



Cisco TelePresence System Administration Guide

Published October 2015

Revised October 2018

Software Release IX 8 and later

Cisco Systems, Inc.

www.cisco.com

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

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 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: 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. (1721R)

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.

Cisco TelePresence System Administration Guide
© 2014-2018 Cisco Systems, Inc. All rights reserved.



What's in This Guide	vii
Before You Begin	vii
Immediate Software Upgrade Requirement for Your IX System	vii
Unified CM Device Package Requirements	vii
Assembly and Wiring Guidelines	viii
Obtaining the MAC Address of Your System	viii
Network Time Protocol (NTP) Requirements	ix
Unified CM and COP File Download Support	x
IX System Web Browser Support	x
Related Documents	x
Obtaining Documentation and Submitting a Service Request	x
CHAPTER 1	IX System Network and Bandwidth Requirements
	1-1
Quality of Service	1-1
Packet Loss	1-2
Jitter	1-2
Understanding Jitter and Defining Jitter Thresholds	1-2
How Your IX System Measures Jitter	1-3
Latency	1-4
Bandwidth Management for the IX System	1-4
Bandwidth Management Overview	1-4
Gradual Decoder Refresh (GDR)	1-5
Encoder Pacing	1-5
Bandwidth Provisioning Guidelines	1-5
Bandwidth Requirements for 1080p 60-fps Main Video	1-7
Required Main Video Configuration	1-7
Understanding How Endpoints Determine fps and Video Quality	1-8
Checking IX Bandwidth Quality On the System Display	1-12
High-Definition Presentation	1-14
HD Presentation Overview	1-14
Supported Presentation Devices and Tested Adapters	1-14
Resolution Support	1-14
Required Configuration For HD Presentation	1-15

Scaling HD Presentation Video Resolution	1-16
Bandwidth Requirements for the HD Presentation Feature	1-16
Multiple Presentation Streams	1-17
Video Bandwidth Allocation Weights	1-17
Sample Bandwidth Calculations	1-18

CHAPTER 2

Using the Interface	2-1
Contents	2-1
Overview	2-1
Cisco TelePresence IX5000 Administrator Home Page	2-3
System Status Header Bar	2-3
Administrator Tasks Panel	2-4
System Status	2-4
Status Indicators	2-4
Navigation	2-5
Typing and Selecting Information in Fields	2-5
Validating System Information in Fields	2-5
Where to Go Next	2-6

CHAPTER 3

Understanding the Fields in the Interface	3-1
Contents	3-1
Accessing the TelePresence IX5000 Administrator User Interface	3-1
Fields in the Monitoring Area	3-3
System Status	3-3
Call Statistics	3-4
Network Data	3-5
Fields in the Configuration Area	3-6
Network	3-7
Display Frequency and Proximity	3-8
Call Control Manager	3-9
Certificates	3-10
Fields in the First Time Setup Area	3-11
Fields in the Hardware Area	3-12
Echo Capture	3-13
Presentation Audio Capture	3-14
Touch 10 Screenshot	3-15
Fields in the Logs Area	3-15
System Operations Log	3-16

SIP Log	3-16
Reports	3-17
Captures	3-18
Fields in the Restart/Reset Area	3-18
System Restart	3-19
Factory Reset	3-19
Where to Go Next	3-19

CHAPTER 4**IX Software Features 4-1**

Contents	4-1
Ad Hoc Conferencing for the IX System	4-2
TMS Phone Books Support on the IX System	4-2
Configurable Number of Presentation Streams	4-2
TMMBR Support	4-3
H.265 Support	4-3
3rd Party CA Signed Certificate Support	4-4

CHAPTER 5**Configuring the IX System 5-1**

Contents	5-1
Configuring Cisco Unified Communications Manager for Your IX System	5-1
First Time Setup	5-2
Network Settings	5-3
Call Control Manager Settings	5-5
Certificates Settings	5-5
Authenticating Your IX System Using a Security Certificate	5-6
Installing the LSC	5-6
Examining the Security Certificate in Your IX System	5-6
Downloading a Security Certificate Using the CLI	5-6
Downloading a Security Certificate Using the Administrator Interface	5-7
Troubleshooting Your Configuration	5-7
Resetting Your IX Codec Password	5-7
Troubleshooting Your IX System Components	5-9

CHAPTER 6**Monitoring the System 6-1**

Contents	6-1
System Status	6-1

- Call Statistics 6-2
 - Special Note for Statistics for HD Presentations 6-2
 - Viewing Call Statistics 6-2
- Network Data 6-4
- Using SNMP Traps to Monitor the System 6-4
- Where to Go Next 6-4

CHAPTER 7

IX System Ports and Protocols 7-1

- Contents 7-1
- Overview 7-1
- Ports and Protocols Used by the IX System 7-2
- Ports and Protocols Used by the Cisco Unified Communications Manager 7-4
- Ports and Protocols Used by the Cisco TelePresence Management Suite 7-4
- Ports and Protocols Used by Cisco TelePresence Server 7-4
- Ports and Protocols Used by Cisco TelePresence Multipoint Switch (CTMS) 7-5
- Ports and Protocols Used for Cisco IOS IP Service Level Agreements (IPSLA) 7-6

CHAPTER 8

802.1X Authentication 8-1

- IEEE 802.1X Authentication Overview 8-1
 - 802.1X Authentication Components 8-1
 - Authenticating Your IX System 8-2
- Checking IX 802.1X Authentication Status 8-2
 - Checking 802.1X Authentication Status on the Main Display Screen 8-2
 - Checking 802.1X Authentication Status with a CLI Command 8-4
- Troubleshooting 802.1X Authentication Issues 8-4
 - Troubleshooting Issues in 802.1X Authentication 8-4
 - Viewing the Security Certificate 8-5
 - Viewing the Security Certificate from the CLI 8-6
 - Viewing the Security Certificate from a Third-Party Tool 8-6

INDEX



What's in This Guide

Revised: May 11, 2017

This preface contains the following sections

- [Before You Begin](#), page vii
- [Related Documents](#), page x
- [Obtaining Documentation and Submitting a Service Request](#), page x

Before You Begin

Before beginning the tasks in this guide, familiarize yourself with the following:

- [Immediate Software Upgrade Requirement for Your IX System](#), page vii
- [Unified CM Device Package Requirements](#), page vii
- [Assembly and Wiring Guidelines](#), page viii
- [Obtaining the MAC Address of Your System](#), page viii
- [Network Time Protocol \(NTP\) Requirements](#), page ix
- [Unified CM and COP File Download Support](#), page x
- [IX System Web Browser Support](#), page x

Immediate Software Upgrade Requirement for Your IX System

Before you begin first-time setup, you must load the latest IX software version from Cisco.com and load it to your IX system. For more information, see the “[Immediate Software Upgrade Requirements](#)” section of the *IX5000 and IX5200 First-Time Setup* document.

Unified CM Device Package Requirements

Make sure that your Unified CM software has the latest device package version. To find out the latest Unified CM device package for your IX version, see the *Cisco Unified Communications Manager Device Package Compatibility Matrix*.



Tip

For an IX5200, configure the Cisco TelePresence type as either Cisco TelePresence IX5000 (14 seats) or Cisco TelePresence IX5000 (18 seats). For more information, refer to the “[Product Specific Layout Configuration Area](#)” section of the *Configuring Cisco Unified Communications Manager for the IX System* document.

Assembly and Wiring Guidelines

Make sure your IX system is properly assembled and wired according to the guidelines in the Cisco TelePresence System installation guide. The *Cisco TelePresence IX5000 and IX5200 Installation Guide* is located at the following URL:

https://www.cisco.com/c/dam/en/us/td/docs/telepresence/ix5000/assembly_guide/ix5000_install_guide.pdf

For additional hardware and software information on your product, do one of the following actions:

- Log onto Cisco.com, click **Support**, type the name of the product in the Product Support text box, and click **Find**, or
- Navigate to <http://www.cisco.com>, and then, use the following navigation path to find your system:

Products & Services > Collaboration Endpoints > Immersive TelePresence > Cisco TelePresence IX5000 Series

Obtaining the MAC Address of Your System

The MAC address is required to register your system in the Unified Communications Manager (Unified CM). Find the MAC address using one of the following methods:

- Locate the MAC address number on a label next to the Ethernet port on the Host CPU codec. There are two MAC addresses, the correct one is nearest the Uplink and EX1 Ethernet connections as shown in [Figure 1](#).
- When the system is booting, watch the center display. The MAC address is shown during bootup.
- In the **Monitoring** page of the IX system web interface, the MAC address is shown in the **Network Data** section. For more information, see the “[Network Data](#)” section on page 4.

Unified CM and COP File Download Support

See the “Adding and Configuring COP Files” section in the *Configuring Cisco Unified Communications Manager for the IX System* document for detailed information about managing Cisco Options Package (COP) files. You load these files to Unified CM to upgrade the software for your IX system.

IX System Web Browser Support

The Cisco TelePresence System Administration interface is supported on the following web browsers:

- Internet Explorer (IE) version 10 and later
- Firefox version 31 and later
- Chrome version 36 and later
- Safari version 6.1.5 and later

Related Documents

For the entire documentation set for the Cisco TelePresence IX5000 series, which includes configuration guide, installation guide, and user guides, refer to the [IX5000 support documentation listing page on cisco.com](#).

For more information about Cisco Unified CM, see the [Cisco Unified Communications Manager \(CallManager\) support home page](#).

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see What’s New in Cisco Product Documentation at: <http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html>.

Subscribe to *What’s New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation as an RSS feed and delivers content directly to your desktop using a reader application. The RSS feeds are a free service.



IX System Network and Bandwidth Requirements

First Published: May 11, 2017

This chapter describes the network and bandwidth requirements to ensure the immersive video quality of the IX system. This chapter contains the following sections:

- [Quality of Service, page 1-1](#)
 - [Packet Loss, page 1-2](#)
 - [Jitter, page 1-2](#)
 - [Latency, page 1-4](#)
- [Bandwidth Management for the IX System, page 1-4](#)



Note

The bandwidth requirements in this section are based on network testing in environments without jitter or packet loss. Due to the extremely high-definition of the video, a small amount of packet loss or jitter can cause noticeable disruption to the user experience. To maintain the real-time interaction of human conversations, latency must be kept to an absolute minimum. Networks that have not been configured with proper QoS or inefficient routing over the WAN may cause loss of video quality.

Quality of Service

This section briefly describes Quality of Service (QoS) considerations for the IX5000 and IX5200. The immersive quality of the IX system requires that QoS mechanisms available on Cisco switches and routers throughout the network be configured to reduce packet loss, latency and jitter. Redundant devices and network links that provide quick convergence after network failures or topology changes are also important to ensure a highly available infrastructure. The following sections describe the packet loss, jitter and latency requirements for the IX system.

- [Packet Loss, page 1-2](#)
- [Jitter, page 1-2](#)
- [Latency, page 1-4](#)

For more detailed information, see the *Cisco Collaboration System 11.x Solution Reference Network Designs (SRND)* document at:

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/srnd/collab11/collab11.html

Packet Loss

Because the IX system is highly sensitive to packet loss, your network should be configured so that packet loss does not exceed a target of 0.05%. Cisco TelePresence codecs transmit at approximately 5 Mbps (max) per 1080pdisplay, which translates to more than 99% compression. The overall effect of packet loss is proportionally magnified, and dropping even one packet in 2000 (0.05% packet loss) becomes noticeable to end users.

For more detailed information about packet loss requirements for TelePresence systems, see the *Cisco TelePresence Network Systems 1.1 Design Guide* at:

https://www.cisco.com/c/dam/en/us/td/docs/solutions/TelePresence_Network_Systems_1-1_DG.pdf

Jitter

- [Understanding Jitter and Defining Jitter Thresholds, page 1-2](#)
- [How Your IX System Measures Jitter, page 1-3](#)

Understanding Jitter and Defining Jitter Thresholds

Jitter is defined as the difference between the time the video frame is expected to arrive at the endpoint, and the actual time that it arrives. There are two types of jitter: packet jitter, and video frame jitter. The video frames are enclosed in packets.

For packet jitter, you should follow the guidelines in the “[Network Infrastructure](#)” section of the *Cisco Collaboration System 11.x Solution Reference Network Designs (SRND)*. Currently the jitter level at the packet level is set at a maximum of 100 milliseconds (ms).

You should measure jitter at the video frame level (application layer) for Cisco TelePresence systems, rather than the packet level (network layer). A network with 0 ms of packet frame jitter can still have jitter at the video frame level if the RX buffer of the codec is overwhelmed with a large number of packets. Therefore, you should measure the arrival time of the entire video frame vs. the expected arrival time of that frame, based on the clock rate of video frame intervals. The clock rate for 30 fps is 33ms, while the clock rate for 60 fps is 16.5ms. Use the information in [Table 1-1](#) as the guideline for jitter in your network.

Measure jitter from the Ethernet port of the system codec on the far end to the Ethernet port of the system codec on the near end.

Table 1-1 Jitter Value

Metric	Target	Thresholds			
		1st	2nd	3rd	4th
Video Jitter	50 ms	85 ms	125 ms	165 ms	245 ms

Your system monitors jitter in the following ways:

- During a call, you can view the jitter information on the Touch device by tapping **More > Status > Call Status** and viewing the Jitter field. If the jitter value is Good, the jitter rate is lower than 125 ms. A value of Marginal represents jitter rates between 125 and 165 ms. A value of Poor represents jitter rates above 165 ms.

