Cisco TelePresence Video Communication Server

Getting started

Contents

General information

About the Cisco TelePresence Video Communication Server (Cisco VCS)

The Cisco VCS enhances the video experience and provides seamless communication between SIP and H.323 devices utilizing IETF and ITU standards. The Cisco VCS is the center of the video communication network and connects all H.323 and SIP endpoints, infrastructure, and management devices. The Cisco VCS provides unrivaled scalability and redundancy to video communications, and is integral to interoperability with unified communications and Voice over IP systems.

The Cisco VCS can be deployed with either the Control application, the Expressway™ application or the Cisco VCS Starter Pack Express application, with various optional packages including FindMe™ and Dual Network Interfaces.

Installing the Cisco VCS

Package contents

To avoid damage to the unit during transportation the Cisco VCS is delivered in a special shipping box, which should contain the following components:

- Cisco VCS unit
- rack ears, screws and Torx driver
- rubber feet
- cables:
  - power cables
  - Ethernet cable
  - shielded serial cable

Report any discrepancies to your Cisco representative immediately.

We recommend that the shipping box is kept in case the Cisco VCS needs to be returned.

Before you start

IMPORTANT: Before installing the Cisco VCS, you must read the safety information at
www.cisco.com/go/telepresence/safety.

Preparing the installation site

Before installing the Cisco VCS:

- Ensure that the Cisco VCS is accessible and that all cables can be easily connected.
- Ensure that the power outlet is near to the Cisco VCS and is easily accessible.
- To ensure adequate ventilation, leave a space of at least 10cm (4 inches) behind the unit's rear panel and 10cm (4 inches) in front of the front panel.
  - The Cisco VCS has side air intakes and rear air exhaust. A check should be made to ensure there is sufficient ventilation, particularly at the sides.
  - Ensure that other devices are not exhausting directly into the air intake on the Cisco VCS. Note that Codian MCU airflow is from right to left, so be especially careful if racking them to the right of Cisco VCS.

Figure 1: Cisco VCS ventilation

- The room in which you install the Cisco VCS should have an ambient temperature between 0ºC and 35ºC (32ºF and 95ºF) and between 10% and 90% non-condensing relative humidity.
- Use a grounded AC power outlet for the Cisco VCS.

Preparing the unit

1. Unpack the unit.
2. Mount the rack ears (using a Torx T10 driver) or rubber feet.
3. Turn the unit back on its feet or mount it in the rack.

If this product is mounted in a rack you are recommended to use additional support accessories such as rack side support angles (rack angle brackets) or rack shelves, due to the unit's weight and depth. Ensure that units in the rack do not touch each other. Contact your rack supplier to request the accessories best suited for your rack.

Connecting the cables

1. Connect the power cable to the back of the Cisco VCS (see Figure 2).
2. Connect the Ethernet LAN cable from the LAN1 port on the front of the Cisco VCS to your network (see Figure 3).

Powering on the Cisco VCS

1. Turn on the power switch on the back right of the unit (adjacent to the power cable). The system will power up. If the unit does not start after 3 seconds, press the soft power button.
   Wait until:
   - the green PWR LED on the front of the unit is a steady green color (it may flash briefly during power up)
   - the red ALM LED on the front of the unit has gone out
   - the IP address is showing in the display panel on the front of the unit

If the red ALM LED flashes rapidly it indicates a hardware fault. Contact your local Cisco representative. The yellow HDD LED indicates disk activity and may flicker during normal operation, more so on a busy system.
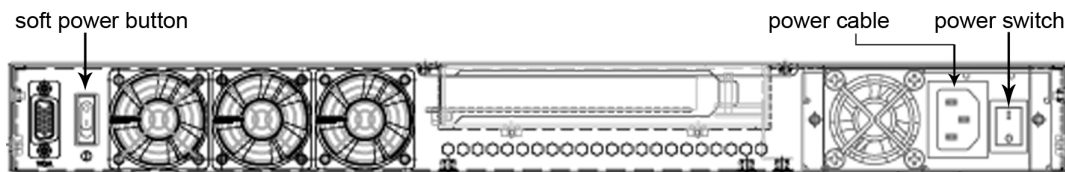

Figure 2: Cisco VCS back view

Initial configuration

Before you can use the Cisco VCS, you must configure its IPv4 address, subnet mask and default gateway. Consult your network administrator for information on which addresses to use. Note that the Cisco VCS must use a static IP address.

