Cisco NCS 2000 Series Upgrade Guide, Release 11.1.x.x

First Published: 2019-10-04

Last Modified: 2026-04-28

Cisco NCS 2000 Series Upgrade Guide , Release 11.1.x.x

This document has all the information required for upgrading NCS 2002, NCS 2006, NCS 2015 nodes.

Cisco NCS 2000 Series Upgrade Guide, 11.1.x.x

This document explains how to upgrade the Cisco Transport Controller (CTC) software to the NCS fixed grid or NCS flex software using the control cards. For a complete list of compatible control cards, see Card Compatibility

NCS Upgrade Paths

Source Release	Upgrade Options
R9.6.0.7 (SONET or SDH) MSTP	R10.1.x.x (NCS fixed grid)
R9.8.1.1 (SONET or SDH) MSTP	
R10.0.1 (SONET or SDH) MSTP	
R10.0.2 (SONET or SDH) MSTP	
R10.0.1, 10.0.2 (NCS flex)	R10.1.x.x (NCS flex)
R10.0.1, 10.0.2 (NCS fixed grid)	R10.1.x.x (NCS fixed grid)

Source Release	Upgrade Options
R9.6.0.5 (SONET or SDH) MSTP	R10.0.1.x, 10.0.2 (NCS fixed grid)
R9.8.0 (SONET or SDH) MSTP	
R10.0 (SONET or SDH) MSTP	
R10.0.1 (SONET or SDH) MSTP	
R10.0, 10.0.1 (NCS flex)	R10.0.1.x, 10.0.2 (NCS flex)
R10.0, 10.0.1 (NCS fixed grid)	R10.0.1.x, 10.0.2 (NCS fixed grid)

For upgrade path details, refer the NCS Software Matrix

Some of the key limitations to be considered before proceeding with the upgrade are:

- When a node is upgraded from R9.80 (SONET or SDH), R10.0 (SONET or SDH) MSTP to NCS fixed grid, the database backup taken from the originating release cannot be restored after the upgrade.
- When a node is upgraded from NCS fixed grid to NCS flex, the database back-up taken from the originating release cannot be restored after the upgrade.
- When a node is upgraded from NCS fixed grid to NCS fixed grid or from NCS flex to NCS flex, the database is retained during the upgrade.

Caution Do not attempt to upgrade a configuration that contains Cisco ONS 15454 M12 nodes to Cisco NCS software.

Errorless Upgrades and Exceptions

This section describes important information to be aware of before you begin the upgrade process:

- When a node installed with GE_XP, GE_XPE, 10GE_XP, or 10GE_XPE cards configured with REP or a channel group is upgraded from R9.2.0 or later releases, traffic loss occurs. The traffic loss is less than 60 seconds for each GE_XP, GE_XPE, 10GE_XP, or 10GE_XPE card that undergoes a soft reset during the upgrade process.
- After you upgrade to R9.6.0 or later releases, use the **Force FPGA Update** button in the CTC card view > Provisioning > Card tab to update the SWAN FPGA image on OTU2_XP cards. This allows detection of the HI-BER alarm when OTU2_XP cards are configured in the 10G Ethernet LAN Phy to WAN Phy mode.
- The MXP_MR_2.5 and MXPP_MR_2.5 cards automatically download a new field-programmable gate array (FPGA) image during an upgrade from a software release prior to R7.0 to . The upgrades for DWDM configurations are expected to be errorless with the following exceptions if nodes are running MXP_MR_2.5 and MXPP_MR_2.5 cards:
  - If Y-cable protection is not provisioned, the data path incurs a traffic hit of up to 10 seconds or less.
  - If Y-cable protection is provisioned on cards running Fiber Channel (FC) payloads, traffic switches away from the card downloading the new FPGA causing the FC link to be reinitialized.
  - If Y-cable protection is provisioned on cards running Gigabit Ethernet (GE) payloads, there is no traffic interruption.

Cisco NCS Software Packages

Caution Do not download and activate the Cisco NCS software package on a Cisco ONS 15454 M12 shelf.