- You can monitor the jitter rate for your system by logging into the IX Administration Console for your system and navigating to **Monitoring > Call Statistics**, then clicking the **AV Call Video Stream Statistics** tab and checking the jitter rates in both the Transmit and Receive areas.

The jitter rates are color-coded. Jitter rates that are less than 125 ms is marked in green. Jitter rates between 125 and 165 ms are marked in yellow, and rates above 165 ms are marked in red.

Although no system actions are performed when jitter levels are exceeded, jitter at the video frame level is closely related to dropped video frames. If the RX buffer is exceeded, the system starts dropping frames. The Cisco TelePresence system changes the call quality based on the number of dropped frames.

- You can use the status bars on the IX system screen to monitor packet drop, which is closely related to jitter. For more information, see the [“Checking IX Bandwidth Quality On the System Display” section on page 1-12](#).



Note The status bars are not shown on calls that use a Cisco TelePresence Server; however, the same steps are taken, whether or not the bars are shown.

How Your IX System Measures Jitter

The IX system measures jitter upon the arrival of each frame and reports the jitter based on per 10-second and per call averages. The jitter period report provides the jitter measurement for the last 10-second period. The jitter call report shows the average jitter measurement per call. You can access both reports in the **Monitoring > Call Statistics** page in the IX Administration interface.



Note The IX system measures jitter between video frames and not packet frames, which applies to network devices. A video frame is a compressed picture that is used to update the screen.

The IX system calculates jitter as the sum of the maximum deviation (both late and early packets) from the expected arrival time as given by the frame period. (A late packet is a packet delivered after the picture has been reassembled and sent to the display. These packets are not lost but have the same impact as lost packets because they cannot be used by the video decoder.) The IX system computes frame jitter based on the arrival time of the last packet of a frame.

For example, for a 30 fps video stream with a measurement period of 165 ms or 5 frames (instead of 10 seconds and 300 frames), the IX system performs 5 jitter calculations. The Jitter (Period) would be reported as 5 ms (or 1 ms per frame [5 ms/5 frames = 1 ms jitter per frame]).

```
Frame Actual Arrival Time(ms) = 0 33 70 99 131
Frame Expected Arrival Time(ms) = 0 33 66 99 132
Offset = 0 0 +4 0 -1
Max Late = 4ms (absolute value)
Min Late = 1ms (absolute value)
Jitter/Period = 5ms (for this 165ms period)
```

If there were only 2 jitter periods in this call, the first period jitter measurement would be 5 msec and the second period jitter measurement would be 10 msec. The Jitter/Call would be reported as 7.5 msec.

```
Jitter/Call = (((PerCallJitter * (NumMeasurementIntervals - 1)) + CurrentJitter) /
(NumMeasurementIntervals)
Where: PerCallJitter = 5msecs
NumMeasurementIntervals = 2 (1-relative)
CurrentJitter = 10 msec
Jitter/Call = 7.5msecs = ((5msecs * (2-1)) + 10msecs) / 2
```

Latency

The IX system, like other Cisco TelePresence systems, has a network latency target of 150ms. This target includes network flight time but does not include codec processing time. For more detailed information about latency requirements for TelePresence systems, see the *Cisco TelePresence Network Systems 1.1 Design Guide* at:

https://www.cisco.com/c/dam/en/us/td/docs/solutions/TelePresence_Network_Systems_1-1_DG.pdf

Bandwidth Management for the IX System

This section describes bandwidth management considerations for the IX5000 and IX5200. The following sections describe the enhanced bandwidth control mechanisms and how they are implemented on the IX5000 and IX5200:

- [Bandwidth Management Overview, page 1-4](#)
- [Bandwidth Provisioning Guidelines, page 1-6](#)
- [Bandwidth Requirements for 1080p 60-fps Main Video, page 1-7](#)
- [High-Definition Presentation, page 1-14](#)
- [Required Configuration For HD Presentation, page 1-15](#)
- [Video Bandwidth Allocation Weights, page 1-17](#)



Note

This section was previously included in the “[IX Software Features](#)” section on page 4-1.

Bandwidth Management Overview

To provide the immersive video experience for the IX5000 and IX5200, the system requires careful planning for peak bandwidth requirements. Make sure to provision enough bandwidth from your service provider to account for total traffic requirements. The IX supports the following bandwidth management mechanisms:

- [Gradual Decoder Refresh \(GDR\), page 1-5](#)
- [Encoder Pacing, page 1-5](#)

Due to the nature of the video compression, the amount of TelePresence traffic may fluctuate with microbursts. Peak rates during a video conference generally occur at the following times:

- At the beginning of the call (or when a held call is resumed).
- When repair frames are generated (for example, recovering from packet loss).
- During periods of high motion in the video (for example, when participants all stand up or walk about the room).
- When there are details and high motion in the content, or when there is a complete scene change in the presentation video.

When microbursts happen, it may cause network packet loss and trigger repair frames to be created, which introduce further traffic variability in the bandwidth utilization profile. The IX system uses enhanced encoder rate control and packet pacing to maintain constant average bandwidth usage and reduce microburst in network data traffic. See the “[Gradual Decoder Refresh \(GDR\)](#)” section on

[page 1-5](#) and the “Encoder Pacing” section on [page 1-5](#) for more information.

Gradual Decoder Refresh (GDR)

Gradual Decoder Refresh is used to replace IDR (Instantaneous Decoder Refresh) to fulfill frame repair requests. Because IDR frames are much larger than other frames, IDR is usually the source of microbursts in video traffic. GDR gradually refreshes the picture over several frames, providing a smoother, less bursty bitstream. The IX system supports GDR for H.264 Main video on point-to-point calls between the IX system and the following systems:

- Another IX system
- TX Series systems
- CTS Series systems

GDR is supported for H.264 point-to-point Presentation video on calls between an IX system and the following systems:

- Another IX system
- TX Series systems

For more conceptual information about GDR, see the “Bandwidth Management” chapter of the [Cisco Collaboration System 11.x Solution Reference Network Designs \(SRND\)](#) document.

Encoder Pacing

Encoder pacing is a bandwidth management technique used to spread packets as evenly as possible, smoothing out the peaks of the bursts of bandwidth. Network packet pacing is used in the IX5000 after the video encoder.

Encoder pacing is supported in all call scenarios. For more conceptual information about encoder pacing, see the “Bandwidth Management” chapter of the [Cisco Collaboration System 11.x Solution Reference Network Designs \(SRND\)](#) document.

Microbursts are observed more frequently when bandwidth is measured in smaller intervals such as 100 milliseconds. Microbursts are observed less frequently when bandwidth is measured in intervals of one second or longer over the duration of the video call.

When measuring bandwidth statistics for how the IX system performs encoder pacing, note the following:

- Perform measurements at the network interface.
- Do not rely on statistics taken from the Touch 10 device or the Administrator user interface.

Statistics shown on the Touch 10 device show only instantaneous measurements on the encoder and decoder behavior, and the jitter buffer state. These statistics do not necessarily represent accurate measurements of the bandwidth used. These statistics should be interpreted as the bandwidth prior to the encoder pacing mechanism.

Bandwidth Provisioning Guidelines

To ensure the immersive video experience of the IX system, make sure to provision sufficient bandwidth from your service provider. Like other systems, the IX system requires bandwidth consumption headroom on top of average bandwidth usage to account for network overhead and microburst absorption.

Table 1-2, Table 1-3, Table 1-4, and Table 1-5 show the recommended amount of bandwidth to provision from a service provider to handle different call scenarios.

The following information applies to the recommended bandwidth guidelines:

- The bandwidth provisioning guidelines add 20 percent over normal bandwidth requirements to account for Layer 2-to-Layer 4 and other overhead. The calculations also include allowance for bursts and microbursts.
- The guidelines shown are for best motion quality only. Bandwidth requirements for good and better motion quality are less.

For information on calculating bandwidth requirements, see the [“Understanding How Endpoints Determine fps and Video Quality”](#) section on page 1-8.

- Calls from one IX system to another include two 1080p30 presentation streams (H.264).

Table 1-2 shows the bandwidth provisioning guidelines for 1080p30 content over H.264.

Table 1-2 *Bandwidth Provisioning Guidelines: H.264 for 1080p30 Content*

Call Scenario	Total Bandwidth Consumption		
	Resolution	30 fps	60 fps
		Best	Best
IX system to IX system	1080p	24.4 Mbps	31.6 Mbps
	720p	18.1 Mbps	22.1 Mbps
IX system to CTS or TX system ¹	1080p	19.5 Mbps	26.7 Mbps
	720p	13.2 Mbps	17.3 Mbps
IX system to Cisco TelePresence Server ²	1080p	16.8 Mbps	NA
	720p	13.2 Mbps	NA
IX system Native SIP	1080p	9.7 Mbps	12.1 Mbps
	720p	7.6 Mbps	8.9 Mbps

1. 60 fps supported for TX systems only.

2. Cisco TelePresence Server supports “Better” motion quality only in TIP/MUX calls.

Table 1-3 shows the bandwidth provisioning guidelines for 1080p5 content over H.264.

Table 1-3 *Bandwidth Provisioning Guidelines: H.264 for 1080p5 Content*

Call Scenario	Total Bandwidth Consumption		
	Resolution	30 fps	60 fps
		Best	Best
IX system to IX system	1080p	17.2 Mbps	24.4 Mbps
	720p	10.9 Mbps	14.9 Mbps
IX system to CTS or TX system ¹	1080p	15.9 Mbps	23.1 Mbps
	720p	9.6 Mbps	13.7 Mbps

1. 60 fps supported for TX systems only.

Table 1-4 shows the bandwidth provisioning guidelines for 1080p30 content over H.265.

Table 1-4 *Bandwidth Provisioning Guidelines: H.265 for 1080p30 Content*

Call Scenario	Total Bandwidth Consumption		
	Resolution	30 fps	60 fps
		Best	Best
IX system to IX system	1080p	18.6 Mbps	22.9 Mbps
	720p	14.8 Mbps	17.3 Mbps
IX system Native SIP	1080p	6.5 Mbps	NA
	720p	5.4 Mbps	6.1 Mbps

Table 1-5 shows the bandwidth provisioning guidelines for 1080p5 content over H.265.

Table 1-5 *Bandwidth Provisioning Guidelines: H.265 for 1080p5 Content*

Call Scenario	Total Bandwidth Consumption		
	Resolution	30 fps	60 fps
		Best	Best
IX system to IX system	1080p	11.4 Mbps	15.7 Mbps
	720p	7.6 Mbps	10.1 Mbps

Bandwidth Requirements for 1080p 60-fps Main Video

The Cisco TelePresence IX5000 System can send and receive main video at 60 fps (frames per second) with 1080p quality (1080p 60) during a point-to-point call. The following sections describe the 1080p 60-fps Main Video functionality:

- [Required Main Video Configuration, page 1-8](#)
- [Understanding How Endpoints Determine fps and Video Quality, page 1-8](#)
- [Checking IX Bandwidth Quality On the System Display, page 1-12](#)

Required Main Video Configuration

The following configuration is required to enable the 60-fps main video feature in your Cisco TelePresence environment:

- For IX endpoints, make the following changes in Unified CM version 10 or later:
 - Set Main Display Frames Per Second in the Phone Configuration page to “60 fps main”. For more information, refer to the “[Product Specific Configuration Layout Area](#)” section of the *Configuring Cisco Unified Communications Manager for the IX System* document.

- (Optional) Set Video Bandwidth Allocation Weights on the Phone Configuration page appropriately. For more information about this parameter, see the “[Video Bandwidth Allocation Weights](#)” section on page 1-17.

After performing the required configuration, the IX endpoints can send and receive main video at a maximum frame rate of 60 fps.

Understanding How Endpoints Determine fps and Video Quality

During Cisco TelePresence call setup, the sending and receiving endpoints determine the fps (30 or 60 fps) and video quality (1080p or 720p) for the sent and received video streams.

The determination is made as a result of the following factors:

- The amount of Transport Independent Application Specific (TIAS) bandwidth that is negotiated between the sending and receiving endpoints.

The minimum amount of bandwidth is determined by the settings of Main Display Frames Per Second and Quality (Per Display) in the Phone Configuration page of Unified CM. [Figure 1-1](#) and [Table 1-6](#) show the bandwidth requirements for H.265 based on the Unified CM configuration for 30 fps and 60 fps calls. [Figure 1-2](#) and [Table 1-7](#) show the corresponding bandwidth requirements for H.264.

- The video compression standard (H.264 or H.265) that is used.
- The maximum frame size that the network and system can accommodate.
- The negotiation of the video resolution and frame rate (in fps) by the sending and receiving endpoints.
- The maximum bit rate allowed in the Region settings for your device in Unified CM. These settings are applied to the Device Pool, which in turn are applied to your device.

To find your region settings, log in to the Cisco Unified CM Administration GUI and navigate to **System > Region**. The maximum rate is the value shown in the Max Video Call Bit Rate (Includes Audio) field.

- The packet loss that is detected during a call. This loss is shown as status bars that appear on the main display. If the rate changes, the new rate is shown on the main display. [Table 1-11](#) shows the bars and provides a description.

[Table 1-6](#) and [Table 1-7](#) show the required criteria in the first three columns of the table. The resulting video stream that can be sent is shown in the fourth column of the table.

If any factors do not meet the minimum requirements, the system attempts to send and receive video at the next lowest rate as shown in [Table 1-10](#).

