Troubleshooting Tips and FAQs

This appendix covers the Troubleshooting tips and FAQs for:

- Configuration Archive
- NetConfig
- Config Editor
- Software Management
- Job Approval
- cwcli config
- cwcli export
- VRF Lite

For Installation related FAQs and Troubleshooting tips, see the Installing and Migrating to CiscoWorks LAN Management Solution 4.1.

Configuration Archive

This section provides the troubleshooting information and FAQs for Configuration Archive:

- Configuration Archive FAQs
- Troubleshooting Configuration Archive

This section contains:

- Login Authentication in Telnet Mode
- Login Authentication in SSH Mode
- Enable Login Authentication in Telnet Mode
- Enable Login Authentication in SSH Mode
Configuration Archive FAQs

- Q. Can I define the protocol order for configuration fetch and deploy?
- Why does the Telnet session appear in the data capture trace although I have selected TFTP as the configuration transport protocol?
- Q. How Configuration Management interprets device credentials?
- Q. What are the supported device prompts?

Q. Can I define the protocol order for configuration fetch and deploy?

A. Yes, you can define the order of protocol that has to be used for Configuration Management applications (Configuration Archive, Config Editor, and NetConfig). You can define this in the Transport Settings window (Admin > Collection Settings > Config > Config Transport Settings).

Q. When I select:
- a. TFTP alone as the configuration transport protocol
- b. Run Sync Archive Job for a device
- c. Run a data capture trace

The data capture trace shows Telnet traffic along with SNMP/TFTP sessions.

Why does the Telnet session appear in the data capture trace although I have selected TFTP as the configuration transport protocol?

Q. The Telnet session that appears in the data capture trace is a socket connection to the Telnet port. It identifies the IP address of the CiscoWorks LMS server. This is important in multi-homed servers where the IP address that CiscoWorks server uses to contact the device, has to be identified.

Q. How Configuration Management interprets device credentials?

A. You can enter the device credentials when you,

- Add/import devices using the LMS Device Management option (Inventory > Device Administration > Add / Import / Manage Devices). In this flow, you can enter:
  - Primary Username—User name for the device.
  - Primary Password—Password for the device.
  - Primary Enable Password—Console-enabled password for the device.

- If you have enabled Enable Job Password option (Admin > Network > Configuration Job Settings > Config Job Policies) then while scheduling for a job, you can enter these credentials:
  - Login User name—User name for the device.
  - Login Password—Password for the device.
  - Enable Password—Console-enabled password for the device.

These credentials are used while running the job. The credentials that you have entered in the Device and Credential Repository are ignored while running the job.

TACACS (Terminal Access Controller Access Control System) uses a separate centralized server to track usernames and passwords. This simplifies authentication and authorization, because information is maintained in only one database rather than being spread out over many devices.

If your devices are configured to use TACACS, you must provide TACACS device credentials when you add or import the devices.
Login Authentication in Telnet Mode

When LMS logs into non-privileged mode (User mode), depending on your device authentication configuration, the device will prompt for either username and password, or password only.

If the device prompts for username and password, LMS responds with the following:

- If Primary Username and Primary Password credentials are entered in the Device and Credential Repository, LMS sends Primary Username and Primary Password to the device.

  If you have enabled Enable Job Password option in the Job Policy dialog box (Admin > Network > Configuration Job Settings > Config Job Policies) and if you have entered the Login Password at the time of scheduling a job, LMS sends the Login Password entered in this dialog box. The Primary Password entered in the Device and Credential Repository (Inventory > Device Administration > Add / Import / Manage Devices) is ignored.

- If:
  - Authentication fails with the Primary credentials or Login User name and Login Password
  - The Primary credentials or Login User name and Login Password are not present in the database.

  LMS reports the login as failure.

If the device prompts for password only, LMS responds with the following:

- If Primary Password is entered in the database, LMS sends Primary Password to the device.

  If you have enabled Enable Job Password option in the Job Policy dialog box (Admin > Network > Configuration Job Settings > Config Job Policies) and if you have entered the Login Password at the time of scheduling a job, LMS sends the Login Password entered in this dialog box. The Primary Password entered in the Device and Credential Repository (Inventory > Device Administration > Add / Import / Manage Devices) is ignored.

  If you have configured only the Telnet password (without configuring username) on your device. You have to enter a string in the Login Username field. That is, you cannot leave the Login Username field blank.

  The Login Username string will be ignored while connecting to the device as the device is configured only for the Telnet password.

- If:
  - Authentication fails with the Primary Password or Login Password
  - The Primary Password or Login Password is not present in the database.

  LMS reports the login as failure.

Login Authentication in SSH Mode

This section describes how the device credentials are interpreted by LMS in SSH mode.

Open an SSH session to the device.

The device prompts for username and password, LMS responds with the following:

- If Primary Username and Primary Password are entered in the database, LMS sends Primary Username and Primary Password to the device.
If you have enabled Enable Job Password option in the Job Policy dialog box (Admin > Network > Configuration Job Settings > Config Job Policies) and if you have entered the Login Password at the time of scheduling a job, LMS sends the Login Password entered in this dialog box. The Primary Password entered in the Device and Credential Repository (Inventory > Device Administration > Add / Import / Manage Devices) is ignored.

- If:
  - Authentication fails with the Primary credentials or Login User name and Login Password
  Or
  - The Primary credentials or Login User name and Login Password are not present in the database
  LMS reports the login as failure.

**Enable Login Authentication in Telnet Mode**

This section describes how the TACACS and other credentials are interpreted by LMS in Telnet mode. Logging into the Privileged mode (Enable mode) involves two steps:

1. LMS logs into non-privileged mode (See Login Authentication in Telnet Mode).
2. If logging into non-privileged mode is successful, LMS issues “enable” command for the device to enter into privileged mode.
   
   If the device prompts for password, LMS responds with the following:
   - If Primary Enable password is entered in the database, LMS sends Enable Primary password to the device.
   
   If you have enabled Enable Job Password option in the Job Policy dialog box (Admin > Network > Configuration Job Settings > Config Job Policies) and if you have entered the Login Password at the time of scheduling a job, LMS sends the Login Password entered in this dialog box. The Primary Password entered in the Device and Credential Repository (Inventory > Device Administration > Add / Import / Manage Devices) is ignored.
   - If authentication fails or Enable Password or Primary Enable Password is not present in database
   or
   - If logging into non-privileged mode fails or authentication fails in all above cases.
   LMS reports the login as failure.

**Enable Login Authentication in SSH Mode**

This section describes how the TACACS and other credentials are interpreted by LMS in SSH mode. Logging into the Privileged mode (Enable mode) involves two steps:

1. LMS logs into non-privileged mode (See Login Authentication in SSH Mode).
2. If logging into non-privileged mode is successful, LMS issues the `enable` command for the device to enter into privileged mode.
   
   If the device prompts for password, LMS responds with the following:
   - If Primary Enable Password is entered in the database, LMS sends Primary Enable password to the device.
If you have enabled Enable Job Password option in the Job Policy dialog box (Admin > Network > Configuration Job Settings > Config Job Policies) and if you have entered the Login Password at the time of scheduling a job, LMS sends the Login Password entered in this dialog box. The Primary Password entered in the Device and Credential Repository (Inventory > Device Administration > Add / Import / Manage Devices) is ignored.

- If authentication fails or Enable Password or Primary Enable Password is not present in database
  or
- If logging into non-privileged mode fails or authentication fails in all above cases.
  LMS reports the login as failure.

Q. What are the supported device prompts?

A. The supported device prompts are:

The supported Device authentication prompts are:

- **Routers**
  
  “Username:”, “Username:”
  
  “Password:”, “Password:”

- **Switches**
  
  “username:”, “Username:”
  
  “password:”, “Password:”

- **Cisco Interfaces and Modules — Network Analysis Modules**
  
  “login:”
  
  “Password:” “password:”

- **Security and VPN — PIX**
  
  “username:”, “Username:”
  
  “passwd:”, “password:”, “Password:”

- **Content Networking—Content Service Switch**
  
  “Username:”, ”username:”, “login:”, ”username:”, “Username:”, “login:”
  
  “Password:”, “password:”, ”password:”, ”Password:”, “password:”, ”passwd:”

- **Content Networking — Content Engine**
  
  “Username:”, ”login:”
  
  “Password:”

- **Storage Networking — MDS Devices**
  
  “Username:”, “Username:”
  
  “Password:”, “Password:”
## Troubleshooting Configuration Archive

<table>
<thead>
<tr>
<th>Message ID</th>
<th>Error Message</th>
<th>Probable Cause</th>
<th>Possible Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>CM0003</td>
<td>Version $1 does not exist in archive $2</td>
<td>Version may have been deleted</td>
<td>None</td>
</tr>
<tr>
<td>CM0005</td>
<td>Archive does not exist for $1</td>
<td>Error during archive creation.</td>
<td>Check the file system/user privileges.</td>
</tr>
<tr>
<td>CM0006</td>
<td>Archives do not exist</td>
<td>Error during archive creation.</td>
<td>Check the file system/user privileges.</td>
</tr>
<tr>
<td>CM0008</td>
<td>Checkout not permitted on archive $1</td>
<td>You may not have the required permission</td>
<td>Check with the administrator for your privilege.</td>
</tr>
<tr>
<td>CM0010</td>
<td>Checkin not permitted on archive $1</td>
<td>You may not have the required permission</td>
<td>Check with the administrator for your privilege.</td>
</tr>
<tr>
<td>CM0011</td>
<td>Delete not permitted</td>
<td>You may not have the required permission</td>
<td>Check with the administrator for your privilege.</td>
</tr>
<tr>
<td>CM0012</td>
<td>Could not create new version on archive $1</td>
<td>Insufficient disk space or config file may be incomplete.</td>
<td>Check whether disk space is available and that the directory has required permissions</td>
</tr>
<tr>
<td>CM0013</td>
<td>Cannot delete version on archive $1</td>
<td>You may not have the required permission</td>
<td>Check with the administrator for your privilege.</td>
</tr>
<tr>
<td>CM0015</td>
<td>Could not check out config for archive $1</td>
<td>You may not have the required permission</td>
<td>Check with the administrator for your privilege.</td>
</tr>
<tr>
<td>CM0016</td>
<td>Could not undo check out config for archive $1</td>
<td>You may not have the required permission</td>
<td>Check with the administrator for your privilege.</td>
</tr>
<tr>
<td>CM0017</td>
<td>Could not check in config for archive $1</td>
<td>$2</td>
<td>Check whether the file system is full and if you have required permissions</td>
</tr>
<tr>
<td>CM0021</td>
<td>Version does not exist in archive $1</td>
<td>Version may have been deleted</td>
<td>None</td>
</tr>
<tr>
<td>CM0022</td>
<td>Archive already exists</td>
<td>Archive names should be unique</td>
<td>Enter a different name</td>
</tr>
<tr>
<td>CM0023</td>
<td>Archive creation not permitted</td>
<td>You may not have the required permission</td>
<td>Check with the administrator for your privilege.</td>
</tr>
<tr>
<td>CM0024</td>
<td>Error while deleting archive</td>
<td>You may not have the required permission</td>
<td>Check with the administrator for your privilege.</td>
</tr>
<tr>
<td>CM0025</td>
<td>Cannot delete device archive</td>
<td>Only the system purge can delete the device archive</td>
<td>Schedule for a purge job.</td>
</tr>
</tbody>
</table>
| CM0026      | Archive Relocation failed                                          | The destination folder may not have the required disk space or required permission. | • Check if the destination folder has the required permission  
• Check if the disk space is available  
• Check if the user has the write permission. |
<p>| CM0034      | Cannot list versions for $1                                        | You may not have the required permission or version do not exist. | Check with the administrator for your privilege.         |
| CM0037      | Database Connection Error                                          | Database Engine may be down                              | Restart the RMEDbMonitor and CmfDbMonitor services        |</p>
<table>
<thead>
<tr>
<th>Message ID</th>
<th>Error Message</th>
<th>Probable Cause</th>
<th>Possible Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>CM0038</td>
<td>Error in Database</td>
<td>Database Engine may be down</td>
<td>Restart the RMEDbMonitor and CmfDbMonitor services</td>
</tr>
</tbody>
</table>
| CM0040     | Error while reading the file from the system | Either:  
- The file may not exist  
  Or  
- You may not have required permissions. | Verify whether you have the correct privileges and that the file system is not corrupted. |
| CM0041     | Error while writing the file to the system | Either:  
- The file may not exist  
  Or  
- You may not have required permissions. | Verify whether you have the correct privileges and that the file system is not full |
| CM0043     | Error while copying the file | Either:  
- The source or destination file may not exist  
  Or  
- You may not have required permissions. | Verify whether:  
- The files exist  
- The file system is not full.  
- You have permission |
| CM0050     | Cannot compare the configurations since they are not of the same type. | Configuration types are different | Select device of the same type. |
| CM0051     | Cannot connect to ConfigMgmtServer process | Process may be down or maximum connection have been reached. | Restart the ConfigMgmtServer process. |
| CM0054     | Error while initializing Transport for $1 | Device packages may not exist. | Check whether:  
- The user exists in LMS and has required permissions,  
- Device is reachable  
- Required device packages are available in LMS. |
<p>| CM0076     | Job creation failed | $1 | Check whether Jrm and CTMjrmServer processes are running |
| CM0077     | Job modification failed | $1 | Check whether Jrm and CTMjrmServer processes are running |
| CM0080     | Could not send e-mail. | The e-mail configuration in your profile may be either missing or incorrect | Check e-mail configuration. |
| CM0082     | Job execution failed. | The job policy may not be enabled | Enable the policy and try again |
| CM0085     | Cannot list jobs of type | Jobs of this type may not exist in LMS. | Enable the policy and try again. |</p>
<table>
<thead>
<tr>
<th>Message ID</th>
<th>Error Message</th>
<th>Probable Cause</th>
<th>Possible Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>CM0086</td>
<td>Cannot load job with id.</td>
<td>Job may not exist in LMS</td>
<td>Verify that the Job ID exists and try again</td>
</tr>
<tr>
<td>CM0087</td>
<td>Cannot obtain lock on device</td>
<td>Another application/job may have locked the device.</td>
<td>Verify that there are no other jobs running on the device. Retry the job after some time.</td>
</tr>
<tr>
<td>CM0088</td>
<td>Configuration archival failed for $1</td>
<td>Not enough disk space.</td>
<td>Check whether the device is reachable and that the credentials are correct.</td>
</tr>
<tr>
<td>CM0090</td>
<td>Reload task failed on device</td>
<td>Device many not be reachable.</td>
<td>Check whether the device is reachable and that the credentials are correct.</td>
</tr>
<tr>
<td>CM0096</td>
<td>Job ID is not valid</td>
<td>The job may not exist in LMS</td>
<td>Verify that the job exists and try again.</td>
</tr>
<tr>
<td>CM0097</td>
<td>No failed devices in the job</td>
<td>There may not be any failed devices in the job.</td>
<td>Check for failed devices and try again.</td>
</tr>
<tr>
<td>CM0098</td>
<td>Invalid Job-based password specified</td>
<td>The Job-based password data may be null or cannot be used.</td>
<td>Enter the correct Job-based password and try again.</td>
</tr>
<tr>
<td>CM0109</td>
<td>Cannot read admin preferences.</td>
<td>Application may not have been initialized correctly</td>
<td>Retry the task</td>
</tr>
<tr>
<td>CM0122</td>
<td>No commands to write.</td>
<td>Command may not be available</td>
<td>Verify whether there are any commands to deploy</td>
</tr>
<tr>
<td>CM0123</td>
<td>Exception while getting all baseline templates.</td>
<td>Templates may have been deleted</td>
<td>Check if the template exist.</td>
</tr>
<tr>
<td>CM0125</td>
<td>Cannot persist template.</td>
<td>Template may be empty or invalid.</td>
<td>Check whether the commands are valid</td>
</tr>
<tr>
<td>CM0126</td>
<td>Cannot find baseline archive $1</td>
<td>Archive may have been deleted</td>
<td>Check if the archive exist.</td>
</tr>
<tr>
<td>CM0128</td>
<td>Cannot get baseline branch.</td>
<td>Branch may not exist.</td>
<td>Check if the branch exist.</td>
</tr>
<tr>
<td>CM0131</td>
<td>Cannot find template</td>
<td>Template may have been deleted</td>
<td>Check if the template exist.</td>
</tr>
<tr>
<td>CM0132</td>
<td>Cannot find result for job</td>
<td>Job may not exist.</td>
<td>Check if the job has been deleted.</td>
</tr>
<tr>
<td>CM0133</td>
<td>Invalid check-type for command</td>
<td>Check type may be invalid</td>
<td>Verify if the check-type is valid.</td>
</tr>
<tr>
<td>CM0136</td>
<td>Regular expression match failed.</td>
<td>Not a valid Regular expression.</td>
<td>Check if the expression is valid.</td>
</tr>
<tr>
<td>CM0137</td>
<td>No commandlets.</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>CM0138</td>
<td>Cannot find result for device</td>
<td>Device has been deleted.</td>
<td>Check if the device exist.</td>
</tr>
<tr>
<td>CM0139</td>
<td>Could not archive configuration</td>
<td>File system may be full or user may not have the required permission.</td>
<td>Check whether device is reachable and device credentials are correct. Increase timeout value, if required.</td>
</tr>
<tr>
<td>CM0148</td>
<td>User or device authorization failed.</td>
<td>User may not exist or does not have privileges to operate on any or all of the devices in the job.</td>
<td>Check whether the user exists and has required privileges to execute jobs.</td>
</tr>
<tr>
<td>CM0201</td>
<td>Could not start the SdiEngine.</td>
<td>The package path may be incorrect.</td>
<td>Check whether the specified package path is correct.</td>
</tr>
</tbody>
</table>
This section provides the troubleshooting information and FAQs for NetConfig:

- **NetConfig FAQs**
- **Troubleshooting NetConfig**

### NetConfig FAQs

**Q. What are the supported protocols for NetConfig Reload task?**

**A.** The supported protocols for NetConfig Reload task are Telnet, SSH and TFTP. SSH and TFTP protocols are supported by NetConfig Reload task only if these protocols are also supported by the devices.
## Troubleshooting NetConfig

This section provides the troubleshooting information for the NetConfig application:

<table>
<thead>
<tr>
<th>Message ID</th>
<th>Error Message</th>
<th>Probable Cause</th>
<th>Possible Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>CFG0025</td>
<td>Cannot retry.</td>
<td>Retry is not supported on periodic jobs.</td>
<td>None.</td>
</tr>
<tr>
<td>CFG0026</td>
<td>You can retry only failed jobs.</td>
<td>A Successful job has been selected instead of a Failed job.</td>
<td>Select a Failed job and try again.</td>
</tr>
<tr>
<td>CFG0029</td>
<td>Job approval is enabled.</td>
<td>You have scheduled a job that requires Job approval with the Immediate schedule type. The job will run only when it has been approved by the Approver.</td>
<td>Do not select Immediate job type while scheduling the job.</td>
</tr>
<tr>
<td>CFG0009</td>
<td>Error occurred while processing.</td>
<td>Check netconfigclient.log for more details.</td>
<td>Retry the operation. If the problem persists, send the logs to Cisco Technical Assistance Center (TAC). The netconfig logs are available at this location: On Windows: NMSROOT\log\netconfigclient.log On Solaris and Soft Appliance: /var/adm/CSCOpx/log/netconfigclient.log</td>
</tr>
<tr>
<td>CFG0029</td>
<td>Job approval is enabled.</td>
<td>This job requires job approval. So it can run only when the job is approved. So you cannot schedule a job with immediate schedule type.</td>
<td>Do not select Immediate schedule type.</td>
</tr>
<tr>
<td>CFG0041</td>
<td>You have selected an instance that does not have a task associated with it.</td>
<td>None.</td>
<td>Select an instance that has an associated task.</td>
</tr>
</tbody>
</table>
# Config Editor

This section provides the troubleshooting information for the Config Editor application:

<table>
<thead>
<tr>
<th>Message-ID</th>
<th>Error Message</th>
<th>Probable Cause</th>
<th>Possible Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>CEDT0001</td>
<td>No device selected</td>
<td>You have not selected a device.</td>
<td>Select a device and try again.</td>
</tr>
<tr>
<td>CEDT0002</td>
<td>There is no configuration file for the device.</td>
<td>There is no configuration file for the selected device in the archive.</td>
<td>Perform Synch Archive to get the configuration file for the device</td>
</tr>
<tr>
<td>CEDT0003</td>
<td>Modified Config not selected.</td>
<td>You have not selected a modified configuration from the Modified Configs list.</td>
<td>Select a configuration file from Modified Configs list.</td>
</tr>
<tr>
<td>CEDT0004</td>
<td>No Config Selected for Download.</td>
<td>You have not selected a configuration file for downloading either from the archive or from Modified Configs list.</td>
<td>Select a configuration file for downloading either from the archive or the Modified Configs list.</td>
</tr>
<tr>
<td>CEDT0005</td>
<td>Enter job description.</td>
<td>You have not entered a job description while creating a job</td>
<td>Enter the job description. This is mandatory.</td>
</tr>
<tr>
<td>CEDT0007</td>
<td>No job selected.</td>
<td>You have not selected a job.</td>
<td>Select a job</td>
</tr>
<tr>
<td>CEDT0009</td>
<td>Job {JobId} cannot be {Action}.</td>
<td>You have tried to do any of the following:</td>
<td>User should select the appropriate job and appropriate action.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Edit a completed job</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Copy an incomplete job</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Stop a completed job</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Stop an already stopped job.</td>
<td></td>
</tr>
<tr>
<td>CEDT0010</td>
<td>Cannot get details for Job {JobID}.</td>
<td>The Job was recorded incorrectly.</td>
<td>None.</td>
</tr>
<tr>
<td>CEDT0011</td>
<td>Could not get the summary of the job.</td>
<td>None.</td>
<td>Check Cfgedit.log for more details.</td>
</tr>
<tr>
<td>CEDT0012</td>
<td>Job not found.</td>
<td>None</td>
<td>Check Cfgedit.log for more details.</td>
</tr>
<tr>
<td>CEDT0013</td>
<td>Some change in Jsp leading to incompatible with Action class.</td>
<td>None.</td>
<td>Contact Cisco TAC with log details for further assistance.</td>
</tr>
<tr>
<td>CEDT0014</td>
<td>Label not selected for search</td>
<td>You have tried to search labeled configurations without selecting a label</td>
<td>Select a label from the drop down.</td>
</tr>
<tr>
<td>CEDT0015</td>
<td>Cannot open configuration file.</td>
<td>None.</td>
<td>Check Cfgedit.log for more details.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Contact Cisco TAC with log details for further assistance.</td>
<td></td>
</tr>
<tr>
<td>Message-ID</td>
<td>Error Message</td>
<td>Probable Cause</td>
<td>Possible Action</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>CEDT0016</td>
<td>Cannot open Baseline Template.</td>
<td>Template may be deleted</td>
<td>Check whether the template exists.</td>
</tr>
<tr>
<td>CEDT0017</td>
<td>Baseline Templates not present for the selected device.</td>
<td>There are no templates for the selected device type.</td>
<td>Create a Baseline Template for the selected device type from the archive.</td>
</tr>
<tr>
<td>CEDT0018</td>
<td>No Config found for the specified search pattern</td>
<td>The pattern you have entered cannot be found in any of the configs</td>
<td>Change the search pattern.</td>
</tr>
<tr>
<td>CEDT0019</td>
<td>External Config to be opened not selected</td>
<td>You have not selected an External Config.</td>
<td>Select the External Config File from the browser.</td>
</tr>
<tr>
<td>CEDT0021</td>
<td>Version to be opened not selected.</td>
<td>None.</td>
<td>Select a valid version</td>
</tr>
<tr>
<td>CEDT0022</td>
<td>Cannot load query. Check whether the query exists</td>
<td>The query you selected may have been deleted.</td>
<td>Use Configuration &gt; Configuration Archive &gt; Views &gt; Custom Queries to check whether the query exists. Create a query if it does not exist.</td>
</tr>
<tr>
<td>CEDT0023</td>
<td>Cannot find query. Check whether the query exists</td>
<td>The query you selected may have been deleted.</td>
<td>Use Configuration &gt; Configuration Archive &gt; Views &gt; Search Archive&gt; to check whether the query exists. Create a query if it does not exist.</td>
</tr>
<tr>
<td>CEDT0024</td>
<td>No External Syntax Checker is registered with CMIC.</td>
<td>Either:</td>
<td>Register the syntax checker tool correctly with CMIC before Launching External Syntax checker.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• You may have launched the External Syntax checker without registering the syntax checker tool with CMIC.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>or</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The syntax checker is not registered correctly with CMIC.</td>
<td></td>
</tr>
<tr>
<td>CEDT0025</td>
<td>Syntax Checking functionality is not supported by this device image.</td>
<td>The device image you have selected does not support Syntax Checking functionality.</td>
<td>Select another device image that supports Syntax Checking functionality.</td>
</tr>
<tr>
<td>CEDT0029</td>
<td>One or more of the devices selected are already added to this job.</td>
<td>A config for the device has already been added</td>
<td>Only one config can be downloaded to a device in a Job.</td>
</tr>
<tr>
<td>CEDT0030</td>
<td>No configuration file exists for the device</td>
<td>There is no configuration file for the selected device in the archive.</td>
<td>Perform Synch Archive to get the configuration file for the device</td>
</tr>
<tr>
<td>CEDT0031</td>
<td>There are no commands to download.</td>
<td>None.</td>
<td>Remove the device from job and try again.</td>
</tr>
</tbody>
</table>
This section provides the troubleshooting information and FAQs for the Software Management applications:

- **Software Management FAQs**
- **Troubleshooting Software Management**

### Software Management FAQs

- **Q.** What are the high-level features of Software Management?
- **Q.** What privilege level is required to run Software Management functions?
- **Q.** How do I know which functions I can access in Software Management?
- **Q.** Are there DNS dependencies for Remote Copy Protocol (RCP) to work properly for a device?
- **Q.** Can I use Remote Copy Protocol (RCP) to transfer images to devices?
- **Q.** What connection mechanism does Software Management use to upgrade software?
- **Q.** What is the default Simple Network Management Protocol (SNMP) timeout used by Software Management? Can I configure it?
- **Q.** Can I configure TACACS or Radius authentication for devices that Software Management has upgraded?
- **Q.** Can I configure default privileges on terminal lines for Cisco IOS devices that Software Management has upgraded?
- **Q.** What is Job Approval?
- **Q.** What is the approver list?
- **Q.** Is the Job Approval policy enforced system-wide?
- **Q.** How do I configure Job Approval for Software Management?

