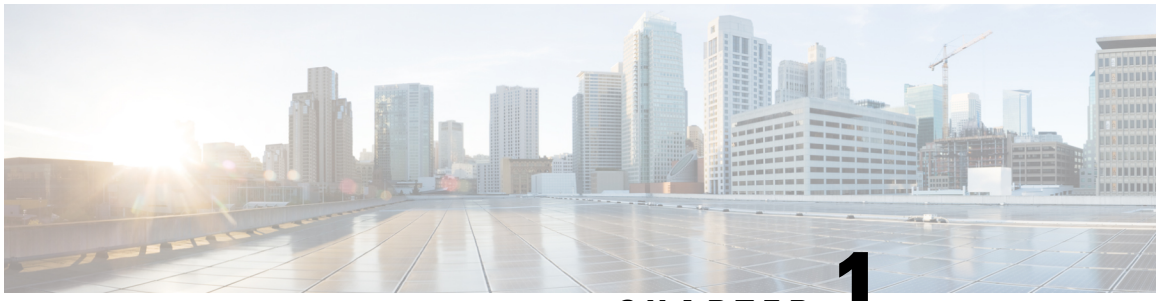


Troubleshooting Guide for Cisco Optical Site Manager, IOS XR Release 25.x.x

First Published: 2025-03-30

Last Modified: 2026-07-06

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.

- AUD-LOG-LOSS, on page 2
- CARLOSS, on page 2
- DBBACKUP-IN-PROGRESS, on page 3
- DBREST-IN-PROGRESS, on page 3
- DEGREE-MISMATCH, on page 3
- DISK-SPACE-FULL, on page 4
- DISK-SPACE-LOW, on page 5
- IMPROPRMVL, on page 5
- INTRUSION-PSWD, on page 6
- LOCAL-CERT-CHAIN-VERIFICATION-FAILED, on page 6
- LOCAL-CERT-EXPIRED, on page 7
- LOCAL-CERT-EXPIRING-WITHIN-30-DAYS, on page 7
- LOCAL-CERT-ISSUED-FOR-FUTURE-DATE, on page 7
- MEA, on page 8
- MEM-LOW, on page 9
- NE-DISCONNECTED, on page 9
- NE-EVENT-DISCONNECTED, on page 10
- NE-NOT-AUTH-ACCESS, on page 11
- NE-VER-NOT-SUPP, on page 12
- PROTNA, on page 13
- PROV-MISMATCH, on page 13
- RAMAN-CALIBRATION-FAILED, on page 14
- RAMAN-GAIN-NOT-REACHED, on page 15
- SNTP-HOST, on page 15
- SYSBOOT , on page 16
- UNTRUSTED-APPLICATION, on page 16
- USAGE-NOT-REPORTED, on page 16

AUD-LOG-LOSS

Default Severity: Warning, Non-Service-Affecting (NSA)

Resource Type: NE / System

The Audit Log 100 Percent Full - Oldest records will be lost (AUD-LOG-LOSS) alarm is triggered whenever the audit log reaches full capacity and older records are overwritten.

Clear the AUD-LOG-LOSS Alarm

Procedure

The alarm is cleared once log space is reclaimed and log rotation or archival is functioning correctly.

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

CARLOSS

Default Severity:

Major (MJ), Service-Affecting (SA)

Minor (MN), Non-Service-Affecting (NSA)

Resource Type: ETHLAN

The CARLOSS alarm is triggered whenever carrier is lost on the LAN interface. When managing NCS 1000 devices, if the management interfaces are down, this condition can also trigger the CARLOSS alarm. This behavior is based on syslog reports observed on Cisco IOS XR systems, indicating loss of carrier due to management interface outages.

Clear the CARLOSS Alarm

Procedure

The alarm is cleared once physical connectivity and interface status are restored.

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

DBBACKUP-IN-PROGRESS

Default Severity: Warning, Non-Service-Affecting (NSA)

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).

DBREST-IN-PROGRESS

Default Severity: Warning, Non-Service-Affecting (NSA)

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).

DEGREE-MISMATCH

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

Resource Type: OPT

The DEGREE-MISMATCH alarm checks fiber connections by comparing the configured "Expected" remote details with the "Actual" telemetry data. If there is any discrepancy, an alarm is triggered to ensure connectivity.

