Cisco Policy Suite 25.2.0 Release Notes for vDRA

First Published: Oct 29, 2025

Introduction

This Release Note identifies installation notes, limitations, and restrictions, and open and resolved CDETS in Cisco Policy Suite (CPS) software version 25.2.0. 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

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 25.2.0 software package (ISO/VMDK image) from:

https://software.cisco.com/download/home/284883882/type/284979976/release/CPS_25.2.0

Md5sum Details

DRA

9d25ea406dd41e916181a6a2ad16f343	CPS_Microservices_DRA_25.2.0_Base.release.vmdk.SPA.tar.gz
39bfca69749ff8a12e4bd4a6e7f28c61	CPS_Microservices_DRA_25.2.0_Deployer.release.vmdk.SPA.tar.gz

b89e914cc5ad2e62aaa04d208a4d62b6	CPS_Microservices_DRA_25.2.0.release.iso.SPA.tar.gz
6df8b23d38ca4bb647966d45a6e12e95	CPS_Microservices_DRA_Binding_25.2.0.release.iso.SPA.tar

Component Versions

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

Table 1 - Component Versions

Component	Version
Core	25.2.0
Custom Reference Data	25.2.0
DRA	25.2.0
Microservices Enablement	25.2.0

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 25.2.0 in a VMware environment, see the *CPS vDRA Installation Guide for VMware*.

Prerequisite for upgrading to 25.2 from 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 only checks defaultWriteConcern on all members(primary/secondary).

Additional Notes

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

- **CSCwq27394:** Upgrade prometheus to 3.5.0 version

  Issue: During upgrade, there is a risk of up to 2 hours of data loss. In-memory and uncompacted data stored by Prometheus may not be fully written to disk, resulting in up to a 2-hour gap in Grafana data.

  Workaround: The Prometheus binary in Prometheus containers has been upgraded from version 2.3.1 to 3.5.0:

- The data directory for the new Prometheus 3.5.0 binary is:
  - On the VM: /stats/prometheus-hi-res/3.5
  - In the container: /data-3
- The data directory for the old Prometheus 2.3.1 binary is:
  - On the VM: /stats/prometheus-hi-res/2.0
  - In the container: /data-2
- All existing Prometheus data will remain in the /data-2 directory
- All new Prometheus data will be stored in the /data-3 directory
- Ensure Prometheus is shut down gracefully before starting the upgrade by running the following command:

```
docker exec prometheus- "supervisorctl stop all"
```

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=

Open CDETS

The following table lists the open CDETS in this release.

Table 2 - vDRA Open CDETS

CDETS ID	Headline
CSCwq11542	In fPAS, slowness is seen when connecting mtls-ipv6-client peers in overlay network
CSCwq83519	haproxy-common containers unhealthy after DB ISO upgrade with OVERLAY enabled.
CSCwr12961	During Active-Active and Failover longevity,observed Rx_AAR timeouts when setup is in Overlay and mongo_TLS enabled
CSCwr13040	Mongo over TLS Enabled (All Sites) + Overlay Network, Non-VoLTE traffic fails
CSCwr26245	Grafana data loss observed after DB/DRA ISO upgrade to 25.2

Resolved CDETS

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

Table 3 - vDRA Resolved CDETS

CDETS ID	Headline
CSCwn77580	ICMP Timestamp Request Remote Date Disclosure
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
CSCwo85260	vDRA : Add CLI to rollback fluentbit configs
CSCwo87107	vDRA, 23.2 P2, During upgrade faced 4xxx Binding DB errors from few containers
CSCwp07009	libxml,Linux kernel,OpenSSH,libarchive Vulnerabilities
CSCwp12396	Monitor Activity/age trace logs are not capturing Rx AAR Final if Rx AAR Inital is not present
CSCwp23618	CPS vDRA, 22.2, Mongo DB WireTiger DB Recovery Script not working due to common cps pem access logic
CSCwp30043	vDRA : 403 error is returned for http://drm-ip/ instead of DRA Central page
CSCwp32106	Linux kernel,PostgreSQL, Open VM Tools,SQLite Vulnerabilities
CSCwp90097	Setuptools, GNU C Library, Linux kernel, Apport,systemd Vulnerabilities
CSCwp91526	New format consolidated QNS old logs are not getting deleted
CSCwq00466	vDRA : prometheus API query not working with public ip
CSCwq58637	db connect admin cli is not working
CSCwq64135	Apache HTTP,SQLite,Linux kernel,cloud-init,iputils vulnerabilities
CSCwq95240	TCP FIN is not sent during a TLS connection breakdown
CSCwr02395	vDRA/ Rx_STR Looping caused in DRA Relay Scenario due to AF FQDN in both Origin and Destination Host AVPs
CSCwr13401	Python, Linux kernel,UDisks,LibTIFF,GCC 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.