The Cisco NCS software is shipped in two packages:

- NCS Flex: contains software that supports flex cards and configurations in NCS 2002 and NCS 2006 . WSON is supported in this package.
- NCS Fixed Grid: contains software that supports fixed grid cards and configurations in NCS 2002 and NCS 2006. WSON is supported in this package.

Note You can download the NCS fixed grid package on a NCS flex node and vice versa. The node database is deleted during the activation. After the activation, it is recommended to relaunch CTC to view the new package that is activated. The database is not lost during activation, for Optical Line Amplifier (OLA) nodes with these cards- OPT-AMP-C, OPT-EDFA-xx, OPT-RAMAN-CTP, OPT-RAMAN-COP.

This table describes the node controller and shelf controller for NCS packages.

Package	Node Type	Node Controller	Shelf Controller
NCS Flex	Flex NCS Node	TNC / TNCE / TSC / TSCE / TNCS / TNCS-O / TNCS-2 / TNCS-2O	TNC / TNCE / TSC / TSCE / TNCS / TNCS-O / TNCS-2 / TNCS-2O
NCS Fixed Grid	Fixed Grid Node	TNC / TNCE / TSC / TSCE / TNCS / TNCS-O / TNCS-2 / TNCS-2O	TNC / TNCE / TSC / TSCE / TNCS / TNCS-O / TNCS-2 / TNCS-2O

Document Procedures

Procedures in this document must be performed in consecutive order unless noted otherwise. Ensure that the procedure is completed for each node in a given network. If you are new to upgrading the software, make a printed copy of this document and use it as a checklist.

Each non-trouble procedure (NTP) is a list of steps designed to accomplish a specific procedure. Follow the steps until the procedure is complete. If you need more detailed instructions, refer to the detail-level procedure (DLP) specified in the procedure steps. Throughout this guide, NTPs are referred as “procedures” and DLPs as “tasks.” Every reference to a procedure includes its NTP number, and every reference to a task includes its DLP number.

The DLP (task) supplies additional task details to support the NTP. The DLP lists numbered steps that lead you through completion of a task. Some steps require that equipment indications be checked for verification. When a proper response is not obtained, a trouble clearing reference is provided.

This section lists the document procedures (NTPs). Turn to a procedure for applicable tasks (DLPs).

1. NTP-U487 Preparing to Upgrade to a New Release, on page 4—This procedure contains critical information and tasks that you must read and complete before beginning the upgrade process.
2. NTP-U488 Back Up the Cisco NCS Software Database, on page 5—Complete the database backup to ensure that you have preserved your node and network provisioning in the event that you need to restore them.

3. NTP-U489 Upgrade the Cisco NCS Software , on page 6—Complete this procedure to complete the upgrade.
4. NTP-U490 Install Public-Key Security Certificate, on page 13— Complete this procedure to be able to run the software.
5. NTP-U491 Restore the Previous Software Load and Database, on page 14— Complete this procedure if you want to return to the previous software load you were running before activating the new release.

NTP-U487 Preparing to Upgrade to a New Release

Purpose	This procedure provides critical information checks and tasks you must complete before beginning an upgrade to the latest release.
Tools/Equipment	Cisco NCS nodes
Prerequisite Procedures	"DLP-G46 Log into CTC" in the "Connect the PC and Log into the GUI" document.
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Superuser

Procedure

Step 1 Before you begin, make sure that information related to your site, for example, date, street address, site phone number, and dialup number are stored in a safe and accessible location. The data will be useful during and after the upgrade.

Step 2 Read the release notes of the release you are upgrading to. Visit Release Notes to download the release notes.

Step 3 Ensure your workstation meets the minimum hardware and software requirements before starting the upgrade. For more information on the hardware and software requirements, read the release notes.

Step 4 Refer to the Software Upgrade Matrix to verify if the upgrade path is supported.

Step 5 Make sure that the control cards are installed in the appropriate slots on all the nodes in the network and on both the slots as indicated here. For a complete list of supported control cards, see Supported Control Cards:

- NCS 2015 shelf — control cards in Slots 1 and 17
- NCS 2006 shelf— control cards in Slots 1 and 8
- NCS 2002 shelf— control cards in Slot 1

Step 6 Repeat the above step for every node in the network.