For example, if the network cannot meet the minimum requirements to send a video stream with the maximum video quality of 1080p 60, the system attempts to negotiate a video stream of 720p 60. If the system cannot meet the requirements to send a video stream of 720p 60, it attempts to negotiate a video stream of 720p 30 as shown in [Table 1-10](#).

If a call is put on hold, then resumed, the amount of bandwidth is renegotiated using the same factors.



Note

These rates are given per video stream, and do not include the presentation stream. Since the IX system has three video streams for the three displays, multiply this number by three. Then add the bandwidth required for the presentation given in [Table 1-15](#) to obtain the required network bandwidth.

Table 1-6 Possible Values of Network Parameters and Resulting Resolution/Frame Rate (H.265)

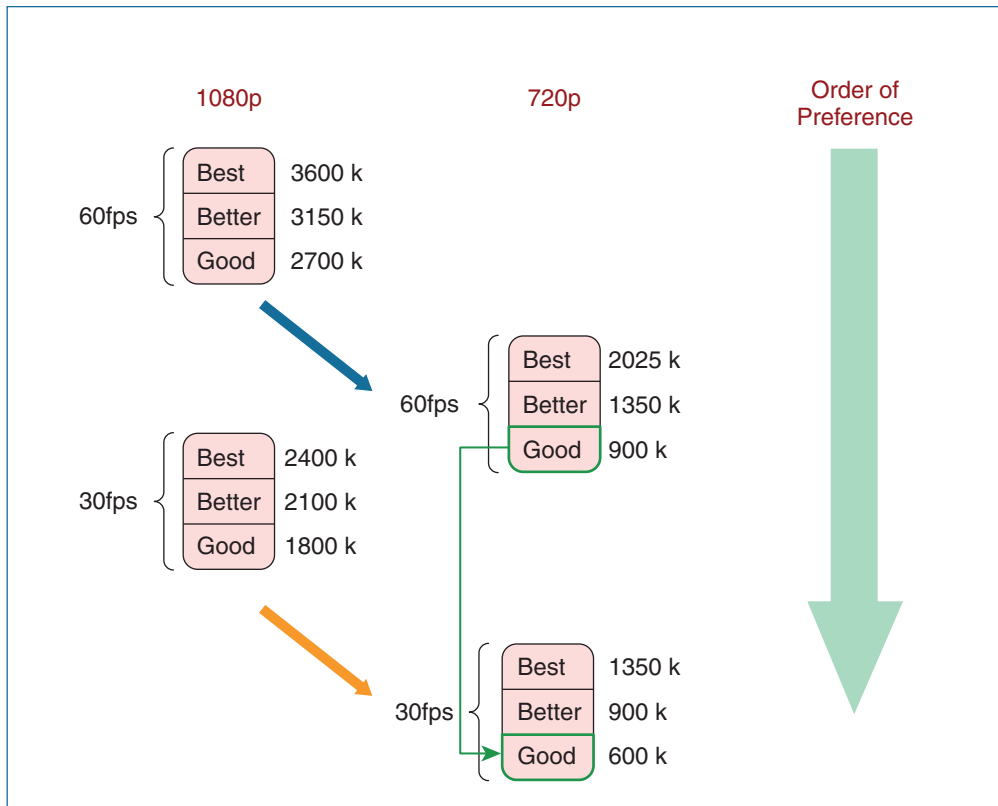
Minimum Preferred Bit Rate (Kbps)	Minimum Frame Size	Minimum fps	Resulting Resolution and fps
2700	8100	60	1080p 60
900	3600	60	720p 60
1800	8100	30	1080p 30
600	3600	30	720p 30

Table 1-7 Possible Values of Signaling Parameters and Resulting Resolution/Frame Rate (H.264)

Minimum Preferred Bit Rate (Kbps)	Minimum Frame Size	Minimum fps	Resulting Resolution and fps
4500	8100	60	1080p 60
1500	3600	60	720p 60
3000	8100	30	1080p 30
1000	3600	30	720p 30

Figure 1-1 shows the bandwidth required when using the H.265 video compression format, while Figure 1-2 shows the bandwidth required when using the H.264 format.

Figure 1-1 H.265 Bandwidth Requirements Per Unified CM Quality (Per Display)



393419

Figure 1-2 H.264 Bandwidth Requirements Per Unified CM Quality (Per Display)

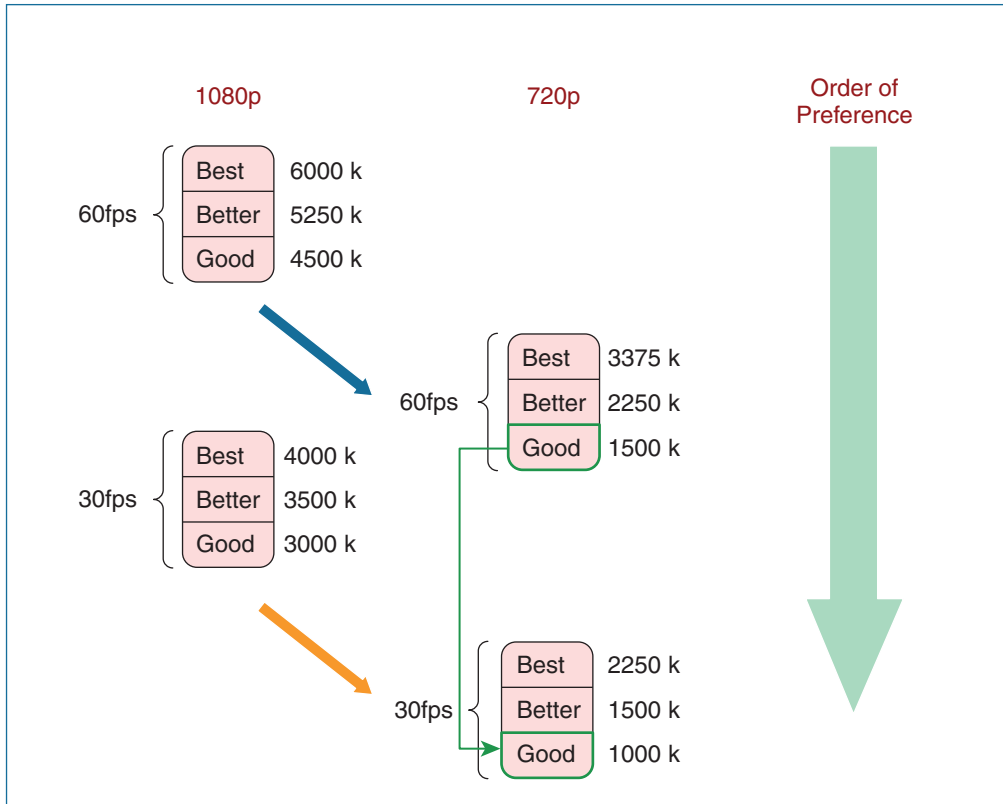


Table 1-8 provides the bandwidth requirements for H.265 for 30 fps and 60-fps calls; Table 1-9 provides the same information for H.264.

Table 1-8 H.265 Bandwidth Requirements Based On Unified CM Quality (Per Display)

Main Display Frames Per Second Setting	Quality (Per Display) Setting		
	Best	Better	Good
1080p Bandwidth Requirements (kbps)			
60 fps main	3600	3150	2700
30 fps main	2400	2100	1800
720p Bandwidth Requirements (kbps)			
60 fps main	2025	1350	900
30 fps main	1350	900	600

Table 1-9 H.264 Bandwidth Requirements Based On Unified CM Quality (Per Display)

Main Display Frames Per Second Setting	Quality (Per Display) Setting		
	Best	Better	Good
1080p Bandwidth Requirements (kbps)			
60 fps main	6000	5250	4500
30 fps main	4000	3500	3000
720p Bandwidth Requirements (kbps)			
60 fps main	3375	2250	1500
30 fps main	2250	1500	1000

Table 1-10 Negotiated Downgrade Paths

Initial Negotiated Resolution and Frame Rate	Downgrade Path During Call
Initially Negotiated 60 fps Calls	
1080p@60 fps	720p@60 fps, then 720p@30 fps
720p@60 fps	720@30 fps
Initially Negotiated 30 fps Calls	
1080p@30 fps	720@30 fps
720p@30 fps	720@30 fps

The 60 fps-capable Cisco TelePresence endpoints and device send the main video stream at 30 fps under the following circumstances:

- When in a call with an endpoint or device that supports a maximum frame rate of 30 fps.
- When in a call with a Cisco TelePresence endpoint that is registered with a Cisco Unified CM version that does not support 60 fps as a setting for Main Display Frames Per Second in the Phone Configuration page.
- When in a call with a Cisco TelePresence endpoint that is registered with a Unified CM version that supports 60 fps, but “30 fps main” is the setting for Main Display Frames Per Second in the Phone Configuration page.

Checking IX Bandwidth Quality On the System Display

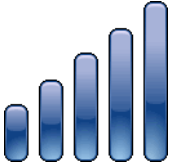
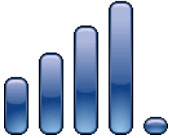

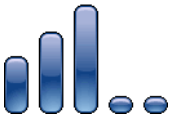


When the IX software detects changes in network quality in the network, an icon is displayed on the main display screen. When connection quality reaches the poor state, the call is terminated.

Table 1-11 describes the call connection status icons that display on the main display.

**Note**

Five, four, and three bars are reserved to show the video rates (1080p, 720p, or CIF) for the call. The remaining bars are reserved to show packet loss. A call dropping to one or two bars indicates that your network is having excessive packet loss at the rates shown in [Table 1-11](#).

Table 1-11 Call Connection Network Status Bars

Status Bars	Description
Five Bars 	<ul style="list-style-type: none"> All received streams are 1080p with no packet loss above the 1% warning threshold, and The received presentation (if active) has no packet loss above 2%.
Four Bars 	<ul style="list-style-type: none"> The lowest Resolution of received HD Streams is 720p with a packet loss less than or equal to 1%, and The received presentation (if active) has a packet loss less than or equal to 2%. <p>Note  In cases where a 1080P call at 30 fps is made with Cisco TelePresence Server (TS), the system shows only four bars even though there is no packet loss.</p>
Three Bars 	<ul style="list-style-type: none"> The lowest Resolution of received HD Streams is Common Intermediate Format (CIF) with a packet loss less than or equal to 1%, and The received presentation (if active) has a packet loss less than or equal to 2%.
Two Bars 	<ul style="list-style-type: none"> The highest percentage packet loss is above the 1% warning threshold, but less than 10%, or The received presentation, if active, has a loss between 2% and 10%.
One Bar 	<ul style="list-style-type: none"> The highest percentage packet loss of all received HD streams is more than 10%, or The received presentation has loss above 10% if active

High-Definition Presentation

This section provides you with information about the supported presentation resolutions and presentation audio and video cables and includes the following sections:

- [HD Presentation Overview, page 1-14](#)
- [Supported Presentation Devices and Tested Adapters, page 1-14](#)
- [Resolution Support, page 1-14](#)
- [Required Configuration For HD Presentation, page 1-15](#)
- [Scaling HD Presentation Video Resolution, page 1-16](#)
- [Bandwidth Requirements for the HD Presentation Feature, page 1-16](#)

HD Presentation Overview

Systems running IX software support high-definition (HD) presentations up to a maximum of 1080p resolution at 30 frames per second (1080p 30). The Cisco TelePresence IX5000 and IX5200 systems support the HD presentation feature.

Supported Presentation Devices and Tested Adapters

The presentation cable for the IX5000 system includes the following digital connectors: DisplayPort, Mini-DisplayPort, and HDMI.

Various third-party presentation devices are supported by connectors on the IX system's presentation cable. Supported presentation devices include:

- Laptop (PC) using the HDMI connector
- MacBook Air and MacBook Pro using the following connectors:
 - HDMI connector
 - DisplayPort connector
 - Mini DisplayPort connector



Note Some Apple devices show flickering on the screen when being used for presentation sharing. If you encounter this issue, change the resolution quality to a lower resolution.

- iPad products using a proprietary HDMI adapter available from Apple

If an adapter is required for VGA presentations, Cisco recommends the following tested adapter:

- SYBA USA VGA to HDMI converter

Resolution Support

The proportional relationship between the width and height (also known as *aspect ratio*) of the HD presentation signal is 16:9, whereas an analog presentation signal is 4:3.

[Table 1-12](#) outlines the common resolutions shared by the presentation devices, the corresponding aspect ratios, and the presentation digital cables that support the resolutions. While the IX system supports all of the presentation resolutions indicated in the table, EDID (Extended Display Identification Data) only supports 1080p, 720p, and VGA.

Table 1-12 Aspect Ratios For Resolutions Shared By Presentation Device

Resolutions Shared By Presentation Device	Aspect Ratio
1920x1080 (1080p) @ 30, 15, or 5 fps	16:9
1280x720 (720p) @ 30, 15, or 5 fps	16:9
1024x768 (XGA) @ 30, 15, 5, or 1 fps	4:3
640x480 (VGA) @ 30, 15, 5, or 1 fps	4:3

**Note**

Some presentation resolutions do not take up the full space of the presentation display area. For example, if a laptop that is sending the presentation is set to a resolution of 1600x900, and the presentation display is set to a resolution of 1920x1080, the image shown on the display is 1600x900 pixels with a black border around it to make a total pixel size of 1920x1080.

To eliminate this black border around the presentation display when using a PC, open the PC's Control Panel, navigate to the laptop's Change Desktop Background, and change the picture position to "Fill."

