Using Cisco TelePresence Immersive System CLI Commands

Revised: April 22, 2020

This chapter explains how to use command-line interface (CLI) commands with your immersive Cisco TelePresence system. This chapter contains the following information:

Starting a CLI Session

You can only access the CLI remotely. Use Secure Shell (SSH) from a personal computer or workstation to connect securely to the system.

Before You Begin

Before you begin, be sure that you have the following information:

- System IP address
- Administrator ID and password

You will need this information to log into the system.

Note The administrator ID and password can be changed in the Cisco Unified Communications Manager (Cisco Unified CM) device page. See the *Cisco Unified Communications Manager Configuration Guide for the Cisco TelePresence System* for more information.

Procedure

To start a CLI session, follow these steps:

Step 1 From a remote system, use SSH to connect securely to the system. In your SSH client, enter the following:

```
ssh adminname@hostname
```

Where **adminname** specifies the Administrator ID and **hostname** specifies the hostname that was defined during installation. For example, **ssh admin@ipt-1**.

Step 2 Enter your administrator ID. The system prompts you for a password.

Step 3 Enter your password. The CLI prompt displays. The prompt represents the Administrator ID. For example:

```
admin:
```

Step 4 Proceed by entering CLI commands.

Managing Passwords

This section contains the following password information:

Password Aging

To ensure that your system is protected when using Cisco TelePresence Command Line Interface (CLI), you must periodically update your password. The system alerts you to the number of days remaining on your current password in the login banner when you log onto the system. The system issues a warning when 14 days remain on your current password, and so on until the password expires. You may get a message similar to the following at login:

"Password change required in 10 days."

Warning **If the password is allowed to expire, the system will ignore the login attempt and you cannot access the system. You must create a new password using Cisco Unified Communications Manager. See the "Resetting Your Password in Cisco Unified CM" section on page 1-4 for more information.**

In CTS Release 1.6.1, the password life (the maximum age, in days) can be configured using new fields on the Cisco Unified CM **Device > Phone > Product Specific Configuration Layout > Secure Shell Information** page:

- SSH Admin Life
- SSH Helpdesk User
- SSH Helpdesk Password
- SSH Helpdesk Life

The password expiration can be set to have a value between 0 and 365. A setting of 0 disables password aging, and the default is 60 days. Unless the configured life has been disabled (by being set to 0), password age is set to have 2 days remaining in the following situations:

- New installations and factory resets.
- Software upgrades (if the password age is less than the configured age).
- Password recovery (using the **pwrecovery** command).

Password Notices

When the password age has expired, a warning message is shown briefly on-screen before logging out. Notice information is printed at login when there are 14 days or less remaining on the current password.

When you log in, you will receive one of three banners:

Example 1-1 7 to 14-Day Warning

If your password is about to expire within 7 to 14 days, you will see a message similar to the following:

```
customer@mypc #1000:ssh admin@108.100.000.25
admin@108.100.000.25's password:
Command Line Interface is starting up, please wait ...

Welcome to the TelePresence Command Line Interface (version 1.1)

Last login: Wed Dec 9 22:22:58 PST 2009 from philly.cisco.com
Password change required in 10 days

admin:
```

Example 1-2 0 to 7-Day Warning

If your password is about to expire within 0 to 7 days, you will see a message similar to the following:

```
customer@mypc #1000:ssh admin@108.100.000.25
admin@108.100.000.25's password:
Command Line Interface is starting up, please wait ...

****** Warning ******
You must change your admin password in the next 2 days
****** Warning ******

Welcome to the TelePresence Command Line Interface (version 1.1)
Last login: Fri Nov 13 13:12:42 PST 2009 from mypc.cisco.com
Password change required in 2 days

admin:
```

Example 1-3 0 Days Remaining

If your password is expiring with 0 days remaining on the current password, the following banner is shown. The session waits for 10 seconds then disconnects.

```
customer@mypc #1000:ssh admin@108.100.000.25
admin@108.100.000.25's password:
Command Line Interface is starting up, please wait ...

****** Warning ******

You have not changed your admin password in more than 60 days
The admin account login has been disabled

*****************************************************
* *
* Please go to the CUCM and change the password *
* *
*****************************************************

****** Warning ******

Connection to 108.100.000.25 closed.
```

Resetting Your Password in Cisco Unified CM

See the *Cisco Unified Communications Manager Configuration Guide for Cisco TelePresence System* and follow these steps to create a new password:

Step 1 Log into the Cisco Unified CM Administration application.