This initial configuration can be done:

■ by connecting from a PC to the Cisco VCS using a serial cable. This is the recommended process, and is described in the following section
■ by using the buttons on the front panel (see "Configuration using the front panel" on page 8)
■ if your network is set up to allow it, by connecting using a web browser to the default IP address of 192.168.0.100 (see "Using the web interface" on page 10)
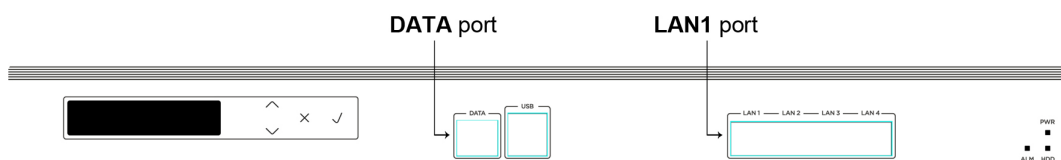

Figure 3: Cisco VCS front view

Configuration using a serial cable

To set the initial configuration using a PC connected to the Cisco VCS **DATA** port via a serial cable:

1. Connect the Ethernet LAN cable from the **LAN1** port on the front of the unit to your network.
2. Connect the supplied serial cable from the **DATA** port on the front of the unit to the serial port on a PC.
3. Start a terminal emulator program on the PC and configure it to use the PC's serial port as follows:
   - baud rate: 115200 bits per second
   - data bits: 8
   - parity: none
   - stop bits: 1
   - flow control (hardware and software): none

> ⚠ Do not leave a terminal emulator session open after it is no longer in use. An open session may cause issues during a system restart.

4. Turn on the power switch on the back right of the unit (adjacent to the power cable). The system will power up. If the unit does not start after 3 seconds, press the soft power button on the back left of the unit.
5. Wait until:
   - the green PWR LED on the front of the unit is a steady green color (it may flash briefly during power up)
   - the red ALM LED on the front of the unit has gone out
   - the default IP address (192.168.0.100) is showing in the display panel on the front of the unit

   The terminal emulator program on the PC will display the Cisco VCS's startup information. After approximately four minutes you will get the login prompt (if the Cisco VCS was already on when you connected the serial cable, press **Enter** to get the login prompt):

   ```
   cisco login:
   ```

6. Enter the username **admin** and press **Enter**.
   You will get the password prompt:

```
Password:
```

7. Enter the default password of **TANDBERG** and press **Enter**.
   You will get the install wizard prompt:

```
Run install wizard [n]:
```

8. Type **y** and press **Enter**.
9. Follow the prompts given by the install wizard to specify the following:
   - the password you want to use for your admin account

   For security reasons you are advised to change the password from the default of **TANDBERG**.

   - whether you want to use IPv4, IPv6 or Both
   - the LAN 1 IP address of the Cisco VCS
   - the LAN 1 IPv4 subnet mask of the Cisco VCS (if you have selected IPv4)
   - the IP default gateway of the Cisco VCS
   - the Ethernet speed

   Use the default value of **Auto** unless the switch to which you are connecting is unable to auto-negotiate.

   - whether you want to use SSH to administer the Cisco VCS

   After the wizard is finished the following message will appear:

```
Setting other settings...
OK. The system must be restarted for new
settings to take effect..
```

   And you will get a restart prompt:

```
Restart Now?
```

10. Type **y** and press **Enter**.
11. Disconnect the serial cable and store it in a safe place.

After it has rebooted, the Cisco VCS is ready to use. For security reasons you are advised to change the password for the default admin account (if you have not already done so) and the root account from the default of TANDBERG. See the sections "Changing the admin account password" on page 9 and "Changing the root account password" on page 9 for details.

   The IP configuration made using the install wizard applies to the LAN 1 Ethernet port only. If you have enabled the LAN 2 port (by installing the Dual Network Interfaces option key) you must use the web interface or CLI to configure the LAN 2 settings.

Configuration using the front panel

The LCD panel and buttons at the front of the Cisco VCS allow you to configure and check the IP settings as well as to reboot the system (see Figure 3). You are not recommended to perform the initial configuration using the front panel, but you may need to use this method if you do not have access to a PC and serial cable.
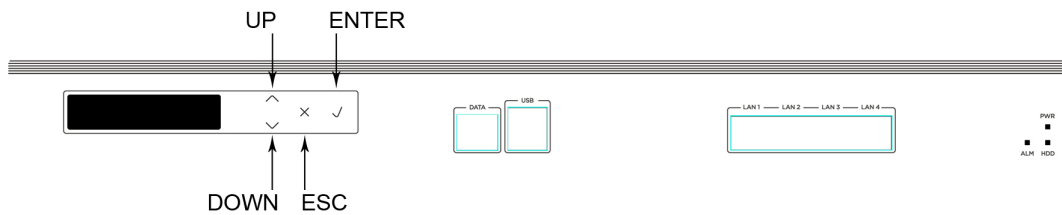

Figure 3: Cisco VCS LCD panel

By default, during normal operation the front panel shows a rotating display of status items, including the Cisco VCS's system name, IP addresses, warnings, and the number of current traversal calls, non-traversal calls and registrations.

