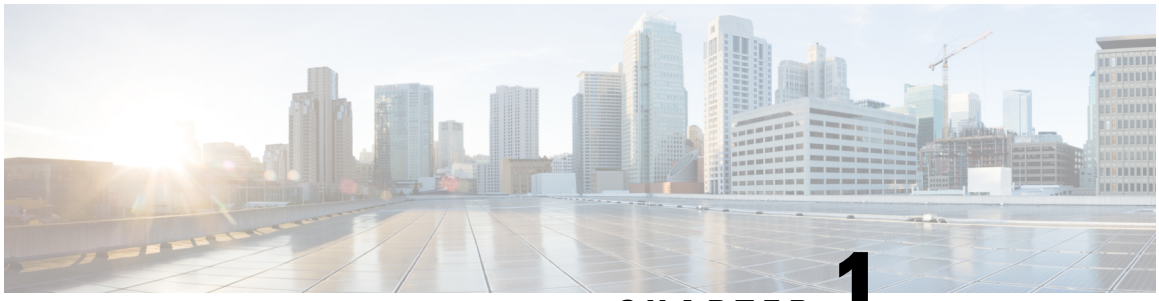
Troubleshooting Guide for Cisco Optical Site Manager, IOS XR Release 25.x.x

First Published: 2025-03-30

Last Modified: 2025-09-16

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



CHAPTER 1

Alarms

This chapter provides description, severity, and troubleshooting procedure for each commonly encountered alarm in Cisco Optical Site Manager.

DBBACKUP-IN-PROGRESS

Default Severity: Warning

Logical Object: Standing

Resource Type: SYSTEM

The DBBACKUP-IN-PROGRESS alarm is triggered when the user initiates the database backup procedure.

Clear the DBBACKUP-IN-PROGRESS Alarm

Procedure

The alarm is cleared automatically when the database backup procedure is completed.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/cisco/web/support/index.html for more information or call Cisco TAC (1 800 553-2447).

DBBACKUP-FAIL

The Database Backup Failed (DBBACKUP-FAIL) alarm is triggered when Cisco Optical Site Manager fails to complete a database backup after initiating a backup. This failure may result from network or server issues.

Clear the DBBACKUP-FAIL Alarm

The alarm is cleared once a database backup completes successfully.

To clear the alarm:

Procedure

Check for any network connectivity issues that could be interrupting the backup process.

If the alarm does not clear, log into the Technical Support Website at for more information or call Cisco TAC (1 800 553-2447).

DBREST-IN-PROGRESS

Default Severity: Warning

Logical Object: Standing

Resource Type: SYSTEM

The DBREST-IN-PROGRESS alarm is triggered when the user initiates the database restore procedure.

Clear the DBREST-IN-PROGRESS Alarm

Procedure

The alarm is cleared automatically when the database restore procedure is completed.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/cisco/web/support/index.html for more information or call Cisco TAC (1 800 553-2447).

DBRESTORE-FAIL

The Database Restore Failed (DBRESTORE-FAIL) alarm is triggered when Cisco Optical Site Manager fails to restore the backed up database after initiating a restore. This failure may result from network or server issues.

Clear the DBRESTORE-FAIL Alarm

The alarm is cleared once a database restore completes successfully.

To clear the alarm:

Procedure

Check for any network connectivity issues that could be interrupting the restore process.

If the alarm does not clear, log into the Technical Support Website at for more information or call Cisco TAC (1 800 553-2447).

NE-NOT-AUTH-ACCESS

Default Severity: Major (MJ)

Logical Object: Standing

Resource Type: NE

The NE-NOT-AUTH-ACCESS alarm is raised when a XR device has more than one syslog (configuration) logging and/or telemetry destination entries on port 7514.

Clear the NE-NOT-AUTH-ACCESS alarm

The alarm clears when the incorrect syslog and/or telemetry destination entries, which have a destination other than the current Cisco Optical Site Manager IP, are removed from the XR device

Follow these steps to clear the alarm:

Procedure

Step 1 Run the **show run** command to display the currently active configuration.

Step 2 Check the command output for multiple Cisco Optical Site Manager logging and model-driven telemetry server entries that use port 7514.

