



Cisco Policy Suite 23.1.0 Release Notes

First Published: February 24, 2023

Last Updated: January 24, 2024

Introduction

This Release Note identifies installation notes, limitations, and restrictions, and open and resolved CDETS in Cisco Policy Suite (CPS) software version 23.1.0. Use this Release Note in combination with the documentation listed in the *Related Documentation* section.

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>.

This Release Note includes the following sections:

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

New and Changed Feature Information

For information about a complete list of features and behavior changes associated with this release, see the *CPS Release Change Reference*.

Installation Notes

Download ISO Image

Download the 23.1.0 software package (ISO image) from:

<https://software.cisco.com/download/home/284883882/type/284979976/release/23.1.0>

Md5sum Details

PCRF

ae93b88d26ccc0ced5bdb19479cfe5	CPS_23.1.0_Base.release.qcow2_signed.tar.gz
e095adac3ab9717c15caa487c57ba395	CPS_23.1.0_Base.release.vmdk_signed.tar.gz
ac3dea39677c36dba166685ce47dca61	CPS_23.1.0.release.iso_signed.tar.gz

DRA

aa7556746baa40e1bd9d618d56b684b7	CPS_Microservices_DRA_23.1.0_Base.release.vmdk_signed.tar.gz
ef8959140b0a871b5a3f1e87164607e8	CPS_Microservices_DRA_23.1.0_Deployer.release.vmdk_signed.tar.gz
7306a8f34ca9c0e7b22c816c43221350	CPS_Microservices_DRA_23.1.0.release.iso_signed.tar.gz
09fd5300673422d9a934f45ca7fb4fb7	CPS_Microservices_DRA_Binding_23.1.0.release.iso_signed.

Component Versions

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

Table 1 - Component Versions

Component	Version
API Router	23.1.0.release
Audit	23.1.0.release
Balance	23.1.0.release
Cisco API	23.1.0.release
Cisco CPAR	23.1.0.release
Congestion Reference Data	23.1.0.release
Control Center	23.1.0.release
Core	23.1.0.release
CSB	23.1.0.release
Custom Reference Data	23.1.0.release
DHCP	23.1.0.release
Diameter2	23.1.0.release
DRA	23.1.0.release
Fault Management	23.1.0.release
IPAM	23.1.0.release
ISG Prepaid	23.1.0.release
LDAP	23.1.0.release
LDAP Server	23.1.0.release
LWR	23.1.0.release
Microservices Enablement	23.1.0.release
Notification	23.1.0.release
Policy Intel	23.1.0.release
POP-3 Authentication	23.1.0.release

Component	Version
Recharge Wallet	23.1.0.release
SCE	23.1.0.release
Scheduled Events	23.1.0.release
SPR	23.1.0.release
UDC	23.1.0.release
UDSN Interface	23.1.0.release
Unified API	23.1.0.release

Additional security has been added in CPS to verify the downloaded images.

Image Signing

Image signing allows for the following:

- **Authenticity and Integrity:** Image or software has not been modified and originated from a trusted source.
- **Content Assurance:** Image or software contains code from a trusted source, like Cisco.

Software Integrity Verification

To verify the integrity of the software image you have from Cisco, you can validate the md5sum checksum information against the checksum identified by Cisco for the software.

Image checksum information is available through **cisco.com Software Download Details**. To find the checksum, hover the mouse pointer over the software image on cisco.com.

If md5sum is correct, run `tar -zxvf` command to extract the downloaded file.

The files are extracted to a new directory with the same name as the downloaded file name without extension (.tar.gz).

The extracted directory contains the certificate files (.cer), python file (cisco_x509_verify_release.py), digital certificate file (.der), readme files (*.README), signature files (.signature) and installation files (.iso .vmdk, .qcow2 and .tar.gz).

Certificate Validation

To verify whether the installation files are released by Cisco System Pvt. Ltd and are not tampered/modified or infected by virus, malware, spyware, or ransomware, follow the instruction given in corresponding *.README file.

NOTE: Every installation file has its own signature and README file. Before following the instructions in the README file, make sure that cisco.com is accessible from verification server/host/machine/computer. In every README file, a Python command is provided which when executed connects you to cisco.com to verify that all the installation files are released by cisco.com or not. Python 2.7.4 and OpenSSL is required to execute cisco_x509_verify_release.py script.

