CPS Release Change Reference, Release 25.2.0

First Published: 2025-10-29

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

Preface

About This Guide

Note The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. While any existing biased terms are being substituted, exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

This document is a part of the Cisco Policy Suite documentation set.

For information about available documentation, see the *CPS Documentation Map* for this release at Cisco.com.

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.

Audience

This guide is best used by these readers:

- Network administrators

- Network engineers
- Network operators
- System administrators

This document assumes a general understanding of network architecture, configuration, and operations.

Additional Support

For further documentation and support:

- Contact your Cisco Systems, Inc. technical representative.
- Call the Cisco Systems, Inc. technical support number.
- Write to Cisco Systems, Inc. at support@cisco.com.
- Refer to support matrix at https://www.cisco.com/c/en/us/support/index.html and to other documents related to *Cisco Policy Suite*.

Conventions (all documentation)

This document uses the following conventions.

Conventions	Indication
bold font	Commands and keywords and user-entered text appear in **bold** font.
italic font	Document titles, new or emphasized terms, and arguments for which you supply values are in *italic* font.
[ ]	Elements in square brackets are optional.
{x | y | z }	Required alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
courier font	Terminal sessions and information the system displays appear in courier font.
< >	Nonprinting characters such as passwords are in angle brackets.

Conventions	Indication
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Note Means reader take note. Notes contain helpful suggestions or references to material not covered in the manual.

Caution Means reader be careful. In this situation, you might perform an action that could result in equipment damage or loss of data.

Warning IMPORTANT SAFETY INSTRUCTIONS.

Means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device.

SAVE THESE INSTRUCTIONS

Note Regulatory: Provided for additional information and to comply with regulatory and customer requirements.

Communications, Services, and Additional Information

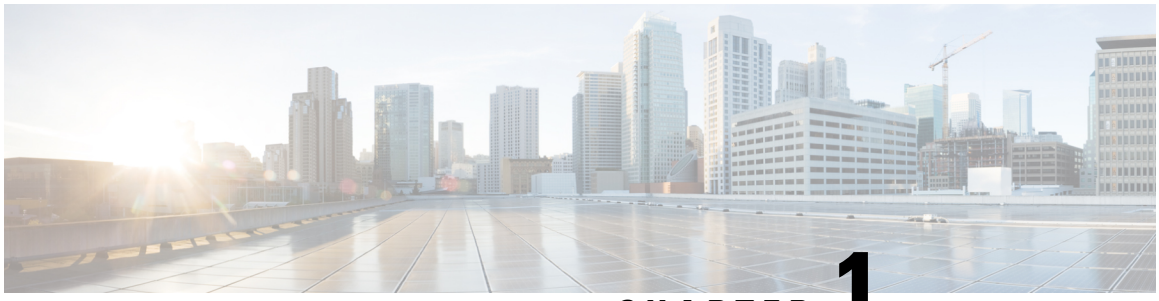
- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business results you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco DevNet.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

Important Notes

Important Any feature or GUI functionality that is not documented may not be supported in this release or may be customer specific, and must not be used without consulting your Cisco Account representative.