Required Configuration For HD Presentation

If both Binary Floor Control Protocol (BFCP) and TelePresence Interoperability Protocol (TIP) are negotiated for a call, TIP takes precedence, and BFCP is not used to control presentation. BFCP is the preferred protocol for controlling the presentation for systems that run IX software.

[Table 1-13](#) describes the Unified CM configuration that enables HD presentation to function on IX endpoints. No additional configuration is required.

Table 1-13 Unified CM Configuration Required For Each IX Endpoint

Unified CM Configuration	Notes
For each IX endpoint, use the Standard SIP Profile (not the Standard SIP BFCP Profile) for the SIP profile, even if you use BFCP.	If you specify the Standard SIP BFCP profile, calls might be dropped and BFCP might not function properly.
Make sure that you check the Allow Presentation Sharing Using BFCP check box in the Protocol Specific Information area of the Phone Configuration window.	For more information about configuring BFCP, refer to the "Configuring the BFCP over UDP Collaboration Feature" section of the <i>Configuring Cisco Unified Communications Manager for the IX System</i> document.
In the Phone configuration, the default value of Video Bandwidth Allocation Weights is 8 Main/2 Presentation. Adjust this setting if desired.	For more information about this parameter, see the "Video Bandwidth Allocation Weights" section on page 1-17.

For more details about the Unified CM configuration, see the [Configuring Cisco Unified Communications Manager for the IX System](#) document.

Scaling HD Presentation Video Resolution

For HD presentation, the system running IX software that is sharing content can automatically change resolutions for the content being shared, such as a slide presentation, document, or video. [Table 1-14](#) outlines common presentation device display resolutions, and the higher or lower resolutions to which content can be scaled and sent by the IX endpoint.

In general, HD presentation supports the following scaling schemes:

- Scaling to a higher resolution is not supported except for 1280x720 (720p), which can be scaled to XGA.
- Scaling to lower resolutions of XGA is supported.

Scaling is done to accommodate lower network bandwidth. Before the system running IX software scales the presentation, it lowers the frame rate of the presentation, which preserves the video clarity.

Table 1-14 Common Device Display Resolutions and Scaled Resolutions

Resolutions Shared By Presentation Device	Scaled Resolutions			
	1920x1080 (1080p)	1280x720 (720p)	1024x768 (XGA)	640x480 (VGA)
1920x1080 (1080p)	Yes	No	Yes	Yes
1280x720 (720p)	No	Yes	Yes	Yes
1024x768 (XGA)	No	No	Yes	Yes
640x480 (VGA)	No	No	No	Yes

Bandwidth Requirements for the HD Presentation Feature

The resolutions and frame rates at which each type of video can be sent is based on the available bandwidth.

[Table 1-8 on page 1-11](#) and [Table 1-9 on page 1-12](#) display the bandwidths required for supported 60 fps main video send resolutions and frame rates, while [Table 1-15](#) displays the bandwidth required for supported HD presentation send resolutions and frame rates.



Note

Regardless of how much network bandwidth is actually used as described in [Table 1-15](#), the IX system always negotiates the maximum amount of bandwidth for an HD presentation (4000Kbps).

Table 1-15 Bandwidth Required For Supported HD Presentation Send Resolutions and Frame Rates

Send Resolution	30 fps (Kbps)	15 fps (Kbps)	5 fps (Kbps)	5 fps (minimum) ¹ (Kbps)
1920x1080 (1080p)	4000	2500	1000	500
1680x1050	3700	2200	900	450

Table 1-15 Bandwidth Required For Supported HD Presentation Send Resolutions and Frame Rates

Send Resolution	30 fps (Kbps)	15 fps (Kbps)	5 fps (Kbps)	5 fps (minimum) ¹ (Kbps)
1440x900	2900	1750	725	350
1280x800	2450	1450	600	300
1280x720 (720p)	2250	1350	550	250
1024x768 (XGA)	2000	1200	500	250
800x600	1400	825	350	175
640x480 (VGA)	1000	600	250	100

1. These bandwidth rates are the lowest possible rates required. The higher bandwidths are the recommended minimum bandwidth for best performance.

For calls that support more than one presentation stream, the required bandwidth is multiplied for each additional stream. When two presentation streams are used in a P2P call between IX endpoints, the required bandwidth is doubled. For example, two presentation streams at 1080p60 would require 8 Mbps.

For more information about calculating bandwidth for video and presentation content, see the [“Sample Bandwidth Calculations”](#) section on page 1-18,



Tip

If, in a limited bandwidth scenario, you want to send a presentation with a higher fps but a lower resolution, you can change the resolution of the presentation at the source of the presentation. For example, given a maximum rate of 1000 Kbps, if you are sending a 1920x1080 presentation at 5 fps, you can instead send 640x480 at 30 fps by changing the resolution of your presentation to 640x480.

Multiple Presentation Streams

On an IX-to-IX point-to-point conference, you can share up to two presentation streams - for example, one presentation content source and one whiteboard source. If hosting a meeting locally with no video conferencing, you can share up to three presentation streams.

Video Bandwidth Allocation Weights

The Video Bandwidth Allocation Weights parameter allows you to balance the bandwidth ratio for main video and presentation video during a conference.

Use this feature when the amount of session bandwidth that is used by a Cisco TelePresence endpoint to send audio, main video, and presentation video media streams exceeds the amount of available session bandwidth.

You add this value in the Bandwidth Allocation Weights field in the Product Specific Configuration Layout Area of the Unified CM administration console.

The weight is based on a total number of 10m and the default value of this parameter is a weight of 8 for main video and a weight of 2 for presentation video (8 main / 2 presentation).

The Cisco TelePresence System IX5000 supports the bandwidth allocation feature.

The following values are supported for this feature. The first value is the weight for main video, and the second value is the weight for the presentation video.

9 main / 1 presentation

8 main / 2 presentation (**default**)

6 main / 4 presentation

4 main / 6 presentation

3 main / 7 presentation



Note

If you see bandwidth allocation weights used in the System Operations Log, check the Unified CM region settings and ensure enough video bandwidth is allowed for video and immersive video calls. The Unified CM region settings frequently can trigger the bandwidth allocation weights, which can significantly reduce call quality.

Sample Bandwidth Calculations

Bandwidth for a full 1080p60 “best” quality call with a 1080p30 presentation would require the following bandwidth:

H.265: 8.1 Mbps main video + 4 Mbps (presentation video@1080p 30) = 12.1 Mbps

H.264: 13.5 Mbps main video + 4 Mbps (presentation video@1080p 30) = 17.5 Mbps



Note

The main video rates are derived from the rate per display multiplied by the number of screens (three). For H.265, given the rates in [Table 1-8](#), the rate is 2.7 Mbps per screen for 1080p60 (Good), and for H.264, given the rates in [Table 1-9](#), the rate is 4.5 Mbps per screen for 1080p60 (Good). Multiplying these numbers gives you the video rates of 8.1 and 13.5 Mbps, respectively.

Bandwidth Calculations

To fit the available bandwidth, the endpoint performs calculations based on these general formulas, which include values from the Video Bandwidth Allocation Weights parameter:

Definitions:

Session Video Bandwidth (**SVB**) = Total session bandwidth - Audio bandwidth

Main Video Weight (**Mwt**) = Configured weight for main video stream

Total Weight for main video (**T_Mwt**) = Number of Streams x Main Video weight

Presentation Video Weight (**Pwt**) = Configured weight for presentation video stream

Total Weight for presentation video (**T_Pwt**) = Number of streams x Presentation video weight

Total Weight (**TW**) = T_Mwt + T_Pwt

Formula to allocate main video bandwidth:

SVB x (T_Mwt/ TW) = Mwt

Formula to allocate presentation video bandwidth:

SVB x (T_Pwt/ TW) = Pwt

Rate Calculation Example

Given a total available network bandwidth of 6.0 megabits per second (Mbps), and a single presentation stream:

$$\mathbf{T_Mwt = (3 \text{ (number of main video streams)} \times 8) \text{ (Mwt)} = 24}$$

$$\mathbf{T_Pwt = (1 \text{ (number of presentation video streams)} \times 2) \text{ (Pwt)} = 2}$$

$$\mathbf{TW = 26}$$

Allocated main video bandwidth = $6 \times (24/26) = \mathbf{5.53 \text{ Mbps (1.84 Mbps per display)}}$

Allocated presentation video bandwidth = $6 \times (2/26) = \mathbf{0.47 \text{ Mbps}}$

For H.265, the 1.84 Mbps per display is sufficient to support either 720p60 (better) or 1080p30 (good), per the rates in [Table 1-8](#), depending on whether the initial call was negotiated at 60 or 30 fps.

For H.264, the 1.84 Mbps per display is sufficient to support 720p30 (better), per the rates in [Table 1-9](#).

Both H.265 and H.264 encoding support a resolution stream of 720p @ 5 fps if receiving, and 640x480 @ 5 fps if sending, per the rates in [Table 1-15](#).

**Note**

This example assumed a single presentation stream. Additional content streams change the calculation in that the available bandwidth stream is divided by 2 for each content.



Using the Interface

Revised: October 26, 2015

Contents

This chapter contains the following sections:

- [Overview, page 2-1](#)
- [Cisco TelePresence IX5000 Administrator Home Page, page 2-3](#)
- [Navigation, page 2-5](#)
- [Where to Go Next, page 2-6](#)

Overview

Use the Cisco TelePresence IX5000 Administrator user interface to maintain and manage your IX system.



Note

No more than one administrator should access the Administrator user interface at a time.

Administration tasks include:

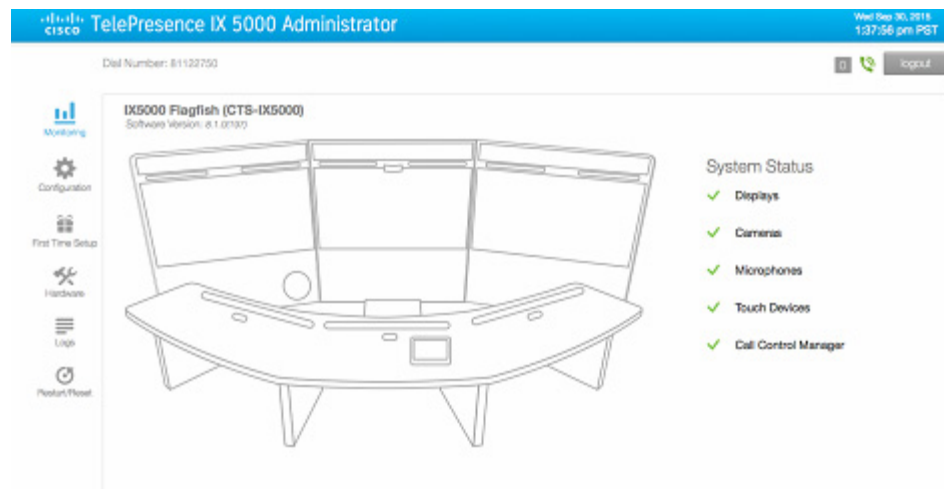
- Setting up the Cisco TelePresence IX system equipment
- Configuring all system settings
- Viewing device information and detailed system status information
- Monitoring the operating status of system equipment

For first-time setup instructions, refer to the *IX5000 and IX5200 First-Time Setup* document at the following URL:

https://www.cisco.com/c/en/us/td/docs/telepresence/ix5000/first_time_setup/ix5000_first_time_setup.html

Figure 2-1 is an example Cisco TelePresence IX5000 Administrator home page. This is the first page that displays after you log in to the user interface. Click the icons in the left panel of this page to navigate to that area.

Figure 2-1 Cisco TelePresence IX5000 Administrator Home Page (Top Half)



Note

Figure 2-1 shows the top half of the Administrator home page. Scroll down the page to view additional Monitoring task information and system details (Figure 2-2). The other user tasks listed in the left pane of this page also require scrolling to view all of their task-specific information.

Figure 2-2 Cisco TelePresence IX5000 Administrator Home Page (Lower Half)

Call Statistics			
General	AV Call Video	AV Call Audio	Audio Only
Data Type	Value		
Total Calls In System Lifetime			
Total Call Duration In System Lifetime			
Last Call Duration			
Total Call Duration Since Reboot			
Last Call Start Time			
Total Calls Since Last Reboot			
Time Call Stats Were Last Cleared			

Network Data			
Call Control Manager: 10.22.140.47	MAC Address: 00:0e:0b:70:0a:e0	Hostname: SEP0003AD700AF9	Domain Name: cisco.com cisco.com
DHCP Setting: Full	IP Address: 10.35.192.43	Gateway: 10.35.192.1	Subnet: 255.255.255.0
DNS Server 1: 173.36.131.10	DNS Server 2: 171.70.168.163	Operational VLAN: 300	

Cisco TelePresence IX5000 Administrator Home Page

The Administrator home page consists of three sections:

- System status header bar
- Administrator tasks panel
- System status

System Status Header Bar

The header bar at the top of all Administrator pages contains the following information about your IX system:

- Dial Number—Indicates the directory (phone) number of the system in use.
- Red, numbered icon—Indicates the number of system services that have stopped running.
- Call status icons—Indicates if your system is in or out of a call. The two call indicator icons are:



- Green unmuted phone—Indicates the IX system is in a call.



- Gray phone with slash mark—Indicates the IX system is out of (not in) a call.

- **Logout** button—Click to log out of the IX system.