The example output highlights the multiple Cisco Optical Site Manager logging and model-driven telemetry in the command output in bold.

```
RP/0/RP0/CPU0:1014-txp-246#show run
!! Building configuration...
!! IOS XR Configuration 25.3.1.39I
!! Last configuration change at Mon Sep  8 11:57:24 2025 by cisco
!
hostname 1014
logging 10.1.1.1 vrf default severity all port 7514 source-address 10.1.1.1
logging 10.1.1.11 vrf default severity all port 7514 source-address 10.1.1.11
service timestamps log datetime localtime msec show-timezone year
username cisco
 group root-lr
 group cisco-support
 secret 10
$6$/25p40lFhVIP640.$nyB6.WUJUj2HlEGFwITSFs1l.M9cd40fVq9bk8ENHeGRzPUU56kUXqIWByEDluxNgHa3mmU8WTPlV2KFoc.UA1
!
grpc
!
telemetry model-driven
 include empty values
 destination-group COSM-DESTINATION
  address-family ipv4 10.1.1.1 port 7514
   encoding json
   protocol udp
  !
  destination 10.1.1.1 port 7514
   encoding json
   protocol udp
telemetry model-driven
 include empty values
 destination-group COSM-DESTINATION
  address-family ipv4 10.1.1.11 port 7514
   encoding json
   protocol udp
  !
  destination 10.1.1.11 port 7514
   encoding json
   protocol udp
  !
 !
 sensor-group COSM-FPD-GROUP
  sensor-path
Cisco-IOS-XR-show-fpd-loc-ng-oper:show-fpd/locations/location/fpds/fpd/fpd-info-detail/status
 !
```

Step 3 Run the **no logging** command to remove the incorrect configuration.

Example:

```
RP/0/RP0/CPU0:1014(config)#no logging 10.1.1.11 vrf default severity all port 7514 source-address
10.1.1.11
```

Step 4 Run the **no telemetry model-driven** to remove the incorrect configuration for model-driven telemetry.

Example:

```
RP/0/RP0/CPU0(config):1014#no telemetry model-driven destination-group COSM-DESTINATION address-family
 ipv4 10.1.1.11 port 7514
no telemetry model-driven destination-group COSM-DESTINATION destination 10.1.1.11 port 7514
```

If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

SYSBOOT

Default Severity: Major (MJ), Service-Affecting (SA)

Logical Object: NE

The System Reboot alarm indicates that new software is booting on the control card. No action is required to clear the alarm. The alarm clears when all cards finish rebooting the new software. The reboot takes up to 30 minutes. However, if several line cards are present on the nodes in the network or if the line cards reboot many times, the alarm clears before all the line cards reboot completely.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

Note SYSBOOT is an informational alarm. It only requires troubleshooting if it does not clear.

PROTNA

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: EQPT

The Protection Unit Not Available (PROTNA) alarm is raised when the link between the Cisco Optical Site Manager active and standby application is lost. This can happen due to any of these reasons.

- The device hosting the standby application is not discoverable or unreachable.
- There is a cut in the fiber cable connecting to the device hosting the standby application.

Clear the PROTNA Alarm

The alarm is cleared when the link between the Cisco Optical Site Manager Active and Standby application is restored.

To clear the alarm:

Procedure

Step 1 Ensure the device hosting the standby application is discoverable and reachable by the device hosting the active application.

Step 2 Check and repair any cuts in the fiber cable connecting to the device hosting the standby application.

If the alarm does not clear, log into the Technical Support Website at for more information or call Cisco TAC (1 800 553-2447).

RAMAN-CALIBRATION-FAILED

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: OTS

The RAMAN-CALIBRATION-FAILED alarm is raised on the EDRA-1-xx, EDRA-2-xx, and RAMAN-CTP cards when automatic Raman pump calibration is failed and will not run again. The alarm indicates insufficient Raman Amplification by customer fibre. The Raman calibration can also fail due to the setup issues that include:

- Wrong patch-cords or cabling
- Incorrect ANS
- Missing communication channel between nodes.

Clear the RAMAN-CALIBRATION-FAILED Alarm

SUMMARY STEPS

1. Use optical time domain reflectometer (OTDR) to identity any excess loss between the Raman card LINE-RX port and the customer fibre. After the inspection, a new Raman Calibration is triggered and if the physical problem is fixed, the alarm will clear.
2. If the alarm is caused by a set-up problem, re-verify all node installation steps and manually trigger a Raman Calibration.