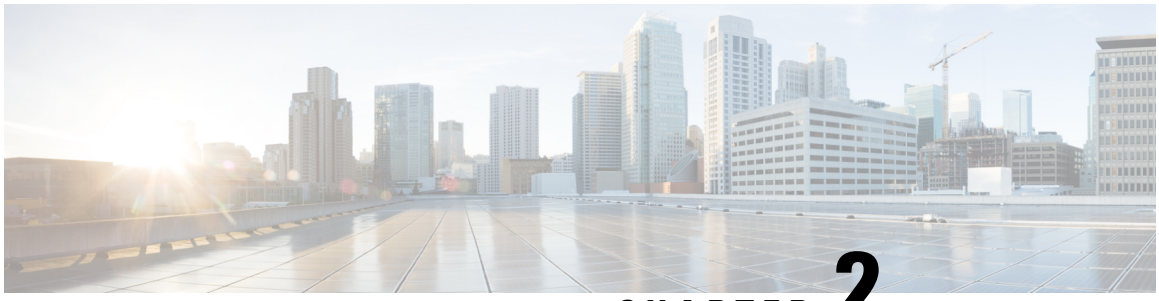
CHAPTER 1

Feature Changes

25.2.0 Features and Changes

Table 1: New feature information

Features	Applicable Product(s)/ Functional Area	Release Introduced/ Modified
MFA Support for Orchestrator CLI, on page 14	vDRA	25.2.0
PSB Requirements , on page 5	PCRF/vDRA	25.2.0
Generate Logs for specific Diameter Endpoint or binding container, on page 11	vDRA	25.2.0
Promethus upgrade, on page 4	vDRA	25.2.0
Support for TLS/SSL Encryption in MongoDB, on page 16	vDRA	25.2.0
Support for VMware ESXi Hypervisor 8.0, on page 3	vDRA	25.2.0



CHAPTER 2

Platform

Support for VMware ESXi Hypervisor 8.0

Feature Summary and Revision History

Table 2: Summary Data

Applicable Product(s) or Functional Area	vDRA
Applicable Platform(s)	Not Applicable
Default Setting	Enabled – Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	• *CPS VDRA Installation Guide for VMware*

Table 3: Revision History

Revision Details	Release
First introduced	25.2.0

Feature Description

In this release, vDRA supports ESXi 8.0, with **Firmware** set to **BIOS** during the creation of CPS installer virtual machines. This configuration helps prevent system failures.

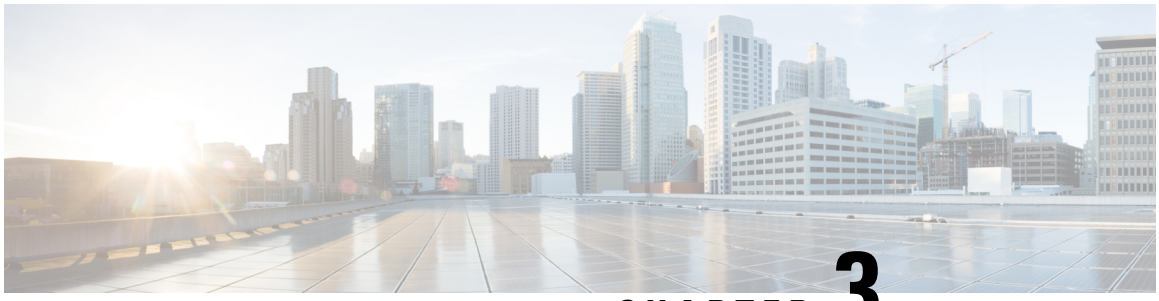
For details about deploying vDRA on ESXi 8.0, refer to the *CPS vDRA Installation Guide for VMware* and the *CPS Migration and Upgrade* Guides.

