



# Cisco Policy Suite 25.1.0 Release Notes for vDRA

First Published: April 29, 2025

## Introduction

This Release Note identifies installation notes, limitations, and restrictions, and open and resolved CDETS in Cisco Policy Suite (CPS) software version 25.1.0. 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 25.1.0 software package (ISO/VMDK image) from:

<https://software.cisco.com/download/home/284883882/type/284979976/release/25.1.0>

## Md5sum Details

### DRA

5f38e41f94e6f65fd242e7368f2af4d6	CPS_Microservices_DRA_25.1.0_Base.release.vmdk.SPA.tar.gz
ecbb5fd0c4f636b12ed8fd257b2f1fbf	CPS_Microservices_DRA_25.1.0_Deployer.release.vmdk.SPA.tar.gz
0613da140dfe4dfada0dfc5f4bd550ee	CPS_Microservices_DRA_25.1.0.release.iso.SPA.tar.gz
76f7260fef802ff6172ad012397cdb07	CPS_Microservices_DRA_Binding_25.1.0.release.iso.SPA.tar.gz

## Component Versions

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

**Table 1 - Component Versions**

Component	Version
Core	25.1.0
Custom Reference Data	25.1.0
DRA	25.1.0
Microservices Enablement	25.1.0

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

### VMware Environment

To perform a new installation of CPS 25.1.0 in a VMware environment, see the *CPS vDRA Installation Guide for VMware*.

### Prerequisite for upgrading from 24.2.0 to 25.1.0

The following are the common prerequisites:

1. Run the following CLI before upgrade:

```
#database genericfcvcheck 6.0
```

**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).

3. Run the following CLI before upgrade:

```
#database dwccheck
```

**NOTE:** CLI automatically takes care of Default Write Concern version on all databases. This CLI will be available in 24.2 P1 and if it is upgraded from 24.2 CCO then the following steps should be performed manually.

4. Specify any one of the CLI options:

- a. **Set:** This option checks and sets dwc on primary members.

- b. **Check:** This option only checks dwc on all members.

```
(set/check) << set
```

- i. **Set:** This option checks and sets defaultWriteConcern.

- ii. **Check:** This option only checks defaultWriteConcern on all members(primary/secondary)..

## Additional Notes

This section provides additional notes necessary for proper installation/working of CPS.

- **CSCwo31311:** weave network still showing, after enabling docker overlay network in CPS vDRA & DB Vnf; Vice-Versa

**Issue:** weave network still showing, after enabling docker overlay network in CPS vDRA & DB Vnf; Vice-Versa

**Workaround:** run one more time network detach-<weave/overlay> CLI command

- **CSCwo39695:** In fPAS MTLs IPV6 links are not establishing after docker overlay is enabled

**Issue:** In fPAS MTLs IPV6 links are not establishing after docker overlay is enabled

**Workaround:** issue with IPV6 alone, IPV4 works as we expected

## Open and Resolved CDETS

The following sections list open and resolved CDETS for this release. For your convenience in location 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=](https://tools.cisco.com/RPF/register/register.do?exit_url=)

### Open CDETS

The following table lists the open CDETS in this release.

**Table 2 - vDRA Open CDETS**

CDETS ID	Headline
CSCwo31311	weave network still showing, after enabling docker overlay network in DRA & DB Vnf; Vice-Versa
CSCwo39695	In fPAS MTLs IPV6 links are not establishing after docker overlay is enabled

### Resolved CDETS

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

**Table 3 - vDRA Resolved CDETS**

CDETS ID	Headline
CSCwm55802	vDRA unstable due QTP thread Issue and healthcheck failures
CSCwk62956	Drop Message option not working as expected while Rate limiting
CSCwm01342	Some logs are missing in consolidated qns logs when debug is enabled
CSCwm49281	Cannot delete a Table Group (CRD subset) while backing out the configuration
CSCwn04983	Topology loop not detected in DRA
CSCwn39670	P2, AT&T fPAS, CPS vDRA, 23.2, Grafana access is not working with Halo-e OIDC
CSCwn85594	CPS vDRA 22.2 P4 mongo and redis password lost after vDRA powered down for 48 hours and power on
CSCwn99268	Change in vmname value affecting Prometheus generated files
CSCwn91465	'status' label in diameter_request_total needs to be removed

CDETS ID	Headline
CSCwn12639	Add support for vip failover in fluentbit config
CSCwn16097	Add http status check to keepalived-monitor to avoid vip failovers
CSCwm63789	Expat, Linux kernel, Python,vim,curl vulnerabilities
CSCwm90683	CUPS,VIM,APR,ConfigObj Vulnerabilities
CSCwn14938	Linux kernel, urllib3, AMD Vulnerabilities
CSCwn39115	Glib,Python Vulnerabilities
CSCwn59547	Linux kernel,curl,PostgreSQL,Expat,Vim Vulnerabilities
CSCwn93295	Git,rsync,Bind,Linux kernel vulnerabilities
CSCwn86836	MongoDB 6.0.x < 6.0.17 / 7.0.x < 7.0.13 / 7.3.x < 7.3.4 incorrect enforcement of index constraints
CSCwo20345	Kerberos ,GNU C,Jinja2 ,Bind ,libxml2 Vulnerabilities

## Related Documentation

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

### Release-Specific Documents

For more information on the Cisco Policy Suite, refer to the documents for this release available at:

<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](http://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](http://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)

© 2025 Cisco Systems, Inc. All rights reserved.