Administrator Tasks Panel

A system administrator can monitor, configure, or change his IX system and hardware components after accessing the Administrator home page. The left panel of this page contains links to these administrative task pages:

- Monitoring
- Configuration
- First Time Setup
- Hardware
- Logs
- Restart/Reset

System Status

System Status is always in view in the upper right of the Administrator home page as shown in [Figure 2-1](#). The system administrator should closely monitor this area for changes in the status of the IX system functions and equipment. System status is updated every 5 seconds.

Status Indicators

IX system components include the following:

- Displays
- Cameras
- Microphones
- Touch Devices
- Call Control Manager

The System Status section shows an operating status icon for each system component:

- ✓ • Green check mark — Component is configured and operational.

- ✗ • Red X — Component is not connected or configured:
 - Displays -- The video display cable is not connected, or the display has no power.
 - Cameras -- The camera video cable is not connected or is loose, or the Ethernet cable is not connected.
 - Microphones -- The microphones are offline or not connected.
 - Touch Devices -- Touch 10 devices have no power.
 - Call Control Manager -- The system is not registered with the Call Control Manager (Unified CM).

For more information, see [Chapter 3, “Understanding the Fields in the Interface”](#).

Navigation

Click any of the task options in the panel on the left side of the Administrator home page to navigate to that option’s interface page. After you access an option’s page, you can view specific systems tasks and monitor their statuses. Scroll down the window of each page to see the system data displayed in the main content areas.

The following sections describe objects, functions, and information that is displayed in the pages associated with the Administrator user interface:

- [Typing and Selecting Information in Fields, page 2-5](#)
- [Validating System Information in Fields, page 2-5](#)

Typing and Selecting Information in Fields

To modify information in fields, use the mouse to highlight and delete existing information. Type in new information. Some fields offer drop-down menus from which you choose settings.

Validating System Information in Fields

All Administrator pages contain an initially disabled **Restart/Reset** button in the left administrator task panel. When you change or add settings to any of the administrator task pages, this button becomes enabled.

- Use the **Restart** button to reboot your IX system.
- Use the **Reset** button to discard changes and restore the factory default IX system values.

Other Administrator pages have fields containing such information as IP addresses, domain names, media port numbers (view only), and so on, that are validated when you exit the field. When information in a field is found to be invalid, a message describing the error is displayed.

Where to Go Next

Proceed to [Chapter 3, “Understanding the Fields in the Interface”](#) to access the Administrator user interface and to view full descriptions of the fields in the interface,



Understanding the Fields in the Interface

Revised: November 22, 2016

Contents

This chapter contains the following sections:

- [Accessing the TelePresence IX5000 Administrator User Interface, page 3-1](#)
- [Fields in the Monitoring Area, page 3-3](#)
- [Fields in the Configuration Area, page 3-6](#)
- [Fields in the First Time Setup Area, page 3-11](#)
- [Fields in the Hardware Area, page 3-12](#)
- [Fields in the Logs Area, page 3-15](#)
- [Fields in the Restart/Reset Area, page 3-18](#)
- [Where to Go Next, page 3-19](#)

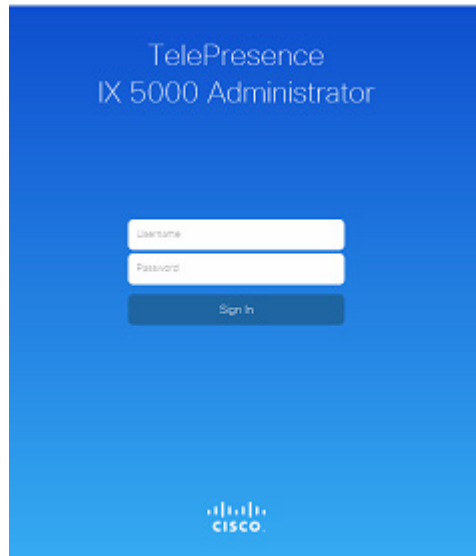
Accessing the TelePresence IX5000 Administrator User Interface

The TelePresence IX5000 Administrator user interface is where you can monitor, configure, setup, troubleshoot, log, and restart or reset your IX system.

To view information about the Cisco TelePresence devices on your system:

-
- Step 1** Log in to the Administrator user interface by completing the following steps:
- a. Select an Internet browser from the list in the [“IX System Web Browser Support”](#) section on page x.
 - b. Open the browser window, type the IP address of your IX system in the URL field, and click **Enter**. The Administrator Login screen appears, as shown in [Figure 3-1](#).

Figure 3-1 Administrator Login Screen



- c. In the Username field, type **admin**.
- d. In the Password field, type **cisco**.

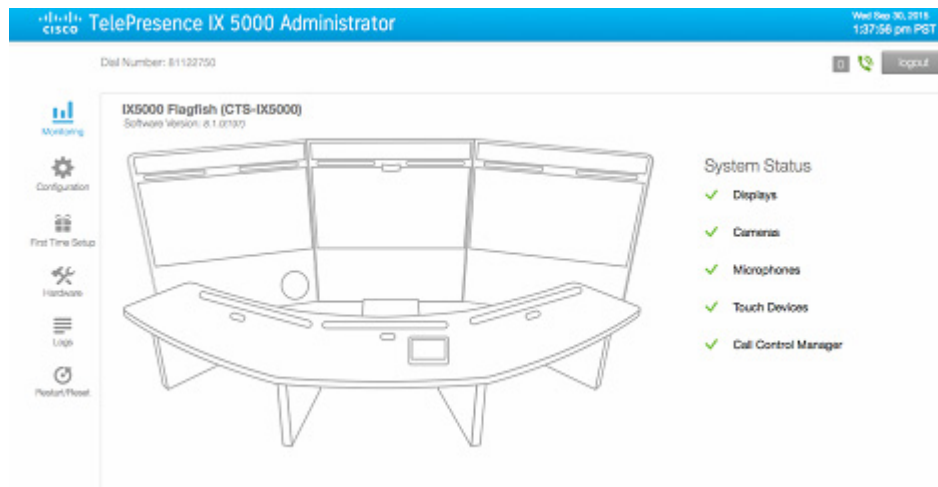
**Note**

You can change the default password in Unified CM by changing the SSH admin Password field. For more information, see the “SSH Information Area” section of the *Configuring Cisco Unified Communications Manager for the IX System* document.

- e. Click **Sign In**.

The Administrator home page opens as shown in Figure 3-2.

Figure 3-2 Administrator Home Page



Step 2 From the Administrator home page, you can navigate to and access data fields on various administrator tasks in the following areas:

- [Fields in the Monitoring Area](#)
- [Fields in the Configuration Area](#)
- [Fields in the First Time Setup Area](#)
- [Fields in the Hardware Area](#)
- [Fields in the Logs Area](#)
- [Fields in the Restart/Reset Area](#)



Note

The Administrator home page always opens in the Monitoring area of the user interface.

Fields in the Monitoring Area

The Monitoring area contains details about the settings that were configured in the IX system and the Unified CM. This section describes the data fields that display in the Monitoring area. The following system monitoring information is available:

- [System Status](#)
- [Call Statistics](#)
- [Network Data](#)



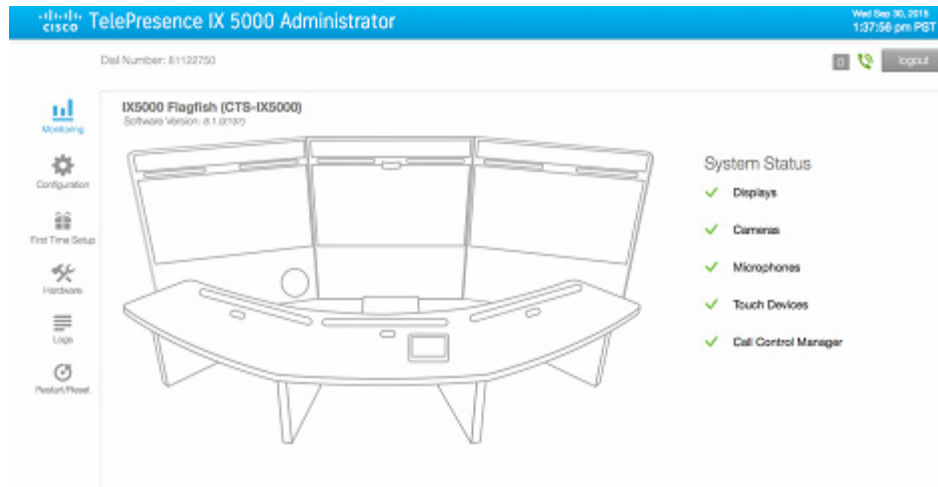
Note

After accessing the Monitoring area of the Administrator interface, scroll down the page to view the data fields.

System Status

View the current operating status of the hardware components of the IX system from the System Status section. [Figure 3-3](#) is an example of the top right section of the interface home page with the System Status component status indicators.

Figure 3-3 Monitoring > System Status Section



The **System Status** area shows you the operational statuses of your IX system devices. Configured and operational components are indicated by a green check mark; components not connected or configured are indicated by a red X.

Table 2-1 describes the System Status fields.

Table 3-1 System Status Fields

Field or Button	Setting or Description
Displays	Indicates the operational state of the Main and Aux video displays. A non-operational state may be caused by the video cable not being connected or a display not having power.
Cameras	Indicates the operational state of the system cameras. A non-operational state may be caused by an unconnected or loose video cable or an unconnected Ethernet cable.
Microphones	Indicates the operational state of the system microphones. A non-operational state may be caused by microphones being offline.
Touch Devices	Indicates the operational state of the system Touch 10 devices.
Call Control Manager	Indicates whether the IX system is registered or not registered to the Call Control Manager (Unified CM).

Call Statistics

Use **Call Statistics** to view audio and video statistics collected by the codecs. The reports include descriptions to help you understand the type of information being collected.

To view **Call Statistics**, choose **Monitoring**, and scroll down to **Call Statistics**. Click the appropriate tab to view a specific set of Call Statistics fields. Table 3-2 describes the Call Statistics fields which provide a history of all of your received and transmitted calls, including streaming video and audio calls.

Figure 3-4 Monitoring > Call Statistics Section

Call Statistics			
General	AV Call Video	AV Call Audio	Audio Only
Stats Type	Value		
Total Calls in System Lifetime	6		
Total Call Duration in System Lifetime	22:06:16		
Last Call Duration	0:27:09		
Total Call Duration Since Reboot	0:27:09		
Last Call Start Time	Tue Sep 23 09:58:10 2014		
Total Calls Since Last Reboot	1		
Time Call Stats Were Last Cleared	Thu Sep 11 14:07:31 2014		

Table 3-2 Call Statistics Fields

Field or Button	Setting or Description
General	Provides general system call data and values, including current and cumulative system call information, for the following: <ul style="list-style-type: none"> • Total Calls in System Lifetime • Total Call Duration in System Lifetime • Last Call Duration • Total Call Duration Since reboot • Last Call Start Time • Total Calls Since Last Reboot • Time Call Stats Were Last Cleared
AV Call Video	Displays TelePresence video stream statistics for multipoint audio/video calls on the Right, Center, and Left displays.
AV Call Audio	Displays TelePresence audio stream statistics for multipoint audio/video calls on the Right, Center, and Left displays.
Audio Only	Displays stream statistics for IP phone audio-only calls on the Right, Center, and Left displays.

Network Data

View network name and address information in the **Network Data** section. [Figure 3-5](#) shows the Network Data section in the Monitoring page.

To view **Network Data**, choose **Monitoring**, and scroll down to Network Data. The Network Data fields for the IX system are described in [Table 3-3](#).

Figure 3-5 *Monitoring > Network Data Section*

Network Data			
Call Control Manager: 10.22.146.47	MAC Address: 00:0b:ab:76:0a:e9	Hostname: SEP000BAB76DAE9	Domain Name: cisco.com cisco.com
DHCP Setting: full	IP Address: 10.35.192.43	Gateway: 10.35.192.1	Subnet Mask: 255.255.255.0
DNS Server 1: 173.36.131.10	DNS Server 2: 171.70.168.183	Operational VLAN: 300	

Table 3-3 *Network Data Fields*

Field or Button	Setting or Description
Call Control Manager	IP address of your Cisco Unified Communications Manager.
MAC Address	The Media Access Control hardware address that uniquely identifies your IX system.
Hostname	The host name of the system codec.
Domain Name	The domain name of the system codec.
DHCP Setting	Indicates if DHCP addressing is set for Full, Mixed or Static setting.
IP Address	The location (IP Address) of the primary system codec.
Gateway	The location (IP Address) of the router on your network that serves as an access point to another network.
Subnet Mask	The IP subnet mask of the IX system.
DNS Server 1	The primary network server by its IP address.
DNS Server 2	Provides the address of a second DNS server if the primary server is unavailable.
Operational VLAN	The virtual LAN used by the standard IEEE 802.1Q. This value is a display-only VLAN ID.

Fields in the Configuration Area

The Configuration area is where you configure DHCP and TFTP settings and upload 802.1X authentication certificates for your IX system. This section contains information on the data fields in the Configuration area. The following system configuration information is available:

- [Network](#)
- [Display Frequency and Proximity](#)
- [Call Control Manager](#)
- [Certificates](#)



Note

After accessing the **Configuration** area, you may need to scroll down the page to view the data fields.

Network

The **Network** section in the Configuration area is where you can view or configure your IP address settings.

Figure 3-6 is an example of the Network and Display Frequency sections of the user interface. Table 3-5 describes the main Network fields and buttons.