Step 7 Collect the node diagnostics logs from the node. This action is very useful incase the upgrade fails, as the diagnostics help in understanding if the node had issues before the upgrade.

Step 8 Export the current alarms and conditions to your local storage. After the upgrade, if new alarms or conditions arise, then comparing the time stamp of the alarm to the previously saved time stamp helps in identifying new alarms or conditions.

Step 9 Perform a backup of the node database. This is very useful incase the upgrade fails, then the database can be restored using the backup. The detailed procedure for backing up the database is discussed in the next section.

Stop. You have completed this procedure.

NTP-U488 Back Up the Cisco NCS Software Database

Purpose	This procedure retains all configuration data for your network before performing the upgrade.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	• "DLP-G46 Log into CTC" in the "Connect the PC and Log into the GUI " document. • NTP-U487 Preparing to Upgrade to a New Release, on page 4
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Superuser

Procedure

Step 1 In the node view, click the **Maintenance**>**Database** tabs.

Step 2 In the database pane, click the **Backup** button.

The Database Backup dialog box is displayed.

Step 3 Click **Browse**. Navigate to the local PC directory or network directory and type a database name using the IP address of the node to upgrade in the File Name field and click **OK**. To overwrite an existing file, click **Yes**.

Step 4 When the backup is complete, click **OK.**

Step 5 Repeat Steps 1 through 5 for each node in the network.

Step 6 (Optional) It is recommended that you manually log critical information by either writing it down, printing screens, or by exporting the data to an appropriate format, as applicable. Use the following table to determine the information that should be logged.

Information	Record Data Here
IP address of the node	

Information	Record Data Here
Node name	
Timing settings	
DCC[1] connections—list all optical ports with active DCCs	
User IDs of all users, including at least one Superuser	
Inventory—A print screen of the Inventory window	
Active card	NCS 2015 - Slot 1 and Slot 17 NCS 2006 - Slot 1 and Slot 8
Network information—A print screen of the Provisioning tab in the network view	
List all protection groups in the system—A print screen of the Protection group window	
List alarms—A print screen of the Alarm window	
List circuits—A print screen of the Circuit window	

[1] DCC=data communications channel

Stop. You have completed this procedure.

NTP-U489 Upgrade the Cisco NCS Software

Purpose	This procedure upgrades the CTC software to R11.1 and must be performed on all nodes, or groups of nodes to be upgraded.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	NTP-U488 Back Up the Cisco NCS Software Database, on page 5
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Superuser

Caution Do not perform maintenance or provisioning activities during the activation task.

Note When you perform software activation on nodes, if there is any circuit in the partial state, then you should relaunch the CTC. Ensure that all the nodes in the network are in the R11.12 version.

Procedure

Step 1 Insert the software CD into the workstation CD-ROM drive (or otherwise acquire access to the software) to begin the upgrade process.

Note
Inserting the software CD activates the CTC Java Setup Wizard. Use the setup wizard to install the components or click **Cancel** to continue with the upgrade.

Step 2 Complete the DLP-U546 Download the NCS Software, on page 8 task for all nodes to be upgraded.

Step 3 Complete the DLP-U548 Activate the New Cisco NCS Software, on page 9 task for all nodes to be upgraded.

Note
Only one node can be activated at a time. During a parallel upgrade, activate another node as soon as the controller cards reboot successfully. To perform parallel upgrade remotely, wait five minutes for the controller cards to reboot completely.

Step 4 Complete the DLP-U549 Delete Cached JAR Files, on page 11 task, as necessary.

Step 5 (Optional) If you want to prevent a software revert to an earlier software release, complete the DLP-U546 Download the NCS Software, on page 8 task on all nodes, or groups of nodes you are upgrading a second time.

Caution
If the software is downloaded again after a version is activated, a revert to the previous version cannot be performed.

Step 6 If you need to return to the software and database you had before activating Software R11.1, proceed with the NTP-U491 Restore the Previous Software Load and Database, on page 14 procedure.

Step 7 To back up the Software R11.1 database for the working software load, see NTP-U488 Back Up the Cisco NCS Software Database, on page 5 procedure in order to preserve the database for the current release.