<table>
<thead>
<tr>
<th>Message-ID</th>
<th>Error Message</th>
<th>Probable Cause</th>
<th>Possible Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>CEDT0032</td>
<td>Approval is enabled. Cannot schedule immediate jobs.</td>
<td>You cannot schedule Immediate jobs if Approval is enabled.</td>
<td>Select Schedule type, Once instead of Immediate</td>
</tr>
<tr>
<td>CEDT0033</td>
<td>Selected Job Execution date is invalid.</td>
<td>You have selected a past date for running a job.</td>
<td>Select a valid future date.</td>
</tr>
</tbody>
</table>
| CEDIT0034  | Job user name or password not entered. | You have enabled the Job based password option but not entered password. | Either:  
  - Deselect the Job-based password option  
  Or  
  - Enter the user name and password fields. |
| CEDT0039   | Enter at least one pattern. | You have not entered any search patterns. | Either:  
  - Select one of the queries listed  
  Or  
  - Enter a search pattern. |
• Q. Which Cisco IOS devices support bootldr images?
• Q. How do you identify bootldr image files?
• Q. How does the Software Management bootldr recommendation process work?
• Q. Where is the storage location of the bootldr image on the Cisco IOS device?
• Q. Does Software Management erase Bootflash if there is not enough free space on Bootflash?
• Q. Does Software Management change the configuration file for bootldr upgrades?
• Q. Can Software Management back up the current bootldr image while Software Management runs the Distribute Images job?
• Q. Does Software Management recommend bootldr images from Cisco.com in the Distribute Images function?
• Q. Can I upgrade modules on the device using advanced Distribution mode?
• Q. What image extension type are not supported in Software Management?
• Q. How can secured image upgrades be performed using Software Management?
• Q. How to use Reboot order configuration feature?
• Q. Is Image import from URL is treated as separate Job?
• Q. What is the best effort verification performed while distributing the image using Advance mode?
• Q. When does Software Management Application use SSH?
• Q. How can a protocol be Enabled/Disabled for a job?
• Q. How are devices upgraded using Secured Copy Protocol?
• Q. How much Disk space should be available while performing parallel image upgrade to large number of devices (more than 100)?
• Q. What is the swap file size required for Software Management application?
• Q. What Version of SCP is supported in Software Management application?
• Q. What are the pre requisites for using SCP for image upgrade?
• Q. Why is the job still running after I cancel it?
• Q. Why do I get an error message such as, Navigation to other areas of this application is not available until the opened wizard is finished or canceled.?
• Q. The Cisco.com profile window is sometimes filled with user and password and sometimes not. Why?
• Q. I am not able to select both sequential execution and sequential reboot at ‘Schedule Job’ step during distribution?
• Q. During Distribution by Advance flow, I get “Software Management application could not verify the flash inputs since there was no flash information available. Edit the expert input file and verify once again. If you do not edit the expert input file, you can continue with the task by clicking Next. However, the results may be inaccurate.”?
• Q. Why am I not able to see “Immediate” during software management jobs?
• A. Check if approval is enabled. If approval is enabled for Software Mgmt Jobs, you will not be able to schedule Immediate job.
• Q. I am not able to select the device (greyed box) at Software Management device selector page, but I’m able to select at inventory.
Appendix C  Troubleshooting Tips and FAQs

Software Management

- Q. I am not able to select a user script which is in xxx path.
- Q. In ACS login mode, I'm not able to see links that I usually get to see.
- Q. In the Job Details Window (clicking on job ID in the Software Management Job Browser) I don't see the job status being updated.
- Q. What validations are performed by Software Management before actual image distribution onto the device?
- Q. What is the minimum software version required to be running on the device for Software Management to upgrade the software?
- Q. Can I have a different script for each device in a job?
- Q. What device types can be used as remote stage device?
- Q. What device types cannot be upgraded using remote stage flow?
- Q. What are the pre-requisites for using the device as remote stage?
- Q. What Configuration changes are performed by Software Management on the remote stage device?
- Q. If I use the device as remote stage device does it impact the device's other functionalities or what are the performance implications of using the device as remote stage device?
- Q. Are there any Bad version of IOS for Remote stage device?
- Q. Can I perform module upgrade (like Bootloader/mica/microcom etc.) using remote stage flow?
- Q. How many devices in a job can be upgraded using remote stage?
- Q. Can I perform Parallel upgrade using remote stage flow?
- Q. Can I perform Slam dunk upgrade using the remote stage?
- Q. What is the difference between Run-from-RAM and Run-from-Flash devices?
- Q. When does Software Management use the remote copy protocol (rcp) to transfer images?
- Q. How does Software Management ensure that file corruption does not occur during transfer?
- Q. After an upgrade, why does Software Management sometimes leave behind image files in the tftpboot directory?
- Q. How much temporary space do you need during image distribution?
- Q. Is Cisco.com connection mandatory for Software Management?
  A. Cisco.com connection is not mandatory for using basic Software Management functionality. Image distribution, library management, tracking software upgrade changes, and other functions can run without Cisco.com connectivity.
- Q. How does Software Management handle proxy environments?
- Q. Does Software Management support proxy with user authentication environments?
- Q. Why is the Cisco.com filter option on the Software Management Edit Preferences screen not provided for Catalyst or Cisco 700 Series images?
- Q. How come the Cisco.com filter option does not work in LS1010 devices?
- Q. Can I configure Software Management to retrieve images from a Cisco.com mirror site rather than the main Cisco.com site?
- Q. Why I cannot download crypto images?
- Q. How does Software Management verify the integrity of the images after importing them from Cisco.com?
• Q. Why does the Flash size displayed in the Add Image to Repository (Source: Cisco.com) function not match the actual size for some Cisco IOS devices?

• Q. What is a Dual Flash Bank device?

• Q. Does Software Management support software upgrades on dual RSP-based systems?

• Q. Why does Software Management require static IP routes or dynamic IP routing protocol for configuration for the upgrade of a run-from-Flash (RFF) partition on a Single Flash Bank (SFB) device?

• Q. Although the configuration of the Single Flash Bank (SFB) device includes an IP default gateway, why does Software Management not upgrade the device?

• Q. How do you change the IP default gateway configuration to allow Software Management to upgrade a device?

• Q. Why does Software Management require Cisco IOS Software Release 11.1 or later to run on a Single Flash Bank (SFB) device for an upgrade when you have configured the device with Frame Relay subinterfaces?

• Q. How is the job directory organized?

• Q. Which modem cards does Software Management support?

• Q. Which devices and software versions get support for the modem upgrades?

• Q. Which formats of Microcom firmware images does Software Management support?

• Q. Which format of Modem ISDN channel aggregation (MICA) portware do Cisco 3600 devices support?

• Q. Why does the Undo option not receive support for modem upgrades?

• Q. What connection mechanism does Software Management use for modem upgrades?

• Q. Does Software Management erase Flash for modem upgrades if there is not enough free space on Flash?

• Q. What is CIP?

• Q. Which devices support the Channel Interface Processor (CIP) microcode upgrade? What is the minimum software version necessary?

• Q. What is the minimum Channel Interface Processor (CIP) version that Software Management supports?

• Q. How can you import Channel Interface Processor (CIP) images to the Software Management library?

• Q. Is there support for the Undo option for Channel Interface Processor (CIP) upgrades?

• Q. What connection mechanism does Software Management use to upgrade Channel Interface Processor (CIP)?

• Q. Does Software Management change the configuration file for the Channel Interface Processor (CIP) upgrade?

• Q. Does Software Management support CIP2?

• Q. In which order does Software Management upgrade modules on a Cisco Catalyst 5500/5000 device?

• Q. Does the Supervisor Engine card reboot after the upgrade of all modules?

• Q. Does Software Management determine if the newly deployed Supervisor Engine software or module software is compatible with the module types (or module hardware versions)?
- Does Software Management support the upgrade of software on redundant Supervisor Engine card-based systems?
- Does Software Management update the configuration file on Cisco Catalyst 5500/5000 devices during the software upgrade?
- Does Software Management determine if the Supervisor Engine has the minimum required RAM to run a new image?
- Are there restrictions on the downgrade of the software on the Supervisor Engine card and other modules?
- Do you need to reconfigure the device when you downgrade the Supervisor Engine software?
- In the 4.1(1) software release and later, Supervisor Engine III cards allow the storage of configuration files on Flash cards. Does Software Management preserve the backed up configuration files on Flash during a software upgrade?
- Does Software Management allow you to upgrade epsboot images on Token Ring cards on Cisco Catalyst 5500/5000 devices?
- Why does the Add Image to Repository (Source: Cisco.com) task not display Token Ring LAN Emulation (LANE) or Permanent Virtual Circuit (PVC)-only ATM software images?
- How do you identify software image files for each of the ATM modules that Software Management does support? What are the file-name conventions on Cisco.com?
- How can I make the Image Recommendation faster?
- Why do the software version numbers that the show module command output displays from the Supervisor Engine command-line interface (CLI) and the version numbers that Software Management uses fail to match in some cases?
- Does Software Management recommend the right ATM image for your ATM module type?
- Should you use special images with Software Management for Cisco Catalyst 2900XL/3500XL devices?
- How does Software Management handle image import functionality of TAR and bin types of images for Catalyst 2900XL/3500XL devices?
- Why do software upgrades take longer on Cisco Catalyst 2900XL/3500XL devices?
- How do you upgrade Route Switch Module (RSM) and LightStream 1010 (LS1010) module software on Cisco Catalyst 5500/5000 and 6500/6000 series switches?
- Why does the Distribute Images task show all the images from Cisco.com for LightStream 1010 (LS1010) and Cisco Catalyst 8500 devices, even though you have configured Cisco.com filtering?
- What is the minimum version that Cisco 700 series ISDN routers support?
- What connection mechanism does Software Management use for Cisco 700 series upgrades?
- Both Cisco 760 and 770 series devices run the same image. Why do you see only some images with versions later than 4.0(1) for 770 series devices but see all images for 760 series devices?
- Why do you not see the option to reboot the device later on the Job Control page for Cisco 700 series routers?
- Why do you not see the option to modify the boot commands on the Job Control page for Cisco 700 series routers?
- Why does Software Management report download failures for some images even though the device runs the new image after the job completes?
- In which order does Software Management upgrade modules on a Catalyst 5000 device?
• Q. Does Software Management check to see that the newly deployed Supervisor software or module software is compatible with the module types (or module hardware versions)?
• Q. Does Software Management support upgrading software on redundant Supervisor card-based systems?
• Q. What is the purpose of user scripts?
• Q. What if the user script crashes? Will it crash the Software Management job also?
• Q. When a Software Management job is scheduled, how is the baseline determined? When I distribute a job, is an automatic backup performed?
• Q. Can I set up a periodic download of Software Management images from Cisco.com?
• Q. Is browser timeout something I should consider when downloading?
• Q. What are crypto images?
• Q. How much temporary space is required during image distribution?
• Q. At what time will the images directory get created during the process of obtaining images from a device? Does this happen during the initial step?
• Q. How can I speed up Image Recommendation?
• Q. When a job is rejected, can it be edited or should I resubmit?
• Q. Can different group members edit jobs? What are the restrictions?
• Q. What is the role of the registry files?
• Q. How do I upgrade Network Analysis Module (NAM) using Software Management?
• Q. Can I change the job scheduled time?
• Q. How does Software Management handle the job status for an abnormally terminated job?
• Q. How does Software Management handle the job status of a pending job whose scheduled time has passed?
• Q. Why are some files left in the Software Management folder after Software Management has been uninstalled?
• Q. How can I enable or disable the SSH to Telnet fallback for Software Management jobs?
• Q. How can I export the images from SWIM repository to a local drive or a file system mounted to the LMS server?
• Q. Does Flash get erased if there is no sufficient space for Patch Distribution?
• Q. When I try to copy images, the Image Copy option fails indicating that the External TFTP server is inaccessible.
• Q. Can I specify the name of my input file as imagenames.txt when I try to export images using the Software Management (SWIM) CLI exportimages command?
• Q. I am getting timeout exception in cmdsvc (command service library) during a device connection/socket establishment. How do I change the default timeout and delays in cmdsvc?
Q. What are the high-level features of Software Management?

A. Software Management offers the following management functions:

- **Software Distribution**—Schedules download of software images to a single device or groups of devices. Hardware and firmware validation verifies whether the new image can run on the device. Image Upgrade can be performed in Sequential or in parallel. Also the In Parallel mode of upgrade device reboot can be controlled for the job.

  Provides several workflow to achieve this functionality
  - Distribute By Device [Basic]
  - Distribute [Advance]
  - Distribute by Image
  - Distribute by Remote Stage/ External TFTP server
  - Patch Distribution

- **Software Repository**—Builds and maintains a library archive of software images. Software images can be added to repository from,
  - Device—Allows to archive the current software images on the device
  - Cisco.com—Integrates with Cisco Connection Online (Cisco.com) to download software images.
  - File System—Allows to import an image from a directory accessible from the LMS server
  - Network—Allows the library to synchronize with the software images running on the devices. A periodic job can generate a list of images that are not in the library. You then have the option to import new images into the library and check them for discrepancies between software images running on the network and images in the library.
  - URL—Allows to download images from URL you specify.

- **Upgrade Analysis**—Determines the hardware upgrades required on network devices to enable them to run new software. Software Management allows analysis based on the location of image to be analyzed. Following locations are supported.
  - Cisco.com
  - Local Repository

- **Job Management**
  - **Job Approval** — Allows organizations to require approvals before allowing software upgrades.
  - Software Management jobs can be operated upon to,
    - Retry
    - Undo
    - Cancel
    - Stop

- **Reports**
  - **Work order**—Displays changes that will be made to network devices as part of the software upgrade.
  - **Synchronization report**—Displays which Software Management-supported devices are running software images that are not in the software image repository.
  - **Audit trail**—Tracks software changes made on the LMS server
Q. What privilege level is required to run Software Management functions?

A. Different options in Software Management require different levels of user privileges. Privilege levels are known as “roles” in LMS. For a list of LMS functions and required user roles, use the Permissions Report function (Reports > System > Users > Permission).

Q. How do I know which functions I can access in Software Management?

A. To find which functions you can access in Software Management:
   - Select Reports > System > Users > Who Is Logged On to find your assigned roles.
   - Select Reports > System > Users > Permission to verify which LMS and Software Management tasks you can run.

Q. Are there DNS dependencies for Remote Copy Protocol (RCP) to work properly for a device?

A. Yes. If there are multiple IP addresses configured on the device, all IP addresses on the device must be configured in the Domain Name System (DNS). Examples of devices with multiple IP addresses are those having many interfaces, with each interface configured with its own IP address, or a device that interfaces configured with primary and secondary IP addresses.

Configure the DNS so that all IP addresses are resolved to the same host name. The host name in the DNS should match the host name entered in the Device and Credential Repository.

Q. Can I use Remote Copy Protocol (RCP) to transfer images to devices?

A. Use the RCP transport protocol for image transfers only on Cisco IOS devices that support the CISCO-FLASH-MIB. Catalyst switches that run Supervisor software older than 5.2, and 700 Series devices do not support the RCP protocol.

The Cisco IOS devices can not use RCP if they only support OLD-CISCO-FLASH-MIB, (for example, MC3810) or if they do not support any Flash Management Information Base (MIB) (for example, RSP 7000 devices running Cisco IOS Software Releases 10.3-11.0).

Q. What connection mechanism does Software Management use to upgrade software?

A. Simple Network Management Protocol (SNMP) is the preferred mechanism used by Software Management to upgrade software. Some devices, however, cannot be upgraded using SNMP alone.

For such devices, Software Management uses a Telnet interface to do the upgrades. SNMP upgrades all Run-from-RAM Cisco IOS devices, Dual Flash Bank Run-from-Flash (DFB RFF) devices, and all Catalyst switches. If SSH is preferred for device connection then SSH is Used for connecting to the device.

Software Management uses Telnet to perform the following upgrades:
   - Single Flash Bank Run-from-Flash Cisco IOS devices (SFB 2500s, 1600s, AS5200)
   - RSP 7000 devices running Cisco IOS Software Releases 10.3 - 11.0
   - Cisco 700 Series
   - CIP, MICA, Microcom upgrades
   - 3500/2900 series of devices
   - 1900/2820 Series
   - VPN 3000 Series of devices.

For complete list of supported protocols see Supported Device Table for Software Management.
Q. What is the default Simple Network Management Protocol (SNMP) timeout used by Software Management? Can I configure it?
A. Default retry is 2 and default SNMP time out value is 2. This value is configurable using Admin > Collection Settings > Inventory > Inventory, Config Timeout and Retry Settings.

Q. Can I configure TACACS or Radius authentication for devices that Software Management has upgraded?
A. Software Management supports upgrading devices that are configured for TACACS or Radius authentication. An exception is software upgrades on the Run-from-Flash partition if the device is configured with Radius protocol authentication. The Device and Credential Repository must be configured with the appropriate information to access the device.

Q. Can I configure default privileges on terminal lines for Cisco IOS devices that Software Management has upgraded?
A. Software Management upgrades software by using the Telnet interface or Command-Line Interface (CLI) on devices that do not support enough Management Information Base (MIB) instrumentation for software management.

Software Management uses Telnet to connect into the devices and executes privileged commands such as copy tftp flash, copy flash tftp, erase flash, show version, copy flash modem to perform upgrades.

Software Management modifies the configuration file using the Telnet interface to upgrade the software. For Software Management to work on a device, there are some restrictions on how default privileges and enable mode authentication are configured.

The restrictions apply to only those Cisco IOS devices that are managed by Software Management through the Telnet interface. Cisco 700 Series and Catalyst 5000/6000/4000 devices are not affected. Restrictions include the following:

- Software Management tries to run the above CLI commands from privilege level 15. The user must always configure an enable password/secret for privilege level 15, and the same password/secret must be entered in the Device and Credential Repository.

  If the device is configured with TACACS authentication for enable mode access, then the Enable TACACS user name and password must be entered in the Device and Credential Repository. The Enable User name and password authenticated by TACACS+ server always should receive a privilege level of 15.

- The default privilege level configured on a vty line must allow Software Management to run the CLI commands mentioned earlier as well change the configuration file on the device. The privilege level does not need to be 15, but setting the privilege level to 15 guarantees Software Management can always work on the device.

Q. What is Job Approval?
A. Job Approval allows an organization to require approvals before an administrator distributes software images. When an image distribution job is created, the administrator (or whoever creates the job) selects from a list of users who can approve the job.

For the job to run, one of the users on the approver list must approve it before its scheduled time. If the job is not approved, it will be rejected at the scheduled time.
Q. What is the approver list?
A. An approver list consists of user names in LMS who have the authority to approve software upgrades.

The following steps are required:
   b. Create the list by using the Create Approver List (Admin > Network > Configuration Job Settings > Create/Edit Approver Lists). Only users who have an Approver role can be added to the Approver List.

Q. Is the Job Approval policy enforced system-wide?
A. Yes. To create a job that does not require approval, disable the Software Management option.

Q. How do I configure Job Approval for Software Management?
A. To configure Job Approval, do the following:
   a. Add the approver user.
   b. Create an Approver List
   c. Enable the Job Approval option

Q. Which Cisco IOS devices support bootldr images?
A. The following Cisco IOS device families support bootldr images:
   • Cisco 4500 and 4700
   • Cisco 7500, Route Switch Processor (RSP)-based 7000
   • Cisco 7200
   • Cisco AS5200, AS5300, and AS5800 Access Servers
   • Route Switch Module (RSM) on Cisco Catalyst 5500/5000
   • ESR 10K, 10K2 devices

See the Supported Device Table for Software Management application on Cisco.com for further information.

Q. How do you identify bootldr image files?
A. Bootldr image files follow this name convention, platform-boot-mz.version

An example is rsp-boot-mz.11.0(17)BT. If the second part (feature part) of the image file name contains “boot”, then the image is a bootldr image. The software library recognizes the file name and imports the image as a bootldr image. Bootldr images earlier than Cisco IOS Software Release 10.3 contain xboot in the feature part of the image. Software Management does not support such images.
Q. How does the Software Management bootldr recommendation process work?
A. Different hardware platforms in Cisco IOS Software have different bootldr images. For example, the bootldr image for the Cisco 4500 device is c4500-boot-mz; the bootldr image for the Cisco 7200 is c7200-boot-mz.

From the library, Software Management determines which bootldr images belong to the same family as the target device. Software Management then recommends the most current of all available images.

Unlike system software images, bootldr images do not have RAM requirements. Therefore, Software Management does not perform prerequisite matches between the device and the image.

Q. Where is the storage location of the bootldr image on the Cisco IOS device?
A. Software Management always uses the Bootflash card as the target Flash for the bootldr image. Software Management stores bootldr images on the Bootflash card only, even though Cisco IOS Software allows the store of bootldr images on a Flash card.