Figure 3-6 Configuration > Network Section

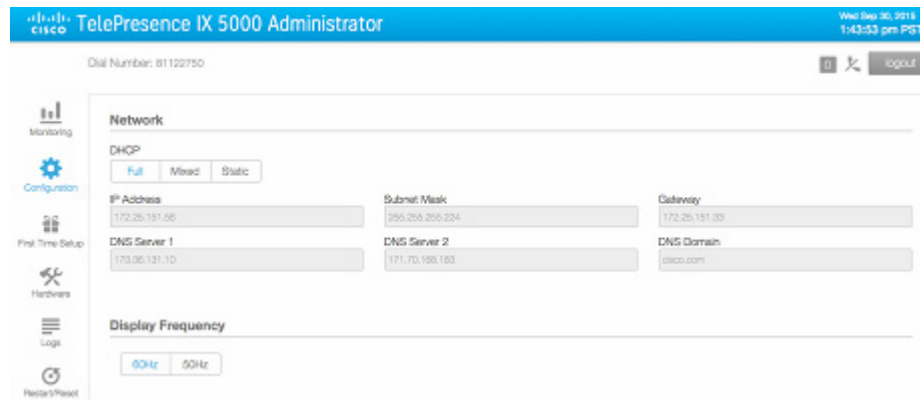


Table 3-4 Network Fields

Field or Button	Setting or Description
DHCP	Choose how you would like to set your network addressing by either enabling or not enabling DHCP. Options for setting DHCP addressing are Full, Mixed, or Static. If your system uses DHCP, select either Full or Mixed; if it does not use DHCP, select Static.
IP Address	<p>These configuration options are available:</p> <ul style="list-style-type: none"> • Full—If your network uses DHCP, click this option to enable DHCP and to allow the network to dynamically assign a network address and configure all address settings. • Mixed—If your network uses DHCP, you can also click this option to manually assign the IP address while the network assigns the remainder of the settings. • Static—If your network does not use DHCP, click this option to manually assign all of the network address settings. (The network will provide none of these values.) <p>For more information about this field, see the “Network Settings” section on page 5-3.</p>
Subnet Mask	Identifies the subnet mask of the system IP address.
Gateway	Identifies the location (IP Address) of the router on your network that serves as an access point to another network.
DNS Server 1	The primary network server identified by its IP address.

Table 3-4 Network Fields (continued)

Field or Button	Setting or Description
DNS Server 2	The secondary network server identified by its IP address.
DNS Domain	The domain name server of the IX system.

Display Frequency and Proximity

Figure 3-7 shows an example of the Display Frequency and Proximity sections of the user interface. Table 3-5 describes the fields in these sections.

Figure 3-7 Configuration > Display Frequency and Proximity Sections

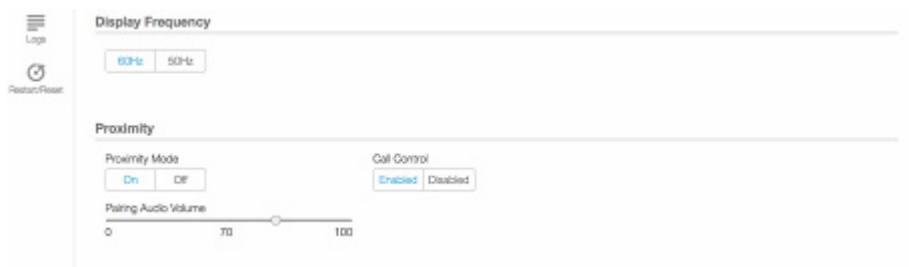



Table 3-5 Display Frequency and Proximity Fields

Field or Button	Setting or Description
Display Frequency	Radio buttons allow users to choose between 50 Hz and 60 Hz: <ul style="list-style-type: none"> 50 Hz—Sets up the camera for operating with 50 Hz lighting. 60 Hz—Sets up the camera for operating with 60 Hz lighting.
Proximity	These options are available: <ul style="list-style-type: none"> Proximity On/Off—Enables or disables the proximity feature on IX 5000 systems. Call Control Enabled/Disabled—Enables or disables call control functionality from BYOD devices. Pairing Audio Volume—Changes audio volume of paired devices. <p> Note The Proximity On/Off setting in the IX5000 Administrator user interface will be overridden by the Proximity Mode setting configured in Unified CM. For more information, see the “Proximity Information Area” section of Configuring Cisco Unified Communications Manager for the IX System.</p>

Call Control Manager

To view or configure your TFTP server settings, scroll down to the **Call Control Manager** section in the **Configuration** area. Use Call Control Manager to specify TFTP server locations and view a list of available settings for your system. Four TFTP options and a **Delete Certificate Trust List** button provide additional configuration options for your TFTP servers.

Figure 3-8 is an example of the Call Control Manager section (**Manual** mode) of the Administrator user interface. Table 3-6 describes the main Call Control Manager fields and buttons.

Figure 3-8 Configuration > Call Control Manager

Table 3-6 Call Control Manager Fields

Field or Button	Setting or Description
TFTP	Options for setting TFTP server addressing are Automatic or Manual: <ul style="list-style-type: none"> • Automatic - allows the system to set all TFTP server addresses. Click to set the default condition (the TFTP server will reply to DHCP requests for option 150), or for a list of TFTP servers that point to endpoints in the network where the Unified CM configuration files are located for your system. • Manual - allows you to manually set specific TFTP addresses. Click to manually supply IP addresses of the Unified CM servers.
TFTP Server 1	Enter an IP address if the Manual TFTP option was selected.
TFTP Server 2 - 5	Enter an IP address for up to four additional TFTP servers.
CAPF Authentication String	Enter the Certificate Authority Proxy Function authentication string. The characters entered in this field must match the CAPF Authentication string entered in Unified CM.
Delete Certificate Trust List	Click Delete Certificate Trust List to delete all entries on the Certificate Trust List (CTL). This button becomes active when the IX system is provided with a CTL by a Unified CM configured in mixed authentication mode.

Certificates

To set up and view your 802.1x security authentication, scroll down to the **Certificates** section in the **Configuration** area of the user interface. For more information about certificates and configuring 802.1x security, see the “[802.1X Authentication](#)” section on page 8-1.

Figure 3-9 is an example of the Certificates section of the user interface. Table 3-7 describes the main Certificates fields and buttons.

Figure 3-9 Configuration > Certificates



Table 3-7 Certificates Fields

Field or Button	Setting or Description
Filename	Identifies a certificate file currently downloaded for the IX system.
Type	Identifies the type of certificate file downloaded. Includes: <ul style="list-style-type: none"> • CAPF Certificate - Identifies the CAPF server inside of Unified CM. • Call Manager Certificate - Identifies Unified CM to the system end point. • Misc Certificate - A Locally Significant Certificate (LSC) created by the system if you do not want to use the MIC. For more information, see the “802.1X Authentication” section on page 8-1. • MIC Certificate - Manufacturing installed security certificate.
Read	Allows you to view the details of that certificate.
Download	Allows you to download a MIC or LSC from a source on your local computer. A dimmed Download button indicates the lack of an available certificate.
Drag or Click Here to Upload Certificate	Drag certificates to this block from the Certificates Scheduled For Upload field, or click to upload a certificate from your local computer to your IX system.
Certificates Scheduled for Upload	View any certificates that are scheduled for uploading to your system. Displays No Certificates Scheduled For Upload if no certificates have been scheduled.

Table 3-7 Certificates Fields (continued)

Field or Button	Setting or Description
Reset	Click Reset to cancel any changes you have just made to the fields on the Configuration page. The fields will reset to the values they had before you started making any changes. Once Apply is selected to accept the changes, however, Reset will no longer be able to reset or cancel those changes.
Apply	Click Apply to activate any certificate field changes.

Fields in the First Time Setup Area

Click the First Time Setup tab to begin the setup process for your IX system. Figure 3-10 shows the First Time Setup area in the Administrator interface.

Figure 3-10 First Time Setup Section

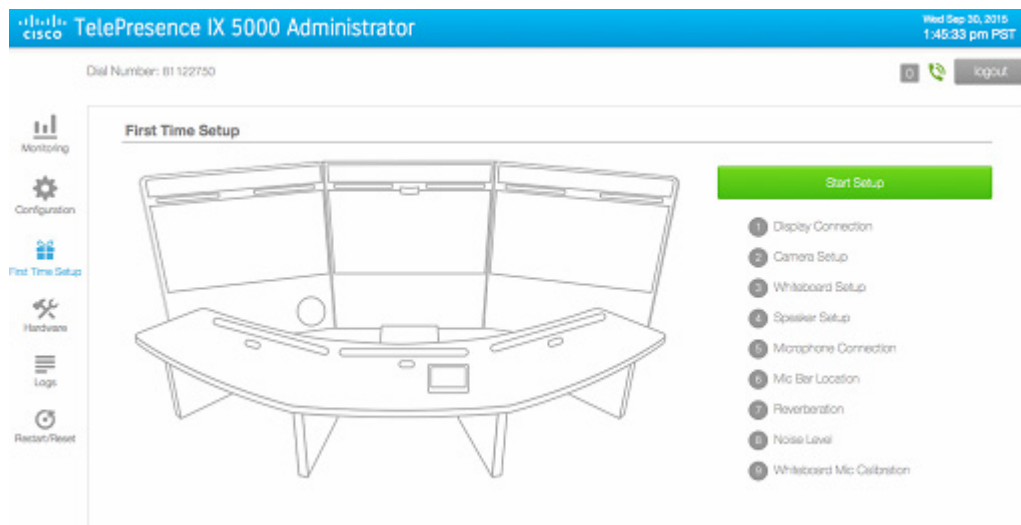


Table 3-8 describes the main setup fields and tests in the First Time Setup area of the Administrator user interface.

For more information about this setup procedure, refer to the *IX5000 and IX5200 First-Time Setup* document at the following URL:

https://www.cisco.com/c/en/us/td/docs/telepresence/ix5000/first_time_setup/ix5000_first_time_setup.html

Table 3-8 First Time Setup Fields

Field or Button	Setting or Description
Display Connection	Checks the layout and connections of your main and auxiliary (if available) displays.
Camera Setup	Positions your camera by aligning it with camera targets on the system table.

Table 3-8 First Time Setup Fields (continued)

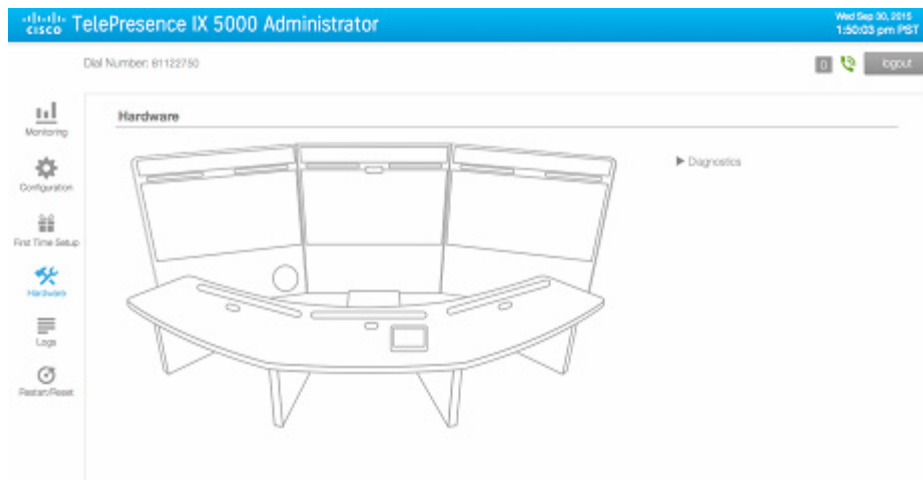
Field or Button	Setting or Description
Whiteboard Setup	Captures an image area of your whiteboard for system display.
Speaker Setup	Tests and verifies the output of your system speakers.
Microphone Connection	Checks and analyzes the cabling of your system's microphones.
Mic Bar Location	Checks and verifies that your system's microphone bars are cabled correctly.
Reverberation	Captures and produces statistics on the reflection of sound by the surfaces of objects, both furniture and people, in the video conference room.
Noise Level	Captures and checks the level of noise in your video conference room, and analyzes the noise level statistics.
Whiteboard Mic Calibration	Checks and adjusts to make the whiteboard microphone sensitivity level equal to that of the table microphone.

Fields in the Hardware Area

Click the Hardware tab to access the available troubleshooting tests for the IX system.

Figure 3-11 shows the Hardware area in the Administrator interface.