Promethus upgrade

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
```



CHAPTER 3

Security Enhancements

PSB Requirements

A product security baseline requirement is a security standard that

- establishes minimum security measures for software and systems,
- aligns with product security features for each release, and
- ensures compliance across essential security domains.

These are the main complaince categories:

- TPS management and vulnerability handling
- Threat modeling and security testing
- Security features and protections
- Documentation and system processes

PCRF PSB requirements

CPS supports these PSB requirements:

Table 4: PSB Requirements

PSB Item	Description
CT2340: SEC-UPS-TPSQUAL-FR1-v3	Remove any TPS component present in the Corona Exclusion List (COR-EL).
CT2337: SEC-UPS-TPSQUAL-FR2-v3	Review high-risk vulnerabilities to determine their applicability to the offering.
CT2349: SEC-UPS-TPSQUAL-FR3-v3	Fix TPS vulnerabilities within the documented timelines.

PSB Item	Description
CT2354: SEC-UPS-TPSQUAL-FR4-v3	Respond to CVR Disposition Requests (DR) within the documented timeline.
CT2336: SEC-UPS-REGI-FR1-v5	Register Third-Party Software.
CT2335: SEC-UPS-REGI-FR2-v5	Update TPS Registrations regularly.
CT2330: SEC-ASU-TMOD-FR1-v4	Create and Review a System-Level Threat model.
CT2329: SEC-ASU-TMOD-FR2-v4	Assess and Mitigate Threats Against High-value assets.
CT2321: SEC-ASU-TMOD-FR3-v4	Create Additional Threat Models for new features.
CT2326: SEC-ASU-TMOD-FR4-v4	Update Threat Models as needed.
CT2322: SEC-ASU-TMOD-FR5-v4	Threat Model review.
CT2325:SEC-ASU-STATIC-4	Perform Static Application Security Testing ([SAST](/library/glossary/CG181)).
CT2339: SEC-WEB-CSRF-4	Prevent CSRF vulnerabilities.
CT2324: SEC-AUT-DEFROOT-3	No default credentials.
CT2323: SEC-DAT-KNOWWHAT-3	Know and document what data your product or service processes and assess the legal, security, and privacy risk.
CT2347: SEC-UPS-REGI-FR3-v5	Create a Distribution-Ready Software Bill of Materials (SBOM).
CT2353: SEC-UPS-UPDATE	Update Third-party Software (TPS) Components regularly.
CT2346: SEC-FOR-DEBUG	Provide secure root/admin access for forensic analysis.
CT682: SEC-CON-PERM	Filter incoming connections by source IP address
CT2327: SEC-ASU-TMOD-FR6-v4	Store Threat models
P8: CT2236: SEC-SW-APPDTCT-FR5-v1	Check all signatures before loading code.
P8: CT2238: SEC-SW-APPDTCT-FR7-v1	Cisco-controlled Authentication roots.
CT2237: SEC-SW-APPDTCT-FR6-v1	Load Verification Trust Chain for Closed code.
CT1890: SEC-NTP-AUTH	Support NTP, NTP authentication, and filtering.
CT2301: SEC-IP-IPv6-2	Support all security requirements over IPv6.

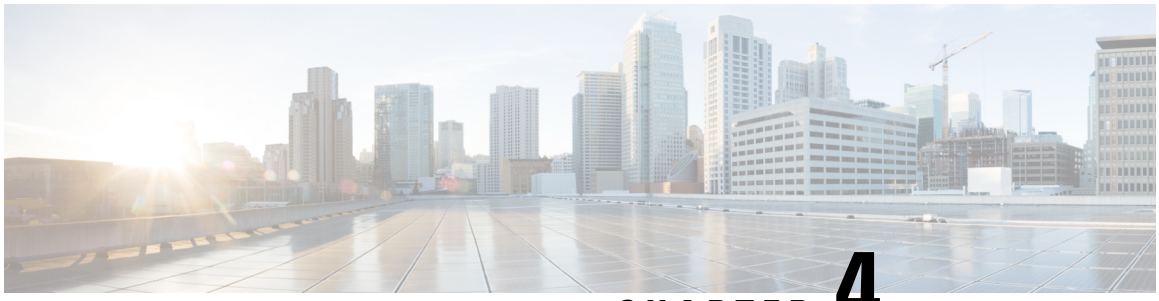
vDRA PSB requirements

CPS supports these PSB requirements:

Table 5: PSB Requirements

PSB Item	Description
SEC-VAL-INEVAL-2	Prevent injection vulnerabilities by not passing uncontrolled data to other Execution Spaces.
SEC-VAL-INXPATH-2	Use prepared statements or validate user input to construct XPath queries.
SEC-VAL-INXXE-2	Disable entity expansion or validate text content after expansion to prevent XML eXternal Entity (XXE) Injection.
SEC-WEB-RESP-3	Specify type and encoding in HTTP responses; disable type sniffing.
SEC-CRY-PRIM-9	Use approved cryptographic primitives and parameters.
SEC-CRY-STDCODE-FR3-v3	Third-Party Libraries.
SEC-TLS-CURR-6	TLS 1.2 and TLS 1.3.
SEC-DAT-KNOWWHAT-3	Know and document what data your product or service processes and assess the legal, security, and privacy risk.
SEC-SCR-CONFLEAK-3	Do not expose critical data
SEC-CRY-ALWAYS-3	Provide cryptographic protection outside controlled space
SEC-ASU-TMOD-4	Create and Review a System-Level Threat Mode
SEC-ASU-TMOD-FR1-v4	Create and Review a System-Level Threat Model.
SEC-ASU-TMOD-FR2-v4	Assess and Mitigate Threats Against High-value assets.
SEC-ASU-TMOD-FR3-v4	Create Additional Threat Models for new features.
SEC-ASU-TMOD-FR4-v4	Update Threat Models as needed.
SEC-ASU-TMOD-FR5-v4	Threat Model review