New Installations

- VMware Environment
- OpenStack Environment

VMware Environment

To perform a new installation of CPS 23.1.0 in a VMware environment, see the *CPS Installation Guide for VMware*.

NOTE: After installation is complete, you need to configure at least one Graphite/Grafana user. Grafana supports Graphite data source credential configuration capability. Graphite data source requires common data source credential to be configured using Grafana for Grafana user. Data source credential must be configured after fresh installation. If you fail to add the user, then Grafana will not have access to Graphite database, and you will get continuous prompts for Graphite/Grafana credentials.

All Grafana users configured will be available after fresh installation. However, you need to configure the Graphite data source in Grafana UI.

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 23.1.0 in an OpenStack environment, see the *CPS Installation Guide for OpenStack*.

NOTE: After installation is complete, you need to configure at least one Graphite/Grafana user. Grafana supports Graphite data source credential configuration capability. Graphite data source requires common data source credential to be configured using Grafana for Grafana user. Data source credential must be configured after fresh installation. If you fail to add the user, then Grafana will not have access to Graphite database, and you will get continuous prompts for Graphite/Grafana credentials.

All Grafana users configured will be available after fresh installation. However, you need to configure the graphite data source in Grafana UI.

For more information on updating graphite data source, see *Configuring Graphite User Credentials in Grafana* in CPS Operations Guide.

Upgrade Alma Linux to 8.6 in PCRF

In CPS 23.1.0 release, Alma Linux version is upgraded from 8.5 to 8.6 along with upgrading to latest rpm packages and their dependencies.

With Alma Linux 8.6, the kernel version is modified to:

```
[root@localhost ~]# rpm -qa | grep kernel-[0-9]
```

```
kernel-4.18.0-372.32.1.el8_6.x86_64
```

```
[root@localhost ~]# cat /etc/redhat-release AlmaLinux release 8.6 (Sky Tiger) [root@localhost ~]# uname -a Linux localhost.localdomain 4.18.0-372.32.1.el8_6.x86_64 #1 SMP Tue Oct 25 05:53:57 EDT 2022 x86_64 x86_64 x86_64 GNU/Linux [root@localhost ~]#
```

Upgrade MongoDB Version to 4.4.18 in PCRF

In CPS 23.1.0 release, MongoDB version is upgraded from 4.2.20 to 4.4.18.

Support for MongoDB 4.4 Version in vDRA

In CPS 23.1.0, MongoDB version in vDRA is upgraded to 4.4.18.

Prerequisite for upgrading to 23.1 from 22.2.0 and rollback from 23.1 to 22.2.0

The following are the common prerequisites for upgrade and roll back:

1. Run the following CLI before upgrade:

```
#database genericfcvcheck 4.2
```

NOTE: Make sure to run the above CLI before upgrade and / or downgrade on all sites.

2. Specify any one of the CLI options:

- a. **Set:** This option checks and sets FCV only on primary.

NOTE: We recommend to use Set option first and then Check to make sure that FCV is replicated on secondary members. Upgrade/downgrade should not be triggered if any error is found in above CLI or FCV is not replicated on secondary members. Make sure to resolve the CLI error, rerun the CLI, and then only proceed for upgrade or downgrade.

- b. **Check:** This option only checks FCV on all members (primary, secondary, and arbiter).

Prerequisite for upgrading grafana

In CPS 23.1.0 release, grafana version is upgraded to v9.2.3. To maintain backward compatibility during downgrade, ensure to take the backup of custom dashboard JSON files before upgrade.

Migrate an Existing CPS Installation

To migrate an existing CPS installation, see the *CPS Migration and Upgrade Guide*. CPS migration is supported only from CPS 22.2.0 to CPS 23.1.0.

NOTE: Before migration, you need to configure at least one Graphite/Grafana user. Grafana supports Graphite data source credential configuration capability. Graphite data source requires common data source credential to be configured using Grafana for Grafana user. Data source credential must be configured before migration. If you fail to add the user, then Grafana will not have access to Graphite database, and you will get continuous prompts for Graphite/Grafana credentials.

All Grafana users configured will be available after migration. However, you need to configure the graphite data source in Grafana UI.

For more information on updating graphite data source, see *Configuring Graphite User Credentials in Grafana* in CPS Operations Guide.

For more information, consult your Cisco Technical Representative.

