host>/repos/run then you can use `svn import` command.

SVN import takes more time than copy command. So this is expected SVN server behavior.

The recommendation is, if you want to publish on different host or cluster, then open Policy Builder of other cluster and use other Cluster's run repository to publish.

3. Export policy configurations from hostA (clusterA) and push the same on hostB (clusterB) in `/repos/configuration` using SVN import command.
4. Open Policy Builder with other Cluster's IP address.
5. Login to Policy Builder with <http://lbvip02/repos/configuration>.
6. Publish to Cluster's to run repository using <http://lbvip02/repos/run>.

Limitations and Restrictions

This section covers the following topics:

- [Limitations](#)
- [Common Vulnerabilities and Exposures](#)

Limitations

- The following restriction applies to LWR:
 - In this release, LWR supports read and write of one user attribute to the replication framework specific to the ADTM bearer counting attribute.
In future releases, UDC and other applications will be enhanced to provide support of new attributes or user profile details that may require replication
- 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 that 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 session 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 that 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 OAM (pcrfclient01/pcrfclient02) VMs.
- The Linux VM message.log files repeatedly report errors similar to the following:

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

This is a known issue affecting ESXi 5.x. Currently, there is no workaround for this. The messages.log file entries are cosmetic and can be safely ignored. For more information, see http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2094561
- CSCva02957: Redis instances continue to run, even after redis is disabled using the parameter `-DenableQueueSystem=false` in `qns.conf(/etc/broadhop/)` file and `/etc/broadhop/redisTopology.ini` file.
- CSCva16388: A split-brain scenario (that is, VIPs are up on both nodes) can still occur when there is connectivity loss between lb01 and lb02 and not with other hosts.

Common Vulnerabilities and Exposures (CVE)

The following is the list of CVEs open in this release:

- CSCvm15802: Evaluation of qps for CVE-2018-5391 (FragmentSmack)
- CSCvm02970 : Evaluation of qps for August CPU Side-Channel Information Disclosure Vulnerabilities
 - CVE-2018-3615 - L1TF SGX - foreshadow
 - CVE-2018-3620 - L1TF OS, SMM
 - CVE-2018-3646 - L1TF VMM

Open and Resolved CDETS

The following sections list open and resolved CDETS for this release. 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 this release.

CPS Open CDETS

Table 3 CPS Open CDETS

| CDETS ID | Headline |
|------------|---|
| CSCve87564 | ISSM: /mnt/iso/migrate.sh rollback cli triggers restart for set-2 |
| CSCvi01695 | Create shards api shows success even though failure was diagnosed due to failed rebalance |
| CSCvi23619 | After ISSU, diag shows list of alarms not cleared, while conn btwn LB & PCEF/CSCF/TDF clients came up |
| CSCvj49386 | Warning messages "Mongo is still not restored:" in consolidated qns logs on CPS18.2 |
| CSCvj52735 | Incorrect calculation of TimerExpired TPS per QNS and limited TPS support on JMS engine |
| CSCvj80096 | ISSM 13.1 to 18.2 - /mnt/iso/migrate.sh traffic restore command success with exceptions. |
| CSCvj88208 | Bulk terminate command not working/getting exception in logs |
| CSCvj93662 | Race condition when qns processes are taken down, diameter peer down alarm may be missed |
| CSCvj94859 | During pcrfclient01 stop and start, stats with Prometheus query stopped coming to pcrfclient01 |
| CSCvj97328 | TPS is not reaching expected level after Traffic Switch over (Site Failure in GR Setup) |
| CSCvk30283 | LDAP TPS unable to recover when QNS are down |
| CSCvk37491 | Time out observed in OSGI for listshards command |
| CSCvk52072 | During longevity run with Redis enable, system response time for CCR-I/T increased upto ~8-9 ms. |
| CSCvk67829 | remove whisper .wsp file older than 90 days or configurable param value. |
| CSCvm02970 | Evaluation of qps for August CPU Side-Channel Information Disclosure Vulnerabilities |
| CSCvm04614 | Disable Remote Scans for Sync Messages and Single Session Update |
| CSCvm08851 | PCRF sending out Sd RARs without dest-host AVP for few calls. |
| CSCvm15802 | Evaluation of qps for CVE-2018-5391 (FragmentSmack) |
| CSCvm24223 | Getting an ArrayIndexOutOfBoundsException in qns logs when PB Publish is issued. |
| CSCvm39678 | Logs in Use case template showing status as true while condition remains false |
| CSCvm42276 | session failover fallback causing 5002 5065 Timeout Errors |
| CSCvm44895 | Diagnostics script display the GR ZMQ alarms details in HA setup also |
| CSCvm49609 | High response time observed during running Sol-3 call model |