After the upgrade is complete, the date and time in CTC is reset.

Stop. You have completed this procedure.

What to do next

After upgrading the software to a different build, if there is a change in the FPGA, the FPGA is upgraded automatically. During the FPGA upgrade process, the card goes for a cold reboot. If Optical Supervisory Channel (OSC) is provisioned, then the transient PPM-IMPROPER-REMOVAL alarm is raised, which gets cleared in a short span of time. This happens because of the power glitches to the PPM while the card is coming up after the cold reboot.

DLP-U546 Download the NCS Software

Purpose	This task downloads software to the NCS nodes before activation.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	NTP-U488 Back Up the Cisco NCS Software Database, on page 5
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Maintenance user or higher

Note If the node running CTC on Windows or VM sends a packet with size greater than 1492 bytes, the packet does not reach the node that is connected to OSC. For example, in a GNE-ENE connection over an OSC link, software download fails on the ENE if the GNE sends a packet with size greater than 1492 bytes.

Note The control card contains flash memory with two partitions—Working and protect (backup). The software is downloaded to the protect (backup) partition of the flash memory on both the standby and active cards. This download is not traffic affecting because the active software continues to run in the primary RAM location. The software can therefore be downloaded at any time.

Note To download and upgrade the software using TL1, see the procedure.

Before you begin

If you want to download the software onto the node connected to OSC, ensure the node running CTC has set the MTU size to 1492.

Procedure

Step 1 From CTC View menu, choose **Go to Network View**.

Step 2 Make sure that the alarm filter is turned off. To do so, complete the following:

a) Click the **Filter** tool that is located at the lower-left side of the window.

The Alarm Filter dialog box appears.

b) Click to select any check box that is not selected in the Show Severity section of the **General** tab.

Step 3 Resolve any outstanding alarms. To view alarms for all the nodes in the network, click the **Alarms** tab.

Note

The SFTWDOWN alarm is raised on the standby and active control cards during software download. The alarms clear when the download is complete.

Step 4 From the CTC View menu, choose **Go to Home View** to go to the node view.

Step 5 Click the **Maintenance**> **Software** tabs.

Step 6 Click the **Download** button. The Download Selection dialog box appears.

Step 7 Locate the software files on the software CD or on your hard drive.

Step 8 To open the folder, choose the file with the PKG extension and click **Open**.

Step 9 From the list of compatible nodes, select the nodes where the software must be downloaded.

Note
It is recommended that simultaneous software downloads on the section data communications channel (SDCC) be limited to eight nodes at a time, using the central node to complete the download. If more than eight concurrent software downloads are selected at a time, it is placed in a queue.

Step 10 Click **OK**. The Download Status column monitors the progress of the download.

Step 11 Return to your originating procedure (NTP).

DLP-U548 Activate the New Cisco NCS Software

Table 1: Feature History Table

Feature Name	Release Information	Feature Description
SSH upgrade	Cisco NCS 2000 Release 11.14	When you upgrade to R11.1.4, the SSH and SSL libraries upgrade to the latest revisions that provides better security, addressing vulnerabilities. New versions CTC supports after upgrade (R11.1.4) CISCOSSL: 1.1.1y.7.3.377 (6/6/2024) CISCOSSH: 1.14.55

Purpose	This task activates the software on each node in the network.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	DLP-U546 Download the NCS Software, on page 8
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Superuser

Note It is recommended that the first node that is activated be connected via LAN. This ensures that the new CTC JAR files download to the workstation as quickly as possible.

If a node is provisioned to have no LAN access, the value is overridden in the case of node isolation. Additionally, if the node is not reachable, the LAN access is turned on. It is recommended that you avoid node isolation.

Note During the activation process, when the node is being upgraded to R11.0 (and later releases), the USB-MOUNT-FAIL alarm is raised. In MSM, the USB-MOUNT-FAIL alarm is raised on all subtended shelf controllers and the node controller. When all the subtended shelf controllers and the node controller complete the upgrade successfully, the USB-MOUNT-FAIL alarm is cleared. No manual intervention is required to clear the USB-MOUNT-FAIL alarm. After the USB-MOUNT-FAIL alarm is cleared, USB sync is triggered. After USB sync is successfully completed, the node is migrated to the latest software successfully.