Clear the DEGREE-MISMATCH Alarm

Procedure

The alarm indicates that the device is not connected to the correct neighbor node. Verify the span connected to the LINE of the device in alarm. Once the device is connected correctly, the alarm will automatically clear within five minutes, provided the telemetry data aligns with the configuration.

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

DISK-SPACE-FULL

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

Resource Type: SYSTEM

The No Space Left On Device (DISK-SPACE-FULL) alarm is triggered when the Cisco Optical Site Manager specific disk quota is exceeded. This serves as a preventive measure and does not necessarily indicate that the physical disk has reached its maximum capacity.

Clear the DISK-SPACE-FULL Alarm

The default size is 6,500,000 Kb. The alarm clears automatically once sufficient disk space is reclaimed or the quota is adjusted.

Follow these steps to clear the alarm:

Procedure

Step 1 Remove large diagnostic files or core dumps from the active Cisco Optical Site Manager node to free up space.

Step 2 If additional space is required, update the disk quota by setting the configuration leaf:
`/cisco-opt-dev/server-resources/disk-monitoring/max-disc-size <value>`

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). Provide the logs collected in Step 1 to Cisco TAC.

DISK-SPACE-LOW

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

Resource Type: SYSTEM / CARD

The Low Disk Space Remaining On Device (DISK-SPACE-LOW) alarm is triggered when the disk occupation reaches a specific threshold, raising attention to potential space issues on both devices and Cisco Optical Site Manager container disk occupation.

Alarm severity increases with disk usage. Default XR thresholds are 80% (Minor), 95% (Severe), and 99% (Critical) for disk utilization.

Clear the DISK-SPACE-LOW Alarm

The alarm will automatically clear if the disk space usage falls below the threshold.

Follow these steps to clear the alarm:

Procedure

Step 1 Remove large diagnostic files or core dumps from the devices to free up storage.

Step 2 Examine the directory and delete any large files.

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

IMPROPRMVL

Default Severity:

Critical (CR), Service-Affecting (SA)

Minor (MN), Non-Service-Affecting (NSA)

Resource Type: CARD/ PPM/ PORT/ SHELF/ PASSIVE_UNIT/ FAN_TRAY/ PWR

The Improper Removal (IMPROPRMVL) alarm is triggered whenever a hardware unit is removed improperly.

Clear the IMPROPRMVL Alarm

Procedure

The alarm is cleared once the removed hardware is correctly reseated or replaced.

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

INTRUSION-PSWD

Default Severity: Warning, Non-Service-Affecting (NSA)

Resource Type: NE / SYSTEM

The Security Intrusion Attempt Detected - See Audit Log (INTRUSION-PSWD) alarm is triggered whenever a suspicious password-based intrusion attempt is detected.

Clear the INTRUSION-PSWD Alarm

Procedure

The alarm is cleared once the access policy is corrected and no further intrusion attempts are detected.

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

LOCAL-CERT-CHAIN-VERIFICATION-FAILED

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

Resource Type: SYSTEM

The Local cert chain verification failed (LOCAL-CERT-CHAIN-VERIFICATION-FAILED) alarm is triggered whenever local certificate chain verification fails.

Clear the LOCAL-CERT-CHAIN-VERIFICATION-FAILED Alarm

Procedure

The alarm is cleared once a valid certificate chain is installed and verified.

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

LOCAL-CERT-EXPIRED

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

Resource Type: SYSTEM

The Local certificate expired (LOCAL-CERT-EXPIRED) alarm is triggered whenever a local certificate expires.

Clear the LOCAL-CERT-EXPIRED Alarm

Procedure

The alarm is cleared once the expired certificate is renewed and activated.

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

LOCAL-CERT-EXPIRING-WITHIN-30-DAYS

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

Resource Type: SYSTEM

The Local cert expiring within 30 days (LOCAL-CERT-EXPIRING-WITHIN-30-DAYS) alarm is triggered whenever a local certificate is within 30 days of expiration.

Clear the LOCAL-CERT-EXPIRING-WITHIN-30-DAYS Alarm

Procedure

The alarm is cleared once the certificate is renewed before expiry.