| CDETS ID | Headline |
|------------|---|
| CSCvm58786 | Known issue in Zookeeper 3.4.6 results in Zookeeper becoming unavailable on cluster manager |
| CSCvm69496 | QNS process are restarting continuously |
| CSCvm73932 | config_br.py -a import --users overwrites required CentOS user accounts |
| CSCvm76441 | CPS is sending Gx_RAR with same Charging-Rule-Name twice when Rx_AAR is received |
| CSCvm78417 | Call model impacted with timeouts post Replication VLAN down in GR VMW |
| CSCvm87759 | with custom haproxy-diameter.cfg, the process stays initializing on lb02. lb01 runs fine |
| CSCvm88058 | CPS shows a 10 to 60 secs offset for rule-retry attempts for configured rule-retry profile |
| CSCvm89234 | Np interface: Missing/wrong functionalities need to be implemented/corrected as per requirement. |
| CSCvm91162 | Diameter - revalidation-time avp is not displayed correctly in the QNS engine log |
| CSCvm91300 | Message prioritization is not working at overload condition |
| CSCvm93097 | Memory utilization on qns vms are high after moving to Zing. |
| CSCvm95474 | stale single Sy session persists after Gx session expiration (non RAA 5002 scenario) |
| CSCvm97345 | Session shards: mongo clients not adding correct parameter values set in qns.conf |
| CSCvn00127 | After reboot of the primary SM, the cps is giving 5002 error code against Gx/Gy_RAR,SY_SNR & Rx_ASR |
| CSCvn02190 | improve performance on GR setups with single sh and single sy enabled |
| CSCvn04062 | session replicaset going to recovering state on leaving load running on vzw setup |
| CSCvn05854 | IPAM not updating mongo replica set status after app initialization |
| CSCvn06265 | cluster id. is missing in lb's iomanager/qns.conf file |
| CSCvn06506 | Security AppScan Test: Older TLS Version Supported |
| CSCvn07203 | Replica-set gone after upgrade, with selinux_state=enable in Configuration.csv. |
| CSCvn07508 | CPS Sharing service rule flapping |
| CSCvn09149 | Issue seen in grafana due to collectd service |
| CSCvn09156 | PCRF is sending wrong CC-Total-Octets |
| CSCvn11048 | Set1 QNS VM's not updated in admin database after abrupt ISSU rollback |
| CSCvn12911 | Missing bulkstats definitions in QPS_statistics documentation |
| CSCvn14019 | Procedure/script required to clear stale alarm to ONLY on the VMs for which stale alarm is present. |
| CSCvn15951 | high cpu/high memory usage(low free memory) on qns vms with zing jvm |
| CSCvn15963 | mongo exception is coming in qns logs |
| CSCvn16071 | SPR Replica-set are not created by AIDO properly during upgrade |
| CSCvn17130 | CPS not processing some CCR-U when Multiple CCR-U is triggered randomly with some TPS |
| CSCvn17263 | BEMS884374 - Arbiter VM is not joining replica set |

Open and Resolved CDETS

| CDETS ID | Headline |
|------------|--|
| CSCvn17334 | svn out-of-sync between pcrfclient01 & pcrfclient02 after policy publish |
| CSCvn17368 | High Disk Write Latency GC Logging |
| CSCvn20340 | mon_db_for_lb_failover falsely detects lb failure due to race condition during puppet update |
| CSCvn24532 | Restartall.sh should not restart udc qns process in sequence |
| CSCvn24592 | During ISSM from CPS 13.1 to CPS 18.2 qns vm's are sending request to disable d udc |
| CSCvn25107 | MOG 18.3 MCPTT is coming as supported for all the call flows in the Feature list |
| CSCvn25155 | Flow info is missing in GET request if we just send duration in PUT request without flows in it |
| CSCvn25604 | Redis services failed on lb02 when upgrade 18.3->18.4->18.5-set1->18.4-set1-rollback |
| CSCvn25648 | PATS upgrade not showing the upgraded version |
| CSCvn25926 | Monit process "stale-session-cleaner-helper" shows in "Execution Failed" state in pcrfclient02 |
| CSCvn25954 | Unencrypted password being written in /var/log/messages |
| CSCvn26775 | Alarms are not clearing |
| CSCvn27259 | After LB failback, Monit process shows qns process are in not monitored state for the failed-back LB |
| CSCvn28599 | Bursts of CCR-Ts that result in a 5002 are also initiating full shard scans. |
| CSCvn35645 | Arbitervip not coming up during fresh install |

Resolved CDETS

This section lists the resolved/verified CDETS in this release.