DETAILED STEPS

Procedure

Step 1 Use optical time domain reflectometer (OTDR) to identity any excess loss between the Raman card LINE-RX port and the customer fibre. After the inspection, a new Raman Calibration is triggered and if the physical problem is fixed, the alarm will clear.

Step 2 If the alarm is caused by a set-up problem, re-verify all node installation steps and manually trigger a Raman Calibration.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

UNTRUSTED-APPLICATION

Default Severity: Critical (CR), Non-Service-Affecting (NSA)

Logical Object: SYSTEM

The *Trust Not Established With CSLU/CSSM* (UNTRUSTED-APPLICATION) alarm is triggered when Smart License is configured in the *Smart Transport* or *CSLU* mode and trust is not established with Cisco Smart Software Manager (CSSM) has not been established.

Clear the UNTRUSTED-APPLICATION Alarm

The alarm is cleared once trust is established between with the CSSM.

To clear the alarm:

Procedure

Ensure that trust is established with CSSM.

For more details on how to establish trust with CSSM, see Configure Smart Transport.

If the alarm does not clear, log into the Technical Support Website at for more information or call Cisco TAC (1 800 553-2447).

USAGE-NOT-REPORTED

Default Severity: Major (MJ), Non-Service-Affecting (NSA)

Logical Object: SYSTEM

The *Licenses Usage Is Not Reported* (USAGE-NOT-REPORTED) alarm is triggered when the Cisco Optical Site Manager is unable to communicate with the Cisco Smart Software Manager (CSSM) or CSLU.

Clear the USAGE-NOT-REPORTED Alarm

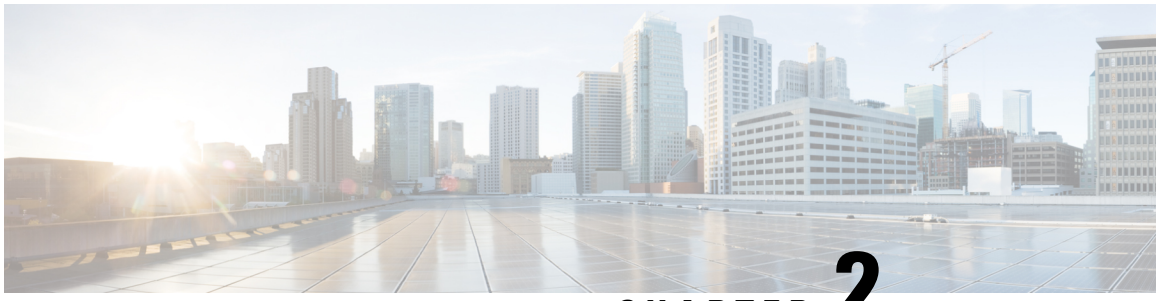
To clear the alarm:

Procedure

Step 1 Verify whether trust has been properly established with CSSM.

Step 2 Verify that CSSM is accessible from Cisco Optical Site Manager, either directly or through CSLU.

If the alarm does not clear, log into the Technical Support Website at for more information or call Cisco TAC (1 800 553-2447).



CHAPTER 2

Transient Conditions

This chapter provides description for each commonly encountered transient condition in Cisco Optical Site Manager.

ADMIN-DISABLE

The Disable Inactive User (ADMIN-DISABLE) condition occurs when a user account is disabled by the administrator or remains inactive for a specified period.

This transient condition does not result in a standing condition.

ADMIN-DISABLE-CLR

The Disable Inactive Clear (ADMIN-DISABLE-CLR) condition occurs when the administrator clears the disable flag on a user account.

This transient condition does not result in a standing condition.

ADMIN-LOCKOUT

The Admin Lockout of User (ADMIN-LOCKOUT) condition occurs when the administrator locks a user account.

This transient condition does not result in a standing condition.

ADMIN-LOCKOUT-CLR

The Admin Lockout Clear (ADMIN-LOCKOUT-CLR) condition occurs when the administrator unlocks a user account or when the lockout time expires.

This transient condition does not result in a standing condition.

ADMIN-LOGOUT

The Admin Logout of User (ADMIN-LOGOUT) condition occurs when the administrator logs off a user session.

This transient condition does not result in a standing condition.

ADMIN-SUSPEND

The Suspend User (ADMIN-SUSPEND) condition occurs when the password for a user account expires.

This transient condition does not result in a standing condition.