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

LOCAL-CERT-ISSUED-FOR-FUTURE-DATE

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

Resource Type: SYSTEM

The Local cert issued for future date (LOCAL-CERT-ISSUED-FOR-FUTURE-DATE) alarm is triggered whenever a local certificate has a future-dated validity start time.

Clear the LOCAL-CERT-ISSUED-FOR-FUTURE-DATE Alarm

Procedure

The alarm is cleared once system time and certificate validity dates are corrected.

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

MEA

Default Severity:

Critical(CR), Service-Affecting (SA)

Minor (MN), Non-Service-Affecting (NSA)

Resource Type: FAN_TRAY/ CARD/ PPM/ PASSIVE_UNIT/ SHELF/ NE/ PASSIVE_SHELF/ PORT

Default Severity:

Minor (MN), Non-Service-Affecting (NSA)

Resource Type:

SHELF/ NE/ PASSIVE_SHELF/ PORT

The Mismatch Of Equipment And Attributes (MEA) alarm is triggered whenever equipment type or attribute values do not match expected inventory data.

Clear the MEA Alarm

Procedure

The alarm is cleared once inventory and equipment attributes match the expected values.

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

MEM-LOW

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

Resource Type: CARD/ SYSTEM

The MEM-LOW alarm is activated when the active containers in the Cisco Optical Site Manager have low Docker RAM availability, surpassing the threshold of 90%.

Clear the MEM-LOW Alarm

The alarm is cleared when memory utilization returns to the normal operating range. The MEM_LOW threshold is set at 90% of RAM usage.

Follow these steps to clear the alarm:

Procedure

Run the `docker stats` command to gather and review docker statistics, including RSS (Resident Set Size) for Java and `ncs.smp`, to address sizing and high memory usage.

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). Provide the logs collected in Step 1 to Cisco TAC.

NE-DISCONNECTED

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

Resource Type: NE

The Connection To Managed NE Lost (NE-DISCONNECTED) alarm is triggered whenever the connection to a managed network element is lost. It takes up to 2 minutes or less for the NE-DISCONNECTED alarm to be raised after the connection loss is detected.

Clear the NE-DISCONNECTED Alarm

Procedure

Step 1 Determine why connectivity to the device is lost. Check if the issue is due to a network problem or if the device itself is unstable or unreachable.

Step 2 The NE-DISCONNECTED alarm is cleared automatically once connectivity to the managed network element is restored.

Step 3 Restart the relevant management application or service and verify network connectivity and device stability.

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

NE-EVENT-DISCONNECTED

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

Resource Type: NE

The Event Channel To Managed NE Lost (NE-EVENT-DISCONNECTED) alarm is triggered whenever the event channel from a managed network element is lost. The event channel refers to the communication path through which COSM receives telemetry or syslog updates from the device. If COSM is unable to receive these automatic updates, this alarm is raised.

In this scenario, it should still be possible to reach the device and perform configuration changes manually. However, automatic updates from the device will not be reflected in COSM until this alarm is cleared.

This list provides the condition / additional text and meaning / potential cause for the NE-EVENT-DISCONNECTED alarm conditions:

- **Addresses config is not correct:** The required COSM IP address or port registration is missing from the device configuration.
- **Telemetry configuration is wrong:** The destination, sensor, or subscription settings on the device are incorrectly configured.
- **Telemetry not received:** Data is not reaching COSM due to potential network connectivity issues or incorrect device configuration.
- **No manager registered:** No COSM manager is currently configured to receive data from the device.
- **Other manager registered:** Unexpected or unauthorized COSM managers have been detected on the device.
- **Communication failure:** The device is either locked or currently unreachable by the COSM application.

Clear the NE-EVENT-DISCONNECTED Alarm

Procedure

The alarm is cleared once the event channel to the managed network element is restored. This involves ensuring that the syslog and telemetry processes on the device are functioning correctly.

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

NE-NOT-AUTH-ACCESS

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

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).

NE-VER-NOT-SUPP

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

Resource Type: NE

The Not Supported Version Of Managed NE (NE-VER-NOT-SUPP) alarm is triggered whenever a managed network element runs an unsupported software version.

Note NE-VER-NOT-SUPP alarm is supported only on NCS 2000 devices.