CPS Resolved CDETS

Table 4 CPS Resolved CDETS

| CDETS ID | Headline |
|------------|---|
| CSCvh30904 | Security Issues Identified in CPS 18.0 PB, CC, UnifiedAPI and Import/Export URLs |
| CSCvi53391 | PCRF retry behavior is not consistent when there are multiple realms for the same application |
| CSCvi81132 | MOG is not throwing error for Abort Cause Values 1, 2 and 3 instead it is ending the session. |
| CSCvj39710 | Unable to locate 'startqps' file intermediately after reboot to pcrfclient VM on CSP 18.2 |
| CSCvj53529 | ISSM 13.1 to 18.2 - After traffic swap grafana should print from pcrfclient02 |
| CSCvk30832 | 18.3 CPS AppScan Issue: Missing HTTP Strict-Transport-Security Header |
| CSCvk36604 | BEMS850443: P1, AT&T, Neo CPS 18/13.1: Updates required in QPS_Statistics.xls |
| CSCvk40979 | Support of Flow Usage and Flow Status in ModifyRxDynamicRule |
| CSCvk49598 | GC pause issue in PCRF in 13.1 |

| CDETS ID | Headline |
|------------|--|
| CSCvk65479 | GC pause due to huge Temp characters |
| CSCvk73844 | build_set.sh and set_priority.sh are failing when NON-Voting members present in replicaset. |
| CSCvm02867 | SVN based CRD publish results in service impact |
| CSCvm04646 | SPR Deletes: Stale SPR Records - Avoiding the extra processing of SPR.find() - failover improvements |
| CSCvm09662 | No alarms when peers go down |
| CSCvm09666 | vPCRF - SPR remote db error alarming does not occur unless qns application is restarted |
| CSCvm10384 | PCRF is sending wrong granted dosage in CCA-U |
| CSCvm10996 | Change CacheRing getKey timeout and retry behavior |
| CSCvm11119 | startall script behavior change |
| CSCvm16034 | about.sh is throwing lot of errors from all the MOG VM's |
| CSCvm16053 | diagnostics.sh --get_peer_status is not working in MOG |
| CSCvm17119 | Diagnostic error post upgrade to CPS_18.4 |
| CSCvm21301 | Support for renaming of interfaces on VM |
| CSCvm21356 | LdapChangeMessage broadcast deserialisation throws exception |
| CSCvm32449 | Error executing IPolicyAsyncAction: null error observed in qns logs |
| CSCvm34004 | Asking for root password of installer during execution of change_password after Fresh Install |
| CSCvm34041 | Central GUI - "Event Logs" functionality not working for many peers |
| CSCvm34914 | limitation of index on _id field in mongo 3.4 |
| CSCvm37043 | about.sh does not properly parse all possible IPv6 address formats in haproxy.cfg |
| CSCvm37391 | UDC is returning the Sy counters only for the First APN for an subscriber |
| CSCvm38981 | null pointer exceptions after publish activity |
| CSCvm42022 | Np Interface support: Rule Deactivation Time not sent based on Throttle Duration |
| CSCvm42670 | No stats to track mongo remote SPR insert operations |
| CSCvm43513 | /var/tmp/monitor-qns not documented, and in place that can be easily removed |
| CSCvm44242 | ShardInterface - MongoException in 18.4 FCV drop 3 fresh install on VMware setup |
| CSCvm44299 | QPS_statistics.xlsx Missing Stats |
| CSCvm44459 | Pb of 29.213 Standard QoS Preliminary Service in VoLTE Call NPLI |
| CSCvm45199 | Random qns throwing exception on restart |
| CSCvm45868 | Error after upgrade to 18.4 FCV drop 3 (CsvReplicationRunner - File handle not found) |
| CSCvm46525 | PCRF is not sending correct rule in case of default_eps_qos_mod_failure |
| CSCvm47483 | diagnostics.sh --get_active_alarms is not working from pcrfclients |