If you use other Flash cards for the store of bootldr images, problems can occur when you have stored other types of images, such as system software, Microcom, or Modem ISDN channel aggregation (MICA), in the same location.

Q. Does Software Management erase Bootflash if there is not enough free space on Bootflash?
A. If the Bootflash card does not have enough free space to store the new bootldr image, Software Management erases the Bootflash to make room for the new boot image. A verification warning alerts you of the Bootflash erase.

To see this warning, click the Failure/Warning link in the Status column of the Verify Image Upgrade window.

Software Management backs up and restores files on Bootflash with sizes of less than 1 MB.

Q. Does Software Management change the configuration file for bootldr upgrades?
A. Upon bootldr upgrade, Software Management changes the device configuration file such that the configuration file that downloads to the device contains:

Assume that the file name of the newly downloaded bootldr image is c4500-boot-mz.112-13.bin.

- no boot bootldr
- boot bootldr c4500-boot-mz.112-13.bin

Q. Can Software Management back up the current bootldr image while Software Management runs the Distribute Images job?
A. Software Management backs up the system software image only during the Cisco IOS Distribute Images job execution. The backup of bootldr images cannot take place. Use the add images function to import the bootldr image from device to library. (Select Configuration > Tools > Software Image Management > Software Repository > Add).

Q. Does Software Management recommend bootldr images from Cisco.com in the Distribute Images function?
A. Yes, Software Management does recommend the download of bootldr images directly from http://www.cisco.com during the Distribute Images job creation.
Q. Can I upgrade modules on the device using advanced Distribution mode?
A. No. Expert flow is not officially tested with all the possible module upgrade scenarios. Current implementation claims only system software upgrades using the expert flow.

Q. What image extension type are not supported in Software Management?
A. The following file/image types are not supported:

doc, txt, pdf, xls, ppt, jpg, jpeg, bmp, csv, mpg, au, xml, html, htm, java, class, tex, ps, pps.

Q. How can secured image upgrades be performed using Software Management?
A. Current Version (4.1) supports new protocols such as, SCP and SSH. You can choose the appropriate protocols based on the device support.

For the devices that are upgraded using Telnet/SSH, new feature called Job based password can be enabled for scheduled job. You can specify a temporary password for the upgrade job and it will take precedence over all the credentials in the Device and Credential Repository.

Q. How to use Reboot order configuration feature?
A. This feature is applicable only in case of “parallel” mode of image upgrade. This feature can be used to perform sequential rebooting of devices. You can make this decision based on the network topology or any other deployment policy. The devices will be rebooted in the order specified by you.

Q. Is Image import from URL is treated as separate Job?
A. Yes, the workflow results in a job.

Q. What is the best effort verification performed while distributing the image using Advance mode?
A. Verification in Advance distribution mode is referred as the best effort verification because you can proceed to schedule the image upgrade even without the inventory data. This is designed to support devices that are not yet managed in CiscoWorks (pre-deployed devices).

Q. When does Software Management Application use SSH?
A. If the device type selected is to be upgraded using the CLI then Software Management application uses SSH (if opted in the preference). Even for fetching information required during the job creation stage, SSH is used.

Q. How can a protocol be Enabled/Disabled for a job?
A. Using the User Interface, Admin > Network > Software Image Management > View/Edit Preferences. Available protocols list the Software Management supported protocols. You have to add or remove the protocols to selected protocol order in order to enable or disable the protocol used for image transfer.

Q. How are devices upgraded using Secured Copy Protocol?
A. Image staging and other checks performed before the image distribution remains same for upgrade using SCP. The options such as Flash erasure, Delete, etc. are performed using Cisco Flash mib or old Cisco flash mib only.

The difference lies in the model used for image upgrade. LMS positions itself as a client for the Secured Copy options. Devices with SCP server are (like 2650XM) requested to initiate a file transfer job. The image is transferred from LMS to the devices.
Q. How much Disk space should be available while performing parallel image upgrade to large number of devices (more than 100)?
A. The amount of disk depends upon the number of images staged in the upgrade job. If the image selected is common for all the devices then disk space required is equal to size of the image. If different images are selected for each job then disk space required is the sum of all the images.

Q. What is the swap file size required for Software Management application?
A. LMS recommend a swap size of 2MB for managing 300 devices.

Q. What Version of SCP is supported in Software Management application?
A. Current implementation of SCP is based on the fcpsvc library that uses the SSHv1 stack. Current version of SCP supported is 1.0.

Q. What are the prerequisites for using SCP for image upgrade?
A. The device should have SCP server. Any image having 3DES feature has SCP server in it. SSH should be enabled on the device.

Q. Why is the job still running after I cancel it?
A. In Sequential mode, the job stops only after the image upgrade for the current device or module is finished. Canceling a running job does not cancel the software upgrade being performed at that time. The job stops only after the current upgrade is complete.

During this time, the Browse Job Status screen shows that the job is still running. In case of parallel upgrades, when a job is cancelled, the current set of devices being processed will be continued and not stopped. However, new devices will be processed only after the current devices have completed running.

Q. Why do I get an error message such as, Navigation to other areas of this application is not available until the opened wizard is finished or canceled.
A. Yes, you get this when you are in a wizard (you will see Back, Next, Finish, and Cancel when you are in a wizard at the bottom) and you click any of the other navigational links.

Q. The Cisco.com profile window is sometimes filled with user and password and sometimes not. Why?
A. If the Cisco.com user name and password is configured for you the same will be pre-populated. You can configure the Cisco.com credentials in the Cisco.com User Account Setup dialog box (Admin > System > Cisco.com Settings > User Account Setup).

Q. I am not able to select both sequential execution and sequential reboot at 'Schedule Job' step during distribution?
A. If you had selected execution to be sequential the same order applies to reboot. However, if the execution is parallel you will be allowed to select reboot sequential.

Q. During Distribution by Advance flow, I get “Software Management application could not verify the flash inputs since there was no flash information available. Edit the expert input file and verify once again. If you do not edit the expert input file, you can continue with the task by clicking Next. However, the results may be inaccurate.”?
A. You get this when there are no inventory information available for the device. You can expect this error for 2900, 3500, 3550 x1 devices.
Q. Why am I not able to see “Immediate” during software management jobs?
A. Check if approval is enabled. If approval is enabled for Software Mgmt Jobs, you will not be able to schedule Immediate job.

Q. I am not able to select the device (greyed box) at Software Management device selector page, but I'm able to select at inventory.
A. Software Management support might not be there. See the Supported Device Table for LMS on Cisco.com

Q. I am not able to select a user script which is in xxx path.
A. The scripts are expected to be available in the specific path. The Software Management scripts are located at:
   - `NMSROOT/files/scripts/swim` (On Solaris and Soft Appliance)
   - `NMSROOT\files\scripts\swim` (On Windows)
   Where `NMSROOT` is the CiscoWorks installed directory.

Q. In ACS login mode. I’m not able to see links that I usually get to see.
A. On the ACS server, check if some role to task mapping (tree) has got changed. The required Software Management task option should be selected on the ACS server for a particular role.

Q. In the Job Details Window (clicking on job ID in the Software Management Job Browser) I don’t see the job status being updated.
A. The job status will not be updated, as only the job running status is getting refreshed.

Q. What Validations are performed by Software Management before actual image distribution onto the device?
A. Software performs the following checks before the job execution:
   - Checks whether job file is Available at the job id and has required data in the format and prepares a list of devices to be upgraded in the job.
   - Checks whether LMS License is valid
     - Whether license file is valid
     - Number of devices managed
   - Removes all devices from the list which are not authorized for the user to perform image distribution.
   - Removes all devices from the list which are in Suspended state or Conflicting state. Pre-deployed state devices are not removed.
   - Checks for the proper pre/post job script (if any) ownership and permission
     - On Solaris and Soft Appliance, check is performed for `rwxr-x---` permissions for script file (0750)
     - On Windows, check is performed if the given script has write permissions for any non-admin and non-casuser
   - Verifies that critical data required for image upgrade are present in the job file.
Q. What is the minimum software version required to be running on the device for Software Management to upgrade the software?
A. For Cisco IOS device minimum supported version is 11.0 where as for Catalyst Images Minimum supported version is 3.8.
   For more details on minimum supported version for each device type refer to Supported Devices Table.

Q. Can I have a different script for each device in a job?
A. No, you cannot have separate script for each device. In Software Management 4.1, script is defined in admin preference option and is common for all Software Management jobs.

Q. What device types can be used as remote stage device?
A. All IOS devices with running image version >=12.0 version and complete CISCO-FLASH-MIB support can be used as Remote-Stage device.

Q. What device types cannot be upgraded using remote stage flow?
A. Content Engines (CE), Network Analysis Modules (NAM), Content Service Switches (CSS), and PIX.

Q. What are the pre-requisites for using the device as remote stage?
A. It must be an IOS device and it must be running >= 12.0 version and it must support CISCO-FLASH-MIB completely.

Q. What Configuration changes are performed by Software Management on the remote stage device?
A. tftp-server flash-partition-name:image-name alias image-name is the only command that will be added to the Remote stage device to make the image copied to Remote Stage device as accessible through TFTP from other devices.

Q. If I use the device as remote stage device does it impact the device's other functionalities? or what are the performance implications of using the device as remote stage device?
A. There will not be any impact on device's other functionalities and also they will no be any performance implications on the device that is used as Remote-Stage.

Q. Are there any Bad version of IOS for Remote stage device?
A. 12.3(5x) series.

Q. Can I perform module upgrade (like Bootloader/mica/microcom etc.) using remote stage flow?
A. No.

Q. How many devices in a job can be upgraded using remote stage?
A. There is no limit specific to remote stage flow. the number of devices in a remote stage job is same as that of other distribution flow.

Q. Can I perform Parallel upgrade using remote stage flow?
A. Yes

Q. Can I perform Slam dunk upgrade using the remote stage?
A. No. The image that you want to use must be in the Software Repository.
Q. What is the difference between Run-from-RAM and Run-from-Flash devices?
A. Most Cisco IOS devices load the software image from Flash to RAM when rebooting, then run the software from RAM. Such devices are called Run-from-RAM (RFR) devices. For these devices, the software image on Flash can be upgraded without rebooting the device.

Certain Cisco IOS devices (namely 2500s, 1600s, and AS5200s) run the system software image directly from Flash. These are Run-from-Flash (RFF) devices. The Flash partition in which the current image is stored is the RFF partition, which is read-only.

Software Management supports upgrading software images on RFF partitions by using a procedure called Rxboot upgrade. Before upgrading, reboot the device and put it into Rxboot mode, which makes the RFF partition available to write a new software image.

Q. When does Software Management use the remote copy protocol (rcp) to transfer images?
A. Generally the order defined in selected protocol list will be used for transferring (to upload and download) Cisco IOS® Soft wares. If RCP is in the top of the selected protocol list then RCP is used as the first protocol for image transferring on to the devices that support CISCO-FLASH-MIB.

Check the supported protocol list for the device to find out whether device supports RCP or not. Cisco Catalyst 5500/5000 switches and Cisco 700 series devices do not support rcp. Cisco IOS devices that do not support rcp include the Cisco 7000 series (route processor [RP]-based 7000 only) and MC3810.

All other Cisco IOS devices support the rcp protocol.

Q. How does Software Management ensure that file corruption does not occur during transfer?
A. Software Management computes the checksum of the image file. Then, Software Management compares this checksum to the checksum from the device after the copy of the image file to the device Flash.

Software Management also verifies the size of the file on the Flash. If either the size or checksum do not match, Software Management aborts the distribution and marks the job status as an error.

Q. After an upgrade, why does Software Management sometimes leave behind image files in the tftpboot directory?
A. Software Management removes the image files from the tftpboot directory after the upgrade unless the TFTP fallback job option is set. If the TFTP fallback option is set, Software Management uploads the image from the device and leaves the image in the tftpboot directory for fallback.

Software Management also modifies the boot system commands on the device to add a fallback command to boot from the original image on the LMS TFTP server if the upgraded image does not boot.

Q. How much temporary space do you need during image distribution?
A. The amount of free space necessary depends on the image file size and the number of devices for simultaneous upgrade. If the TFTP fallback option is set, you need additional free disk space to keep the current image in the tftpboot directory. Both the tftpboot and temp directories use disk space.

Q. Is Cisco.com connection mandatory for Software Management?
A. Cisco.com connection is not mandatory for using basic Software Management functionality. Image distribution, library management, tracking software upgrade changes, and other functions can run without Cisco.com connectivity.
Cisco.com connectivity provides the additional benefits of obtaining images and their attributes from Cisco.com and viewing the status of outstanding bugs against the software images running on the devices in the network.

The following features of Software Management require Cisco.com connectivity:

- Adding image to Repository from Cisco.com. Software Management can import images for all supported devices.
- Distributing images directly from Cisco.com to devices, also called Recommend Images from Cisco.com. Without a Cisco.com connection, the Recommend Images screen Image list box will not show any images from Cisco.com when it creates the Distribute Images job.
- Cisco.com upgrade analysis.
- Cisco IOS image deferral processing.

Q. How does Software Management handle proxy environments?
A. Software Management uses HTTP protocol to communicate to Cisco.com about downloading images and their attributes. If you use an HTTP proxy for Internet connectivity, configure Proxy URL information in Admin > System > Cisco.com Settings > Proxy Server Setup.

Q. Does Software Management support proxy with user authentication environments?
A. Yes, Software Management supports proxy that requires user authentication.

Q. Why is the Cisco.com filter option on the Software Management Edit Preferences screen not provided for Catalyst or Cisco 700 Series images?
A. During the Distribute Images task, Software Management communicates with Cisco.com to obtain a list of applicable images and their attributes. Based on this information, Software Management recommends an image.

There are many Cisco IOS images available on Cisco.com, which can cause a substantial delay in retrieving image attributes from Cisco.com. Some of these images will not be relevant to the user. Software Management filters the amount of images being considered to make a more meaningful and manageable subset.

For Catalyst and 700 devices, fewer images are available on Cisco.com than for Cisco IOS; therefore, it is not necessary to filter the images.

Q. How come the Cisco.com filter option does not work in LS1010 devices?
A. Although LS1010 devices run Cisco IOS images, there are some differences in how the LS1010 images are released. LS1010 images do not follow the Cisco IOS-type image releases like general deployment (GD), limited deployment (LD), and early deployment (ED).

Therefore, Software Management cannot effectively filter LS1010 type images. Nor does Software Management filter Catalyst 8500 Series images.

Q. Can I configure Software Management to retrieve images from a Cisco.com mirror site rather than the main Cisco.com site?
A. No. Although the mirror Cisco.com sites contain the images, they do not store image attributes, such as minimum RAM and FLASH requirement. This information is available only from the main Cisco.com site at http://www.cisco.com.
Q. Why I cannot download crypto images?
A. Crypto images are available only to authorized Cisco.com users. All users can view the images during the Recommendation stage but only users with the right privileges can download the image. Make sure that the Cisco.com Login user configured in CiscoWorks has permission to download crypto images.

Q. How does Software Management verify the integrity of the images after importing them from Cisco.com?
A. Software Management checks the validity of the downloaded images by comparing the MD5 checksum of the image with the MD5 checksum value retrieved from the Cisco.com database.

Q. Why does the Flash size displayed in the Add Image to Repository (Source:Cisco.com) function not match the actual size for some Cisco IOS devices?
A. Software Management does not erase files whose sizes are less than 1 MB on Cisco IOS devices because those files may be config files that are backed up to Flash partitions or .html files or Java applets used for management.

Software Management subtracts sizes of all files whose sizes are less than 1 MB from the size of the Flash partition. The result of the subtraction is displayed as the size of the Flash partition in the Software Management user interface.

The Software Repository Management window (Configuration > Tools > Software Image Management > Software Repository) displays the size of the largest Flash partition on the device. The size is displayed as an integer-truncated value in megabytes.

The Distribute Images screen displays information for all Flash partitions on the device. The values are displayed with two-decimal-digit precision.

The example below illustrates Software Management’s behavior on a Cisco IOS device, which has two files whose sizes are 10 KB and 50 KB respectively.

The Flash card’s total size is 8 MB. Because it has two files whose sizes are less than 1 MB, the Add Image to Repository screen displays the size as 7 MB. The Distribute Images screen displays the size as 7.94 MB.

```
enm-2502> show flash
System flash directory:
File Length Name/status
1 8089628 c2500-js-l.112-14.bin
2 10470 test_file1
3 52995 test_file2
8153288 bytes used, 235320 available, 8388608 total
8192K bytes of processor board System flash (Read ONLY)
```

Q. What is a Dual Flash Bank device?
A. The Flash card can be partitioned into two equal banks. Each bank is called a Flash partition. A Flash card that is not partitioned is Single Flash Bank (SFB) and the device is called an SFB device. A device that has its Flash card divided into two partitions is a Dual Flash Bank (DFB) device.

When Flash is partitioned into two separate banks, they are named flash1 and flash2. Software image files have to be completely stored in a single partition, so the maximum size of a software image is limited by the total size of any Flash partition.

On a Dual Flash Bank Run-from-Flash (DFB RFF) device, Software Management supports upgrading the flash partition that does not contain the running image. In other words, Software Management cannot upgrade the RFF partition on DFB devices.
This is because the other partition, which can be upgraded directly, is the recommended partition for storing the new software image.

The AS5200 device has two Flash cards, Bootflash and Flash. The Flash is an RFF system and Bootflash is an RFR system. The Bootflash is intended for storing bootldr images on the AS5200 and flash is for storing Cisco IOS System Software.

Q. Does Software Management support software upgrades on dual RSP-based systems?

A. Software Management updates the software on the master RSP processor by copying the software image file to the master RSP Flash card (bootflash: slot0: slot1:) and updating the config file on the master RSP. Software Management cannot do a complete job of upgrading the software on the slave RSP processor.

Software Management can only copy the software image file to the slave RSP processor, but it cannot update the config file on that processor. Users will have to run a separate Distribute Images job to copy the software image file to the slave RSP processor.

Since Software Management cannot update the config file on the slave RSP processor, users must select Don't touch config file and select the No Reboot option in the job created for upgrading software on the slave RSP processor.

Q. Why does Software Management require static IP routes or dynamic IP routing protocol for configuration for the upgrade of a run-from-Flash (RFF) partition on a Single Flash Bank (SFB) device?

A. Software Management upgrades SFB devices that are in Rxboot mode. Rxboot mode does not support IP routing, IP bridging, or Simple Network Management Protocol (SNMP). The Rxboot image can support only one IP interface. Before the reboot of the device while in the Rxboot mode, Software Management determines the:

- Interface that connects the device to LMS servers. Software Management shuts down all interfaces except the one that connects to the LMS server.
- Default gateway IP address for the forward of all IP traffic when the device is in the Rxboot mode.
- Software Management queries the ipRouteEntry MIB variables ipRouteDest and ipRouteIfIndex to determine the default gateway IP address and the interface that connects.

If the device configuration does not include static IP routes or dynamic IP routing protocol, the ipRouteEntry table is not set on the device. Consequently, Software Management cannot determine the default gateway and the interface that connects to LMS.

Q. Although the configuration of the Single Flash Bank (SFB) device includes an IP default gateway, why does Software Management not upgrade the device?

A. Software Management requires an IP default gateway address and an interface that connects. If you configure only the IP default gateway with the configuration command (ip default-gateway ip-address), you do not generate the ipRouteEntry MIB table on the device.

You can parse the IP default gateway from the configuration file; however, there is no reliable way to get the connecting interface from the device without the ipRouteEntry MIB. Without the ipRouteEntry MIB, Software Management does not allow upgrades, even if you have manually configured the IP gateway on the device.
Q. How do you change the IP default gateway configuration to allow Software Management to upgrade a device?
A. Use the IP default gateway configuration command to convert to a static IP route. Replace `ip default-gateway gateway_ip_address with ip route 0.0.0.0 0.0.0.0 gateway_ip_address`, which removes the `ip default-gateway` command from the configuration file. Check the output of the show ip route command to verify the correct configuration of a static IP route on the device.

Q. Why does Software Management require Cisco IOS Software Release 11.1 or later to run on a Single Flash Bank (SFB) device for an upgrade when you have configured the device with Frame Relay subinterfaces?
A. Releases earlier than Cisco IOS Software Release 11.1 do not include Frame Relay subinterfaces in ifTable and ipRouteTable in RFC 1213. Software Management requires information from these tables to perform Rxboot mode upgrades.

Therefore, Software Management requires Cisco IOS Software Release 11.1 or later to run on an SFB device when the device has Frame Relay subinterfaces.

Q. How is the job directory organized?
A. When Software Management schedules a job, it creates a new directory:
   - On Solaris and Soft Appliance: `/var/adm/CSCOpx/files/rme/swim`
   - On Windows, `NMSROOT\files\rme\swim`

   Where `NMSROOT` is the CiscoWorks installed directory.

   The directory name is the integer ID of the job. (Example: `/var/adm/CSCOpx/files/rme/swim/23, where 23 is the Job ID)."

   The Job directory contains the following files depending upon the type of Software Management task:

<table>
<thead>
<tr>
<th>Distribution Job</th>
<th>Image Import Job Image</th>
<th>Synchronization Job</th>
</tr>
</thead>
<tbody>
<tr>
<td>swim_debug.log</td>
<td>workorder.html</td>
<td>swim_debug.log</td>
</tr>
<tr>
<td>workorder.html</td>
<td>distribution.xml</td>
<td>workorder.html</td>
</tr>
<tr>
<td>distribution.xml</td>
<td>PostOperation.txt</td>
<td>import.xml</td>
</tr>
<tr>
<td>PostOperation.txt</td>
<td>SwOperation.txt</td>
<td>PostOperation.txt</td>
</tr>
<tr>
<td>SummaryTable.tab</td>
<td>SummaryTable.tab</td>
<td>SwOperation.txt</td>
</tr>
<tr>
<td>Hostname.upgStatus</td>
<td>Hostname.upgStatus</td>
<td>SummaryTable.tab</td>
</tr>
<tr>
<td>HostName_Config_Snap</td>
<td>HostName_Config_Snap</td>
<td>Hostname.upgStatus</td>
</tr>
</tbody>
</table>

Where,
- `swim_debug.log` contains the debug information during the job execution.
- `workorder.html` contains the changes that user has chosen to perform with the job
- `deviceName.upgStatus`- a serialized file created on job completion for Retry and Undo options.
- `PostOperation.txt` used for all jobs scheduled through UI.
- SwOperation.txt indicates Job has been triggered. Absence indicate job has crashed for whatever reasons.
- SummarTable.tab for UI purposes always exists for executed job.
- _Config_snap contains the changes that are performed by Software Management on the original configuration.
- HostName_telnet.log for some device types only.

Q. Which modem cards does Software Management support?
A. Software Management upgrades Modem ISDN channel aggregation (MICA) and Microcom 56K modems.

Q. Which devices and software versions get support for the modem upgrades?
A. Support is available for Modem ISDN channel aggregation (MICA) portware upgrades on:
   - Cisco AS5200 that runs Cisco IOS Software Release 11.3(2)T or later and Bootldr version 11.2(11)P or later.
   - Cisco AS5300 that runs Cisco IOS Software Release 11.2(9)XA, 11.3(2)T, or later.
   - Cisco 3640 that runs Cisco IOS Software Release 11.2(12)P, 11.3(2)T, or later.
   Support is available for Microcom firmware upgrades on:
   - AS5200 that runs Cisco IOS Software Release 11.2(10a)P or later.
   - AS5300 that runs Cisco IOS Software Release 11.1(14)AA, 11.2(7a)P, or later.