SEC-ASU-SCAN-3	Evaluate the attack surface of an operational offering using automated scanning tools
SEC-UPS-REGI-FR1-v5	Register Third-Party Software
SEC-UPS-REGI-FR2-v5	Update TPS registrations regularly.
SEC-UPS-TPSQUAL-FR2-v3	Review high-risk vulnerabilities to determine their applicability to the offering

PSB Item	Description
SEC-UPS-TPSQUAL-FR3-v3	Fix TPS vulnerabilities within the documented timelines.
SEC-UPS-TPSQUAL-FR4-v3	Respond to CVR Disposition Requests (DR) within the documented timeline.
SEC-RUN-ASLR-FR1-v3	Randomize memory segments.
SEC-RUN-ASLR-FR2-v3	Randomization Entropy.
SEC-RUN-ASLR-FR3-v3	ASLR can not be disabled



CHAPTER 4

Operations

Behavior of db_user authentication issues during Repair CLI execution—CSCwq73829

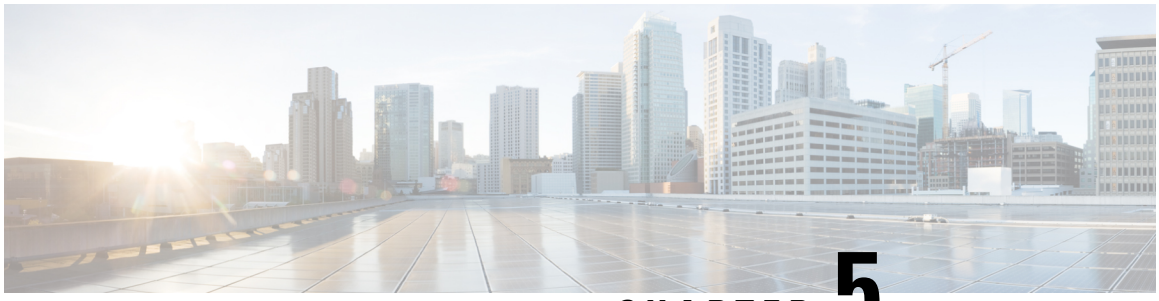
Revision History

Revision details	Release
First Introduced	CPS 25.2

Behavior Change

Previous behavior: A dedicated user named "db_user" was not uniformly created or utilized across all sites, and recovery scripts or CLI executions did not default to using "db_user" for logging into VMs.

New Behavior: A new user named "db_user" is created across all sites. Recovery scripts are modified to use "db_user" as the default user for signing in to each VM. CLI executions will now use "db_user" as the default user. For "db_user", the password is set, and PEM file-based authentication is enabled on all VMs across all sites.



CHAPTER 5

vDRA

Generate Logs for specific Diameter Endpoint or binding container

Feature summary and revision history

Table 6: Summary Data

Applicable Product(s) or Functional Area	vDRA
Applicable Platform(s)	Not Applicable
Default Setting	Enabled – Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	• *CPS vDRA Operations Guide*

Table 7: Revision History

Revision Details	Release
In this release, enhancement is supported to enable logs for a specifc DRA application's container (max 3 containers per module) to reduce the log size and simplify troubleshooting.	25.2.0

Enabling application logs for specific containers

Enabling application logs for specific containers is a feature that:

- reduces log flooding and out-of-order messages,
- simplifies troubleshooting for DRA applications, and
- allows granular control over logging by targeting individual or multiple containers.

In Diameter Routing Agent (DRA), enabling application logs is crucial for troubleshooting, debugging, performance monitoring, and audit and accountability of the DRA application. Previously, enabling trace, error, debug, warn, or info logs would apply to all application containers, causing excessive logging, log misses, and out-of-order messages. This feature addresses these issues by allowing you to enable application logs only for specific containers, making troubleshooting more efficient.

Limitations

The limitations are:

- Even when the debug level is enabled for specific containers, WARN and ERROR application logs are always included in the consolidated QNS logs for all containers.
- If you specify more than three containers in the command-line interface (CLI), only the first three containers are considered for logging. A message will indicate that logs are enabled only for the first three containers. Similarly, the show logger level command will display only these first three containers, and application logs will be generated in the consolidated QNS logs for only these three.

Manage loggers during system upgrades

This task allows you to manage existing loggers during system upgrades to a newer version, for example, from 25.1 to 25.2.

Use these steps to perform pre-upgrade actions and recovery (if pre-upgrade clearing was missed).

Procedure

Step 1 Perform pre-upgrade actions using these steps:

a) Before initiating the upgrade, take a backup of all currently enabled or disabled loggers.
b) Remove all existing loggers from your system.
c) After the upgrade is complete, re-configure your desired loggers using the new CLI format, which supports specifying containers.