Step 2 Navigate to **Device > Phone > Product Specific Configuration Layout**.

Step 3 Scroll down to the Secure Shell Information window.

Step 4 Change your password using the following guidelines:

- Maximum field length—64 characters
- Minimum field length—6 characters

Step 5 Save your changes by clicking **Restart**. This enables the updated configuration to be read and applied to the system; and then Calling Service is restarted. Alternately you can click **Reset**, which causes the system to reboot. On startup, the system reads the Cisco Unified CM configuration and applies any changes.

Resetting Your Password

To reset your system codec password, follow these steps:

Step 1 SSH into the codec from your laptop.

Step 2 Login with the following:

- Username: **pwrecovery**
- Password: **pwreset**

The following message appears in the SSH client window:

```
Could not chdir to home directory /nv/home/pwrecovery: No such file or directory
**********************************************
**********************************************
** **
** Welcome to password reset **
** **
**********************************************
**********************************************
Do you want to continue ? (y/n):y
Preparing the system...
Please enter the passcode:
```

Note You must be in the room to read the passcode that shows on the main display.

If you encounter any difficulty, open a case with Technical Assistance Center (TAC) via the Internet at https://www.cisco.com/c/en/us/support/index.html, or contact your Cisco technical support representative and provide the representative with the information you have gathered about the problem.

Restoring Connectivity to the Codec

If you lose connectivity to the codec, refer to the Cisco TelePresence System Assembly, Use & Care, and Field-Replaceable Unit Guide for your system on Cisco.com:

Support > Products > TelePresence > Cisco TelePresence System

Password Character Support

Cisco CLI accepts the "$" (currency) symbol in passwords, but other components of the Cisco TelePresence System do not support the "$" symbol, including the immersive TelePresence endpoints and Cisco Unified CM. Therefore, Cisco recommends that you do not use the "$" symbol in your CLI passwords.

Login History

For enhanced security, the system reports the most recent login history when you initially log into the system. The login history reports the user, time, and location of the last successful login.

Password Troubleshooting

See the Cisco TelePresence System Troubleshooting Guide for information about system passwords and troubleshooting the system and Cisco Unified CM Administration interfaces and related hardware components.

CLI Basics

The following sections contain basic tips for using the command-line interface:

Completing Commands

Use the **Tab** key to complete CLI commands and observe the following guidelines:

- Enter the start of a command and press **Tab** to complete the command. For example, if you enter **se** and press **Tab**, the **set** command is completed.
- Enter a full command name and press **Tab** to display all the commands or subcommands that are available. For example, if you enter **set** and press Tab, you see all the **set** subcommands. An * identifies the commands that have subcommands.
- When a command is fully expanded using the **Tab** key, additional **Tab** key entries cause the current command line to repeat. This indicates that no additional expansion is available.

Getting Help with Commands

You can get two kinds of help on any command:

- Detailed help that includes a definition of the command and an example of its use
- Short query help that includes only command syntax

Procedure

To get help with commands, follow these steps:

Step 1 To get detailed help, at the CLI prompt, enter the following:

help *command*

Where *command* specifies the command name or the command and parameter. See Example 1-4.

Note If you enter the **help** command without specifying the name of a particular command as the optional parameter, the system provides information about the CLI system.

Step 2 To query command syntax, enter the following at the CLI prompt:

***command*?**

Where *command* represents the command name or the command and parameter. See Example 1-5.

Note If you enter a **?** after a menu command, such as **set**, it acts like the **Tab** key and lists the commands that are available.