Post Migration/Upgrade Steps

Re-Apply Configuration Changes

After the migration/upgrade is complete, 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 Account 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`

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

Change Mongo Storage Engine from MMapV1 to WiredTiger in CPS Product

Starting from CPS 22.1.1 release, MongoDB Storage Engine is changed from MMAPv1 to WiredTiger.

WiredTiger storage engine change in MongoDB Server requires additional CPU resources of ~15% and additional memory (RAM) resources of ~40% in the Session Manager VMs. WiredTiger consumes up to ~40% extra memory from total memory(RAM) than MMapV1.

For example, If the sessionmgr VM (150GB) with MMapV1 uses 60GB, then WiredTiger requires 120GB(MMapV1 usage 60GB + 40% of total memory).

As per mongo documentation, the wiredtigercachegb can be configured as [50% of (RAM - 1 GB)] in the VM.

If "n" mongo processes are running in the VM, the wiredtigercachegb can be configured as [50% of (RAM - 1 GB)]/n per mongo process.

For example, in the setup:

- Sessionmgr VMs configured RAM: 157GB
- The number of mongo processes will be running on VM: 6
- Each process cache size can be configured : [50% of (157GB-1GB)]/6 ==> 78/6 = 13GB(can rounded to 12 GB)

NOTE: OS can consume 40-50GB of buffer/cache memory towards system/kernel operations.

The following values must be configured in mongoConfig.cfg:

- WT_CACHESIZEGB=12
- WT_CACHEARBSIZEGB=1

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 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 disabling 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 using `stopall.sh/startall.sh` or `restartall.sh` command.

- 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 synching:

```
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
```

- Inconsistency in DPR sent by CPS on executing `monit stop` command

Issue: When `monit stop all` is executed on Policy Director (LB) VMs with active VIP, DPR is not sent to all the diameter peers.

Conditions: `monit stop all` executed on Policy Director (LB) VMs with active VIP

Cause: DPR is sent to all the connected diameter peers. However, since `monit stop all` is executed, all the processes on the Policy Director (LB) go down including `corosync/haproxy`. As a result, some of the DPR messages go out and some are not delivered based on the order of the services going down.

Workaround: Instead of `monit stop all`, you can stop all the `qns` process on Policy Director (LB) VMs by executing `monit stop qns-2/3/4` and then issue a `monit stop all` command.

With this workaround, processes such as, `haproxy/corosync` are up when DPR messages are generated, CPS makes sure that all DPR messages generated by the Policy Directors are delivered.

- Grafana page not loading after upgrade or installation.

Issue: Grafana page does not load after upgrade/installation.

Workaround: Restart grafana process with the following command `docker exec grafana:`

```
supervisorctl restart grafana
```

Limitations

This section lists the limitations of this release:

- 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 many 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.
- 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.

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

None in this release.

vDRA Open CDETS

Table 2 - vDRA Open CDETS

CDETS ID	Headline
CSCvx14701	Gx / Rx Timeout dashboard shows incorrect message processing time
CSCwa98187	vPAS - 3002 Error/timeouts observed during longevity randomly
CSCwc07906	Binding storage failed message, mongo exception in consolidated QNS logs
CSCwd89701	During 23.1 DRA-ISO upgrade continuous errors observed when binding/diameters upgraded
CSCwd95673	VDRA : Threshold alerts : Decreasing / increasing alerts not working
CSCwe21072	Halo-E: Unable to Access Grafana from Central DRA as it routes with IP address & not fqdns name
CSCwe11953	Halo-E: Integration with CPS DRA - Page refresh does not land into last visited page
CSCwe28971	Halo E: Assign Roles in Grafana for OIDC authenticated users
CSCwe45228	After DRA VMDK upgrade from 23.1, Grafana UI is not opening 404 error is coming in UI

