Install and Login to Cisco Transport Controller

After you have established a connection to the node using the console port of the system, setup a computer for Cisco Transport Controller (CTC) and login to CTC. CTC is used to perform operations, administration, maintenance and provisioning activities of the system.

- Setup Computer for CTC, on page 1
- Login to CTC, on page 2

Setup Computer for CTC

Component	Specification
Hardware	Intel Core i5, i7, or faster processor. A minimum of 4 GB RAM, 100 GB hard disk with 250 MB of available hard drive space.
Operating Systems	One of the following: • Windows: • Windows 7 • Windows Server 2008, or later • Apple Mac OS X • UNIX workstation with Solaris Version 9 or 10 on an UltraSPARC-III or faster processor, with a minimum of 1 GB RAM and a minimum of 250 MB of available hard drive space. • Ubuntu 12.10
Java Runtime Environment	JRE 1.6 with support for European languages
Browser	One of the following: • Internet Explorer • Mozilla Firefox • Safari • Google Chrome

Before you begin

Ensure that the basic configuration required to establish a connection to the node is complete. See Establish Connection to a Node.

What to do next

Login to CTC and establish network connection to the node.

Login to CTC

Before you begin

Table 1: Feature History

Feature Name	Release Information	Feature Description
DUO Two-Factor Log In	Cisco IOS XR Release 6.5.32	DUO Two-Factor Log In feature enables the CTC to authenticate the user with a secure DUO password. The Two-Factor authentication requires the user to enter a combination of DUO passcode and node password to access a node in the network. This log in feature does not support Automatic Network Discovery.

- Ensure that you have setup a computer that meets the hardware and software requirements to use Cisco Transport Controller (CTC).
- Ensure you have complete image installed. If you have mini.iso image installed, then the ncs4k-mgbl.pkg must be installed on the NCS 4000 system.
- Complete the "Configuring XML Agent" task.
- Complete "Configure HTTP" task.
- Run the **snmp-server ifindex persist** command for Generalized Multi-Protocol Label Switching (GMPLS) to retain its links over a reload.

Step 1 From the computer connected to the NCS 4016 shelves, start Windows Internet Explorer or Mozilla Firefox web browser.

Step 2 In the browser URL field, enter the NCS 4016 IPv4 or IPv6 virtual address.

Step 3 Press **Enter**. The browser displays a window with a Delete CTC Cache field and information about the Cisco Transport Controller Java and System environments.

Note

- The Delete CTC Cache field deletes the CTC JAR (Java Archive) files that are downloaded to your computer when you log into NCS 4000. You perform this action if connectivity problems occur or you want to delete older CTC JAR file versions from your computer.
- If you are logging into NCS 4000 nodes in an operation network that are running different releases of CTC software, log into the node running the most recent release. If you log into a node running an older release, you will receive an INCOMPATIBLE–SW alarm for each node in the network running a new release, and CTC will not be able to manage these nodes. To check the software version of a node, select **About CTC** from the CTC Help menu. This will display the software version for each node visible on the network view. If the node is not visible, the software version can be read from the LCD display.

Step 4 If a Java Plug-in Security Warning dialog box appears, install the public-key security certificate.

The first time you connect to NCS 4000, this process can take several minutes. After the download, a warning message window appears.

Step 5 Click **OK**.

Step 6 In the CTC login window, type a user name and DUO password (both are case-sensitive).

Note DUO password is a combination of the node password and DUO passcode (OTP). For example, if the node password is Abcd123eS and passcode is 123456, then the DUO Password is Abcd123eS123456.

Step 7 Each time you login to CTC, you can select the following login options:

- Additional Nodes — Displays a list of current login node groups.
- Disable Network Discovery — Check this box to view only the NCS 4000 (and additional nodes within the login node group, if any) entered in the Node Name field. Nodes linked to this node through Data Communication Channels (DCC) are not discovered and will not appear in CTC network view. Using this option, you can decrease the CTC startup time in networks with many DCC–connected nodes, and can reduce memory consumption. If Disable Network Discovery is unchecked, CTC attempts to upgrade the CTC software by downloading more recent versions of the JAR files it finds during the network discovery. Click **Yes** to allow CTC to download the newer JAR files, or **No** to prevent CTC from downloading the JAR files.

  Note Upgrading the CTC software will overwrite your existing software. You must restart CTC after the upgrade is complete.

  Note DUO Two-Factor login does not support automatic discovery of other nodes in the network.
- Disable Circuit Management — Check this box to disable discovery of existing circuits. Using this option, you can decrease the CTC initialization time in networks with many existing circuits and reduce memory consumption. After you are logged in, you can enable circuit discovery at any time by choosing the **Enable Circuit Discovery** button on the Circuits tab.
- SSH or Telnet - Select an option to establish a remote connection with the node.

  Note For Duo Two-Factor login, select the **SSH** radio button.

Step 8 Click **Login**.

CTC is displayed with three views: Home Page, Network View, and Node View.

Step 9 To create a NETCONF session, perform the following substeps:

a) In node view, select a NETCONF functional pane. For example, click **Provisioning** > **Timing**.

A confirmation dialog box appears.

b) Click **Yes**.

Admin-Plane Configuration dialog box appears.

c) Enter a user name and DUO password (both are case-sensitive).

Note DUO password is a combination of the node password and DUO passcode (OTP). For example, if the node password is Abcd123eS and passcode is 123456, then the DUO Password is Abcd123eS123456.

d) Click **Login**.

Note Log in to a CLI terminal and use the `show ssh` command to check the creation of the NETCONF session.

```
#show ssh
Mon Jul 12 18:50:15.120 IST
SSH version : Cisco-2.0

id chan pty location state userid host ver authentication connection type
--------------------------------------------------------------------------------------------------
Incoming sessions
1248 1 vty1 0/RP0 SESSION_OPEN root 10.xxx.xx.xxx v2 password Command-Line-Interface
1248 2 vty2 0/RP0 SESSION_OPEN root 10.xxx.xx.xxx v2 password Command-Line-Interface
1249 1 XXXXX 0/RP0 SESSION_OPEN root 10.xxx.xx.xxx v2 password Netconf-Subsystem
```

Note In the terminal, two channels with IDs 1 and 2 are created for one session and one channel (admin-plane) is created for another (NETCONF) session.

What to do next

Use CTC to bring up the node for network connectivity.