ADMIN-SUSPEND-CLR

The Suspend User Clear (ADMIN-SUSPEND-CLR) condition occurs when the user or administrator changes the password.

This transient condition does not result in a standing condition.

AUD-ARCHIVE-FAIL

The Archive of Audit Log Failed (AUD-ARCHIVE-FAIL) condition occurs when the software fails to archive the audit log. The condition normally occurs when the user refers to an FTP server that does not exist, or uses an invalid login while trying to archive. The user must log in again with correct user name, password, and FTP server details.

This transient condition does not lead to a standing condition.

AUD-LOG-LOW

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: NE

The Audit Trail Log Low condition occurs when the audit trail log is 80 percent full.

LOGIN-FAIL-LOCKOUT

The Invalid Login Locked Out (LOGIN-FAIL-LOCKOUT) condition occurs when you attempt to log into a locked account.

This transient condition does not result in a standing condition.

LOGIN-FAIL-ONALRDY

The Invalid Login Already Logged On (LOGIN-FAIL-ONALRDY) condition occurs when a user attempts to log in to a node where the user already has an existing session and a Single-User-Per-Node (SUPN) policy exists.

This transient condition does not result in a standing condition.

LOGIN-FAILURE-PSWD

The Invalid Login Password (LOGIN-FAILURE-PSWD) condition occurs when you attempt to log in with an invalid password.

This transient condition does not result in a standing condition.

LOGIN-FAILURE-USERID

The Invalid Login Username (LOGIN-FAILURE-USERID) condition occurs when you attempt to log in with an invalid username. To log in, use a valid username.

This transient condition is equivalent to a security warning. You must check the security log (audit log) for other security-related actions that have occurred.

LOGOUT-IDLE-USER

The Automatic Logout of Idle User (LOGOUT-IDLE-USER) condition occurs when a user session remains inactive for a certain period of time. When the idle timeout expires, the user session ends and requires the user to log in again.

PSWD-CHG-REQUIRED

The Password Change Required condition occurs when the user password needs to be changed.

This transient condition does not result in a standing condition.

ROLE-SWITCH-ACTIVE

The *Role is Switched to active* (ROLE-SWITCH-ACTIVE) condition occurs when the Cisco Optical Site Manager *Active* device fails and the *Standby* device takes over the active role.

USER-LOCKOUT

The User Locked Out (USER-LOCKOUT) condition occurs when an account is locked due to failed login attempts. The account can be unlocked by an administrator or when the lockout time expires.

USER-LOGIN

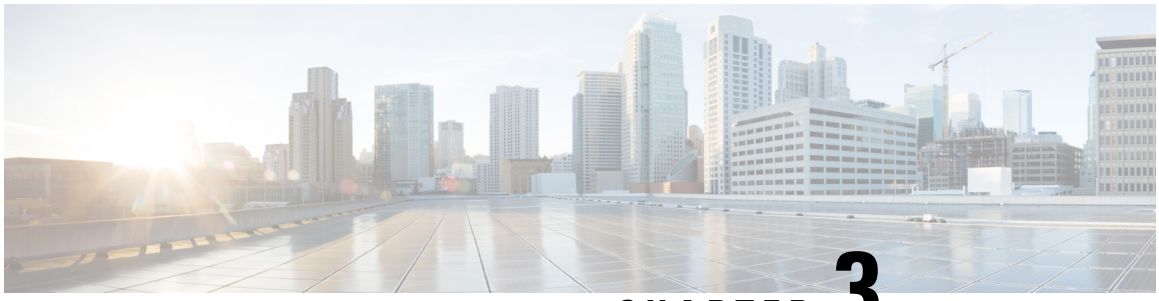
The Login of User (USER-LOGIN) occurs when you begin a new session by verifying your user ID and password.

This transient condition does not result in a standing condition.

USER-LOGOUT

The Logout of User (USER-LOGOUT) condition occurs when you stop a login session by logging out of your account.

This transient condition does not result in a standing condition.



CHAPTER 3

NCS 1000 Alarms Troubleshooting

This chapter describes the NCS 1000 devices alarms and their clearing procedures.

Alarm Troubleshooting

For information about NCS 1000 devices alarms and clearing procedures, see these guides:

- Troubleshooting Guide for Cisco NCS 1014
- Troubleshooting Guide for Cisco NCS 1010
- Troubleshooting Guide for Cisco NCS 1001