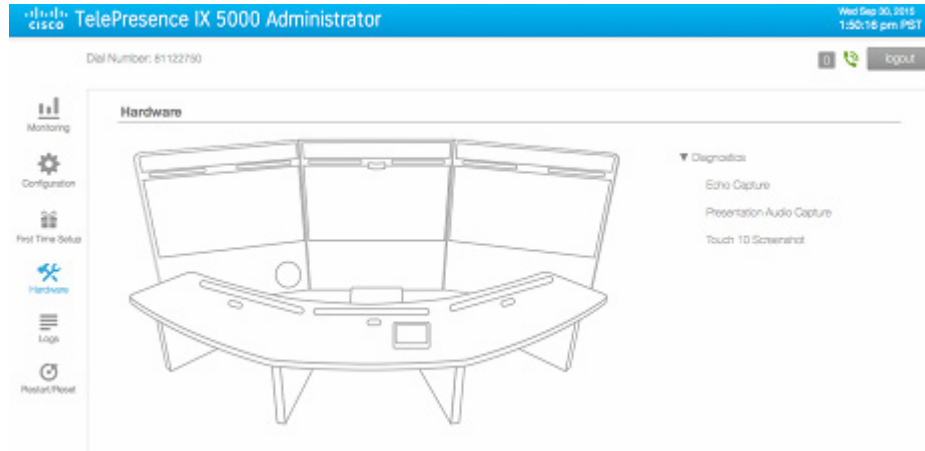
Figure 3-11 Hardware Area



Click on the **Diagnostics** tab on the Hardware page to see the available diagnostic tests as shown in Figure 3-12:

- [Echo Capture](#)
- [Presentation Audio Capture](#)
- [Touch 10 Screenshot](#)

Figure 3-12 Hardware > Diagnostics Tab

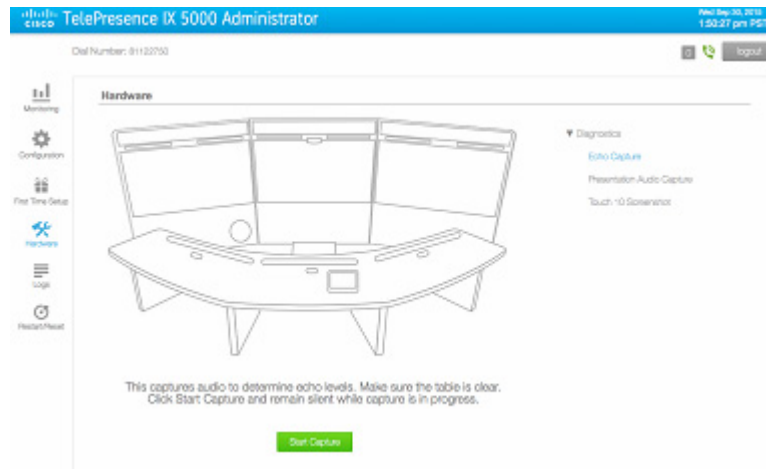


All capture test results and files can be accessed under the **Logs > Captures** tab.

Echo Capture

This test captures audio to determine echo levels. [Figure 3-13](#) shows the Echo Capture test screen.

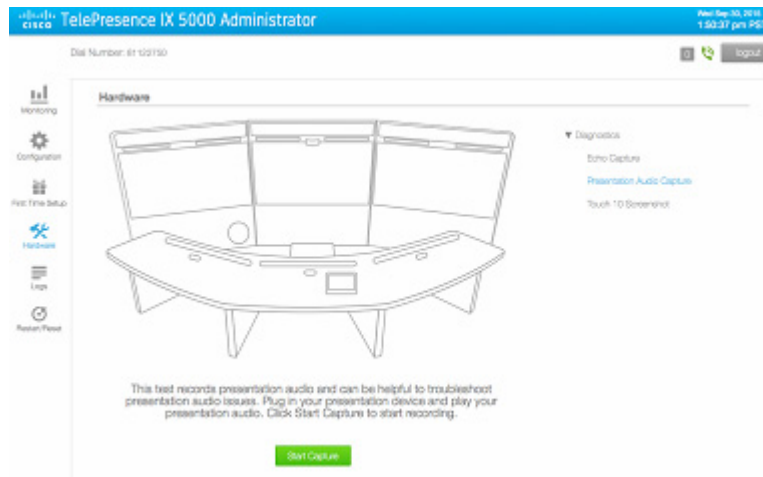
Figure 3-13 Echo Capture Test Screen



Presentation Audio Capture

This test records presentation audio and can be helpful in troubleshooting presentation audio issues. [Figure 3-14](#) shows the Presentation Audio Capture test screen.

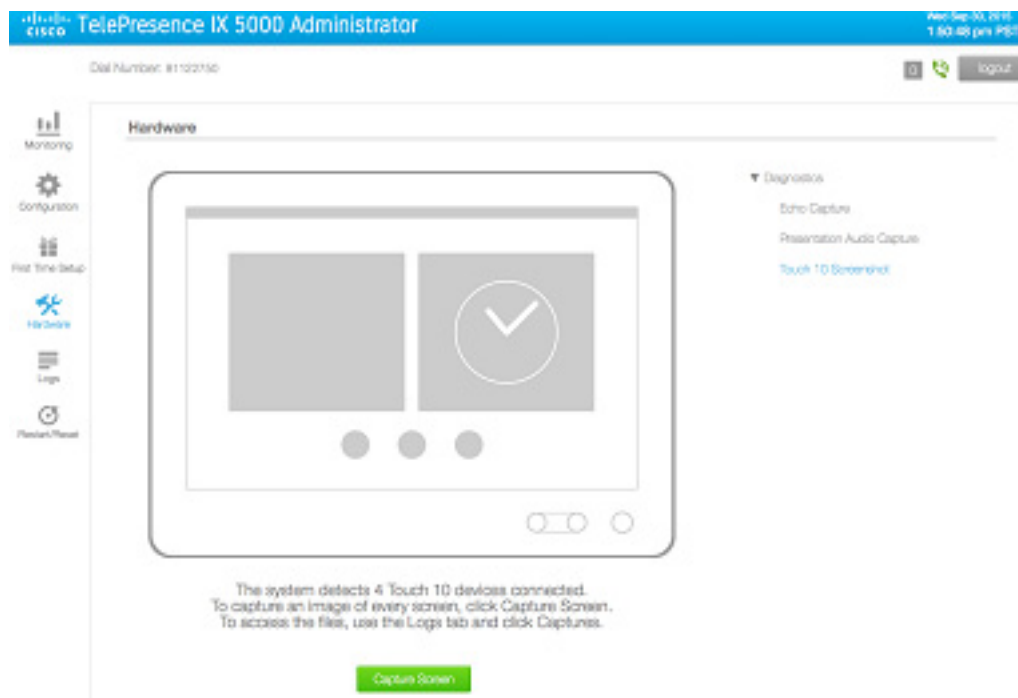
Figure 3-14 Presentation Audio Capture Test Screen



Touch 10 Screenshot

This test displays the number of touch devices that are detected as connected to the system. This test can also capture an image of every screen of the touch device. [Figure 3-15](#) shows the Touch 10 Screenshot test screen.

Figure 3-15 Touch 10 Screenshot Test Screen



Fields in the Logs Area

The Logs area contains details about the configured settings in the IX5000 system and Unified CM. This document section describes the four main tabs in the Logs area. [Tables 3-9](#) and [3-10](#) describe these tabs and their data fields and action buttons.

The four **Logs** page tabs are:

- **System Operations Log**
- **SIP Log**
- **Reports**
- **Captures**

Three action buttons also appear on the **Logs** page tabs:

- **Generate Logs**
- **Download Logs**
- **Download Reports**

System Operations Log

Click the **System Operations Log** tab to view an ongoing log of System Operation (sysop) messages, including call information, call statistics, and call errors. Up to 20 individual files can be saved on the IX system, and each file can contain up to 100,000 characters. [Figure 3-16](#) shows a sample System Operations Log window.

For detailed explanations of each of the sysop log messages, refer to the [Cisco TelePresence System Message Guide](#).

To generate a sysop log file, click the **Generate Logs** button at the top right of the page. To download the sysop log files, click the **Download Logs** button that is located below **Generate Logs**. IX5000 Administration software then prompts you to do one of the following:

- Open to view the sysop log files—The last 100,000 bytes of the log are shown. When you download Sysop files, all available Sysop files will be downloaded.
- Save the sysop log files.

Figure 3-16 Logs > System Operations Log Section

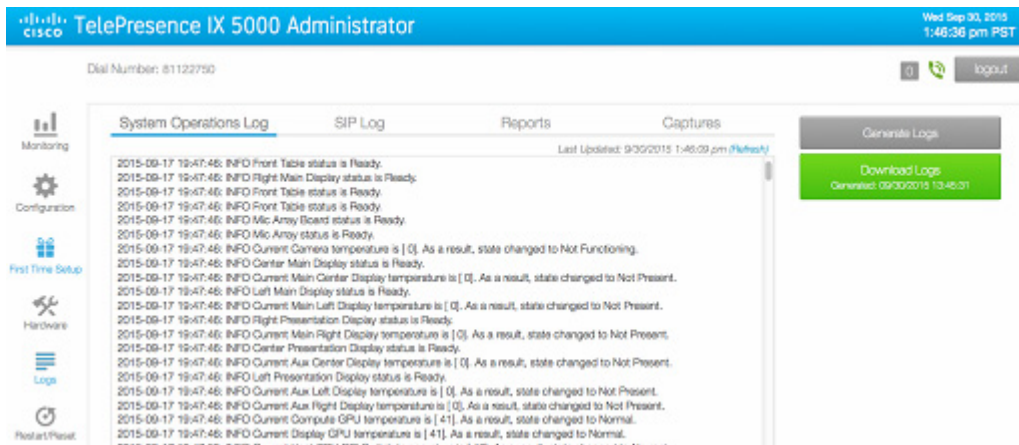


Table 3-9 System Operations Log Fields

Field or Button	Setting or Description
Generate Logs	Click this button to generate a system operations log.
Download Logs	Click this button to download a generated system operations log.

SIP Log

Session Initiation Protocol (SIP) request and response methods are used to establish communications between components in the network and ultimately to establish a call or session between two endpoints.

Click **SIP Log** to view an ongoing log of messages related to SIP negotiation when setting up and ending a call. Use the log filters to customize the content of your logs by changing the Direction, Type, Call ID, To, and From parameters to create a new SIP Log. Besides applying a filter to your SIP Log, you can also generate and download logs.

Figure 3-17 Logs > SIP Log Section

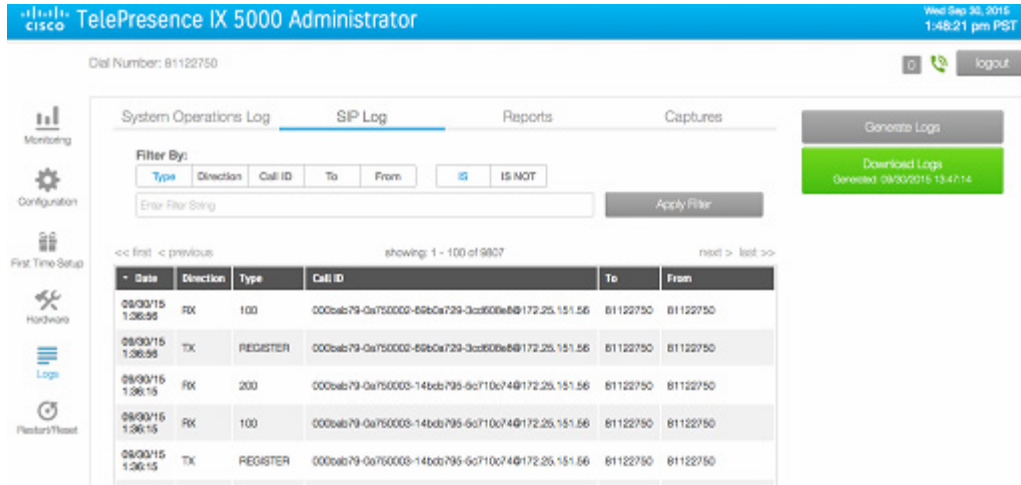


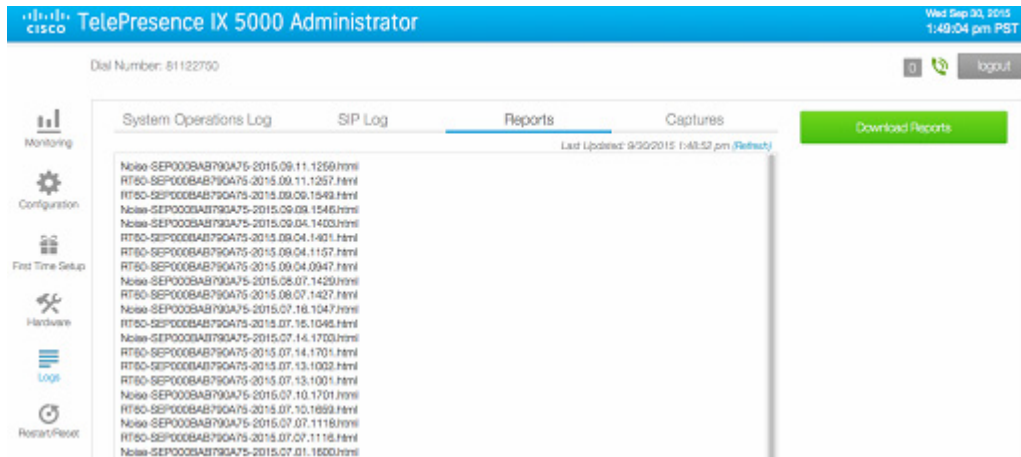
Table 3-10 SIP Log Fields

Field or Button	Setting or Description
Filter By:	
Type	Select the SIP protocol types of the logs to be generated. Options: 100, 200, and REGISTER.
Direction	Select the message direction of the logs to be generated. Options: TX (transmit), RX (receive), or both directions.
Call ID	View the log of a specific call.
To	Generate a log consisting of only the calls going to a specific system/device.
From	Generate a log consisting of only the calls coming from a specific system/device.
IS	Indicates that the SIP log being generated consists only of the field parameters selected as filters.
IS NOT	Indicates that the SIP log being generated will not have the specified field parameters.
Apply Filter	Click this button to apply the filters selected or deselected in the above fields.
Generate Logs	Click this button to generate a specified SIP log. (Click this button to download a selected SIP log.)
Download Logs	Click this button to download a SIP log. (Click this button to delete a selected SIP log.)