Note: Cisco AS5800 devices also have modems. However, the modem microcode for these devices is bundled with the system software only and receives upgrades as part of the system software upgrade.

Q. Which formats of Microcom firmware images does Software Management support?
A. The Microcom firmware for 56K modems is available in two formats:
   - Controller firmware and the Digital Signal Processor (DSP) code as two files, for example, mcom-modem-fw-xx.bin and mcom-modem-dsp-xx.bin.
   - A combination of firmware and the DSP code in a single format, for example, mcom-modem-code-xx.bin.

The Cisco AS5300 supports only the image combination. If the Cisco AS5200 runs a Cisco IOS Software release later than Cisco IOS Software Release 11.2(10)P, the AS5200 supports only the combination file format.

Software Management supports only the combination format files (for example, mcom-modem-code-xx.bin). Software Management does not support separate firmware and DSP code files. You cannot import the files to the software library.
Q. Which format of Modem ISDN channel aggregation (MICA) portware do Cisco 3600 devices support?
A. The 3640 digital modem network modules can run two types of modem microcode.
   - 3600-Specific Modem Microcode File—This file has a 3600-specific header and should have the characters c3600-mica in the file name. Software Management does not support such files.
   - Cisco AS5300 Modem Microcode File—In Cisco IOS Software Release 11.2(12)P, 11.3(2)T, and later, the 3640 supports the AS5300 microcode files directly and the 3600-specific microcode files.

   The AS5300 microcode files have Executable and Linking Format headers that contain the version and other information about the image file. Even though the microcode file formats differ between the 3600 and the AS5300, the actual microcode that downloads to the MICA modems is the same.

   Software Management supports only AS5300 format files. Therefore, the earliest Cisco IOS Software release that the 3640 supports is Cisco IOS Software Release 11.2(12)P.

Q. Why does the Undo option not receive support for modem upgrades?
A. To support the Undo option, Software Management must determine the version of software that runs and identify the image file on the device that corresponds. The image file must be present in the library or available on Cisco.com.

   In the case of modem upgrades, Software Management cannot precisely determine the current software version on the modems in all cases. Moreover, different modems can run different software versions, which makes the undo process difficult to support.

Q. What connection mechanism does Software Management use for modem upgrades?
A. Software Management uses Simple Network Management Protocol (SNMP) to initiate the modem image file transfer to the device Flash. After Software Management copies the image to Flash, Software Management uses the Telnet interface to the device to run a command line interface (CLI) command that downloads the code to the modems. (The command is `copy flash modem`.)

Q. Does Software Management erase Flash for modem upgrades if there is not enough free space on Flash?
A. Yes, if the target Flash card does not have enough free space for the store of the new modem image, Software Management erases the target Flash. Software Management does not erase the Flash card if:
   - The upgrade of the system software does not occur within the same job as the modem upgrade.
   - The target Flash partition for the modem upgrade contains the current system software image.

   Instead, Software Management prevents the modem upgrade on that Flash partition. On the Cisco AS5200, the Bootflash card stores modem images, which can contain the bootloader image that currently runs.

   If there is not enough free space to contain the new modem image, Software Management erases the Bootflash card. Back up and restore bootloader images in the case that an erase of the Bootflash is necessary for the upgrade of the modem image. Software Management issues a verification warning if Software Management needs to erase the Bootflash.

Q. What is CIP?
A. CIP stands for Channel Interface Processor card. This interface card allows you to connect the Cisco 7000 router to IBM or IBM-compatible mainframes.
Q. Which devices support the Channel Interface Processor (CIP) microcode upgrade? What is the minimum software version necessary?
A. Software Management supports CIP upgrades on Cisco 7000 and 7500 routers that run Cisco IOS Software Release 11.1(1) or later.

Q. What is the minimum Channel Interface Processor (CIP) version that Software Management supports?
A. Software Management supports CIP version 22.0 at minimum.

Q. How can you import Channel Interface Processor (CIP) images to the Software Management library?
A. The Add Images function (Configuration > Tools > Software Image Management > Software Repository > Add) does not support the import of CIP microcode images from Cisco.com.
   a. You first must download the images to the file system on the LMS server.
   b. Then, choose Add option with source as File System to import them to the software repository.
      Software Management does not recommend the download of CIP microcode directly from Cisco.com for an upgrade.
   c. Populate the software Repository with modem images before you run the Distribute Images function.

Q. Is there support for the Undo option for Channel Interface Processor (CIP) upgrades?
A. No, there is no support for the Undo option for CIP upgrades.

Q. What connection mechanism does Software Management use to upgrade Channel Interface Processor (CIP)?
A. Software Management uses the Telnet interface to the device to copy the CIP image to the Flash. Software Management uses TFTP (via Simple Network Management Protocol [SNMP]) for the configuration upgrade to add the boot command to load CIP microcode.

Q. Does Software Management change the configuration file for the Channel Interface Processor (CIP) upgrade?
A. To load the new CIP microcode, the CIP upgrade process adds these configuration commands:
   ```
   microcode cip flash new_cip_image_name
   microcode reload
   ```

Q. Does Software Management supports CIP2?
A. Yes, Software Management supports CIP2 images for CIP supported device types.

Q. In which order does Software Management upgrade modules on a Cisco Catalyst 5500/5000 device?
A. Software Management upgrades the Supervisor Engine module on the device before other modules. Software Management upgrades the remainder of the modules in slot-number order. For example, Software Management upgrades the module on Slot 3 before Slot 5.
Q. Does the Supervisor Engine card reboot after the upgrade of all modules?

A. If you elect to reboot devices immediately after the upgrade of software, Software Management reloads the Supervisor Engine card. The reload of the card results in the reload of all modules, before the upgrade of software on other intelligent modules. This process supports instances in which the new module requires a newer version of Supervisor Engine software.

If you choose not to reboot the device after the download of software, you then must reload the Supervisor Engine module manually. You also should consider that software that you have newly loaded on a module may require new Supervisor Engine software.

If a new Supervisor Engine software is necessary, you should reload the Supervisor Engine module before you load the new software to the other intelligent modules (such as ATM, FDDI, and Token Ring).

For example, you may download 3.1(1) FDDI software and 4.1(1) Supervisor Engine software in a single job. The 3.1(1) FDDI software may require 4.1(1) Supervisor Engine software. Then, you must reset the Supervisor Engine module before you can upgrade the FDDI software. In such cases, you must have already chosen the Reboot Immediately option.

Q. Does Software Management determine if the newly deployed Supervisor Engine software or module software is compatible with the module types (or module hardware versions)?

A. Software Management does not verify whether the newly deployed Supervisor Engine software supports all modules that are available on the chassis.

Usually, with the upgrade of Supervisor Engine software to a newer release, the software provides backward compatibility for all the modules that exist on the chassis. However, you should check the release notes of the Supervisor Engine software or module software to be sure that the software versions are compatible.

Q. Does Software Management support the upgrade of software on redundant Supervisor Engine card-based systems?

A. The redundant architecture of Cisco Catalyst devices ensures that when the device reboots after a software upgrade, the redundant Supervisor Engine automatically synchronizes all the data from the primary Supervisor Engine. No special processes are necessary.

Q. Does Software Management update the configuration file on Cisco Catalyst 5500/5000 devices during the software upgrade?

A. Software Management updates the configuration file on Catalyst 5500/5000 devices only when the device has a Supervisor Engine III card. Software Management updates the boot system commands and the config register value if necessary.

For Supervisor Engine I and II and other module upgrades, Software Management does not update the configuration file on the device. Instead, Software Management uses CISCO-STACK-MIB and TFTP to download the configuration file. Before Software Management changes the configuration file on the device, Software Management backs up the file to the Job Schedule directory.

The example below illustrates the Software Management update of the configuration file. Assume that a Supervisor Engine III card runs 3.1(1) software. Also, assume that the software image file is on slot0 with the name cat5000-sup3.3-1-1.bin.

The configuration file boot system commands before the upgrade are:

```
set boot system flash slot0:cat5000-sup3.3-1-1.bin
```
Software Management has upgraded the software to 4.1(2). The new software image is on the same Flash card as cat5000-sup3-4-1-2.bin. Software Management then performs these configuration updates:

```
clear all boot system all
```
This removes all boot system commands on the device.

```
set boot system flash slot0:cat5000-sup3.4-1-2.bin
set boot system flash slot0:cat5000-sup3.3-1-1.bin
```

The update modifies the BOOT environment variable on the Supervisor Engine III card. You can display the environment values on the device if you issue the `show boot` command from the Supervisor Engine command-line interface (CLI).

The config register update occurs only if the least significant four bits of the config register are not all set to “1”.

For example, if the current config register value is 0x10F (with the least significant four bits all 1s), Software Management requires no change to the config register. If the current config register value is, for example, 0x111 or 0x11A, Software Management modifies the config register to 0x11F. The action generates this command:

```
set boot config-register 0x11F
```

Q. Does Software Management determine if the Supervisor Engine has the minimum required RAM to run a new image?

A. Software Management uses the Minimum Required RAM field for the Supervisor Engine software image. You can set this field when you import the image into the library. If you do not input a value in this field, Software Management uses this matrix to determine the RAM requirement:

<table>
<thead>
<tr>
<th>Image Type Software Version RAM Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>I, II sup &lt; 2.1(1) 4 MB</td>
</tr>
<tr>
<td>I, II sup &gt; = 2.1(1) &amp; &lt; 3.1(1) 8 MB</td>
</tr>
<tr>
<td>I, II sup8 &gt; = 3.1(1) &amp; &lt; 4.1(1) 8 MB (8 MB RAM image)</td>
</tr>
<tr>
<td>I, II sup &gt; = 3.1(1) &amp; &lt; 4.1(1) 16 MB</td>
</tr>
<tr>
<td>I, II sup &gt; = 4.1(1) 16 MB</td>
</tr>
<tr>
<td>III sup3 &gt; = 3.1(1) 32 MB</td>
</tr>
</tbody>
</table>

Images that are 8 MB RAM are available in 3.1 and 3.2 software releases only for Supervisor Engine I and II cards.

Software Management tries to use CISCO-MEMORY-POOL MIB to determine the available memory on a device. The MIB is implemented from 4.1(1) Supervisor Engine software (on all different Supervisor Engine card types—I, II, and III).

- If a device runs the software that implements this MIB, Software Management performs a memory check between the image requirement and the size of DRAM that is on the device.
- If the device does not have enough RAM to run the image, Software Management generates a verification warning.
- If the current software on the device is earlier than 4.1, Software Management generates a generic verification warning about memory requirements.
Q. Are there restrictions on the downgrade of the software on the Supervisor Engine card and other modules?
A. You can downgrade Supervisor Engine card software to version 4.1(1) or later.

For example, if a Supervisor Engine card runs 4.2(1) software, you can downgrade the software to 4.1(2) or 4.1(1). However, you cannot downgrade the same Supervisor Engine card to 3.2(1b). If a Supervisor Engine card runs 3.2(2), you cannot downgrade the software to 3.1(1) or 2.4(1).

There are no restrictions for the downgrade of software on other modules, such as ATM, FDDI, and Token Ring. However, you should check the release notes of new software before you attempt downgrades on modules.

Q. Do you need to reconfigure the device when you downgrade the Supervisor Engine software?
A. When you downgrade Supervisor Engine software, parts of the configuration may be lost. You must check the configuration file and reconfigure as necessary. Use the backed up Software Management configuration file from the Job Schedule directory as a reference, or use the backed up configuration file from the Config Archive.

Q. In the 4.1(1) software release and later, Supervisor Engine III cards allow the storage of configuration files on Flash cards. Does Software Management preserve the backed up configuration files on Flash during a software upgrade?
A. Software Management erases a Flash card on Supervisor Engine III if the free space on the Flash card cannot store the target software image. Software Management does not erase files of sizes that are less than 1 MB during software upgrades. Since configuration files generally do not exceed 1 MB, Software Management does not erase these files.

Q. Does Software Management allow you to upgrade epsboot images on Token Ring cards on Cisco Catalyst 5500/5000 devices?
A. Software Management does not allow upgrades of epsboot images on Catalyst 5500/5000 devices. An epsboot string in the file names can identify epsboot images. Epsboot upgrades are not often necessary. You can perform the upgrades with the Supervisor Engine card command-line interface (CLI).

Q. Why does the Add Image to Repository (Source: Cisco.com) task not display Token Ring LAN Emulation (LANE) or Permanent Virtual Circuit (PVC)-only ATM software images?
A. The Add Image to Repository (Source: Cisco.com) function in Software Management displays software images for only a subset of these ATM modules:
   - WS-X5153
   - WS-X5154
   - WS-X5155
   - WS-X5156
   - WS-X5157
   - WS-X5158

Software images for these modules have version numbers that range from 2.2 to 3.2(8).
The WS-X5153 to WS-X5158 modules can run:
- ATM LANE
- PVC Traffic Shaping
- Token Ring LANE software images

Software Management also supports the upgrade of software on these modules:
- WS-X5161
- WS-X5162
- WS-X5165
- WS-X5167
- WS-X5168

However, no mechanism exists to import the images from Cisco.com directly into the Software Management software library for these modules. The software images that run on the modules support LANE on Ethernet, Token Ring, and PVC traffic shaping.

You must download the software images for these modules directly from Cisco.com. Then, import the images into the library with the Add Image to Repository function.

Software Management does not support software management on WS-X5166 modules.

Q. How do you identify software image files for each of the ATM modules that Software Management does support? What are the file-name conventions on Cisco.com?

A. ATM software image file names and version numbers determine on which modules the software image can run and identify the features that receive support. This table provides details on version numbers and file-name conventions.

Q. How can I make the Image Recommendation faster?

A. If you select Cisco.com image recommendation, try to limit the images by filtering.

<table>
<thead>
<tr>
<th>Module IDs</th>
<th>Image Feature/Version</th>
<th>Image File Name Format (Example)</th>
<th>Version to Input in Software Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>WS-X5153 to WS-X5158</td>
<td>Ethernet LAN Emulation (LANE) 2.2 to 3.2(7)</td>
<td>cat5000-atm.ver_number 3.2(7) cat5000-atm.3-2-7.bin</td>
<td>2.2-3.2(7)</td>
</tr>
<tr>
<td>WS-X5153 to WS-X5158</td>
<td>Ethernet LANE 3.2(8)</td>
<td>c5atm-wblane.Cisco_IOS_Software_rel_number c5atm-wblane.113-2.5.WA4.4m.bin</td>
<td>3.2(8)</td>
</tr>
<tr>
<td>WS-X5153 to WS-X5158</td>
<td>Token Ring LANE 70.x</td>
<td>c5k-trlane.ver_number c5k-trlane.70-1-1.bin</td>
<td>70.x</td>
</tr>
<tr>
<td>WS-X5153 to WS-X5158</td>
<td>Permanent Virtual Circuit (PVC) Traffic Shaping 50.x</td>
<td>cat5000-atm-pvcshape.ver_number cat5000-atm-pvcshape.50-1-1.bin</td>
<td>50.x</td>
</tr>
</tbody>
</table>
ATM version-number conventions differ for different classes of ATM images. PVC, Token Ring LANE, and Truckee types of ATM images have unique version-number conventions. Software Management recognizes the version numbers that appear in the last column of the table. The input of an incompatible version number results in upgrade job failures.

ATM software release notes give the original version number of the image as well as a version number that is close to the Software Management version-number scheme. Check the release notes for version-number schemes.

Q. Why do the software version numbers that the `show module` command output displays from the Supervisor Engine command-line interface (CLI) and the version numbers that Software Management uses fail to match in some cases?

A. ATM module software for Cisco Catalyst devices uses Cisco IOS Software code as a basis. The software release for Truckee ATM modules as well as ATM software releases 3.2(7) and later use the Cisco IOS Software version-number scheme.

Software Management does not recognize the Cisco IOS Software version-number scheme for Catalyst ATM software images. Use the simple version-number scheme that appears in the table in this document. (See the Version to Input in Software Management column.)

Output of the `show module` command of the Supervisor Engine CLI and the `show` command on the ATM module can display different versions. If the software that runs on the Supervisor Engine is earlier than 4.1, the Supervisor Engine software does not recognize the Cisco IOS Software version-number scheme of ATM images.

Therefore, the Supervisor Engine displays a different version number than the output of the `show version` command on the ATM module.

Q. Does Software Management recommend the right ATM image for your ATM module type?

A. Yes, Software Management distinguishes different flavours of ATM images and recommends images based on current class of ATM card on the device.
Q. Should you use special images with Software Management for Cisco Catalyst 2900XL/3500XL devices?

A. The 2900XL/3500XL devices have three images:

- Regular Cisco IOS Software image.
- A TAR format HTML image that contains files for Visual Switch Manager.
- A TAR format image that contains both of these images.

Software Management uses the TAR format image that contains the Cisco IOS Software and HTML image. This image posts on Cisco.com, as do other images for 2900XL/3500XL.

When you use LMS for software upgrades, you should use images with the description Enterprise-IOS and HTML-Use. When you use Add Image to Repository from Cisco.com/Slam Dunk, you are able to see only these images.

Q. How does Software Management handle image import functionality of TAR and bin types of images for Catalyst 2900XL/3500XL devices?

A. For 2900/3500 device types Both .tar format and .bin format images are supported as system software. Network Synchronization option (Add image from network as source) will not be able import tar images because when the image downloads to the switch, the image distributes as small individual files on the Flash in different directories.

The switch command-line interface (CLI) does not provide commands to combine all the files and make a new TAR file that Software Management can then upload. Whereas the .bin image can be imported from the device as well as from the Network Synchronization option.

Q. Why do software upgrades take longer on Cisco Catalyst 2900XL/3500XL devices?

A. Software Management uses command-line interface (CLI) to download software to 2900XL/3500XL devices. Because the software on these devices has many HTML/gif files on the Flash, the software must first delete all the files and then proceed with the new software download. Deletion of the images takes time, which is why software downloads to devices can take up to 20 minutes.

Q. How do you upgrade Route Switch Module (RSM) and LightStream 1010 (LS1010) module software on Cisco Catalyst 5500/5000 and 6500/6000 series switches?

A. The RSM (also called the VLAN router) on a Catalyst 5500/5000 or 6500/6000 switch and the LS1010 module on a Catalyst 5500/5000 switch run Cisco IOS Software. RSMs and LS1010 modules have individual IP addresses and Simple Network Management Protocol (SNMP) agents. The LMS Inventory manages these modules as separate devices.

You can find the IP address of the RSM if you look at the Detailed Inventory report of the Catalyst 5500/5000 and 6500/6000 device that has the RSM on the chassis. The Module IP Address column in the Stack Modules section shows the IP addresses of all modules on the chassis.

If you do not find the addition of RSM or LS1010 to Inventory, you must first add the module as a device to Inventory before you attempt Software Management functions. Software Management functions that run on Cisco IOS devices also can run on an RSM or an LS1010.
Q. Why does the Distribute Images task show all the images from Cisco.com for LightStream 1010 (LS1010) and Cisco Catalyst 8500 devices, even though you have configured Cisco.com filtering?

A. Although LS1010 and the 8500 devices run Cisco IOS Software images, differences exist in the means of image release. The images do not follow the Cisco IOS Software image releases, such as general deployment (GD), limited deployment (LD), and early deployment (ED). Therefore, Software Management cannot effectively filter LS1010-type and 8500-type images.

Q. What is the minimum version that Cisco 700 series ISDN routers support?

A. For Cisco 760 Series ISDN routers, Software Management requires a minimum software version of 3.2(4) on the device. For Cisco 770 Series ISDN routers, the minimum version necessary is 4.0(1).

Q. What connection mechanism does Software Management use for Cisco 700 series upgrades?

A. Software Management uses the Telnet interface to the device to copy the 700 series image to the Flash. Software Management uses TFTP protocol. The LMS workstation is the TFTP client, and the device is the TFTP server.

Q. Both Cisco 760 and 770 series devices run the same image. Why do you see only some images with versions later than 4.0(1) for 770 series devices but see all images for 760 series devices?

A. When you load an image with a version earlier than 4.0(1) onto a 770 series device, the sysObjectID box changes to something other than Cisco-assigned. Also, LMS identifies the device as a non-Cisco device. Therefore, Software Management does not list images with versions earlier than 4.0(1) for Cisco 770 series upgrades.

Q. Why do you not see the option to reboot the device later on the Job Control page for Cisco 700 series routers?

A. There is no option to reboot the device later because 700 series routers reboot at the time of the new image download.

Q. Why do you not see the option to modify the boot commands on the Job Control page for Cisco 700 series routers?

A. Only one image at a time can appear on the 700 series devices, which means the boot command does not apply to these devices.

Q. Why does Software Management report download failures for some images even though the device runs the new image after the job completes?

A. Some new Cisco 700 series images use nonstandard name convention or nonstandard versions. Software Management incorrectly parses the version number from file names of those images. After the download of the new image, the device reboots.

Software Management retrieves the new image version from the device and compares that with the version that Software Management parsed. The two versions do not match. As a result, the software download appears to have failed, which generates as an error.

This problem occurs with c760-in.b-US.42-3.5.bin and c760-in.b-US.43.1.bin images for all countries.

You can resolve this issue by entering the correct version number when you import the image from the file system.

For example, for c760-in.b-US.42-3.5.bin, enter 4.2(3.5). For c760-in.b-US.43.1.bin, enter 4.3(1) as the version number.
Q. In which order does Software Management upgrade modules on a Catalyst 5000 device?
A. Software Management upgrades the Supervisor module on the device before other modules. The remainders of the modules are upgraded in the order of their slot number. For example, the module on Slot #3 is upgraded before Slot #5.

Q. Does Software Management check to see that the newly deployed Supervisor software or module software is compatible with the module types (or module hardware versions)?
A. Software Management does not verify whether the newly deployed Supervisor software supports all modules that are available on the chassis.

Usually, when Supervisor software is upgraded to a newer release, the software provides backward compatibility for all the modules that exist on the chassis. Users are encouraged to check the release notes of the Supervisor software or module software to make sure that the software versions are compatible.

Q. Does Software Management support upgrading software on redundant Supervisor card-based systems?
A. The redundant architecture of Catalyst devices ensures that when the device reboots after a software upgrade, the redundant Supervisor automatically synchronizes all the data from the primary Supervisor. No special processing is required.

Q. What is the purpose of user scripts?
A. User-supplied scripts are run before and after each device upgrade. They can be used for pre- and post validation checks. For example,
- The pre-upgrade script can check whether the device is accessible.
- The pre-upgrade script can check whether any users are connected to the access server. If the script finds that some users are connected, it can decide whether to disable the connections before proceeding with the upgrade.
- The post-upgrade script can check whether the device has upgraded successfully or not. Depending on the return value, Software Management either halts or continues with the rest of the upgrade job.

Q. What if the user script crashes? Will it crash the Software Management job also?
A. No, crashing of the script will not stop the Software Management job. Software Management executes the script in a different process space so the script crashing will not crash the Software Management job. However, Software Management will assume the script has failed.

Q. When a Software Management job is scheduled, how is the baseline determined? When I distribute a job, is an automatic backup performed?
A. There are two options that import images from the network to the Software Repository:
- Baseline tasks
- Synchronization

The baseline task (Configuration > Tools > Software Image Management > Software Repository > Add > Network) should be done only once as a part of the initial setup. This imports the images running on the network to your Repository.

To keep the Repository synchronized with any new images and changes caused by upgrades from sources other than Software Management, schedule a synchronization job to run periodically at appropriate intervals.
When this synchronization job runs, it looks for differences between the Repository and the network and allows any new images to be imported. During job distribution, Software Management backs up the current running image only if the option, Use current running image as tftp fallback image was selected when the job was created.