```
admin@orchestrator[site3-dra-master0]# logger set  logger-name
logger-level container-name,container-name2,containers-name3
```

Example:

logger set com.example.app debug container1,container2

Step 2 If you upgraded from version 25.1 or earlier without clearing the existing loggers, complete these steps after the upgrade is complete:

a) Execute the following command to list loggers set with the previous format:

```
consul kv get --recurse cisco-policy/logging/loggers/
```

b) Review the output from Step a and collect the names of loggers that do not include attributes such as "instance1, instance2, instance3, level".

Example:

if the output contains `cisco-policy/logging/loggers/com.broadhop.dra:warn`, then `com.broadhop.dra` is the logger name to target.

c) For each logger name identified in Step b, run the delete command:

```
consul kv delete cisco-policy/logging/loggers/<logger-name>
```

Example:

```
consul kv delete cisco-policy/logging/loggers/com.broadhop.dra
```

d) Repeat Step c for all loggers identified in Step b.

e) Run the **consul kv get** command again to confirm that no loggers from the old format remain.

```
consul kv get --recurse cisco-policy/logging/loggers/
```

Note
If you upgrade from a version later than 25.2, all existing loggers will be automatically available in the new version.

Managing loggers during downgrades

This task allows you to manage existing loggers during system downgrades, especially those configured with container-specific settings.

This task allows you to downgrade your system to a newer version, for example, from 25.2 to 25.1.

Before you begin

Use these steps to perform pre-downgrade actions and recovery (if pre-downgrade clearing was missed).

Procedure

Step 1 Perform pre-downgrade actions using these steps:

a) Before initiating the downgrade, take a backup of all currently enabled or disabled loggers.

b) Remove all existing loggers from your system.

c) Proceed with the system downgrade to the older version.

d) After the downgrade is complete, re-configure your desired loggers using the new CLI format, which supports specifying containers.

```
admin@orchestrator[site3-dra-master0]# logger set  logger-name logger-level
```

Example:

```
logger set com.example.app info
```

Step 2 If you downgraded from version 25.2 or earlier without clearing the existing loggers, complete these steps after the downgrade is complete:

a) Execute the following command to list loggers set with the newer format:

```
consul kv get --recurse cisco-policy/logging/loggers/
```

b) Review the output from Step a and collect the names of loggers that do not include attributes such as "instance1, instance2, instance3, level".

Example:

if the output contains `cisco-policy/logging/loggers/instance1/com.broadhop.dra:binding-s107`, then `instance1/com.broadhop.dra` is the logger name to target.

c) For each logger name identified in Step b, run the delete command:

```
consul kv delete cisco-policy/logging/loggers/<instanceX>/<logger-name>
```

Example:

```
consul kv delete cisco-policy/logging/loggers/instance2/com.broadhop.dra
```

d) Repeat Step c for all loggers identified in Step b.

e) Run the **consul kv get** command again to confirm that no loggers from the old format remain.