Resolved CDETS

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

CPS Resolved CDETS

Table 3 - CPS Resolved CDETS

CDETS ID	Headline
CSCwc95002	Feature details are not listing in about.sh output
CSCwd09339	Zookeeper process not coming up on its own on new installer VM
CSCwd27597	start_svn_sync.sh, statusall.sh, and summaryall.sh scripts not working with allow_user_nologin true.
CSCwd36674	show_peers is not showing connections, which are using ports 9100 and above
CSCwd43203	Bulk Terminate script output is not formatted properly after python upgrade
CSCwd88911	BEMS01542112: DSCP configuration not working on CPS 22.2.
CSCwd95465	Zookeeper 4lw external command stat cli not working
CSCwd95595	Observed Clock_skew issue in diagnostic
CSCwd25595	Session terminate script does not work
CSCwd29064	PCRF Sending Sd RAR w/o Destination-Host
CSCwd79214	Reduced number of Sy-SLR traffic to Active Charge OCS during Enabler OCS outage
CSCwe02366	UDC session soft-delete-timer change
CSCwe10059	Race Condition Scenarios - Unintentional removal of UDC session when there are back to back CCR-I/Ts

vDRA Resolved CDETS

Table 4 - vDRA Resolved CDETS

CDETS ID	Headline
CSCwd67026	Remove 128 bit IP support from zone sharding configuration
CSCwd56534	DRA IPv6 export is not working for Subscriber Utility feature
CSCwd76496	DraActivePeerManager bean is not creating during application start
CSCwe14919	Sync latest pwd and Allow complex pwd to protect JKS file for TLS cert installation.
CSCwd09291	Peer monitoring gui, select any peer for its detailed prop for TLS, we see transport medium as TCP
CSCwd81465	VM's are not getting install from Deployer 22.2 latest P1 due to upgrade of Python PyVmomi module
CSCwd02227	Add new SNMP alert for FLUENTBIT_SERVER_NOT_REACHABLE
CSCwd09637	Validation of essential plugins for threadingConfiguration is not working as expected
CSCwd19544	External fluentbit forwarding is not working for VIP interfaces

CDETS ID	Headline
CSCwd69632	Relevant msg not displaying for IPV6 zone overlap & Duplicate entry scenario at CLI level Validation
CSCwd47203	Manual verification failed for "active_peer_count" KPI.
CSCwe13005	All sites Database Monitoring dashboard - Cluster dropdown not displaying any options
CSCwb96525	Site id is missing for KPI diameter_request_total with label late
CSCwc17548	Add new labels for KPI and CLI peer_dynamic_rate_limit_throttling
CSCwd28102	IPV6 Zone: Change Exception and fix clustername error
CSCwc79874	One of Consul is Unhealthy after downgrade from 22.1 MR EFT to 22.1 release is Finished 100%
CSCwd92277	Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS / 22.10 : Python vulnerabilities (USN-5767-1)
CSCwd76608	Ubuntu 18.04 LTS :Sysstat,shadow,linux-kernel,binutils,heimdal,libxml vulnerabilities
CSCwd66230	Ubuntu 18.04 LTS / 20.04 LTS Expat, Linux-Kernel,sqlite Vulnerabilities
CSCwd42135	Ubuntu 16.04 ESM/18.04 LTS/20.04 LTS:GMP vulnerability/Perl vulnerability/Heimdal vulnerabilities
CSCwd12354	Ubuntu 18.04 LTS / systemd vulnerability, Vim vulnerabilities, Open VM Tools vulnerability
CSCwd86818	CIAM: Grafana 5.2.3 Security Vulnerabilities
CSCwe42544	Ubuntu 18.04 LTS / 20.04 LTS OpenSSL, Heimdal, Linux Kernel
CSCwe12737	Ubuntu 18.04 LTS/20.04 LTS : Heimdal vulnerabilities(USN-5800-1)

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 Advanced Tuning 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 Documentation Map*
- *CPS Geographic Redundancy Guide*
- *CPS Installation Guide - OpenStack*
- *CPS Installation Guide – VMware*
- *CPS Migration and Upgrade Guide*
- *CPS Mobile Configuration Guide*
- *CPS Operations Guide*

- *CPS Policy Reporting Guide*
- *CPS Release Change Reference*
- *CPS Release Notes*
- *CPS SNMP, Alarms, and Clearing Procedures Guide*
- *CPS Troubleshooting Guide*
- *CPS Unified API Reference Guide*
- *CPS vDRA Administration Guide*
- *CPS vDRA Advanced Tuning Guide*
- *CPS vDRA Configuration Guide*
- *CPS vDRA Installation Guide for VMware*
- *CPS vDRA Operations Guide*
- *CPS vDRA SNMP and Alarms Guide*
- *CPS vDRA Troubleshooting 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 un-Controlled 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)

© 2023 Cisco Systems, Inc. All rights reserved.