Q. Can I set up a periodic download of Software Management images from Cisco.com?
A. No. However, you can schedule a one-time import from Cisco.com to occur at a later time. Software Management does not allow you to automatically import images from Cisco.com to the Repository based upon your preferences.

Q. Is browser timeout something I should consider when downloading?
A. The Image Import option from Cisco.com and other devices can be done on a scheduled basis. Since this process runs as a background task on the server, the browser is not involved. However, when an Immediate Import job runs, it is performed as a foreground task, and the browser can still timeout.

Q. What are crypto images?
A. Crypto images are software images that use 56-bit Data Encryption Standard (DES) (or higher) encryption, and are subjected to export regulations. You must be a registered Cisco.com user, and be eligible and authorized to download such images.

Q. How much temporary space is required during image distribution?
A. The amount of free space that is required depends upon the image file size and the number of devices that are being upgraded simultaneously. If the tftp fallback option is set, additional free disk space is required to keep the current image in the tftpboot directory. Disk space is used both in the tftpboot and temp directories.

Q. At what time will the images directory get created during the process of obtaining images from a device? Does this happen during the initial step?
A. The software images directory gets created at the time of importing an image to the Repository; however, this should be transparent to you.

Q. How can I speed up Image Recommendation?
A. If you include Cisco.com for Image Recommendation, try to limit the images by filtering (Admin > Network > Software Image Management > View/Edit Preferences).

Q. When a job is rejected, can it be edited or should I resubmit?
A. No. You cannot edit or retry the rejected job. You should schedule a new job.

Q. Can different group members edit jobs? What are the restrictions?
A. The only job attribute that can be edited is the schedule time for non-Job Approval jobs. Any user who has the Network Administrator role defined can edit jobs or create new jobs; however, in the Job Approval model, the jobs can only be approved by users who are in the approver list specified during the creation of the job.
Q. What is the role of the registry files?
A. Software Management manipulates the Windows registry to automatically manage remote authentication during the rcp transfers on Windows. The following registry parameters are important for rcp service on Windows:

- **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\crmrsh\Parameters\DEBUG**
  Dictates the amount of debug information written in the Windows event log.
  (Default = 0, Maximum = 0xff)

- **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\crmrsh\Parameters\rhosts**
  Contains the list of authenticated hosts that can run remote commands on this machine. This list is automatically managed by Software Management.

- **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\crmrsh\Parameters\rusers**
  Contains the list of authenticated remote users that can run remote commands on this machine. This list is automatically managed by Software Management.

- **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\crmrsh\Parameters\NoRuserCheck**
  If set to 1, the remote user authentication is skipped or, in other words, any remote user from authenticated hosts can run commands on this machine. (Default = 0)

- **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\crmrsh\Parameters\NoRhostCheck**
  If set to 1, the remote host authentication is skipped or, in other words, commands can be run on this machine from any remote machine.
  (Default = 0)

Q. How do I upgrade Network Analysis Module (NAM) using Software Management?
A. To upgrade NAM using Software Management:

- Ensure that the passwords for NAM’s application and maintenance modes are the same.
  This is because Software Management takes the password information from Inventory.
  However, Inventory requires the application mode password to manage the device, and Software Management requires the maintenance mode password to upgrade the device. Therefore, the passwords for NAM’s application and maintenance modes should be the same.

- For a NAM card present in a Catalyst 6000 device running CatOS, ensure that you set auto logout to a value that is high enough to allow the copying of the new image.
  This is because a NAM image is usually very large (nearly 65 MB), and it may take between 1 to 2 hours to copy this image during Software Management upgrade. We recommend that you set the auto logout to 0 to ensure that there is no auto logout while the image is being copied.
  To set the auto logout value, use the CLI command, `set logout 0`.
  For a NAM card present in a Catalyst 6000 device running IOS, ensure that you set exec timeout to a value that is high enough to allow the copying of the new image. We recommend that you set the exec timeout value to 0 (`exec-timeout 0 0`) on all the vty lines.

- Ensure that the htdocs directory under CSCOpx has enough space to stage the NAM image.
  During the NAM upgrade, Software Management first copies the NAM image from the NMSROOT/files/sw_images directory (On Solaris and Soft Appliance) or NMSROOT/files\sw_images (On Windows), to the NMSROOT/CSCOpx/htdocs/swimtemp (On Solaris and Soft Appliance) or NMSROOT\CSCOpx\htdocs\swimtempdirectory (On Windows), and then copies the NAM image to the NAM card, using HTTP.
- Ensure that NAM is added with the correct Local User (root) and its password.
- Ensure that NAM is added with the correct SNMP read/write community strings.
- Ensure that the switch, which contains NAM, is added with the correct attributes.

Q. Can I change the job scheduled time?
A. The job scheduled time can be modified only for pending jobs that do not require approval. For a job that requires approval, you must cancel the job and retry or recreate the job.

Q. How does Software Management handle the job status for an abnormally terminated job?
A. Software Management checks the last modification time of the job results file for each running job when the Browse Job Status screen is displayed. If the results file has not been modified for the last six hours, Software Management assumes that the job was terminated abnormally (server reboot is a probable cause for the termination), and the job status is changed to Error.

Q. How does Software Management handle the job status of a pending job whose scheduled time has passed?
A. Software Management checks the scheduled time for each pending job when the Browse Job Status screen is displayed. If the current time is an hour past the scheduled time for starting the job, (lack of operating system resources is a probable cause for the job not running at the scheduled time), the job status is changed to Error.

Q. Why are some files left in the Software Management folder after Software Management has been uninstalled?
A. When uninstalled, Software Management does not remove the software images directory from the LMS server. The software images directory contains subdirectories for storing software images for various device families.

Q. How can I enable or disable the SSH to Telnet fallback for Software Management jobs?
A. To enable or disable SSH to Telnet fallback for Software Management jobs:

Step 1 Go to Admin > Network > Software Image Management > View/Edit Preferences.
Under the Distribution pane, there is a checkbox option, Use SSH for software image upgrade and software image import through CLI (with fallback to TELNET).

Step 2 Do either of the following:
- Check this option, to enable the use of SSH for software image upgrade and software image import through CLI along with fallback to Telnet.
- Uncheck this option, to disable the use of SSH for software image upgrade and software image import through CLI along with fallback to Telnet.

Step 3 Click Apply to save your changes.
Q. How can I export the images from SWIM repository to a local drive or a file system mounted to the LMS server?
A. To export the image from Software Repository to a local drive or a file system:

Step 1 Select Configuration > Tools > Software Image Management > Software Repository.
The Software Repository Management dialog box appears.

Step 2 Select images that you want to export, then click Export.
A confirmation message appears, The selected images will be exported.

Step 3 Click OK.
The Select directory to export window appears.

Step 4 Click on Browse to select a directory to which you want to export the selected images.
The Server Side File Browser dialog box appears.

Step 5 Choose the required directory and click OK.
The Image Directory field in the Select directory to export window displays the directory location which you had selected.

Step 6 Click Next
A progress bar appears indicating the progress of the export of images.
The Export Images Summary Report appears after completion of the export of the images with these details:
- Number of Selected Images
- Target Directory
- Summary

Step 7 Click Finish.
You have successfully exported the images to the selected directory.

Q. Does Flash get erased if there is no sufficient space for Patch Distribution?
A. No. Patch Distribution requires sufficient amount of free space in Flash and so it cannot be erased.

Q. When I try to copy images, the Image Copy option fails indicating that the External TFTP server is inaccessible.
A. If you come across this error, try any of these:
- Check whether TFTP service is running or stopped in the External TFTP server. If stopped, start it.
- Check if any security agent is preventing the application. If so register the application with security agent or disable the security agent.

Q. Can I specify the name of my input file as imagenames.txt when I try to export images using the Software Management (SWIM) CLI exportimages command?
A. Do not name your input files similar to arguments.
For example, if you specify
```
cwcli swim exportimages -input imagenames.txt -u admin -p admin
```
the following error message will be displayed

```
Invalid argument: imagenames
```

For example, you can specify the input filename as sample.txt

You can enter the following argument in your sample.txt

```
-imagenames image1,image2,image3,image4...........
```

So the `exportimages` command with input file will be:

```
cwcli swim exportimages -input sample.txt -u admin -p admin
```

Q. I am getting timeout exception in cmdsvc (command service library) during a device connection/socket establishment. How do I change the default timeout and delays in cmdsvc?

A. You can change the default timeout and delays in cmdsvc using the cmdsvc.properties file available in the following directory: `$NMSROOT/objects/cmf/data`

To change the default timeout and delay values:

1. Go to the directory `$NMSROOT/objects/cmf/data`
2. Open the `cmdsvc.properties` file.
   Various timeout and delay values are listed in the file.
3. Remove the Hash symbol(#) to uncomment a particular timeout or delay value.
4. Remove the existing timeout or delay value.
5. Enter new timeout or delay value.
6. Save the `cmdsvc.properties` file.

---

**Troubleshooting Software Management**

<table>
<thead>
<tr>
<th>Message-ID</th>
<th>Error Message</th>
<th>Probable Cause</th>
<th>Possible Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>SWIM0013</td>
<td>Image Import option not supported for the selected devices</td>
<td>Image Import option is not supported because of device limitations. Check Software Management feature support matrix against the selected device platform.</td>
<td>None.</td>
</tr>
</tbody>
</table>
| SWIM0014   | No images to import into library from the selected devices | Either:  
- There are no images on the Flash  
Or  
- Cannot get Flash information from inventory. | Check the Inventory Detailed Device Report to ensure that Flash file information exists for the device. If report generation fails, schedule an inventory collection job and redo the Software Management image import job. |
<table>
<thead>
<tr>
<th>Message-ID</th>
<th>Error Message</th>
<th>Probable Cause</th>
<th>Possible Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>SWIM0019</td>
<td>Could not perform Image recommendation for the selected devices because of insufficient data.</td>
<td>Could not fetch Image information from the Inventory database.</td>
<td>Check the Inventory Detailed Device Report to ensure that Inventory data exists for the device. If report generation fails, schedule an inventory collection job and perform Software Management recommendation.</td>
</tr>
<tr>
<td>SWIM0020</td>
<td>Image Import option not supported for the selected devices</td>
<td>Image Import option is not supported because of device limitations.</td>
<td>None.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Check Software Management feature support matrix against the selected device platform.</td>
<td></td>
</tr>
<tr>
<td>SWIM0021</td>
<td>Error encountered while parsing Job Data.</td>
<td>Either the Job Data file could not be located or the data for Image Upgrade was not provided.</td>
<td>Check whether you have access permissions to Job Directory, or re-create the job. If the problem persists, send all log files under job directory to TAC.</td>
</tr>
<tr>
<td>SWIM0027</td>
<td>Staging of the Image on the Remote Stage Device failed.</td>
<td>Image Copy to Remote Stage device failed because of SNMP Agent problems during transfer.</td>
<td>Check for any known bugs against the Image running on Remote Stage, or choose a different device. If the problem persists, send all log files under job directory to TAC.</td>
</tr>
<tr>
<td>SWIM0034</td>
<td>Device reboot failed.</td>
<td>Either:</td>
<td>Check whether the \texttt{snmp-server shutdown} command is configured on the device. You can do any of the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>\begin{itemize} \item The device configuration for reboot is missing \item Or \item The image downloaded onto the device is not suitable for the device to come up. \end{itemize}</td>
<td>\begin{itemize} \item Configure the devices and re-schedule the jobs. \item Use NetConfig reload template to reload the devices. \item Reload manually if you have only a few set of devices. \end{itemize}</td>
</tr>
<tr>
<td>SWIM0036</td>
<td>Image addition to Software Library failed</td>
<td>Either an invalid image was imported into library or the image is corrupted.</td>
<td>Check whether the image is downloaded completely in the directory</td>
</tr>
<tr>
<td>SWIM0056</td>
<td>Invalid Remote Stage device selected.</td>
<td>Cannot use this device as Remote stage because of device limitations.</td>
<td>Check the Help documentation to see which devices can be used as Remote Stage.</td>
</tr>
<tr>
<td>SWIM0067</td>
<td>System software analysis failed</td>
<td>This is an unexpected runtime error.</td>
<td>contact Cisco TAC.</td>
</tr>
<tr>
<td>Message-ID</td>
<td>Error Message</td>
<td>Probable Cause</td>
<td>Possible Action</td>
</tr>
<tr>
<td>------------</td>
<td>-------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SWIM0089</td>
<td>Could not perform Image Import from Cisco.com on the selected devices.</td>
<td>Add Image from Cisco.com not supported for the device. This is because Cisco.com could not find the device platform in the supported list.</td>
<td>Check the Software Management feature support matrix against the selected devices platform.</td>
</tr>
<tr>
<td>SWIM0092</td>
<td>Could not perform Image Import from Cisco.com on the selected devices because of insufficient data.</td>
<td>The device information needed to fetch images from Cisco.com does not exist in Inventory.</td>
<td>Check the Inventory Detailed Device Report to ensure that Chassis information exists for the device. If Chassis information is missing, schedule an inventory collection job and retry the import workflow.</td>
</tr>
<tr>
<td>SWIM0093</td>
<td>Could not get Image information from Cisco.com</td>
<td>Could not connect to Cisco.com from CiscoWorks Server either because of incorrect Cisco.com credentials or missing proxy configuration.</td>
<td>Check whether Cisco.com credentials are correct. If they are correct, check whether the proxy server is configured with right proxy credentials. To configure proxy, go to: CiscoWorks Home page &gt; Server &gt; Security &gt; Proxy Server Setup.</td>
</tr>
<tr>
<td>SWIM0101</td>
<td>The current version of the image on the device is different from the earlier version of the image.</td>
<td>This message is displayed when you retry a failed distribution job. This mainly happens when other jobs change the current running image of this device before scheduling the retry.</td>
<td>Try a new distribution job instead of retrying.</td>
</tr>
<tr>
<td>SWIM0118</td>
<td>Software Management application could not verify the inputs since there was no running image information. The device package may not have been installed. You can install it now and retry the task or you can install it before running the job. However, the results may not be accurate.</td>
<td>Advanced Distribution Flow: Either: • The selected device is not yet deployed in the network (pre-provisioned device) Or • It is still not supported by LMS.</td>
<td>Schedule the distribution job for a future date when the device is deployed Otherwise, the device package for this unsupported device will be installed and available in the LMS server.</td>
</tr>
<tr>
<td>Message-ID</td>
<td>Error Message</td>
<td>Probable Cause</td>
<td>Possible Action</td>
</tr>
<tr>
<td>------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SWIM0119</td>
<td>Software Management application could not verify the Flash inputs since there was no Flash information available. Edit the expert input file and verify it again. If you do not want to edit the expert input file, you can continue with the task by clicking Next. However, the results may not be accurate.</td>
<td>The selected device does not have any Flash related information. Generally the Flash details are present in the Inventory. You can check the Detailed Device Report to see the Flash details. If there are no Flash details for this device, Software Management will allow the user to schedule a distribution job without verifying the Flash details.</td>
<td>None.</td>
</tr>
<tr>
<td>SWIM0120</td>
<td>Software Management application did not verify the inputs since there was no running image information. If you find that the device package is not installed, install it before running the job. The image distribution will proceed based on the unverified inputs. However, the results may not be accurate.</td>
<td>Advanced Distribution Flow: Either:  - The selected device is not yet deployed in the network (pre-provisioned device) Or  - It is still not supported by LMS.</td>
<td>Schedule the distribution job for a future date when the device is deployed. Otherwise, the device package for this unsupported device will be available and installed in the LMS server.</td>
</tr>
<tr>
<td>SWIM0121</td>
<td>Software Management application did not verify the Flash inputs as there was no Flash information. The image distribution will proceed based on the unverified inputs. However, the results may not be accurate.</td>
<td>The selected device does not have any Flash related information. Generally the Flash details are present in the Inventory. You can check the Detailed Device Report to see the Flash details. If there are no Flash details for this device, Software Management allows a user to schedule a distribution job without verifying the Flash details.</td>
<td>None.</td>
</tr>
</tbody>
</table>
Software Management