```
consul kv get --recurse cisco-policy/logging/loggers/
```

Note
If you downgrade from a version later than 25.2, all existing loggers will be automatically available in the new version.

MFA Support for Orchestrator CLI

Feature Summary and Revision History

Table 8: Summary Data

Applicable Product(s) or Functional Area	CPS vDRA
Applicable Platform(s)	Not Applicable
Default Setting	Disabled – Configuration Required to Enable
Related Changes in This Release	Not Applicable
Related Documentation	*CPS vDRA Operation Guide*

Table 9: Revision History

Revision Details	Release
First introduced.	25.2.0

Feature Description

This feature enhances the security of the vDRA orchestrator system by introducing Multi-Factor Authentication (MFA) for CLI access. With this update, users attempting to access the orchestrator CLI must provide two authentication factors: a PEM file (private key) and a password. This dual-factor requirement adds an extra layer of security, reducing the risk of unauthorized CLI access.

The commands introduced are:

- **mfa-cli enable user-id** <*USER_ID*> CLI command enables the MFA for a user. To disable the MFA support for a user, use the **no mfa-cli enable user-id** <*USER_ID*> CLI command.
- **show running-config mfa-cli enable** CLI command displays MFA-enabled users.
- **cli-mfa -i user.pem -p 2024 user@localhost** CLI command helps to access the confd CLI interface for MFA users.

Configure MFA Support for Orchestrator CLI

Prerequisite:

Before using the MFA CLI commands, ensure the SSSD configuration is updated. Update the `/etc/sssd/sssd.conf` file on DRM and DRC VMs. This configuration allows GTAC users to list their IDs.

Follow this procedure to configure the MFA support for orchestrator CLI.

1. Add the alias in artifacts before VMDK upgrade or fresh installation procedure.

   ```
   alias cli-mfa="/etc/ssh-mfa"
   ```

2. Manually create the alias in Deployer VM.

   ```
   alias cli-mfa="/etc/ssh-mfa"
   ```

3. Copy the script from deployer and create alias to install the package as given in the jump server.

   ```
   alias cli-mfa="/etc/ssh-mfa"
   sudo apt-get install sshpass # For Debian/Ubuntu
   ```

4. Add the given configuration in the DRM/DBM to allow only the admin to execute the MFA enable CLI access.

   ```
   admin@orchestrator[TEST-Binding-master](config)# nacm groups group mfa user-name admin
   admin@orchestrator[TEST-Binding-master](config)# commit
   Commit complete.
   admin@orchestrator[vpas-B1-master-0](config)# nacm rule-list allow-mfa-access group [
   mfa ] rule allow-access module-name tailf-cps-orchestrator path /mfa-cli/
   access-operations create,read,update,delete,exec action permit
   admin@orchestrator[vpas-B1-master-0](config-rule-allow-access)# commit
   Commit complete.
   admin@orchestrator[vpas-B1-master-0](config)# nacm rule-list restrict-mfa-access group
   [ * ] rule restrict-access module-name tailf-cps-orchestrator path /mfa-cli/
   access-operations create,read,update,delete,exec action deny
   admin@orchestrator[vpas-B1-master-0](config-rule-restrict-access)# commit
   Commit complete.
   ```

5. Verify `external-aaa pam gid-mapping` configurations. These mappings ensure MFA-enabled users can access applications like Grafana or CPS Central by linking user roles to Group IDs (GIDs).

   ```
   admin@orchestrator[M3-vpas-A-master-0]# show running-config external-aaa pam
   external-aaa pam gid-mapping 100 admin
   !
   external-aaa pam gid-mapping 100 grafana-viewer
   ```

