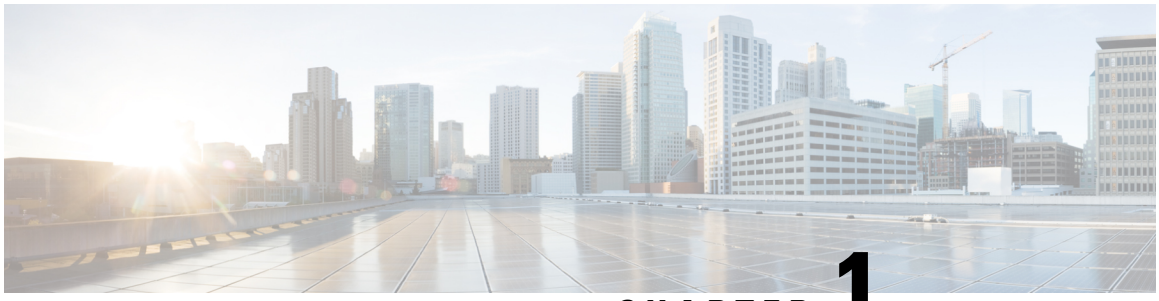
# Troubleshooting Guide for Cisco Optical Site Manager, IOS XR Releases 7.11.x, 24.1.x, and 24.2.x

**First Published:** 2024-06-14

**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.


- NE-NOT-AUTH-ACCESS, on page 1
- INTRUSION-PSWD , on page 1
- MEM-LOW , on page 2
- SYSBOOT , on page 2
- NE-VER-NOT-SUPP, on page 3
- RAMAN-CALIBRATION-FAILED, on page 3


# NE-NOT-AUTH-ACCESS

Default Severity: Major (MJ)

Logical Object: Standing

Resource Type: NE

The NE-NOT-AUTH-ACCESS alarm is raised when incorrect credentials are used to access the device.

## Clear the NE-NOT-AUTH-ACCESS Alarm

The alarm clears when the device is accessed using the correct credentials.

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).

# INTRUSION-PSWD

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

Logical Object: NE

The Security Intrusion Incorrect Password condition occurs after a user attempts a provisionable (by Superuser) number of unsuccessful logins, a login with an expired password, or an invalid password. The alarmed user is locked out of the system, and INTRUSION-PSWD condition is raised. This condition is only shown in Superuser login sessions, not in login sessions for lower-level users. The INTRUSION-PSWD condition is automatically cleared when a provisionable lockout timeout expires, or it can be manually cleared in CTC by the Superuser if the lockout is permanent.

## Clear the INTRUSION-PSWD Condition

**Step 1** Log in as a user ID with superuser rights. (For more information about this, refer to the .)

**Step 2** In node view (single-shelf mode) or multishelf view (multishelf mode), click the .

**Step 3** Click **Clear Security Intrusion Alarm**.

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).

# MEM-LOW

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

Logical Object: EQPT

The Free Memory of Card Almost Gone alarm occurs when data generated by software operations is close to exceeding the memory capacity of the control cards. The alarm clears when additional memory becomes available. If additional memory is not made available and the memory capacity of the card is exceeded, the user interface ceases to function.

The alarm does not require user intervention.

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).

# 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.

# NE-VER-NOT-SUPP

Default Severity: Major (MJ)

Logical Object: NE

Resource Type: NE

The NE-VER-NOT-SUPP alarm is raised when the managed NE version is not supported.

## Clear the NE-VER-NOT-SUPP Alarm

Upgrade the device with a supported version.

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).

# 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.

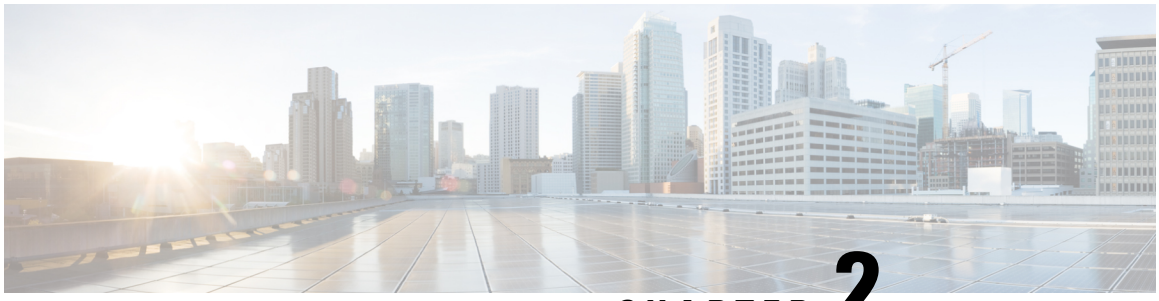
2. If the alarm is caused by a set-up problem, re-verify all node installation steps and manually trigger a Raman Calibration.

## DETAILED STEPS

**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).



CHAPTER 2

# Transient Conditions

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


- ADMIN-DISABLE, on page 5
- ADMIN-DISABLE-CLR, on page 5
- ADMIN-LOCKOUT, on page 6
- ADMIN-LOCKOUT-CLR, on page 6
- ADMIN-LOGOUT, on page 6
- ADMIN-SUSPEND , on page 6
- ADMIN-SUSPEND-CLR, on page 6
- AUD-ARCHIVE-FAIL, on page 6
- AUD-LOG-LOW, on page 7
- LOGIN-FAIL-LOCKOUT, on page 7
- LOGIN-FAIL-ONALRDY, on page 7
- LOGIN-FAILURE-PSWD, on page 7
- LOGIN-FAILURE-USERID, on page 7
- LOGOUT-IDLE-USER, on page 7
- PSWD-CHG-REQUIRED, on page 8
- USER-LOCKOUT, on page 8
- USER-LOGIN, on page 8
- USER-LOGOUT, on page 8


## 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.

# 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.