<table>
<thead>
<tr>
<th>Message-ID</th>
<th>Error Message</th>
<th>Probable Cause</th>
<th>Possible Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>SWIM0122</td>
<td>Software Management application could not verify the inputs since there was no running image information available.</td>
<td>Either: • The selected device is not yet deployed in the network (pre-provisioned device) Or • It is still not supported by LMS.</td>
<td>Schedule the distribution job for a future date when the device is deployed. Otherwise, the device package for this unsupported device will be available and installed in the LMS server.</td>
</tr>
<tr>
<td>SWIM0123</td>
<td>Software Management application could not verify the inputs since there was no running image information.</td>
<td>Advanced Distribution Flow: The selected device is not yet deployed in the network (pre-provisioned device) or it is not supported by LMS.</td>
<td>Schedule the distribution job for a future date when the device is deployed. Otherwise, the device package for this unsupported device will be available and installed in the LMS server.</td>
</tr>
<tr>
<td>SWIM0125</td>
<td>An unexpected error has occurred. Contact Cisco support and attach the swim_debug.log file.</td>
<td>None.</td>
<td>Please contact Cisco TAC with the UI log available under: Windows: CSCOpx\logs\swim_debug.log Solaris and Soft Appliance: /var/adm/CSCOpx/log/swim_debug.log</td>
</tr>
<tr>
<td>SWIM0126</td>
<td>An unexpected error has occurred. Contact Cisco support and attach the swim_debug.log file.</td>
<td>None.</td>
<td>Please contact Cisco TAC with the UI log available under: Windows: CSCOpx\logs\swim_debug.log Solaris and Soft Appliance: /var/adm/CSCOpx/log/swim_debug.log</td>
</tr>
<tr>
<td>Message-ID</td>
<td>Error Message</td>
<td>Probable Cause</td>
<td>Possible Action</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SWIM0138</td>
<td>Cannot connect to the Job Manager. Check whether the jrm process is running properly. If it is not running, restart it and try scheduling the job again.</td>
<td>None</td>
<td>To check whether jrm is running, run command: pdshow jrm  If jrm is down, restart CiscoWorks.</td>
</tr>
<tr>
<td>SWIM0139</td>
<td>Running image information is not available in Inventory for Remote-Stage device <em>Devicename</em>. Perform Update Inventory and check whether the required Flash data appears in the Detailed Device report. If it appears, retry the job; else, the data is not yet available from the device.</td>
<td>Either: ● The Inventory is not updated Or ● The image device running on the device is not populating the required Flash MIB information.</td>
<td>If data is not available from the device (due to bug in the image), upgrade the device with the higher version image. This higher image populates the Detailed Device report with the required Flash data.</td>
</tr>
<tr>
<td>SWIM0141</td>
<td>There is not enough free space on the repository to store the selected files. Please free up some disk space and retry the job.</td>
<td>Disk space is not sufficient on the server.</td>
<td>Free up some disk space and retry the job.</td>
</tr>
<tr>
<td>SWIM0142</td>
<td>RepositoryException while checking for disk space.</td>
<td>Disk space is not sufficient on the server.</td>
<td>Free up some disk space and retry the job.</td>
</tr>
<tr>
<td>SWIM0146</td>
<td>Could not get active image information. Either the device is not reachable or the sysconfigName OID information is not provided by the device.</td>
<td>A distribution job scheduled using Advanced flow for pre-provisioned devices has failed and you have tried a Retry task on this job. The pre-provisioned devices does not have running images and so this error message is displayed.</td>
<td>Ensure that the device is deployed or the device package for this device is installed before a distribution job is run on this device.</td>
</tr>
<tr>
<td>SWIM1001</td>
<td>The input parameters to the Image Distribution/Image Import/Image Activate are invalid.</td>
<td>You may have used incorrect Device Data for this task.</td>
<td>Check the application log file for more details.</td>
</tr>
<tr>
<td>SWIM1002</td>
<td>An error occurred in staging Image <em>Image Name</em>.</td>
<td>There may not be correct permissions for the image in the software repository or for the directories required for staging.</td>
<td>Retry the Image Upgrade option.</td>
</tr>
<tr>
<td>Message-ID</td>
<td>Error Message</td>
<td>Probable Cause</td>
<td>Possible Action</td>
</tr>
<tr>
<td>------------</td>
<td>-------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SWIM1003</td>
<td>SNMP Agent does not support the required instrumentation to get information about the Flash File system.</td>
<td>The SNMP Agent on the device does not support CISCO-FLASH-MIB/OLD-CISCO-FLASH-MIB.</td>
<td>Check for any known bugs related to these MIBs for the image version running on the device.</td>
</tr>
<tr>
<td>SWIM1004</td>
<td>Cannot get details about the Flash File system on the device.</td>
<td>There may be a faulty implementation of the MIB on the device.</td>
<td>Check the Bug Toolkit application for any known issues on the running image version.</td>
</tr>
<tr>
<td>SWIM1005</td>
<td>Flash Device or Partition does not exist on the device.</td>
<td>Either the Inventory data on the device is stale, or the selected Flash Device or Partition is invalid.</td>
<td>Trigger inventory collection on the device.</td>
</tr>
<tr>
<td>SWIM1006</td>
<td>Flash Partition does not exist on the device.</td>
<td>Either the Inventory data on the device is stale, or the selected Flash Partition is invalid.</td>
<td>Update the inventory collection on the device.</td>
</tr>
<tr>
<td>SWIM1007</td>
<td>You have specified the storage location on the device in an invalid format.</td>
<td>None.</td>
<td>Enter a valid format. For example: <code>moduleNumber\flashPartitionName:partitionNumber:filename</code> In case of Andiamo devices: <code>flashDeviceName://flashPartitionName/filename</code></td>
</tr>
<tr>
<td>SWIM1008</td>
<td>You have specified an invalid format for the destination storage location.</td>
<td>None.</td>
<td>Enter a valid format. For example: <code>moduleNumber\flashPartitionName:partitionNumber:filename</code> In case of Andiamo devices: <code>flashDeviceName://flashPartitionName/filename</code></td>
</tr>
<tr>
<td>SWIM1009</td>
<td>Inventory reported enough space on Flash partition, but the distribution task found that the space is insufficient and requires erasure.</td>
<td>The inventory data may be stale.</td>
<td>Update the inventory for the device and retry the job.</td>
</tr>
<tr>
<td>SWIM1010</td>
<td>The size of the partition selected to copy the image, is less than the image size.</td>
<td>None.</td>
<td>Select another partition to copy the image.</td>
</tr>
<tr>
<td>Message-ID</td>
<td>Error Message</td>
<td>Probable Cause</td>
<td>Possible Action</td>
</tr>
<tr>
<td>------------</td>
<td>-------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SWIM1011</td>
<td>Destination file size on storage location and the source file size are different.</td>
<td>This may be because of a network problem or a bug on the device.</td>
<td>Check the Bug Toolkit application for any known issues on the running image version. If there are no issues, retry the task.</td>
</tr>
<tr>
<td>SWIM1012</td>
<td>The file copied on the destination storage location is invalid.</td>
<td>The File Copy may have failed because of temporary network errors.</td>
<td>Retry the File Copy option.</td>
</tr>
<tr>
<td>SWIM1013</td>
<td>You have specified an invalid Job directory.</td>
<td>The destination directory that has been specified to copy the configuration file from the device is invalid.</td>
<td>Check whether the destination directory exists. If the directory exists, check whether there are write permissions. Also check whether there is enough disk space.</td>
</tr>
<tr>
<td>SWIM1014</td>
<td>Cannot generate configuration changes for Remote Stage option.</td>
<td>None.</td>
<td>Check for file permissions on the Job directory.</td>
</tr>
<tr>
<td>SWIM1015</td>
<td>Cannot generate configuration changes for activating the device.</td>
<td>None.</td>
<td>Check for file permissions on the Job directory.</td>
</tr>
<tr>
<td>SWIM1016</td>
<td>Cannot load new configuration to Remote Stage Device.</td>
<td>None.</td>
<td>Check the Bug Toolkit application for any known issues on the running image version. If there are no issues, retry the task.</td>
</tr>
<tr>
<td>SWIM1017</td>
<td>Cannot fetch configuration file from the device.</td>
<td>None.</td>
<td>Check the Bug Toolkit application for any known issues on the running image version. If there are no issues, retry the task.</td>
</tr>
<tr>
<td>SWIM1018</td>
<td>Cannot upload new configuration to the device during image activation.</td>
<td>None.</td>
<td>Check the Bug Toolkit application for any known issues on the running image version. If there are no issues, retry the task.</td>
</tr>
<tr>
<td>SWIM1019</td>
<td>Cannot reload the device. Device is not responding after the Reload command.</td>
<td>The image upgraded on the device has some issues.</td>
<td>Check the Bug Toolkit application for any known issues on the upgraded image version. Manually restore the device through the console.</td>
</tr>
<tr>
<td>SWIM1020</td>
<td>The device is not running the new image.</td>
<td>This may be because the new image is invalid or corrupted and the device has booted from another image.</td>
<td>Check the Bug Toolkit application for any known issues on the upgraded image version.</td>
</tr>
<tr>
<td>SWIM1021</td>
<td>Cannot get the IP Address of the server.</td>
<td>The DNS resolution of the LMS server may have failed.</td>
<td>Enable DNS resolution.</td>
</tr>
<tr>
<td>SWIM1023</td>
<td>Distribution task is not supported for this device.</td>
<td>The device packages that are installed may not be the correct package.</td>
<td>Check whether the correct device packages are installed on the server.</td>
</tr>
<tr>
<td>SWIM1024</td>
<td>Either the file already exists in the directory or the system cannot create this file.</td>
<td>Check whether another file with the same name already exists in the directory, or check whether there is enough disk space.</td>
<td>Create disk space and retry the task.</td>
</tr>
<tr>
<td>Message-ID</td>
<td>Error Message</td>
<td>Probable Cause</td>
<td>Possible Action</td>
</tr>
<tr>
<td>------------</td>
<td>-------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SWIM1025</td>
<td>The Configuration Register on the device does not allow you to boot the image from Flash.</td>
<td>The Configuration Register is not set to value 0x2102.</td>
<td>Change the Configuration Register on the device and retry the job.</td>
</tr>
<tr>
<td>SWIM1026</td>
<td>Cannot create a file and store the modified configuration.</td>
<td>There may not be sufficient permissions for the application to create the file, or there may not be enough disk space.</td>
<td>None.</td>
</tr>
<tr>
<td>SWIM1027</td>
<td>Error while fetching inventory information.</td>
<td>The data required for the selected task is either incomplete or missing in Inventory.</td>
<td>Check whether the Inventory data exists for the device in the Inventory Detailed Device Report. If there is no inventory data for the device, schedule an Inventory Collection job and retry the task.</td>
</tr>
<tr>
<td>SWIM1029</td>
<td>Cannot get the required inventory information for the device.</td>
<td>Either there was no inventory collection for the device or the device is not responding.</td>
<td>Update inventory for the device and retry the task.</td>
</tr>
<tr>
<td>SWIM1030</td>
<td>This is a Run From Flash (RFF) device, but the application cannot find the running image on the Flash.</td>
<td>Either the inventory has not been updated or the Flash file is deleted from the Flash.</td>
<td>Update the inventory and retry the task.</td>
</tr>
<tr>
<td>SWIM1031</td>
<td>No Candidate Images found for the running software.</td>
<td>Either:</td>
<td>Check Admin preference or add images to software repository.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Cisco.com is not included in the admin preferences</td>
<td>Or</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• There are no applicable images in the software repository or Cisco.com</td>
<td>Or</td>
</tr>
<tr>
<td>SWIM1032</td>
<td>Images obtained for Recommendation do not meet the hardware and software requirements of the selected device.</td>
<td>Either:</td>
<td>Check the Admin Preference or add more images to software repository and retry the job.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The Candidate Images were filtered based on the selected Admin Preferences</td>
<td>Or</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• They did not meet the Flash/RAM/BootROM needed to run on the device.</td>
<td>Or</td>
</tr>
<tr>
<td>Message-ID</td>
<td>Error Message</td>
<td>Probable Cause</td>
<td>Possible Action</td>
</tr>
<tr>
<td>------------</td>
<td>-------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| SWIM1033   | Cannot find the Best-fit image for the device by applying compatibility checks. | Either:  
- The Candidate Images were filtered based on the selected Admin Preferences  
- They did not meet the Flash/RAM/BootROM needed to run on the device. | Check the Admin Preference or add more images to software repository and retry the job. |
| SWIM1034   | No applicable images found for the device from the configured image sources.   | Either:  
- Cisco.com is not included in the admin preferences  
- There are no applicable images in the software repository or Cisco.com | Check the Admin Preference or add more images to software repository and retry the job. |
| SWIM1035   | Error while performing Recommendation option.                                 | None.                                                                         | Retry the job. If the problem persists, send the debug logs to Cisco Technical Assistance Center (TAC).  
The debug logs are available at this location:  
On Windows:  
NMSROOT\log\swim\swim\debug.log  
On Solaris and Soft Appliance:  
/var/adm/CSCOpx/log/swim\swim\debug.log |
| SWIM1036   | Runtime error while performing Recommendation.                                | None.                                                                         | Retry the job. If the problem persists, send the debug logs to Cisco Technical Assistance Center (TAC).  
The debug logs are available at this location:  
On Windows:  
NMSROOT\log\swim\swim\debug.log  
On Solaris and Soft Appliance:  
/var/adm/CSCOpx/log/swim\swim\debug.log |
| SWIM1037   | Error while fetching Flash Partition information.                            | Either:  
- The Flash information cannot be got from Inventory  
- There is a problem with the running image on the device. | Update the inventory and retry the task. If the problem persists, check the Bug Toolkit application for any known issues on the running image version. |
<table>
<thead>
<tr>
<th>Message-ID</th>
<th>Error Message</th>
<th>Probable Cause</th>
<th>Possible Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>SWIM1038</td>
<td>No Read-Write Partition found on the device.</td>
<td>None.</td>
<td>Install a Flash device with a read-write partition and update the inventory.</td>
</tr>
<tr>
<td>SWIM1039</td>
<td>No Storage Recommendation is made for the device.</td>
<td>The selected device may not have sufficient free size partition to copy the image.</td>
<td>Check whether the selected device has the sufficient free size partition to copy the image.</td>
</tr>
<tr>
<td>SWIM1040</td>
<td>Cannot get the Flash information for the device.</td>
<td>Either:</td>
<td>Perform Inventory Collection and check whether the Flash information appears in the Detailed Device report. If so, retry the job. Else, data is not available from the device.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The Flash information cannot be got from Inventory</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Or</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• There is a problem with the running image on the device.</td>
<td></td>
</tr>
<tr>
<td>SWIM1041</td>
<td>This device upgrade requires opening an SSH/Telnet connection to the device.</td>
<td>Enable password is not configured correctly in Device and Credential Repository.</td>
<td>Make sure that the appropriate SSH/Telnet passwords are configured correctly in Device and Credential Repository.</td>
</tr>
<tr>
<td>SWIM1042</td>
<td>The amount of Bootflash on the device may not be enough to run the selected image.</td>
<td>The amount of Bootflash on the device may not be enough to run the selected image.</td>
<td>Specify the Bootflash size for the image by editing the attributes of the image stored in the software repository, increase the Bootflash size for the device, or select a different image for upgrading.</td>
</tr>
<tr>
<td>SWIM1043</td>
<td>Runtime error while performing Bootloader image verification.</td>
<td>Selected image version may not be in the standard version format.</td>
<td>Retry the job. If the problem persists, send the debug logs to Cisco Technical Assistance Center (TAC). The debug logs are available at this location: On Windows: NMSROOT\log\swim_debug.log On Solaris and Soft Appliance: /var/adm/CSCOpx/log/swim_debug.log</td>
</tr>
<tr>
<td>SWIM1044</td>
<td>Bootflash partition will be erased before copying new image.</td>
<td>Selected Bootloader image does not fit in available space on Bootflash.</td>
<td>Select a different Bootloader image if available.</td>
</tr>
<tr>
<td>SWIM1046</td>
<td>Selected software does not fit in selected Flash partition.</td>
<td>Selected software image does not fit in the available space on Bootflash.</td>
<td>Select a different Flash partition for upgrading.</td>
</tr>
<tr>
<td>SWIM1047</td>
<td>Minimum software version required for MICA image upgrade is not known.</td>
<td>None.</td>
<td>Select the image in the software repository and update the minimum system software version using View/Edit Image Attributes option.</td>
</tr>
<tr>
<td>Message-ID</td>
<td>Error Message</td>
<td>Probable Cause</td>
<td>Possible Action</td>
</tr>
<tr>
<td>------------</td>
<td>---------------</td>
<td>----------------</td>
<td>----------------</td>
</tr>
<tr>
<td>SWIM1048</td>
<td>The system software that is active on the device, cannot run the selected image.</td>
<td>The system software that is active on the device, is not compatible with the selected image.</td>
<td>Select a different image that can be upgraded with the current system software or upgrade the system software to Software Version.</td>
</tr>
<tr>
<td>SWIM1049</td>
<td>The selected image requires Flash to be erased during image upgrade.</td>
<td>None.</td>
<td>Check whether you have performed the necessary backup.</td>
</tr>
<tr>
<td>SWIM1050</td>
<td>Read-Write SNMP community string is not in the Device and Credential Repository.</td>
<td>The Read-Write SNMP community string is not available in the Device and Credential Repository.</td>
<td>Add Read-Write community string for the device in the credentials repository.</td>
</tr>
</tbody>
</table>
| SWIM1051   | Credential information cannot be obtained for the device. | Either:  
• The device is not managed in the LMS server  
Or  
• The device credentials are not correct or the device access privileges are insufficient. | None. |
<p>| SWIM1052   | Enable password is not configured for the device. | For Run For Flash (RFF) partition software upgrades, the Enable password must be configured. | Configure the Enable password in the credentials repository. |
| SWIM1053   | Selected MICA Image is the same as the running image on the device. | The software version of the image is the latest on the device. | None. |
| SWIM1054   | Error while checking the Telnet credential of the device. | None. | Make sure that the Telnet credentials for the device are correct. |
| SWIM1055   | Selected Flash partition is ReadOnly. | Either the Flash partition is not write-enabled or the Read-Write partition does not exist. | Check whether the Read-Write partition exists. Set the Flash partition to be write-enabled. |
| SWIM1056   | The method to update the software on the selected storage device is unknown. | None. | Select a different Flash partition, if available. |
| SWIM1057   | The device will be put into Rxboot mode for the image upgrade. | None. | Select a different Flash device for the system software, if available. |</p>
<table>
<thead>
<tr>
<th>Message-ID</th>
<th>Error Message</th>
<th>Probable Cause</th>
<th>Possible Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>SWIM1058</td>
<td>The selected software version has some known problems in the Flash MIB options which will make this application unable to perform software upgrades on the device.</td>
<td>None.</td>
<td>Upgrade the device manually or select a later software version, if available.</td>
</tr>
<tr>
<td>SWIM1059</td>
<td>Ensure Dial Shelf runs a compatible software image with the newly loaded Router Shelf software image.</td>
<td>The Router shelf software image is not compatible with the Dial Shelf software image.</td>
<td>See the Release Notes for the Router Shelf software image to make sure the current Dial Shelf software is compatible. If not, upgrade the Dial Shelf software.</td>
</tr>
<tr>
<td>SWIM1060</td>
<td>Cannot obtain the file size of the selected image.</td>
<td>The selected image may have been removed from Cisco.com.</td>
<td>Select another image for upgrading.</td>
</tr>
<tr>
<td>SWIM1061</td>
<td>Image available at Cisco.com is selected for upgrade. This image will be imported from Cisco.com when the job is run.</td>
<td>None.</td>
<td>Verify that connectivity to Cisco.com is available when the job is scheduled to run or select another image from the software repository.</td>
</tr>
<tr>
<td>SWIM1062</td>
<td>Selected image is already running on the device.</td>
<td>None.</td>
<td>Verify that this is the image you want to upgrade for the device. If so, no action is required. If this is not the image you want, select a different image.</td>
</tr>
<tr>
<td>SWIM1063</td>
<td>Minimum RAM requirement of the selected image cannot be determined.</td>
<td>RAM available on the device may not be enough to activate this image.</td>
<td>Update the minimum RAM value using View/Edit Image attributes or make sure that the device has enough RAM to activate the selected image or select a different image.</td>
</tr>
<tr>
<td>SWIM1064</td>
<td>RAM available on the device may not be large enough to activate the selected image.</td>
<td>RAM available on the device may not be large enough to activate the selected image.</td>
<td>Select another image or upgrade the RAM on the device and retry Upgrade.</td>
</tr>
<tr>
<td>SWIM1065</td>
<td>RAM available on the device may not be large enough to activate the selected image.</td>
<td>RAM available on the device may not be large enough to activate the selected image.</td>
<td>Specify the RAM size for the image by editing the attributes of the image stored in the software repository, increase the RAM size for the device, or select a different image for upgrading.</td>
</tr>
<tr>
<td>SWIM1067</td>
<td>Runtime error while performing verification of the selected image.</td>
<td>None.</td>
<td>Select another image for upgrading. If the problem persists, send the debug logs to Cisco Technical Assistance Center (TAC). The debug logs are available at this location: On Windows: NMSROOT\log\swim_debug.log On Solaris and Soft Appliance: /var/adm/CSCOpx/log/swim_debug.log</td>
</tr>
<tr>
<td>Message-ID</td>
<td>Error Message</td>
<td>Probable Cause</td>
<td>Possible Action</td>
</tr>
<tr>
<td>------------</td>
<td>------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SWIM1063</td>
<td>Minimum RAM requirement of the selected image cannot be determined.</td>
<td>RAM available on the device may not be enough to activate the selected image.</td>
<td>Update the minimum RAM value using View/Edit Image attributes or make sure that the device has enough RAM to activate the selected image or select a different image.</td>
</tr>
<tr>
<td>SWIM1068</td>
<td>Selected image does not have the minimum system software version required for the upgrade.</td>
<td>Selected image does not have the minimum system software version required for the upgrade.</td>
<td>Select another image with a version higher than 11.0.</td>
</tr>
<tr>
<td>SWIM1069</td>
<td>Feature subset of the running image cannot be determined. Select a different image.</td>
<td>This is a wrong message caused by a bug. The correct message is: Feature subset of the selected image is a subset or equal to running software feature set.</td>
<td>None.</td>
</tr>
<tr>
<td>SWIM1070</td>
<td>Feature subset of the running image cannot be determined. Select a different image.</td>
<td>This is a wrong message caused by a bug. The correct message is: Feature subset of the selected image is a subset or equal to running software feature set.</td>
<td>None.</td>
</tr>
<tr>
<td>SWIM1071</td>
<td>System software analysis failed.</td>
<td>Some unknown error has occurred during image analysis.</td>
<td>Please contact Cisco TAC with the UI log available under: Windows: CSCOpx\logs\swim_debug.log Solaris and Soft Appliance: /var/adm/CSCOpx/log/swim_debug.log</td>
</tr>
<tr>
<td>SWIM1072</td>
<td>Boot loader analysis failed.</td>
<td>Some unknown error has occurred during analysis of the image.</td>
<td>Please contact Cisco TAC with the UI log available under: Windows: CSCOpx\logs\swim_debug.log Solaris and Soft Appliance: /var/adm/CSCOpx/log/swim_debug.log</td>
</tr>
<tr>
<td>SWIM1074</td>
<td>The selected image does not have any requirement to be analyzed. The image can be used to upgrade the device.</td>
<td>None.</td>
<td>None.</td>
</tr>
<tr>
<td>SWIM1075</td>
<td>Cannot find an image that is newer and can fit on the Bootflash.</td>
<td>None.</td>
<td>Add Bootloader images, to the Software Repository, with version greater than the running image version and that can fit into the Bootflash. Then retry the job.</td>
</tr>
<tr>
<td>Message-ID</td>
<td>Error Message</td>
<td>Probable Cause</td>
<td>Possible Action</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SWIM1076</td>
<td>Cannot find a Read-Write Boot partition on the device.</td>
<td>Read-Write Boot partition is not available on the device.</td>
<td>Insert a read-write Bootflash on the device and update the inventory.</td>
</tr>
<tr>
<td>SWIM1077</td>
<td>Cannot find a Bootflash partition for the Bootloader image.</td>
<td>Bootflash partition is not available on the Bootloader image.</td>
<td>Insert a read-write Bootflash on the device and update the inventory.</td>
</tr>
<tr>
<td>SWIM1078</td>
<td>System and Bootloader images are getting upgraded to the same Flash partition.</td>
<td>System and Bootloader images are getting upgraded to the same Flash partition.</td>
<td>Select individual partitions for both, if available.</td>
</tr>
<tr>
<td>SWIM1079</td>
<td>Image version cannot be compared.</td>
<td>The image formats of both the images may not be compatible for comparison.</td>
<td>Check the format of the version. Select a different image for upgrading.</td>
</tr>
<tr>
<td>SWIM1080</td>
<td>Read-Write partition exists but you have selected the ReadOnly partition.</td>
<td>You may have selected Read only partition instead of Read-Write partition.</td>
<td>Select the Read-Write partition for upgrading.</td>
</tr>
<tr>
<td>SWIM1081</td>
<td>You have selected the Compressed System Image for Run From Flash (RFF) Upgrade.</td>
<td>Wrong image selected for Upgrade.</td>
<td>Select the correct image.</td>
</tr>
<tr>
<td>SWIM1082</td>
<td>Runtime error while comparing Modem Image.</td>
<td>Either a wrong modem image is selected for comparison or the modem image formats or not compatible.</td>
<td>Select a different Modem Image for upgrading. If the problem persists, send the debug logs to Cisco Technical Assistance Center (TAC). The debug logs are available at this location: On Windows: NMSROOT\log\swim_debug.log On Solaris and Soft Appliance: /var/adm/CSCOpx/log/swim_debug.log</td>