```
!
external-aaa pam gid-mapping 100 policy-admin
!
external-aaa pam gid-mapping 100 policy-ro
!
external-aaa pam gid-mapping 500 admin
!
external-aaa pam gid-mapping 500 grafana-admin
!
external-aaa pam gid-mapping 500 policy-admin
!
```

Limitations of MFA Support for Orchestrator CLI

- Only admin users can enable or disable MFA for any user via the CLI. Non-admin users do not have permissions to configure MFA settings.
- MFA can only be enabled for users who have access to both the Orchestrator CLI and the underlying VM (typically external LDAP/GTAC users). MFA is not supported for DRA VM users.
- Orchestrator CLI with MFA can only be accessed from designated servers: DRM, DBM, DIM, or Jump servers. Direct access from other sources is not permitted.
- The same PEM file must be used for both VM authentication and Orchestrator CLI login.
- It is not possible to restrict a user to only the orchestrator CLI without also granting them access to DRM/DBM.
- The `cli-mfa` alias must be properly configured either in artifacts before upgrade or installation to use the MFA CLI command.
- When MFA is enabled for a user, direct SSH login is denied. Access the Orchestrator CLI exclusively through the `cli-mfa` command.
- MFA users must provide both a PEM file and a password to access the CLI. If either credential (PEM file or password) is incorrect or missing, access is denied.
- MFA for CLI does not affect the ability of the user to log in to the GUI, which continues to use password-based authentication.

For more information on the CLI commands, refer to the *CPS vDRA Operation Guide*.

Support for TLS/SSL Encryption in MongoDB

Feature Summary and Revision History

Table 10: Summary Data

Applicable Product(s) or Functional Area	CPS vDRA
Applicable Platform(s)	Not Applicable
Default Setting	Disabled – Configuration Required to Enable

Related Changes in This Release	Not Applicable
Related Documentation	*CPS vDRA Operation Guide*

Table 11: Revision History

Revision Details	Release
First introduced.	25.2.0

Feature Description

This feature introduces TLS/SSL encryption for MongoDB communication within the vDRA environment.

The key aspects of this feature include:

- Securing data in transit between the DRA application and MongoDB, as well as between MongoDB replica set members.
- Utilizing X.509 certificates for authentication and enforcing strong TLS ciphers (TLS 1.2 and 1.3 support).
- Configuring TLS modes such as allowTLS, preferTLS and requireTLS for flexible deployment and migration.

  For more information on the **db-encryption mode set** and **db-encryption enable** CLI commands, refer to the *CLI Commands* chapter in the *CPS vDRA Operation Guide*.
- Importing certificates, enabling, and disabling encryption, changing TLS modes, and synchronizing settings across the cluster through CLI.

Upgrade and downgrade support with TLS encryption

This section describes upgrade, downgrade vDRA versions with TLS encryption, and its limitations.

1. Upgrade support:
   - Upgrading from vDRA version 25.2 to 26.1 or 26.2 with TLS encryption enabled is supported
   - **Prerequisities**: Ensure TLS encryption is properly configured before initiating the upgrade process.
2. Downgrade limitation:
   - Downgrading from version 25.2 to 25.1 with TLS encryption enabled is not supported.
   - TLS encryption must be **disabled** before performing this operation
   - **Recommendation**: Verify that TL.S encryption is disabled prior to downgrade to avoid errors.
3. Upgrade from 25.1 to 25.2:
   - Upgrading from version 25.1 to 25.2 with TLS encryption enabled is not supported.
   - TLS encryption must be disabled before performing this operation
   - **Recommendation**: Consider upgrading directly to a higher version (example, 26.1 or 26.2) if TLS encryption is required.

4. Downgrade from 26.1 to 25.2:
   - Downgrading from version 26.1 to 25.2 with TLS encryption enabled is supported.

Note Ensure the target environment is compatible with TLS encryption settings