Example 1-4 Detailed Help Example:

```
admin:help file list log

 list log help:
This will list logging files

options are:
page    - pause output
detail  - show detailed listing
reverse - reverse sort order
date    - sort by date
size    - sort by size

file-spec can contain * as wildcards

Example:
admin:file list log sysop detail
27 Oct,2008 22:19:04            4  sysop.bin
27 Oct,2008 21:14:31           67  sysop00000.log
28 Oct,2008 15:41:58        3,964  sysop00001.log
dir count = 0, file count = 3
```

Example 1-5 Query Example:

```
admin:file list log ?

Syntax:
file list log file-spec [options]
file-spec   mandatory   file to view
options     optional    page|detail|reverse|[date|size]
```

Ending a CLI Session

At the CLI prompt, enter **quit**. You are logged off, and the SSH session is dropped.

Monitoring Performance Management

Networks are functionally dynamic and fluid and various systems share the infrastructure in measurable increments. Critical applications such as point of sale systems, trading systems, financials, and Cisco TelePresence require specialized service guarantees. These service guarantees are provided by internal IT or by outsourced managed service providers by using agreed upon service level agreements (SLA) or operational level agreements (OLA). It is common for the managed service provider to offer SLAs and OLAs as a value added service assurance. In some cases, if these SLAs/OLAs are not met, the provider might have to credit back portions of the managed service charges or allow the customer to

break the contract. Various methods are deployed to monitor and measure the agreed performance and availability levels for the agreed periods. Reviews of the performance and availability are typically performed monthly or quarterly.

Performance measuring techniques include monitoring various statistical items from devices in the infrastructure and using simulated traffic analysis or probe-based network packet analysis. Many organizations choose to use proactive simulated traffic analysis over packet level probes since they provide in-band analysis through the infrastructure by participating as a host.

Cisco provides a solution called Internet Protocol Service Level Agreement (IPSLA) for in-band simulated traffic analysis. The solution has two components:

- IPSLA Initiators, page 1-8
- IPSLA Responders, page 1-8

IPSLA Initiators

IPSLA initiators configure test probes, such as User Datagram Protocol (UDP) jitter probe, with an IPSLA responder destination. The initiator maintains the configuration and all collection history reporting information needed to generate traps (reaction triggers) and syslog messages. The IPSLA responder interacts with the initiator by responding to the initiators probe request based on the initiator configuration. There is little configuration on the IPSLA responder since IPSLA implements a control message (UDP port 1967) that dynamically configures the responder.

IPSLA functionality in the codec provides customers and service providers with a method available through Cisco to measure and monitor network performance without having to deploy additional equipment to support the Cisco TelePresence implementation. In addition, Cisco Unified Operations Manager (CUOM) supports IPSLA in the current releases. With the codec as a responder, the configuration is simplified because the codec already exists in the network as a host and has the designed QoS trust port settings.

IPSLA Responders

IPSLA responders are daemons that are enabled and disabled with CLI. The responder runs silently in the background under normal user priority and controls and supports the CLI interface and firewall integration for the IPSLA responder in the system.

To ensure preventive security measures, such as preventing random IPSLA initiators from querying the codec, the following security items are included:

- Host/Network based access control that directs which initiators can access the codec. This is controlled with the CLI using the **utils ipsla responder** commands in Chapter 8, “Utils Commands.”

  When the IPSLA responder is started (enabled), an initiators list file will be loaded via /usr/local/bin/firewall.

- IPSLA responder is supported through the control message dynamic port allocation, which is based on the initiators configuration. A constraint option supplied to the **enable** command in the CLI limits the range of tcp/udp ports that are allowed. The user can configure the acceptable UDP/TCP port ranges for initiator requests. The responder code has been updated to deny any request that does not fall within the allowed range. The internal firewall blocks the incoming traffic if the system is not configured using the initiators list.

The IPSLA responder is disabled by default and the firewall blocks inbound requests. A persistent file is maintained in /nv/usr/local/etc/ipsla_resp.allow for the valid initiators and port ranges. The script /etc/rc.d/init.d/ipsla is called during system startup to check if the ipsla_resp.allow file exists with valid initiators. If true, IPSLA responder is started using the stored settings. If not true, IPSLA will not be started during system startup.