

Transient Conditions

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

- ADMIN-DISABLE, on page 1
- ADMIN-DISABLE-CLR, on page 2
- ADMIN-LOCKOUT, on page 2
- ADMIN-LOCKOUT-CLR, on page 2
- ADMIN-LOGOUT, on page 2
- ADMIN-SUSPEND , on page 2
- ADMIN-SUSPEND-CLR, on page 2
- AUD-ARCHIVE-FAIL, on page 3
- DBBACKUP-FAIL, on page 3
- DBRESTORE-FAIL, on page 3
- INTRUSION, on page 3
- INTRUSION-USERID, on page 3
- LOGIN-FAIL-LOCKOUT, on page 3
- LOGIN-FAIL-ONALRDY, on page 4
- LOGIN-FAILURE-PSWD, on page 4
- LOGIN-FAILURE-USERID, on page 4
- LOGIN-MISSING-GROUP, on page 4
- LOGOUT-IDLE-USER, on page 4
- NE-CONFIG-INCONSISTENT, on page 4
- PSWD-CHG-REQUIRED, on page 5
- ROLE-SWITCH-ACTIVE, on page 5
- USER-LOCKOUT, on page 5
- USER-LOGIN, on page 5
- USER-LOGOUT, on page 5

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