Note During the activation process for upgrading the node from Release 11.1.3.2 or earlier to Release 11.1.4 or later, both Active and Standby controller cards perform an additional boot.

Procedure

Step 1 If CTC is not already started, start CTC.

Step 2 Record the IP address of the node. The IP address can be obtained either on the LCD or on the upper left corner of the CTC window.

Step 3 Make sure that the alarm filter is turned off. To do so, complete the following:

a) Click the **Filter** tool at the lower-left side of the window.

The Alarm Filter dialog box appears.

b) Click to select any check box that is not selected in the Show Severity section of the **General** tab.

Step 4 Make sure that all cards that are part of a 1+1 or Y-cable protection group must be active on the working card of the protection group and no protection switches are occurring. Also, ensure that traffic carrying protect cards are in a standby state. To do so, complete the following:

a) In the node view, click **Maintenance** > **Protection** tabs.

b) Select each protection group listed and view the active or standby status of each card in the Selected Group area.

Step 5 In shelf view, click the **Maintenance** > **Software** tabs.

Step 6 Verify that the version in the Protect Version column is .

Step 7 Click the **Activate** button. The Activate dialog box displays a warning message.

Step 8 Click **Yes** to proceed with the activation.

During node activation, all the common control cards in the node reboot beginning with the standby card. As soon as the standby card recovers from the reboot, it signals the active card to reset as a standby card and the standby card transitions to active. An Activation Successful message indicates that the software is successfully activated.

Step 9 Click **OK**.

The connection between CTC and the node is lost and CTC displays the Network view. The INCOMPATIBLE-SW alarm is raised in CTC for the first node that is activated because CTC is unable to connect to the NE due to differing, incompatible versions of the software between CTC and the NE. A CTC alert is displayed to update the CTC software. To clear the INCOMPATIBLE-SW alarm, perform steps 10 through 12 only for the first node that is activated on the network.

During the activation process:

- The SYSBOOT alarms are raised when the common control cards and cross-connect card reset. These alarms clears when all the cards reset.

  The activation process can take up to 30 minutes, depending on the number of cards installed in the node.
- The GCC-EOC, EOC, and EOC-E alarms are transient. These alarms are raised and cleared during the upgrade process when the control cards and line cards reset.
- Protect cards in the Y-cable protection group boot next, in the order that the protection group was created.
- Other line cards reset one after the other in the order of slot number.

If you are upgrading remotely and cannot see the nodes, wait for 5 minutes for the process to complete, then check to ensure that related alarms have cleared before proceeding.

Step 10 In CTC, choose **File > Update CTC**. The CTC software is updated. A CTC alert is displayed to restart CTC.

Step 11 In CTC, choose **File > Exit.**

Step 12 Start CTC again.

Step 13 Click the **Launch CTC** button in the CTC launcher window.

The new CTC applet loads. The login window is displayed.

Step 14 Type the user name and password and click **Login**.

Step 15 Return to your originating procedure (NTP).

DLP-U549 Delete Cached JAR Files

Purpose	This task deletes cached JAR files.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	None
Required/As Needed	You need to complete this task after you activate the first network node.
Onsite/Remote	Onsite or remote
Security Level	Maintenance user or higher

Note Whenever the CTC software is upgraded or reverted, make sure that the browser and hard drive cache files are cleared.

Procedure

Step 1 Delete cached files from your browser directory.

In Netscape:

a) Select **Edit** > **Preferences**. Click the **Advanced** tab and click the **Cache** button.
b) Click the **Clear Memory Cache** button, and click **OK**.
c) Click the **Clear Disk Cache** button, and click **OK** twice.

In Microsoft Internet Explorer:

a) Select **Tools** > **Internet Options**. The Internet Options dialog box appears.
b) Click the **General** tab, and then click the **Delete Files** button.
c) Select the **Delete all offline content** check box.
d) Click **OK** twice.

Step 2 Close the browser.

Note
Cached JAR files cannot be deleted from the hard drive until the browser is closed. Other applications that use JAR files must also be closed.