| CDETS ID | Headline |
|------------|---|
| CSCvm49493 | Custom AVPs don't reload on publish |
| CSCvm50602 | For Default QoS failure events, complete qos info missing in final CCA-U after retry exhaust |
| CSCvm51070 | Clock is not sync between sessionmgr's and lb01 for fresh installtion in OSP for 18.4 CCO build |
| CSCvm51240 | Stale Session RAR does not occur during Full GR |
| CSCvm52309 | CRD schema/cache synchronization and QNS memory optimization issues upon PB publish |
| CSCvm52646 | Better logs for init_pacemaker_res.sh |
| CSCvm53170 | Random GX RAR timeouts when DRA sends 3002 |
| CSCvm53534 | Geo Site Status check is not working for certain configurations |
| CSCvm53645 | Default Setting for Enable Multi Primary Key should be unchecked in PB |
| CSCvm55790 | Multiple concurrent modification exceptions in logs related to custom AVP |
| CSCvm61810 | install rpm need to comment out from patch command script |
| CSCvm65953 | ModifyRxDynamicRule not bounding the MBR values |
| CSCvm66764 | RAA 5002 clears Gx network session but does not clear single Sy session |
| CSCvm66920 | PB_SVN based CRD - import is failed |
| CSCvm67141 | Clear Component Stale alarm from CPS |
| CSCvm67296 | Addshard is taking around 10 mins from the OSGi command prompt |
| CSCvm71969 | PCRF does not have the ability to change rule parameters for dynamic rules in case of gy failure |
| CSCvm72181 | Stale RAR doesnt remove Remote-spr upon session expiry this is cross site SPR |
| CSCvm75990 | There are too many file descriptor which are opened causing unknown host exception |
| CSCvm79427 | Errors during in-service migration to 18.4 caused by missing "SyCacheEntry" class |
| CSCvm89234 | Np interface: Missing/wrong functionalities need to be implemented/corrected as per requirement. |
| CSCvm91246 | Cannot enable/disable root SSH login feature |
| CSCvm91689 | QPS not generating Np_NRA after getting successful Gx_RAA for F1734 |
| CSCvm92367 | PCRF is not sending RAR message on pending counter activation |
| CSCvm95804 | high cpu usage, low mem component alarm does not sent to NMS in snmpv3 |
| CSCvm96591 | GX RAR timeouts-Response comes back after configured action timer, generates timeout message |
| CSCvn02947 | MOG18.3 For the FN startTime calls Duration is getting consumed during the wait time of the vPASquery |
| CSCvn04866 | Redis crash in case of packet drop |
| CSCvn07820 | Memory Leak in Remote Service Manager |
| CSCvn10889 | PCRF is throwing Null Pointer Exception on getting AAR from real MOG |
| CSCvn11875 | Failure while evaluating Mongo based CRD with schema (key) change |

| CDETS ID | Headline |
|------------|--|
| CSCvn19181 | PCRF is not sending netloc AVP's after upgrading to CPS 18.2 from CPS 13.1 |
| CSCvn22793 | PCRF is creating loop on Null Pointer Exception |
| CSCvn23881 | Build_LWR method comparing wrong instances in UdcFeDeviceManager.java |
| CSCvn26781 | Delete session on CCR-T/RAA-5002 error |
| CSCvn27096 | Stale session logging is required for Audit |
| CSCvn28193 | Observed java.lang.NullPointerException during IMS-Sy call. |
| CSCvn31772 | Change in default value for diameter.peer.reload.interval.lb |
| CSCvn32072 | 18.0 Patch 24 - Issue with Logging, Gx- RAR getting printed on NPE |

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 Cisco Policy Suite.

- *CPS ANDSF Configuration Guide*
- *CPS ANDSF SNMP and Alarms Guide*
- *CPS Backup and Restore Guide*
- *CPS CCI Guide for Full Privilege Administrators*
- *CPS CCI Guide for View Only Administrators*
- *CPS Central Administration Guide*
- *CPS Geographic Redundancy Guide*
- *CPS Installation Guide - OpenStack*
- *CPS Installation Guide – VMware*
- *CPS LWR Guide*
- *CPS LWR Installation Guide - OpenStack*
- *CPS LWR Installation Guide - VMware*
- *CPS Migration and Upgrade Guide*
- *CPS Mobile Configuration Guide*
- *CPS MOG API Reference*
- *CPS MOG Guide*
- *CPS MOG Installation Guide - OpenStack*
- *CPS MOG SNMP, Alarms, and Clearing Procedures Guide*
- *CPS MOG Troubleshooting Guide*
- *CPS Operations Guide*

Obtaining Documentation and Submitting a Service Request

- *CPS Policy Reporting Guide*
- *CPS Release Notes*
- *CPS SNMP, Alarms, and Clearing Procedures Guide*
- *CPS Troubleshooting Guide*
- *CPS UDC API Reference*
- *CPS UDC Administration Guide*
- *CPS UDC Installation Guide*
- *CPS UDC Session Migration Guide*
- *CPS UDC SNMP and Alarms Guide*
- *CPS Unified API Reference Guide*

These documents can be downloaded from <https://www.cisco.com/c/en/us/support/wireless/policy-suite-mobile/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, at:

<http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html>.

Subscribe to What's New in Cisco Product Documentation, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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.

All printed copies and duplicate soft copies are considered uncontrolled copies and the original on-line version should be referred to for latest version.

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2018-2021 Cisco Systems, Inc. All rights reserved.