To control the display of status items:

- **ENTER** stops the display from automatically rotating through the status items. This is useful if you need to review all of the warning messages or read a long IPv6 address. Press **ENTER** again to resume the rotating display.
- **UP/DOWN** displays the previous or next status item.

To access the front panel menu options, press **ESC**. The menu options are as follows:
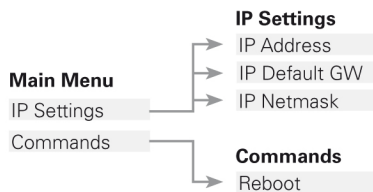
- **UP/DOWN** navigates to the next menu or submenu item.
- **ENTER** selects a menu or submenu item.
- When you have selected an IP setting from the menu:
  - **UP/DOWN** increases or decreases the value of the currently selected digit.
  - **ENTER** moves the cursor on to the next digit and saves your changes when you move off the final digit.
  - **ESC** cancels any changes; returns to the menu.
- When you are on the **Commands** submenu:
  - **ENTER** performs the command.
  - **ESC** returns to the main menu.
- To leave the menu options and return to the rotating display, press **ESC**.

Note that the IPv4 address and IPv4 subnet mask configuration made using the front panel applies to the LAN 1 port only. To configure the system's IPv6 settings and (if you have the Dual Network Interfaces option key installed) the LAN 2 settings, you must use the web interface or CLI.

Using the Cisco VCS

After you have set the initial configuration of the Cisco VCS, the system is ready to use. You can continue to use the serial connection to access and manage the Cisco VCS, or you can connect to the system remotely over IP using either or both:

- HTTPS (see "Using the web interface" on the next page)
- a command line interface via SSH (see "Using the Command Line Interface (CLI)" on the next page)

> ⚠ For security reasons, you should change the passwords for the admin account and the root account from the default of TANDBERG as soon as initial configuration of the Cisco VCS has been completed.

Changing the admin account password

To change the password for the admin account using the web interface:

1. Go to **Users > Administrator accounts**.
   You are taken to the **Administrator accounts** page.
2. Click on **View/Edit** for the admin name.
3. In the **Password** and **Confirm password** fields, enter the new password, and click **Save**.

To change the password for the admin account using the CLI:

1. Type **xConfiguration SystemUnit Password**

> ⚠ You cannot set a blank password for the admin user or any other administrator account, or the root account.

Changing the root account password

To change the password for the root account:

1. Using the CLI, log in as **root** using the existing password.
2. Type the command **passwd**.
   You will be asked for the new password.
3. Enter the new password and when prompted, retype the password.
4. Type **exit** to log out of the root account.

Other recommended configuration

You are now recommended to configure the following:

- The system name of the Cisco VCS. This is used by the Cisco TelePresence Management Suite (Cisco TMS) to identify the system. This can be set from the **System administration** page on the web interface (**System > Administration**).
- Automatic discovery. If you have multiple Cisco VCSs in the same network you may want to disable automatic discovery on some of them. This can be set from the **H.323** page on the web interface (**Configuration > Protocols > H.323**).
- The DNS server address(es), if URI dialing or Fully Qualified Domain Names (FQDNs) are to be used. This can be set from the **DNS** page on the web interface (**System > DNS**).

See the Cisco VCS Administrator Guide, deployment guides and release notes (available for download from www.cisco.com) or the online help for complete information on configuring these and all other options available on your Cisco VCS.

Using the web interface

To use the web interface:

1. Open a browser window and in the address line type either:
   - the IP address of the Cisco VCS
   - the FQDN of the Cisco VCS
   The **Login** page will appear.
2. Select **Administrator Login**.
3. Enter a valid administrator username and password and select **Login**.
   You will be presented with the **Overview** page.

See the online help or the Cisco VCS Administrator Guide for further information on the configuration options available for each page of the Cisco VCS web interface.

Using the Command Line Interface (CLI)

The command line interface is available over SSH and through the serial port by default.

To use the command line interface:

1. Start an SSH session.
2. Enter the IP address or FQDN of the Cisco VCS.
3. Login with a username of `admin` and your system password.
   You will see a welcome message.

For a full list of CLI commands available on the Cisco VCS, see the Cisco VCS Administrator Guide.

Documentation and training

All Cisco VCS documentation including the Cisco VCS Administrator Guide, FindMe™ User Guide, Cisco VCS deployment guides and release notes, plus supporting documentation for other products, is available in PDF format from the Support area of our web site at www.cisco.com. You can download and print these documents locally, if required. Our systems also have intuitive on-page help, which provides a range of useful features and tips.

Training is available on all our products online and at our training locations. For more information on all the training we provide and where our training offices are located, visit www.cisco.com/go/telepresencetraining.

Disclaimers and notices

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. 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. (1005R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.