Step 3 On Windows systems, delete cached files from your workstation in this location:

`C:\Documents and Settings\`*`username`*`\Application Data\Cisco\CTC`

Step 4 Reopen the browser. You should now be able to connect to CTC.

Step 5 Return to your originating procedure (NTP).

DLP-U551 Set the Date and Time

Purpose	This task sets the date and time. If you are not using SNTP, the upgrade procedure can cause the Date/Time setting to change. Perform this task to reset the date and time at each node.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

Note If you are using SNTP, this task is not applicable.

Procedure

Step 1 In CTC node view, click the **Provisioning** > **General** tabs.

Step 2 Set the correct date and time. Click **Apply** .

Step 3 Repeat Steps 1 and 2 on all the remaining nodes.

Step 4 Return to your originating procedure (NTP).

NTP-U490 Install Public-Key Security Certificate

Purpose	This procedure installs the ITU Recommendation X.509 public-key security certificate. The public-key certificate is required to run software R4.1 or later.
Tools/Equipment	None
Prerequisite Procedures	This procedure is performed when logging into CTC. You cannot perform it at any other time.
Required/As Needed	This procedure is required to run software R4.1 or later.
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 Log into CTC.

Step 2 If the Java Plug-in Security Warning dialog box appears, choose one of the following options:

- Grant This Session—Installs the public-key certificate on the PC only for the current session. After the session ends, the certificate is deleted. This dialog box appears at the next login into the node.
- Deny—Denies permission to install the certificate. If this option is chosen, login into the node is denied.
- Grant always—Installs the public-key certificate and does not delete it after the session is over. It is recommended to use this option.
- View Certificate—The public-key security certificate is displayed.

After the completion of the security certificate dialog boxes, the web browser displays information about the Java and system environments. If this is the first login, a CTC downloading message appears while CTC files are downloaded to the computer. The process can take several minutes, if it is the first time. After the download, the CTC Login dialog box appears.

Step 3 Return to the software and database you had before activating the software, proceed with the NTP-U491 Restore the Previous Software Load and Database, on page 14 procedure.

Stop. You have completed this procedure.

NTP-U491 Restore the Previous Software Load and Database

Purpose	This procedure returns to the software and database provisioning that was present before R11.1 was activated. The software load and database cannot be restored to the previous version if the software on both the working and protect cards were upgraded to R11.1.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	"DLP-G46 Log into CTC" in the "Connect the PC and Log into the GUI" document. NTP-U487 Preparing to Upgrade to a New Release, on page 4 NTP-U488 Back Up the Cisco NCS Software Database, on page 5 NTP-U489 Upgrade the Cisco NCS Software , on page 6
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

Note Tasks to revert to a previous load are not part of the upgrade, and are provided here as a convenience to those wishing to perform a revert after an upgrade. If you have successfully performed all necessary procedures up to this point, you have finished the software upgrade.

Caution If a node is set to secure, dual-IP mode, the database information is overwritten with this configuration and cannot be reverted to single-IP repeater mode.

Note All line cards of the subtended shelf controller may undergo a reboot during a software revert from Release 11.0 or earlier to a previous software release and is traffic impacting.

Procedure

Step 1 Complete the DLP-U552 Revert to Protect Load, on page 15 task.

Step 2 If the software revert to your previous release failed to restore the database, complete the DLP-U553 Manually Restore the Database, on page 16 task.

Stop. You have completed this procedure.

DLP-U552 Revert to Protect Load

Purpose	This task reverts to the software you were running prior to the last activation.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	NTP-U487 Preparing to Upgrade to a New Release, on page 4 NTP-U488 Back Up the Cisco NCS Software Database, on page 5 NTP-U489 Upgrade the Cisco NCS Software , on page 6
Required/As Needed	Required for revert
Onsite/Remote	Onsite or remote
Security Level	Superuser

Note Software revert after downloading or replacing the current protect SW version with another older SW version is not supported and might cause service disruption.

Note To perform a supported (non-service-affecting) revert from , the release you want to revert to must have been working at the time you activated to the current software version on that node. Also, a supported revert automatically restores the node configuration at the time of the previous activation. The exception to this is when you have downloaded a second time, ensuring that no revert to a previous load can take place. In this case, the revert occurs, but is not traffic-affecting and does not change the database.