</tr>
<tr>
<td>SWIM1083</td>
<td>Cannot find an image that is newer and fits in the Flash.</td>
<td>None.</td>
<td>Add another image into software repository and retry the task.</td>
</tr>
<tr>
<td>SWIM1084</td>
<td>Cannot find a Minimum Flash Requirement for the device.</td>
<td>The Flash space available on the device may not be sufficient for the selected image.</td>
<td>Check whether the image fits on the device.</td>
</tr>
<tr>
<td>SWIM1085</td>
<td>The MinFlash Attribute is unknown for the selected image.</td>
<td>The selected image does not fit on the selected partition.</td>
<td>Check whether the image fits on the selected partition or select a different image.</td>
</tr>
<tr>
<td>SWIM1086</td>
<td>Device not supported.</td>
<td>The required device packages may not be installed on the server.</td>
<td>Check whether the appropriate device packages are installed correctly on the server.</td>
</tr>
<tr>
<td>Message-ID</td>
<td>Error Message</td>
<td>Probable Cause</td>
<td>Possible Action</td>
</tr>
<tr>
<td>------------</td>
<td>---------------</td>
<td>----------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>SWIM1087</td>
<td>Cannot get the device representation.</td>
<td>The required device packages may not be installed on the server.</td>
<td>Check whether the appropriate device packages are installed correctly on the server.</td>
</tr>
<tr>
<td>SWIM1088</td>
<td>Runtime error occurred while creating the device upgrade data.</td>
<td>None.</td>
<td>Retry the job. If the problem persists, send the debug logs to Cisco Technical Assistance Center (TAC). The debug logs are available at this location: On Windows: \NMSROOT\log\swim_debug.log On Solaris and Soft Appliance: /var/adm/CSCOpx/log/swim_debug.log</td>
</tr>
<tr>
<td>SWIM1091</td>
<td>Minimum BootROM version of the selected image is not available in the software repository, or on Cisco.com.</td>
<td>The minimum BootROM value is not updated in View/Edit Image attributes for the selected image in software repository.</td>
<td>Update the minimum BootROM value using View/Edit Image attributes of the selected image in the software repository.</td>
</tr>
<tr>
<td>SWIM1092</td>
<td>Selected image does not have the minimum system software version required for system upgrade.</td>
<td>None.</td>
<td>Select an image that has a higher version than the minimum supported version. See the documentation for the Compatibility Matrix for Cisco IOS software.</td>
</tr>
<tr>
<td>SWIM1093</td>
<td>Cannot get Chassis Information from the inventory.</td>
<td>Check whether the Inventory data exists for the device in the Inventory Detailed Device Report.</td>
<td>If there is no inventory data for the device, schedule an Inventory Collection job and retry the task.</td>
</tr>
<tr>
<td>SWIM1094</td>
<td>SNMP-V3 parameters not in the Device and Credential Repository.</td>
<td>This could have been caused by any of the following: • The SNMP-V3 password is wrongly configured • The SNMP-V3 algorithm is wrongly configured • The SNMP-V3 engine ID is not configured in the Device and Credential Repository.</td>
<td>Check whether the SNMP-V3 password, SNMP-V3 algorithm, and SNMP-V3 engine ID is configured in the Device and Credential Repository.</td>
</tr>
<tr>
<td>SWIM1095</td>
<td>Error while checking the SNMP-V3 user name in the device context.</td>
<td>The SNMP-V3 credentials in the Device and Credential Repository is not up to date.</td>
<td>Update the SNMP-V3 credentials in the Device and Credential Repository and retry the task.</td>
</tr>
<tr>
<td>SWIM1096</td>
<td>Selected image is not applicable to this module.</td>
<td>The selected image is not applicable to this module.</td>
<td>Use the Cisco.com Upgrade Analysis feature to find an appropriate image.</td>
</tr>
<tr>
<td>SWIM1097</td>
<td>Selected Bootloader image is a lower version than the version of the Bootloader running on the device.</td>
<td>The Bootloader image version running on the device is the latest.</td>
<td>Check whether the higher version is available for upgrading.</td>
</tr>
</tbody>
</table>
### Message-ID | Error Message | Probable Cause | Possible Action
--- | --- | --- | ---
SWIM1098 | The selected image is lower than the running image on the device. | The image version running on the device is the latest. | Select a higher image for device software upgrade. |
SWIM1099 | Image Upgrade procedure may revert to the SSH/Telnet-based approach, based on the MIB instrumentation on the running image. | The SSH/Telnet passwords may not be configured in the Device and Credential Repository. | Make sure that appropriate SSH/Telnet passwords are configured in the Device and Credential Repository. |
SWIM1100 | Cannot find SNMP-V2 Read-Write Community String in the Device and Credential Repository. | The SNMP-V2 credentials may not be correctly configured in the Device and Credential Repository. | Check whether the SNMP-V2 credentials are configured correctly in the Device and Credential Repository. |
SWIM1101 | This Device Upgrade requires opening an SSH/Telnet connection to the device. | Enable password for the device is not configured in Device and Credential Repository. | Make sure that appropriate SSH/Telnet passwords are configured correctly in the Device and Credential Repository. |
SWIM1102 | This Device Upgrade requires opening a SSH/Telnet connection to the device. | There was an error while checking the credentials of the device. | Make sure that appropriate SSH/Telnet passwords are configured correctly in the Device and Credential Repository. |
SWIM1103 | Selected image may not be compatible to the device. | Image belongs to the same device family as the running image on the device. However, it is identified as non-compatible. | Check the Cisco.com documentation whether any caveats are identified for the selected image. |
SWIM1104 | The total space on the selected partition is not enough to upgrade all of the selected modules. | Multiple modules may be selected for upgrading on the same partition. | Select individual partitions for the selected modules, or deselect some modules. |
SWIM1105 | Image status for the selected image cannot be determined. | The selected image might be in the Deferred status. | Ensure that the image is not in the Deferred status. See the relevant documentation on Cisco.com before upgrading the images. |
SWIM1106 | Image selected for upgrade is compressed in .tar format. Flash will be overwritten while upgrading the image. | None. | Ensure that necessary backup jobs are completed before upgrading. |
SWIM1107 | This option requires devicename data in the inventory. | The required device information is not available in the inventory. | Perform Update Inventory and check whether the required data appears in the Detailed Device Report. If so, retry the job. Else the data is not retrieved from the device. |
<table>
<thead>
<tr>
<th>Message-ID</th>
<th>Error Message</th>
<th>Probable Cause</th>
<th>Possible Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>SWIM1109</td>
<td>Image status for the selected image is either Deferred or Not Supported.</td>
<td>Image status for the selected image is either Deferred or Not Supported.</td>
<td>Ensure that the image is supported by Software Management application. Check the documentation on Cisco.com before upgrading the image.</td>
</tr>
<tr>
<td>SWIM1110</td>
<td>.bin images are not supported for Stack Upgrade.</td>
<td>The .bin image has been selected for Stack Upgrade.</td>
<td>Select a tar image for Stack Upgrade.</td>
</tr>
<tr>
<td>SWIM1111</td>
<td>The available free space is not enough for upgrading this type of image.</td>
<td>Insufficient space for image upgrade.</td>
<td>Select a different image or free up some space. Update the inventory and retry the job.</td>
</tr>
<tr>
<td>SWIM1112</td>
<td>This module can be upgraded if managed independently.</td>
<td>This module can be upgraded only if it is managed as a separate device.</td>
<td>Assign an independent IP Address to this module. Manage it as a separate device and select that device to upgrade this module.</td>
</tr>
<tr>
<td>SWIM1113</td>
<td>Device Reboot failed or Reboot Verification failed.</td>
<td>The device is not running the new image after it is rebooted.</td>
<td>Verify the configuration used to load the new image. Verify whether the new image exists on the device in a valid Flash partition.</td>
</tr>
<tr>
<td>SWIM1114</td>
<td>The device cannot be reached after the reboot. Number of attempts to verify the device status has exceeded the maximum retry count.</td>
<td>Either:</td>
<td>Use the device console to determine if the device has reloaded with the desired image.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• An invalid image has been loaded onto the device</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• There are network connectivity problems.</td>
<td></td>
</tr>
<tr>
<td>SWIM1115</td>
<td>Device is booted from TFTP server.</td>
<td>The backup running image is not supported.</td>
<td>None.</td>
</tr>
<tr>
<td>SWIM1116</td>
<td>Read-Write SNMP community string cannot be fetched from the Device Context.</td>
<td>The Read-Write community string is not available in the Device and Credential Repository for this device.</td>
<td>Add the Read-Write community string to the Device and Credential Repository.</td>
</tr>
<tr>
<td>SWIM1117</td>
<td>The selected image is incompatible and cannot run on the selected device.</td>
<td>The selected image is incompatible and cannot run on the selected device.</td>
<td>Use the Cisco.com Upgrade Analysis feature to find an appropriate image.</td>
</tr>
<tr>
<td>SWIM1118</td>
<td>Selected image has a lower version than the version of the running image.</td>
<td>The selected image has a lower version than the version of the running image.</td>
<td>Verify whether the correct image is running on the device. If so, no action is required. If not, select a different image.</td>
</tr>
<tr>
<td>SWIM1119</td>
<td>Telnet credentials are not present for this device. There was an error while checking the credentials of the device.</td>
<td>The SSH/Telnet passwords are not configured correctly in the Device and Credential Repository.</td>
<td>Ensure that appropriate SSH/Telnet passwords are configured correctly in the Device and Credential Repository.</td>
</tr>
<tr>
<td>Message-ID</td>
<td>Error Message</td>
<td>Probable Cause</td>
<td>Possible Action</td>
</tr>
<tr>
<td>------------</td>
<td>---------------</td>
<td>----------------</td>
<td>-----------------</td>
</tr>
</tbody>
</table>
| SWIM1120   | Cannot obtain the sysObjectID of the device. | Either:  
- The device did not respond when you added it to LMS  
Or  
- The device cannot be added correctly. | Manually enter the device type information in the Device and Credential Repository. |
| SWIM1122   | Runtime error found during verification. | None. | Retry the job. If the problem persists, send the debug logs to Cisco Technical Assistance Center (TAC).  
The debug logs are available at this location:  
On Windows:  
`NMSROOT\log\swim_debug.log`  
On Solaris and Soft Appliance:  
`/var/adm/CSCOpx/log/swim_debug.log` |
| SWIM1123   | Telnet username not present for this device. | Either:  
- The Primary Credentials is not configured  
Or  
- It not configured properly for the selected device in the Device and Credential Repository. | Check whether the primary username is configured for the selected device, in Device and Credential Repository. |
| SWIM1124   | Cannot copy the image from Flash with return code of Code. | None. | Retry the job. If the problem persists, check the Bug Toolkit application for any known issues on the running image version. |
| SWIM1125   | Cannot copy the image from Flash with return code of Code. | None. | Retry the job. If the problem persists, check the Bug Toolkit application for any known issues on the running image version. |
| SWIM1126   | Image copy to module failed with return code of Code. | None. | Retry the job. If the problem persists, send the debug logs to Cisco Technical Assistance Center (TAC).  
The debug logs are available at this location:  
On Windows:  
`NMSROOT\files\rme\jobs\swim\JobID`  
On Solaris and Soft Appliance:  
`/var/adm/CSCOpx/files/rme/jobs/swim/JobID` |
<p>| SWIM1127   | Cannot connect to device through SSH/Telnet because of Device. | The SSH/Telnet credentials may not be correctly configured in the Device and Credential Repository. | Check whether the SSH/Telnet credentials are correctly configured in the Device and Credential Repository. |</p>
<table>
<thead>
<tr>
<th>Message-ID</th>
<th>Error Message</th>
<th>Probable Cause</th>
<th>Possible Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>SWIM1128</td>
<td>Cannot disconnect from device because of Device.</td>
<td>the SSH/Telnet credentials may not be correctly configured in the Device and Credential Repository.</td>
<td>Check whether the device is configured correctly.</td>
</tr>
<tr>
<td>SWIM1139</td>
<td>Select any available Boot flash partition, for bootldr upgrade.</td>
<td>This happens when the user has selected a Bootloader image for Distribution and a storage location other than Bootflash.</td>
<td>Select any available boot flash partition for bootldr upgrade.</td>
</tr>
<tr>
<td>SWIM1150</td>
<td>Could not get Command Service instance for device DeviceName because of CmdSvc Exception.</td>
<td>Either:</td>
<td>Check whether the Login credentials in DCR and Login credentials specified during job scheduling are correct.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The device login credentials in DCR are wrong or empty.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Or</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The SSH option is selected in the Swim Admin pane and the target device does not support SSH.</td>
<td></td>
</tr>
<tr>
<td>SWIM1151</td>
<td>Could not connect to the device DeviceName because of CmdSvcException.</td>
<td>Either:</td>
<td>Check whether the Login credentials in DCR and Login credentials specified during job scheduling are correct.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The device login credentials in DCR are wrong or empty.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Or</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The SSH option is selected in the Swim Admin pane and the target device does not support SSH.</td>
<td></td>
</tr>
<tr>
<td>SWIM1161</td>
<td>RXBOOT credentials are not configured for the device. If TACACS is used by the device, configure RXBOOT Mode credentials in the credentials repository.</td>
<td>RXBOOT credentials are not configured for the device in Device Credentials Repository (DCR). This will be used for Run From Flash (RFF) devices when connecting in RX boot mode.</td>
<td>If TACACS is used by the device, configure RXBOOT Mode credentials in the Device credentials repository.</td>
</tr>
<tr>
<td>Message-ID</td>
<td>Error Message</td>
<td>Probable Cause</td>
<td>Possible Action</td>
</tr>
<tr>
<td>------------</td>
<td>---------------</td>
<td>----------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>SWIM1162</td>
<td>Error when recommending image for the device.</td>
<td>Swim recommends the image based on device ROM, RAM and Flash which it collects from LMS Inventory module. If the device is having a faulty hardware (FLASH) then this will not be available in inventory.</td>
<td>Check the Inventory Detailed Device Report to ensure that Inventory data exists for the device (like Flash Partition size). If not, check the device for a faulty hardware or a bug in device software.</td>
</tr>
<tr>
<td>SWIM1163</td>
<td>Image Import from Device failed because of some unexpected error.</td>
<td>None.</td>
<td>Please contact Cisco TAC with the Job logs available under: Windows: \NMSROOT\files\rme\jobs\swim\jobID Solaris and Soft Appliance: /var/adm/CSCOpx/files/rme/jobs/swim/jobID</td>
</tr>
<tr>
<td>SWIM1164</td>
<td>Image Distribute to Device failed because of some unexpected error.</td>
<td>None.</td>
<td>Please contact Cisco TAC with the Job logs available under: Windows: \NMSROOT\files\rme\jobs\swim\jobID Solaris and Soft Appliance: /var/adm/CSCOpx/files/rme/jobs/swim/jobID</td>
</tr>
<tr>
<td>SWIM129</td>
<td>Selected image does not fit on the free Flash size on the device. Selected storage partition will be erased during the distribution.</td>
<td>Either: The boot loader image is selected for upgrade (and no system software image is selected along with it) or The storage location is not erased for the boot loader image to be copied.</td>
<td>Since the system software is not selected for upgrade, ensure that running system software is not in the selected storage partition. Back up the running system software and ensure that the device boots from the backed up image in case the job fails.</td>
</tr>
<tr>
<td>SWIM1501</td>
<td>Supervisor cannot be downgraded to an image version less than 4.1(1).</td>
<td>This happens when you try to distribute a CATOS image lesser than 4.1(1).</td>
<td>If you continue to downgrade, the device may lose its configuration. Use a higher version.</td>
</tr>
<tr>
<td>SWIM1506</td>
<td>Cannot move file from Location 1 to Location 2.</td>
<td>There may not be sufficient permissions for the application to move or copy the file, or there may not be enough disk space.</td>
<td>None.</td>
</tr>
<tr>
<td>Message-ID</td>
<td>Error Message</td>
<td>Probable Cause</td>
<td>Possible Action</td>
</tr>
<tr>
<td>------------</td>
<td>-------------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SWIM1507</td>
<td>Cannot back up the running image.</td>
<td>Either the file name or the storage partition name specified for backup is invalid.</td>
<td>You can stop the job, manually back up the running image, and retry the job.</td>
</tr>
<tr>
<td>SWIM1508</td>
<td>Cannot copy image Imagename to storage partition Partitionname.</td>
<td>Either the filename or the storage destination is invalid or the device does not provide the required MIB instrumentation for copying an image.</td>
<td>Retry the job. If the problem persists, check the Bug Toolkit application for any known issues on the running image version.</td>
</tr>
<tr>
<td>SWIM1510</td>
<td>Runtime error while performing Reload on a device.</td>
<td>None.</td>
<td>Retry the job. If the problem persists, send the debug logs to Cisco Technical Assistance Center (TAC). The debug logs are available at this location: On Windows: NMSROOT\files\rme\jobs\swim\JobID On Solaris and Soft Appliance: /var/adm/CSCOpx/files/rme/jobs/swim/JobID</td>
</tr>
<tr>
<td>SWIM1518</td>
<td>Runtime error during configuration upload.</td>
<td>None.</td>
<td>Check the Bug Toolkit application for any known issues on the running image version. If there are no issues, retry the job. If the problem persists, send the debug logs to Cisco Technical Assistance Center (TAC). The debug logs are available at this location: On Windows: NMSROOT\files\rme\jobs\swim\JobID On Solaris and Soft Appliance: /var/adm/CSCOpx/files/rme/jobs/swim/JobID</td>
</tr>
<tr>
<td>SWIM1525</td>
<td>Unknown package type.</td>
<td>None.</td>
<td>Check whether the module is supported in the Software Management Function and Device Support Matrix on Cisco.com.</td>
</tr>
<tr>
<td>SWIM1529</td>
<td>There is no module information available in the inventory for devicename.</td>
<td>There is no module information available in the inventory for devicename.</td>
<td>Update the inventory and retry the task.</td>
</tr>
<tr>
<td>SWIM1530</td>
<td>Storage not applicable for the module modulename.</td>
<td>This module does not support storage.</td>
<td>None.</td>
</tr>
<tr>
<td>SWIM1532</td>
<td>No read-write partition exists on the device to accommodate the selected image.</td>
<td>None.</td>
<td>Create some free space.</td>
</tr>
<tr>
<td>Message-ID</td>
<td>Error Message</td>
<td>Probable Cause</td>
<td>Possible Action</td>
</tr>
<tr>
<td>------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SWIM1542</td>
<td>Minimum supported version for Supervisor is 3.8.</td>
<td>None.</td>
<td>Select a higher version of the image to upgrade.</td>
</tr>
<tr>
<td>SWIM1543</td>
<td>Selected image has the same or a lower version than the version of the running image.</td>
<td>The selected image has the same or a lower version than the version of the running image.</td>
<td>Verify whether the correct image is running on the device. If so, no action is required. If not, select a different image.</td>
</tr>
<tr>
<td>SWIM1546</td>
<td>The NVRAM size on the device may not be large enough to run the image.</td>
<td>The NVRAM size on the device may not be large enough to run the image.</td>
<td>Select a different image or upgrade the NVRAM on the device and retry the Upgrade option.</td>
</tr>
<tr>
<td>SWIM1547</td>
<td>Available NVRAM size on the selected image cannot be determined.</td>
<td>RAM size on this module may not be large enough to store this image.</td>
<td>Make sure the module has enough NVRAM to run the selected image. Else, select a different image or upgrade the RAM on the module.</td>
</tr>
<tr>
<td>SWIM1548</td>
<td>There are no software requirements found for the selected image.</td>
<td>None.</td>
<td>Select a different image.</td>
</tr>
<tr>
<td>SWIM1549</td>
<td>Verify that the new software selected is compatible.</td>
<td>Software Management cannot determine the features in the ATM software.</td>
<td>Check the Release Notes for the new software to determine if all the features in the old software are available in the new software.</td>
</tr>
<tr>
<td>SWIM1554</td>
<td>The selected image cannot be used to upgrade the device.</td>
<td>The device does not have any module that can run the selected image.</td>
<td>Select a different image.</td>
</tr>
<tr>
<td>SWIM1556</td>
<td>Select the Storage partition.</td>
<td>None.</td>
<td>None.</td>
</tr>
<tr>
<td>SWIM1560</td>
<td>Slot number corresponding to the module cannot be got from inventory.</td>
<td>None.</td>
<td>Update Inventory and retry the task.</td>
</tr>
<tr>
<td>SWIM2001</td>
<td>Telnet error while connecting to the device.</td>
<td>Invalid access information in the inventory.</td>
<td>Verify the username and the passwords in Device and Credential Repository and retry the task.</td>
</tr>
<tr>
<td>SWIM2002</td>
<td>Cannot get details about Flash File system on the device.</td>
<td>Either the Flash device is not available or the Flash information format has changed.</td>
<td>None.</td>
</tr>
<tr>
<td>SWIM2503</td>
<td>Different images have been selected for upgrade of the Active and Stand-by processors.</td>
<td>None.</td>
<td>Select the same image for upgrade of Active and Stand-by CPUs.</td>
</tr>
<tr>
<td>SWIM3501</td>
<td>Cannot fetch device credentials for the selected device.</td>
<td>The credentials may not be configured correctly in Device and Credential Repository.</td>
<td>Check whether there are credentials are configured correctly in Device and Credential Repository.</td>
</tr>
<tr>
<td>Message-ID</td>
<td>Error Message</td>
<td>Probable Cause</td>
<td>Possible Action</td>
</tr>
<tr>
<td>------------</td>
<td>-------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SWIM3502</td>
<td>Cannot fetch the credentials of the parent device, for the selected device.</td>
<td>The NAM device Supervisor is not recognized by the LMS Inventory.</td>
<td>Add the Supervisor of the NAM device to the LMS Inventory.</td>
</tr>
<tr>
<td>SWIM3503</td>
<td>Telnet credentials are not present for the parent device.</td>
<td>The Telnet credentials are not properly configured for the parent device.</td>
<td>Check whether the Telnet credentials are configured for the parent device.</td>
</tr>
<tr>
<td>SWIM3504</td>
<td>If Auto Logout is enabled on the parent device, it may get disconnected during upgrade.</td>
<td>None.</td>
<td>None.</td>
</tr>
<tr>
<td>SWIM3505</td>
<td>NAM images are large.</td>
<td>The disk space available is insufficient.</td>
<td>Ensure that there is enough disk space available in the htdocs/swimtemp directory under the CiscoWorks install directory.</td>
</tr>
<tr>
<td>SWIM3703</td>
<td>Selected image does not have the minimum system software version required for system upgrade.</td>
<td>None.</td>
<td>Select a different Image with a version higher than 11.3(0).</td>
</tr>
<tr>
<td>SWIM3705</td>
<td>This NRP2 is in ROMMON state. Cannot perform software upgrade on this device.</td>
<td>The NRP2 device is not in normal mode.</td>
<td>Manually bring the device into the normal mode and retry the task.</td>
</tr>
<tr>
<td>SWIM5001</td>
<td>Cannot connect to the device devicename using protocol.</td>
<td>The device may not be reachable or there is invalid access information in the Device and Credential Repository.</td>
<td>Verify whether the device is reachable and the credentials in Device and Credential Repository are correct and retry the job.</td>
</tr>
<tr>
<td>SWIM2002</td>
<td>Cannot get details about Flash File system on the device.</td>
<td>Either the Flash device is not available or the Flash information format has changed.</td>
<td>Done.</td>
</tr>
<tr>
<td>SWIM4602</td>
<td>Only image versions 6.2 or above are supported through AUS.</td>
<td>The image version in the device is less than 6.2.</td>
<td>Manually upgrade the device to a version higher than 6.2.</td>
</tr>
<tr>
<td>SWIM4800</td>
<td>The version running on the device is less than the minimum supported version.</td>
<td>None.</td>
<td>Manually upgrade the device to the minimum supported version or higher.</td>
</tr>
<tr>
<td>SWIM5003</td>
<td>Cannot copy the image.</td>
<td>Either the server address is incorrect or the image is inaccessible to the device.</td>
<td>Check whether the server address is correct and whether the image is accessible to the device.</td>
</tr>
<tr>
<td>Message-ID</td>
<td>Error Message</td>
<td>Probable Cause</td>
<td>Possible Action</td>
</tr>
<tr>
<td>-------------</td>
<td>--------------------------------------</td>
<td>-------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SWIM5004</td>
<td>Cannot initiate SNMP set option.</td>
<td>The SNMP Write Community String might be wrong.</td>
<td>Check whether the correct SNMP Write Community String is entered in Device and Credential Repository.</td>
</tr>
<tr>
<td>SWIM5005</td>
<td>Device reboot option failed.</td>
<td>The device is not configured for reboot. The command, <code>snmp-server system-shutdown</code>, should be in the running configuration on the device.</td>
<td>Modify the device configuration and retry the job. If the problem persists, send the debug logs to Cisco Technical Assistance Center (TAC). The debug logs are available at this location: On Windows: <code>NMSROOT\log\swim_debug.log</code> On Solaris and Soft Appliance: <code>/var/adm/CSCOpx/log/swim_debug.log</code></td>
</tr>
<tr>
<td>SWIM5006</td>
<td>Device reboot option failed.</td>
<td>The device is not configured for reboot. The SNMP Write Community string might be wrong.</td>
<td>The command SNMP server system shutdown should be in the running configuration on the device. Modify the device configuration and check whether the Write Community string is configured on the device is same as the one that is entered in Device and Credential Repository.</td>
</tr>
<tr>
<td>SWIM5007</td>
<td>CPU switchover failed.</td>
<td>Either the SNMP set failed or the device is not in hot standby mode or the two CPUs are not running similar images.</td>
<td>Do any of the following: - Check the SNMP credentials in the Device and Credential Repository - Ensure that the device is in hot standby mode, - Ensure that the two CPUs are running similar images, before attempting the switchover.</td>
</tr>
<tr>
<td>SWIM5008</td>
<td>Device not responding after running the <code>switch cpu</code> command.</td>
<td>—</td>
<td>Check the Bug Toolkit application for any known issues on the running image version.</td>
</tr>
<tr>
<td>SWIM5009</td>
<td>Device is not in HotStandby Mode. Switch Operation terminated.</td>
<td>The Standby CPU may be down.</td>
<td>Bring up the standby CPU and retry the job.</td>
</tr>
</tbody>
</table>
# Job Approval