Clear the NE-VER-NOT-SUPP Alarm

Procedure

The alarm is cleared once the managed network element is upgraded or aligned to a supported version.

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

PROTNA

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

Resource Type: CARD / SYSTEM

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).

PROV-MISMATCH

Default Severity:

Major (MJ), Service-Affecting (SA) , Minor (MN), Non-Service-Affecting (NSA), Resource Type: PORT

Minor (MN), Non-Service-Affecting (NSA), Resource Type: CARD / PPM

The Provisioning Mismatch (PROV-MISMATCH) alarm is triggered whenever provisioning values do not match expected configuration.

Clear the PROV-MISMATCH Alarm

Procedure

The alarm is cleared once provisioning values are corrected and synchronized.

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

RAMAN-CALIBRATION-FAILED

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

Resource Type: RAMAN_AMPLIFIER

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 Raman Calibration fails when Raman tuning turns off the Raman pumps and enters a blocked state due to high Raman back reflection (BR). 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

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.

Step 2 To clear the high BR, reconnect the fiber. Once the BR reaches acceptable levels, the system will automatically trigger Raman tuning and activate the Raman pumps, which will clear the alarm. If the alarm is raised due to peer node reachability issues, ensure that the neighbors are established. Raman tuning will then start automatically and complete the calibration process.

Step 3 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).

RAMAN-GAIN-NOT-REACHED

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

Logical Object: Raman amplifier (NearEnd)

Resource Type: RAMAN_AMPLIFIER

The Raman Gain Not Reached (RAMAN-GAIN-NOT-REACHED) alarm is triggered whenever the Raman amplifier cannot reach the configured gain.

Clear the RAMAN-GAIN-NOT-REACHED Alarm

Procedure

The alarm is cleared once the configured Raman gain is achieved.

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

SNTP-HOST

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

Resource Type: NE / CARD / SYSTEM

The NTP/SNTP Host Failure (SNTP-HOST) alarm is triggered whenever the configured NTP/SNTP host is unreachable or not responding.

Note The SNTP-HOST alarm is applicable only to NCS 2000 SVO installations.

Clear the SNTP-HOST Alarm

Procedure

The alarm is cleared once time synchronization with a reachable NTP/SNTP host succeeds.

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

SYSBOOT

Default Severity:

Major (MJ), Service-Affecting (SA)

Minor (MN), Non-Service-Affecting (NSA)

The COSM application restarts when the system object, or Sysboot, is triggered. This can occur automatically or as a result of a user action.

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.

UNTRUSTED-APPLICATION

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

Resource Type: SYSTEM

The *Trust Not Established With CSLU/CSSM* (UNTRUSTED-APPLICATION) alarm is triggered when Smart License is configured in the *Smart Transport* or *CSLU* or *Offline* 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)

Resource Type: 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 Cisco Smart Licensing Utility (CSLU).

Clear the USAGE-NOT-REPORTED Alarm

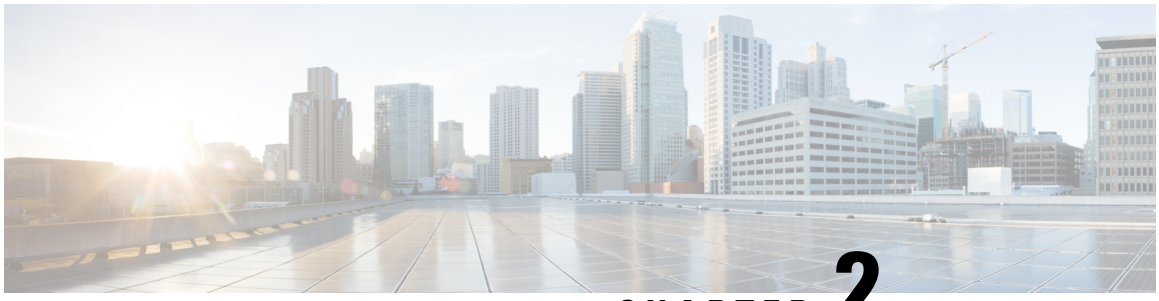
To clear the alarm:

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, on page 19
- ADMIN-DISABLE-CLR, on page 20
- ADMIN-LOCKOUT, on page 20
- ADMIN-LOCKOUT-CLR, on page 20
- ADMIN-LOGOUT, on page 20
- ADMIN-SUSPEND , on page 20
- ADMIN-SUSPEND-CLR, on page 20
- AUD-ARCHIVE-FAIL, on page 21
- DBBACKUP-FAIL, on page 21
- DBRESTORE-FAIL, on page 21
- INTRUSION, on page 21
- INTRUSION-USERID, on page 21
- LOGIN-FAIL-LOCKOUT, on page 21
- LOGIN-FAIL-ONALRDY, on page 22
- LOGIN-FAILURE-PSWD, on page 22
- LOGIN-FAILURE-USERID, on page 22
- LOGIN-MISSING-GROUP, on page 22
- LOGOUT-IDLE-USER, on page 22
- NE-CONFIG-INCONSISTENT, on page 22
- PSWD-CHG-REQUIRED, on page 23
- ROLE-SWITCH-ACTIVE, on page 23
- USER-LOCKOUT, on page 23
- USER-LOGIN, on page 23
- USER-LOGOUT, on page 23

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.

DBBACKUP-FAIL

The Database Backup Failed (DBBACKUP-FAIL) condition occurs when the system fails to back up the database after initiating the backup command.

This condition can occur due to network or server issues. Repeat the operation and check if it succeeds. If it fails again, contact the Cisco Technical Assistance Center (TAC) (1 800 553-2447).

DBRESTORE-FAIL

The Database Restore Failed (DBRESTORE-FAIL) condition occurs when the system fails to restore the backed up database after initiating the restore command.

This condition can be due to server or network issues. If the condition is caused by a network element (NE) failure, contact the Cisco Technical Assistance Center (TAC) (1 800 553-2447) for assistance.

INTRUSION

The Security: Invalid Login Username - See Audit Trail (INTRUSION) condition occurs when a login attempt uses a username not present in the system database. Check the audit trail for related security events.

This transient condition does not result in a standing condition.

INTRUSION-USERID

The Security Intrusion Attempt Detected - See Audit Log (INTRUSION-USERID) condition occurs when multiple unsuccessful login attempts with invalid user IDs trigger a security event. Check the audit log for details.

This transient condition does not result in a standing condition.

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.

LOGIN-MISSING-GROUP

The LOGIN-MISSING-GROUP condition arises when the External Authentication Server fails to supply a valid Authorization Group, potentially impacting user access permissions.

This transient condition does not result in a standing condition.

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.

NE-CONFIG-INCONSISTENT

The Device has the Config Blocked due to an Inconsistency (NE-CONFIG-INCONSISTENT) condition occurs when the device configuration is blocked because of a failure to restore or synchronize configuration, preventing commits until cleared by a specific command. This alarm indicates configuration inconsistency requiring resolution to proceed with changes.

This transient condition does not result in a standing condition.

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.

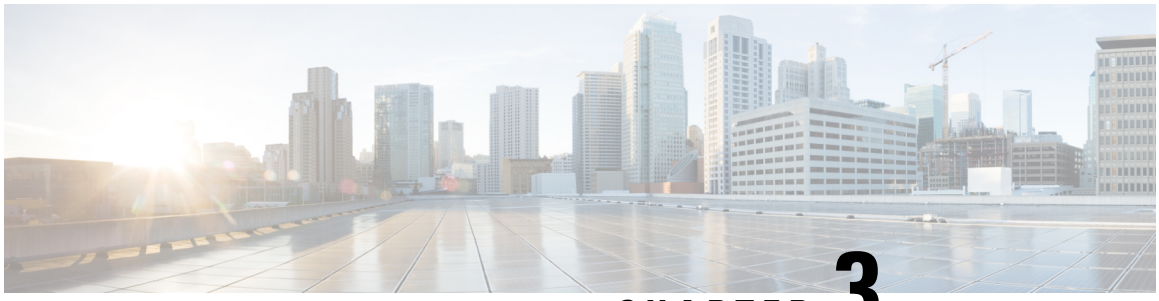
This transient condition does not result in a standing condition.

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.

USER-LOGOUT



CHAPTER 3

NCS 1000 Alarms Troubleshooting

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

- Alarm Troubleshooting, on page 25

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