Note Ensure that all cards that are part of a protection group (1+1 or Y-cable) are active on the working card of that protection group and that no protection switches are occurring. To ensure that traffic carrying protect cards are in a standby state, in the node view click the **Maintenance** tab, and view the Protect column for each of the listed protection groups. View the active/standby status of each card in the Maintenance tab.

Procedure

Step 1 From the node view, click the **Maintenance** tab, then click the **Software** button.

Step 2 Verify that the protect software displays the release you upgraded from.

Step 3 Click the **Revert** button. Revert activates the protect software and restores the database from the previous load. A confirmation dialog box appears.

Note
Any FPGA downgrades during the revert process may affect traffic. Configuration changes made after activation are lost when you revert.

Step 4 Click **OK**. This begins the revert process and drops the connection to the node.

Step 5 Wait until the software revert completes before continuing.

Note
The system reboot may take up to 30 minutes to complete.

Step 6 Wait one minute before reverting another node.

Step 7 After reverting all the nodes in the network, restart the browser and log back into the last node that was reverted. This uploads the appropriate CTC applet to your workstation.

Step 8 Perform the DLP-U549 Delete Cached JAR Files, on page 11 task.

Step 9 Return to your originating procedure (NTP).

DLP-U553 Manually Restore the Database

Purpose	This task manually restores the database. Use this task if you were unable to perform a revert successfully and need to restore the database.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	DLP-U552 Revert to Protect Load, on page 15
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

Note If the node running CTC on Windows or VM sends a packet with size greater than 1492 bytes, the packet does not reach the node that is connected to OSC. For example, in a GNE-ENE connection over an OSC link, database restore fails on the ENE if the GNE sends a packet with size greater than 1492 bytes.

Caution Do not perform these steps unless the software revert failed.

Caution This process is service affecting and should be performed during a maintenance window.

Before you begin

If you want to restore the database onto the node connected to OSC, ensure the node running CTC has set the MTU size to 1492.

Procedure

Step 1 In CTC node view, click the **Maintenance** tab, then click the **Database** button.

Step 2 Click the **Restore** button. The DB Restore dialog box appears.

Step 3 Click **Browse** to locate the database file stored on the workstation hard drive or on network storage.

Step 4 Click the database file to highlight it and click **Open**. The DB Restore dialog box appears.

Step 5 If you need a complete database restore, check the **Complete database (System and Provisioning)** checkbox.

Note
The following parameters are restored only when the **Complete Database (System and Provisioning)** checkbox is checked: node name, IP address, subnet mask and gateway, and IIOP port. If you change the node name and then restore a backed up database on this node, the circuits automatically map to the newly renamed node. It is recommended to keep a record of the old and new node names.

Step 6 Click **Ok**.

The database is restored and the control cards reboot.

Step 7 When the control cards have finished rebooting, log into CTC and verify that the database is restored.

Wait one minute before restoring the next node.

Step 8 Repeat Steps 1 to 7 for each node in the network.

You have now completed the manual database restore.

Note
When the complete database is restored, the node does not report an event regarding the IP change; the node reboots and configures the new IP from the database. If the IP address being restored is not in the CTC network IP addressing scheme, you might lose visibility of the node. To resolve this, you must launch CTC with the IP mentioned in the table against the database backup. Refer to the table, “Manually Recorded Data” in the NTP-U488 Back Up the Cisco NCS Software Database, on page 5 procedure for more information.

Step 9 Return to your originating procedure (NTP).

Related Documentation

Use this document in conjunction with the following publications:

- Release notes:

  http://www.cisco.com/en/US/products/ps13295/prod_release_notes_list.html

- TL1 command guides:

  http://www.cisco.com/en/US/products/ps13295/prod_command_reference_list.html

- Troubleshooting guides:

  http://www.cisco.com/en/US/products/ps13295/prod_troubleshooting_guides_list.html

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly What's New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at: http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the What's New in Cisco Product Documentation as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2026 Cisco Systems, Inc. All rights reserved.