This section provides the troubleshooting information for the Job Approval application:

<table>
<thead>
<tr>
<th>Message ID</th>
<th>Error Message</th>
<th>Probable Cause</th>
<th>Possible Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>JBAP0001</td>
<td>Cannot enable approval for applications that do not have an Approver-List assigned to them</td>
<td>You have attempted to enable Approval without assigning a list to the application.</td>
<td>Go to the <strong>Approval &gt; AssignLists</strong> screen and assign a list to the application. Enable Approval again.</td>
</tr>
<tr>
<td>JBAP0002</td>
<td>Specify a valid E-mail address.</td>
<td>You have entered an invalid E-mail-address.</td>
<td>Enter a valid E-mail address</td>
</tr>
<tr>
<td>JBAP0003</td>
<td>Select at least one job.</td>
<td>You have attempted to perform an action on a job without selecting a job</td>
<td>Select a job before performing an action on it.</td>
</tr>
<tr>
<td>JBAP0004</td>
<td>Select only one job.</td>
<td>You have attempted to view JobDetails, with more than one job selected</td>
<td>Select only one job.</td>
</tr>
<tr>
<td>JBAP0005</td>
<td>List {0} has no users. To save the list successfully, add users and click <strong>Save</strong></td>
<td>This is not an error. This is an Information message when you add a list for the first time.</td>
<td>Add users before saving the list</td>
</tr>
<tr>
<td>JBAP0006</td>
<td>{0} is not a valid Approver. Enter a user with Approver role</td>
<td>You have attempted to add a user who has not been added as Approver in CMF.</td>
<td>You must first add the user as Approver into CMF. Only then can you add this user into LMS.</td>
</tr>
<tr>
<td>JBAP0007</td>
<td>Select an Approver, to change E-mail.</td>
<td>You are trying to save without selecting a user.</td>
<td>Go back and select a user.</td>
</tr>
<tr>
<td>JBAP0008</td>
<td>List {0} already exists.</td>
<td>You have attempted to add a list that already exists.</td>
<td>Add the list with a different list name.</td>
</tr>
<tr>
<td>JBAP0009</td>
<td>Could not approve/reject the job {0}. Verify that the database and mail server are running.</td>
<td>Either approve/reject mails cannot be sent, or the database is not running.</td>
<td>Make sure mail server is configured properly and that the database is running.</td>
</tr>
<tr>
<td>JBAP0010</td>
<td>Cannot reject a job without comments.</td>
<td>You have attempted to reject a job without giving reasons for rejecting</td>
<td>Add comments if you want the job to be rejected.</td>
</tr>
<tr>
<td>JBAP0011</td>
<td>Select a future start date.</td>
<td>You have selected a past date while changing a job schedule</td>
<td>Select a future date.</td>
</tr>
<tr>
<td>JBAP0012</td>
<td>Job {0} is changed successfully.</td>
<td>Not an error message</td>
<td>None.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Error Message</td>
<td>Probable Cause</td>
<td>Possible Action</td>
</tr>
<tr>
<td>-------------</td>
<td>--------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
<td>---------------------------------------</td>
</tr>
<tr>
<td>JBAP0013</td>
<td>Are you sure you wish to delete? Approval will be disabled for applications to which {list-name} is assigned.</td>
<td>Alert message before deleting – not an error message.</td>
<td>None.</td>
</tr>
<tr>
<td>JBAP0014</td>
<td>Enter a valid Approver-List name.</td>
<td>You may have entered invalid characters such as spaces in the Approver name.</td>
<td>Add a valid user-name</td>
</tr>
<tr>
<td>JBAP0015</td>
<td>{list-name} already exists.</td>
<td>You have attempted to add a list name that already exist</td>
<td>Select a different name</td>
</tr>
<tr>
<td>JBAP0016</td>
<td>{user-name} already exists.</td>
<td>You have attempted to add a user name that already exists.</td>
<td>Add a new user name. This field is case-sensitive.</td>
</tr>
<tr>
<td>JBAP0017</td>
<td>Are you sure you wish to delete? This will disable approval for applications having {user-name} as the sole approver.</td>
<td>Warning message for deleting a user. If you have enabled Approval for an application whose sole approver is this user, it will be disabled.</td>
<td>None.</td>
</tr>
<tr>
<td>JBAP0018</td>
<td>You have attempted an action without selecting a user. Select a user before performing the action.</td>
<td>User not selected.</td>
<td>Select a user before performing the action.</td>
</tr>
<tr>
<td>JBAP0019</td>
<td>You have attempted an action without selecting a list. Select a list before performing the action.</td>
<td>List not selected.</td>
<td>Select a list before performing the action.</td>
</tr>
<tr>
<td>JBAP0021</td>
<td>Cannot save a list that has no approvers in it.</td>
<td>No approver available for the selected list.</td>
<td>Add approvers before trying to save the list.</td>
</tr>
<tr>
<td>JBAP0022</td>
<td>Cannot change schedule for {0}. A runtime error occurred when you tried to change the schedule of the job.</td>
<td>None.</td>
<td>This exception will appear in the MakerChecker.log in the following location: NMSROOT\log (On Solaris and Soft Appliance) NMSROOT\log (On Windows) where NMSROOT is the CiscoWorks install directory. Contact Cisco Technical Assistance Center (TAC) with this log file.</td>
</tr>
<tr>
<td>JBAP0024</td>
<td>Cannot send approval E-mails. Make sure that SMTP Server is configured correctly.</td>
<td>None.</td>
<td>Go to Admin &gt; System &gt; System Preferences and configure SMTP Server correctly.</td>
</tr>
</tbody>
</table>
## cwcli config

This section provides the troubleshooting information for the `cwcli config` commands:

<table>
<thead>
<tr>
<th>Message-ID</th>
<th>Error Message</th>
<th>Probable Cause</th>
<th>Possible Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>CCLI0001</td>
<td>Could not get any devices to work on.</td>
<td>This problem occurred because of any of the following:</td>
<td>Do any of the following, depending on what caused the problem:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Specified devices is not managed by LMS.</td>
<td>• Specify valid devices that are managed by LMS.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• You have not used the correct Device Display name</td>
<td>• Use a valid Device Display name.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• DCR server is down</td>
<td>• Use the <code>pdshow</code> command to verify whether the DCR server is running.</td>
</tr>
<tr>
<td>CCLI0002</td>
<td>The job could not be created since no device is available.</td>
<td>This problem occurred because of any of the following:</td>
<td>Do any of the following, depending on what caused the problem:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• You have entered invalid arguments for the command.</td>
<td>• Enter valid arguments.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• You have entered devices that are not managed by LMS.</td>
<td>• Verify that the devices you have entered are managed by LMS.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• CTMJrmServer and jrm are down.</td>
<td>• Use the <code>pdshow</code> command to verify whether the CTMJrm server and jrm are running.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ConfigMgmtServer process is down.</td>
<td>• The ConfigMgmtServer process should be up for the configuration Download and Fetch options.</td>
</tr>
<tr>
<td>CCLI0003</td>
<td>Could not get results for devices within the specified time interval</td>
<td>Less timeout is configured</td>
<td>Either:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Increase the timeout value using the <code>-timeout</code> option.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Or</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Use Configuration Archive Job Browser to see the results.</td>
</tr>
<tr>
<td>CCLI0004</td>
<td>Could not retrieve the Device Identification number for the device.</td>
<td>This problem occurred because of any of the following:</td>
<td>Do any of the following, depending on what caused the problem:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Specified devices are not managed by LMS.</td>
<td>• Specify valid devices that are managed by LMS.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• You have not used the correct Device Display name</td>
<td>• Use a valid Device Display name.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• DCR server is down</td>
<td>• Use the <code>pdshow</code> command to verify whether the DCR server is running.</td>
</tr>
<tr>
<td>CCLI0005</td>
<td>There are no archived configurations for this device</td>
<td>Sync Archive has not happened for the specified device.</td>
<td>Archive the configuration using the Sync Archive feature.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>For details on using the Synch Archive feature, see the Online Help.</td>
</tr>
<tr>
<td>Message-ID</td>
<td>Error Message</td>
<td>Probable Cause</td>
<td>Possible Action</td>
</tr>
<tr>
<td>-------------</td>
<td>------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>CCLI0006</td>
<td>Cannot create a temporary file to store the running configuration.</td>
<td>This problem occurred because of any of the following:</td>
<td>Do any of the following, depending on what caused the problem:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• There is not enough space to create a file in your file system.</td>
<td>• Verify whether there is enough space to create a file in your file system.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• You do not have permissions to create a file in the specified location.</td>
<td>• Verify whether you have permissions to create a file in the specified location.</td>
</tr>
<tr>
<td>CCLI0007</td>
<td>Cannot retrieve the configuration file from the archive.</td>
<td>The specified version does not exist in the archive.</td>
<td>Verify whether the specified version exists in the archive. Use the listversions command to see the available versions.</td>
</tr>
<tr>
<td>CCLI0008</td>
<td>Could not create a temporary file in DCMA temporary directory.</td>
<td>This problem occurred because of any of the following:</td>
<td>Do either of the following, depending on what caused the problem:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• There is not enough space to create a file in your file system.</td>
<td>• Verify whether there is enough space to create a file in your file system.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• You do not have permissions to create a file in the specified location.</td>
<td>• Verify whether you have permissions to create a file in the specified location.</td>
</tr>
<tr>
<td>CCLI0009</td>
<td>Cannot get running configuration.</td>
<td>The archive does not contain any versions for the device.</td>
<td>Verify whether the specified version exists in the archive. Use the listversions command to see the available versions.</td>
</tr>
<tr>
<td>CCLI0010</td>
<td>Device has only one version archived.</td>
<td>Synch Archive has not happened for the specified device</td>
<td>Archive the configuration using the Synch Archive feature.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>For details on using the Synch Archive feature, see the Online Help.</td>
</tr>
<tr>
<td>CCLI0011</td>
<td>The specified version of the configuration does not exist.</td>
<td>You have entered an invalid version of the configuration.</td>
<td>Use the listversions command to see the available versions and enter an existing version</td>
</tr>
<tr>
<td>CCLI0012</td>
<td>No baseline templates exist for this device.</td>
<td>None</td>
<td>Use the listversions command to see the available baseline templates.</td>
</tr>
<tr>
<td>CCLI0013</td>
<td>Data file does not contain any device.</td>
<td>None</td>
<td>Add the devices in the data file and try again</td>
</tr>
<tr>
<td>CCLI0014</td>
<td>The job could not be created because of the errors reported.</td>
<td>This problem occurred because of any of the following:</td>
<td>Do either of the following, depending on what caused the problem:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• You have entered invalid arguments.</td>
<td>• Verify whether you have entered valid arguments.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The data file is missing some parameters.</td>
<td>• Update the data file if there are missing parameters.</td>
</tr>
<tr>
<td>CCLI0015</td>
<td>You should not use the -f option with more than one device.</td>
<td>Multiple devices are specified for the command to be executed along with -f option</td>
<td>Use the -input option to specify the file for every device</td>
</tr>
</tbody>
</table>
**cwcli export**

This section provides the FAQs for the cwcli export tool:

- **Q.** What does cwcli export do?

  **A.** cwcli export is a command line tool that also provides servlet access to export inventory, configuration and change audit data. You can use this tool to export inventory, configuration archive, and change audit data for devices in LMS, in the XML format.

  You can use the **cwcli export** command to generate the Inventory and Configuration data in XML format. In addition to this, you can also export Change Audit data.

  See these topics in the Configuration Management Help:
  - *Running cwcli export changeaudit* for the usage and XML schema details.
  - *Running cwcli export config* for the usage and XML schema details.
  - *Running cwcli export inventory Command* for the usage and XML schema details.

- **Q.** What is ComputerSystemPackage Class?

  **A.** It is the class that contains the InstanceIDs of Cisco-Chassis and Cisco-NetworkElement, and relates the two.

- **Q.** Where does cwcli export collect the configuration information from?

  **A.** cwcli export collects the running configuration data from the latest configuration in the Config Archive.

- **Q.** Is the containment hierarchy in inventory schema exactly the same as that in CIM?

  **A.** No. Although the containment hierarchy in inventory schema is based on Common Information Model (CIM), it does not follow the exact containment hierarchy because of the limitations in the LMS database schema.
Q. What is an XSD file?

A. XSD file is an XML based alternative to Document Type Definition (DTD). It is based on XML schema language which describes the structure of an XML document. An XML schema defines the legal building blocks of an XML document, just like a DTD.

An XML Schema:
- Defines elements that can appear in a document.
- Defines attributes that can appear in a document.
- Defines which elements are child elements.
- Defines the order of child elements.
- Defines the number of child elements.
- Defines whether an element is empty or can include text.
- Defines data types for elements and attributes.
- Defines default and fixed values for elements and attributes.

Q. What is the AdditionalInformation tag in the inventory schema used for?

A. The AdditionalInformation tag is provided to define information that is specific to a device. The inventory schema may not contain information for all the elements in all the devices supported by cwcli export. The AdditionalInformation tag addresses scenarios where the inventory schema does not have tags to define information that you want to collect for some of the elements in a particular device.

Q. How do I know what fields come under AdditionalInformation?

A. For this information, see the topic, Additional Information Table, in the Configuration Management Online Help.

Q. Where can I find information specific to a particular node which I can see in detailed device information but not in cwcli export?

A. For this information, see the topic, Additional Information Table, in the Configuration Management Online Help.

Q. How can I make use of the servlet interface?

A. You must write customized scripts which could connect to the servlet. The arguments and options have to be specified in XML format.

For more details, see the section, Using cwcli Commands in the Configuration Management Online Help.

Q. How can I get data for some particular entity from devices which are managed by different LMS servers?

A. You have to write a script to connect to different LMS servers and aggregate all data into a single file. After you get the aggregated data, you can parse it and get the data for any required entity.

Q. While using the -m option, can I use more than one E-mail id?

A. No. You can use only one E-mail address at a time, when you use the -m option of the cwexport command.
Q. Where can I get the descriptions of each node in the schema?
A. You can find the descriptions in the Configuration Management Online help. See the topic Overview: cwcli export and sub-topics.

Q. Why am I getting parse error when trying to parse some of the output files?
A. Some of the classes in IDU and Optical switches contains some special characters with ASCII code larger than 160. Most of the XML parsers does not support these characters and hence fails to parse these characters.

To overcome this, you have to manually search for those elements with special characters and append CDATA as given in the example below:

If there is an element,

```
checksum ❓โอ /checksum
```

you must change it to

```
checksum <![CDATA[❓โอ ]]>/checksum
```

---

**VRF Lite**

Q. What is VRF Lite?
A. VRF Lite is an application that allows you to pre-provision, provision and monitor Virtual Routing and Forwarding-Lite (VRF-Lite) technology on an enterprise network.

Q. What is Network Virtualization?
A. Virtualization deals with extending a traditional IP routing to a technology that helps companies utilize network resources more effectively and efficiently. Using virtualization, a single physical network can be logically segmented into many logical networks. The virtualization technology supports multiple virtual routing instances of a routing table to exist within a single routing device and work simultaneously.

Q. What is VRF-Lite?
A. Virtual Routing and Forwarding - Lite (VRF - Lite) is the one of the simplest form of implementing virtualization technology in an Enterprise network. A Virtual Routing and Forwarding is defined as VPN routing/forwarding instance. A VRF consists of an IP Routing table, a derived forwarding table, a set of interfaces that use the forwarding table and set of routing protocols that determine what goes into the forwarding table.

Q. What are the pre-requisites to manage a device using VRF Lite?
A. The pre-requisites to manage a device in VRF Lite are:

1. The device must be managed by LMS.
2. The device must either be L2/L3 or L3 device.
3. The devices failing to satisfy pre-requisite # 1 or #2, are not displayed in VRF Lite.

   The device must have the necessary hardware support. For more information on hardware support, see http://www.cisco.com/en/US/products/sw/cscowork/ps563/products_device_support_tables_list.html.

   If the device hardware is not supported then the device will be classified as Other devices.
4. If a device does not support MPLS VPN MIB, it is classified as a capable device.
5. VTP Server must be support MPLS VPN MIB. If the VTP Server does not support MPLS VPN MIB, LMS will not manage VTP Clients.

Q. The device must be managed by LMS to exercise all the functionality of VRF. The desired device is not listed in the device selector for the VRF configuration workflows. What is the reason for a device not listed in the device selector?

A. A device is not listed in the device selector due to the following reasons:

All VRF Lite Configuration workflows like Create, Edit, Extend, Delete VRF and Edge VLAN Configuration.

A device will not be listed in the Device Selector, if a device does not satisfy the pre-requisites as mentioned in the Pre-requisites.

If VRF Lite Configuration workflow is either Edit VRF, or Delete VRF or Edge VLAN Configuration then a device will not be listed in the Device Selector, if a device is not participating in the selected VRF.

In the Readiness Report, a device listed as a supported device may be because it is not managed by LMS. You can check if a device is managed by LMS using the Device Management State Summary. You can access the Summary by selecting Device Management option.

In Extend VRF workflow, the devices listed in the Device Selector are the devices that are not participating in the selected VRF.

In Edge VLAN Configuration workflow, the devices listed in the Device Selector are only L2/L3 devices that are not participating in the selected VRF.

Q. What are the different categories in which the devices are managed by VRF Lite? Or what criteria are used by VRF Lite to categorize the devices in the network?

A. VRF Lite identifies the devices based on the minimum hardware and software support required to configure VRF on the devices.

Based on the available hardware and software support in the devices, VRF Lite classifies the devices into following categories:

- VRF Supported Devices – Represents the devices with required hardware and software support available to configure VRF on the devices.

- VRF Capable Devices – Represents the devices with required hardware support available. But the device software must be upgraded to support MPLS VPN MIB. For information on the IOS version that supports MPLS VPN MIB, refer [http://tools.cisco.com/ITDIT/MIBS/MainServlet](http://tools.cisco.com/ITDIT/MIBS/MainServlet).

  VRF Lite classifies all the devices from Cat 3k and Cat 4k family of devices as VRF Capable devices as these devices do not have the required MPLS VPN MIB support.

- Other – Represents the devices without required hardware support to configure VRF. SysOID of the device needs to be checked.
Q. While performing the VRF Lite Configuration, VRF Lite application prompts the following messages:

“The device(s) with display name(s) are already locked as they are used by configuration workflows. You cannot configure these devices. Wait for some time Or Ensure the devices are not used by configuration workflows and free the devices from Resource Browser.

Or

Selected Device(s) are locked as they are used by configuration workflows. You cannot configure these devices. Wait for some time Or Ensure the devices are not used by configuration workflows and free the devices from Resource Browser.

The above messages appear even if no VRF Lite configuration is performed parallelly. Why do I get these messages?

A. The VRF Lite application prompts with these messages when some other configurations are performed simultaneously.

You can check the status of the configuration workflow using Resource Browser. The JOB Id/Owner column will give the details of the workflows currently running in the application.

These messages also appear if any VRF Lite configuration workflow is abruptly ended or an error has occurred while unlocking the device. You can release the locked devices only after ensuring that no other configuration workflows are running simultaneously. You can release the locked device using the Resource Browser option.

Note

If you unlock a device which is participating in a configuration workflow, the configurations details will be overwritten or corrupted. By default, a lock will be released after two hours.

Q. Sometimes, while performing VRF Lite configuration, I get the following message:

The device(s) with display name(s) are already locked as they are used by configuration workflows. You cannot configure these devices. Wait for some time OR Ensure the devices are not used by configuration workflows and free the devices from CS > Admin > Resource Browser.

Or

Selected Device(s) are locked as they are used by configuration workflows. You cannot configure these devices. Wait for some time OR Ensure the devices are not used by configuration workflows and free the devices from Resource Browser.

Can I get the details of the user who has locked the devices to perform VRF Lite configuration?

A. You cannot get the details of user who has locked the devices to perform VRF Lite configurations.
Q. In the Create, Edit, or Extend workflow, the application do not list the Routing Protocols used while configuring VRF. The Routing Protocol information displayed is NA. What do I need to do to get the routing protocol configurations details?

A. When the Routing Protocol information displayed is NA, it means that the configuration details are not fetched successfully in LMS. You can schedule the Sync Archive job from Configuration > Configuration Archive > Synchronization.

Q. What are the details of the VRF Lite log files? In which location are the VRF Lite log files located?

A. The following are the details of the VRF Lite log files:

1. Vnmserver.log – This log file logs the messages pertaining to the VNMServer process.
2. Vnmcollector.log – This log file logs the messages pertaining to the VRF collection.
3. Vnmclient.log – This log file logs the messages related to the User Interface.
4. Vnmutils.log – This log file logs the messages pertaining to the utility classes used by VRF client and server.

The above-mentioned VRF Lite log files are located in the following location:

In Solaris and Soft Appliance: /var/adm/CSCOpx/log/
In Windows: NMSROOT\logs

Q. When is the VRF Collection process triggered?

A. Manually:

You can manually schedule to run the VRF Collection process by:

Providing the setting details using Admin > Collection Settings > VRF Lite.

Automatically:

If you enable the Run VRF Collector After Every Data Collection in the VRF Collector Schedule page. The VRF Collection process will be automatically triggered after the completion of Data Collection.

You can reach the VRF Collector Schedule page using Admin > Collection Settings > VRF Lite.

Q. After the completion of the Data collection process, the VRF Lite Collector failed to run, What is the reason for failure?

A. Check if the Run VRF Collector After Every Data Collection option is enabled in the VRF Collector Schedule page. You can reach the VRF Collector Schedule page from Admin > Collection Settings > VRF Lite page.
Q. What is the reason for VLANs not getting populated in the VLAN to VRF Mapping page in the Create VRF and Extend VRF workflows?

A. The VLAN to VRF Mapping page lists the links connecting the source and the destination device. The VLANs are not listed in fields displaying the links in the VLAN to VRF Mapping page because VRF Lite tries to find a free VLAN in the devices connected using a link based on the following procedure:

1. An SVI, VRF Lite searches for free VLANs in the range 1-1005
2. An SI, VRF Lite searches for free VLANs in the range 1006-4005

Q. Why do I see the VRF description for all VRF(s) in home page as “Discovered by VRF Lite”?

A. While creating or extending VRF, the description that you have provided is deployed to the selected devices on which VRF is configured. But, the description provided while configuring or extending, is not read by the VRF Lite application. Instead, the VRF Lite application provides the default description for all VRFs as “Discovered by VRF Lite”.

Q. Why some port-channels are not discovered in LMS?

A. VRF Lite does not support port-channel and GRE Tunnel. Also, Currently VRF Lite supports only 802.1Q

Q. What is tested number of devices support in VRF Lite?

A. In an Enterprise network, VRF Lite is tested to support the configuration of 32 VRFs with VRF configuration supported in 550 devices in your network. However, at a given time, you can select up to 20 devices and configure VRF using the Create, Edit and Extend VRF workflow.

Q. What are the property files associated with VRF Lite?

A. The following property files are associated with VRF Lite:

1. The property file used to provide the settings for Purge and Home page auto Refresh is:
   - NMSROOT/vnm/conf/VNMClient.properties (On Solaris and Soft Appliance)
   - NMSROOT\vnm\conf\VNMClient.properties (On Windows)

2. The property file used to provide the SNMP and VNMServer settings is:
   - NMSROOT/vnm/conf/VNMServer.properties (On Solaris and Soft Appliance)
   - NMSROOT\vnm\conf\VNMServer.properties (On Windows)

3. The property file that stores the SNMP Timeout and Retries that you have configured is:
   - NMSROOT/vnm/conf/VRFCollectorSnmp.conf (On Solaris and Soft Appliance)
   - NMSROOT\vnm\conf\VRFCollectorSnmp.conf (On Windows)
Q. In the Interface to VRF Mapping page for the Create, Edit and Extend VRF workflow, why are values for the IP Address and SubnetMask fields empty?
A. If the physical interface that links two devices is not configured with an IP Address, then the IP Address and the SubnetMask fields are empty.

Q. What is protocol ordering for configuration workflows?
A. Configuration workflow uses the protocol ordering similar to ordering used by NetConfig.
Choose the NetConfig as Application Name from using Admin > Collection Settings > Config >
Config Transport Settings page. You can view the protocol ordering in the Transport Settings page.

Q. What is protocol ordering for troubleshooting?
A. Troubleshooting VRF workflow uses the protocol ordering similar to ordering used by NetShow in LMS.
Choose the NetShow as Application Name from using Admin > Collection Settings > Config >
Config Transport Settings page. You can view the protocol ordering in the Transport Settings page.

Q. If you configure commands to be deployed to two different devices, will the commands be deployed parallelly or serially?
A. The commands will be deployed to multiple devices parallelly, whereas a series of commands with-in a single device, will be deployed in serial manner.

Q. Which VRF Lite configuration jobs that are failed can be retried?
A. You can retry all the VRF Lite Configuration jobs which are failed. VRF Lite Configuration jobs are the jobs pertaining to Create, Edit, Extend, Delete VRF and Edge VLAN Configuration workflow.

Q. In the Troubleshooting VRF page, after selecting the source device, no VRFs are listed in the VRF List to troubleshoot. Why?
A. Initially, check if a VRF is configured on the selected source device. The VRF list in the Troubleshooting page enlists the VRF(s) configured in the selected source device as well as in the Global Table, which refers to the global routing table.

Q. Which interfaces are displayed in the Troubleshooting VRF page?
A. When a VRF is selected then all the interfaces that are configured with the selected VRF in the corresponding device is listed.
If you select VRF as “Global Table”, then the application displays all the interfaces that are not configured to any VRF.
Q. In some scenarios, the VRF configuration commands are pushed to unselected devices. What is the reason?

A. In the following scenarios, the VRF configuration commands are pushed to unselected devices:

   The VLANs are created in the VTPServer by default. In any VRF Lite Configuration workflow, if you create a VLAN in VTP Client devices, then VRF Lite application finds the corresponding VTP Server and create VLANs in that device.

   In Delete VRF workflow, the virtualized interface in the connecting device will also be deleted, even if the device is not selected.

Q. Why the FHRP and DHCP configurations are not shown in VRF Lite?

A. VRF Lite does not fetch the details for the FHRP or DHCP configuration from the device. Also, VRF Lite won’t put the list of vlan(s) allowed on a trunk.

The Protocols and DHCP Server details for existing or newly created SVIs are not fetched from the selected devices.