Reports

Click **Reports** to view generated reports on the noise level and reverberation tests that run during First Time Setup. Figure 3-18 is an example of what report files can be downloaded for review.

Figure 3-18 Logs > Reports

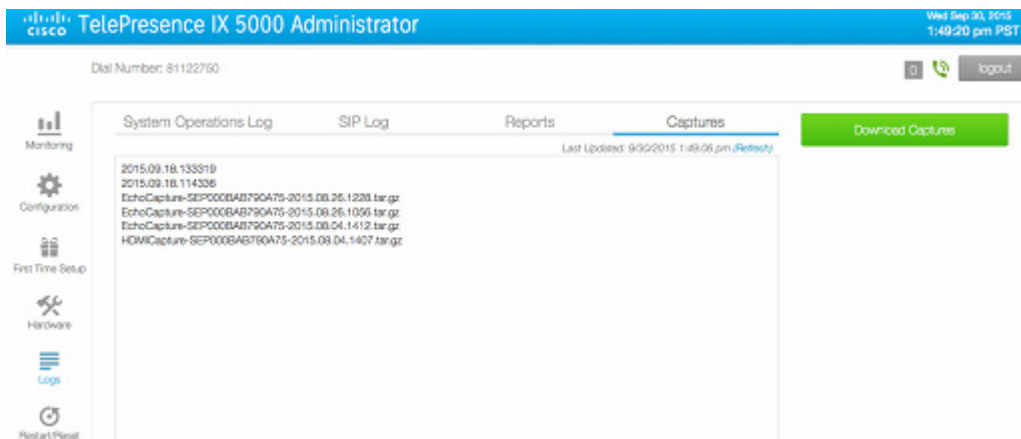


Captures

Click **Captures** to show the log files generated during hardware (troubleshooting) diagnostics. Captured logs include:

- Echo capture
- Presentation audio capture
- Touch 10 diagnostics

Figure 3-19 Logs > Captures Section



Click **Download Captures** to copy the captured log files to your device.

Fields in the Restart/Reset Area

The Restart/Reset area is where you can immediately restart your IX system or return the system back to its original factory default configuration.

This section contains information about the two options in the Restart/Reset area: System Restart and Factory Reset.

System Restart

Click **System Restart** to immediately restart your IX system. If you are in a call, however, note that this action will immediately end that call.

Factory Reset

Click **Factory Reset** to return your IX system settings to their original factory configuration values. As this reboot process may take up to two hours to complete, you should periodically check the status of the reboot on your Touch device.



Note

After the Factory Reset has completed, you **MUST** rerun First Time Setup and re-register your IX system in Unified CM.

For more information on adding your system as a device in Unified CM, refer to the [“Adding an IX System to Unified CM”](#) section in the *Configuring Cisco Unified Communications Manager for the IX System* document.

Where to Go Next

Proceed to [Chapter 4, “IX Software Features”](#), to understand, configure, and implement IX software features.



IX Software Features

Revised: May 11, 2017

This chapter includes an overview of, and configuration information for, IX5000 software features. This chapter also includes information about the features that require an overview or detailed configuration steps. For a description of all features that are introduced in a specific IX software release, see the [Release Notes for Cisco TelePresence Release IX 8 Software](#).

Contents

- [Ad Hoc Conferencing for the IX System, page 4-2](#)
- [TMS Phone Books Support on the IX System, page 4-2](#)
- [Configurable Number of Presentation Streams, page 4-2](#)
- [TMMBR Support, page 4-3](#)
- [H.265 Support, page 4-3](#)
- [3rd Party CA Signed Certificate Support, page 4-4](#)

Ad Hoc Conferencing for the IX System

The IX system supports ad hoc conferencing, in which an existing point-to-point call is escalated into a conference by adding more video and audio participants. The ad hoc conference does not require scheduling the meeting beforehand using a meeting scheduler such as TelePresence Management Suite.

Ad hoc conferencing support is configured using Unified CM. For more information about configuration tasks and support limitations, see the “Ad Hoc Conferencing” section of the *Configuring Cisco Unified Communications Manager for the IX System* document.

TMS Phone Books Support on the IX System

The IX 5000 supports using the directory from the Cisco TelePresence Management Suite (TMS) as an alternative to using the directory in Unified CM. The IX user accesses the directory when tapping the **Contacts** icon on the Touch device.

When configuring the IX in Unified CM, set the Alternate Directory Type and Alternate Directory Server fields in the Product Specific Configuration Layout Area to TMS. For more information, see the “Product Specific Configuration Layout Area” section of *Configuring Cisco Unified Communications Manager for the IX System*.

This feature requires that Phone Books are configured in TMS 15.3 and later. When configuring TMS for the IX system, set the TMS to medium security mode.

For more information, see the “Creating and Managing Phone Books” section of the *Cisco TelePresence Management Suite Administrator Guide* for TMS 15.3 or later.

Configurable Number of Presentation Streams

The IX 5000 supports two presentation streams on point-to-point calls from one IX system to another. The two streams can be single direction (from presenting participant to receiving participant), or both directions (each participant presents to the other participant simultaneously).

When configuring the IX in Unified CM, you can set the maximum number of presentation streams to either one or two. Using this feature, setting the number of presentation streams to one can reduce the bandwidth required for the IX system.

This setting is configured in the Presentation Stream Count field in the Product Specific Configuration Layout Area. For more information, see the “Product Specific Configuration Layout Area” section of *Configuring Cisco Unified Communications Manager for the IX System*.

**Note**

This feature only applies to point-to-point calls from one IX system to another. Multipoint calls and calls to non-IX systems support only one presentation stream.

TMMBR Support

The IX system supports dynamic rate adaption using TMMBR (Temporary Maximum Media Bitrate Request) for flow control purposes. This implementation is based on RFC5104, but only implements a subset of the recommendations in the RFC. TMMBR is a media resiliency mechanism used to help maintain real-time video when the network is impaired. It is a Request-Response mechanism for point-to-point and multipoint scenarios to adjust to network congestion for an improved user experience.

The TMMBR mechanism is triggered when packet loss of 10 percent or more is detected. Once packet loss is detected, the local endpoint sends a TMMBR request to the remote endpoint to down-speed the video bit rate. In turn, the bandwidth used to maintain the user experience is reduced. The remote endpoint responds with a TMMBN message and reduces the bit rate of the transmitting video. Packet loss below 10 percent does not trigger the TMMBR mechanism.

A TMMBR request is sent from the endpoint experiencing packet loss to the endpoint or node transmitting the video. The TMMBR request helps in down-speeding the video bit rate of the receiving video until one of the following occurs:

- The next media negotiation
- The next TMMBR request
- The call is dropped

TMMBR down-speeding happens for both Main and Secondary media bandwidth for the following call scenarios:

- IX system to IX system
- IX system to Native Interoperability endpoints
- IX system to Multipoint systems such as the TelePresence Server, which supports TMMBR

No user configuration is required.

H.265 Support

In addition to H.264 support, systems running IX software also support the H.265 video compression standard. H.265 provides an average 40% bit rate reduction under ideal network conditions compared to H.264.

H.265 is supported for point-to-point calls between an IX5000 and IX5200 and the following systems:

- Another Cisco TelePresence IX5000 or IX5200
- Cisco TelePresence MX700
- Cisco TelePresence MX800
- Cisco TelePresence SX80

**Note**

H.265 requires that your IX system is registered to a Cisco Unified Communications Manager (Unified CM) running release 10.5 or later software. For more information, refer to the [“Product Specific Configuration Layout Area”](#) section of the *Configuring Cisco Unified Communications Manager for the IX System* document.

3rd Party CA Signed Certificate Support

Secure Web Service

The IX system supports secure web communication using 3rd party CA signed IX certificates. The CA signed certificate can be uploaded to the IX system using the web UI under the Service Certificates section.

Secure SIP Service

The IX system supports secure SIP communication using 3rd party CA signed Cisco Unified CM certificates. The CA certificate used for signing the Cisco Unified CM certificate can be uploaded to the IX system using the web UI under the Certificate Authorities section.

For more information, see the *Release Notes for Cisco Telepresence System Software Release IX 8*, located here:

<https://www.cisco.com/c/en/us/support/collaboration-endpoints/ix5000-series/products-release-notes-list.html>



Configuring the IX System

Revised: January 31, 2019

Contents

This chapter contains the following sections:

- [Configuring Cisco Unified Communications Manager for Your IX System, page 5-1](#)
- [First Time Setup, page 5-2](#)
- [Network Settings, page 5-3](#)
- [Call Control Manager Settings, page 5-5](#)
- [Certificates Settings, page 5-5](#)
- [Troubleshooting Your Configuration, page 5-7](#)
- [Resetting Your IX Codec Password, page 5-7](#)
- [Troubleshooting Your IX System Components, page 5-9](#)

Configuring Cisco Unified Communications Manager for Your IX System

Before you can use your IX System, you need to configure the system in Cisco Unified Communications Manager (Unified CM).

You can configure your system and complete all of the steps in this chapter prior to configuring your IX system in Unified CM, but you *will not* be able to complete any of the following actions until you register your device:

- You will not be able to download Touch device software from Unified CM, and you will receive an error in the logs.
- Your Touch device will not be able to place or receive calls.

To configure your device in Unified CM, complete the following steps:

-
- Step 1** Load the Cisco TelePresence Administration Software image onto the Unified CM server. For more information, see the “[Immediate Software Upgrade Requirement for Your IX System](#)” section on page -vii and the “[Unified CM Device Package Requirements](#)” section on page -vii.
- Step 2** Add your system as a device in Unified CM. For more information on adding your system as a device in Unified CM, refer to the “[Adding an IX System to Unified CM](#)” section in the *Configuring Cisco Unified Communications Manager for the IX System* document.
- Step 3** Add the TFTP server for your Unified CM server to your system using the TelePresence IX5000 Administrator interface. For more information, see the “[Call Control Manager](#)” section on page 3-9.
-

**Note**

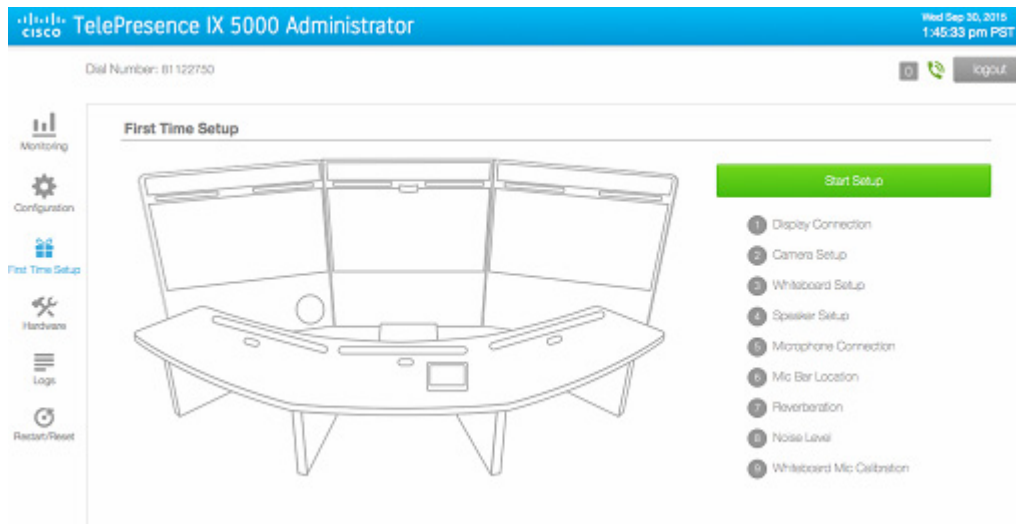
When adding an IX5000 to a device pool in Cisco Unified Communications Manager, configure AAC-LD as the preferred audio codec for the device pool. Other audio codecs are not recommended. If a different audio codec is used, then IX5000 systems in the device pool cannot provide video in audio/video calls.

For more information about configuring Unified CM for your Cisco TelePresence device, refer to the *Configuring Cisco Unified Communications Manager for the IX System*.

First Time Setup

The first time that you log in to the Administrator user interface, you should immediately navigate to the First Time Setup area to set up your IX system.

Figure 5-1 First Time Setup Section



For a full description and configuration steps for the first-time setup procedure, For first-time setup instructions, refer to the *IX5000 and IX5200 First-Time Setup* document at the following URL:

https://www.cisco.com/c/en/us/td/docs/telepresence/ix5000/first_time_setup/ix5000_first_time_setup.html

Network Settings

The Network area displays the Cisco TelePresence IX System's network addressing information. You can view and manage the following network settings:

- DHCP—If your network uses DHCP, select either **Full** or **Mixed**.
 - Full mode allows DHCP to assign all network values (IP address, subnet, gateway, DNS server and Domain).
 - Mixed mode allows you to assign a static IP for the system, and DHCP assigns all other network values.
- If your network does not use DHCP, select **Static** to manually assign all IP address values.
- IP Address
- Subnet
- Gateway
- DNS servers (1 & 2)

To view and manage IP settings:

- Step 1** Choose **Configuration > Network**. The Network area appears, as shown in [Figure 5-2](#) (DHCP) and [Figure 5-3](#) (no DHCP).

Figure 5-2 Configuration > Network Section - (DHCP) Full

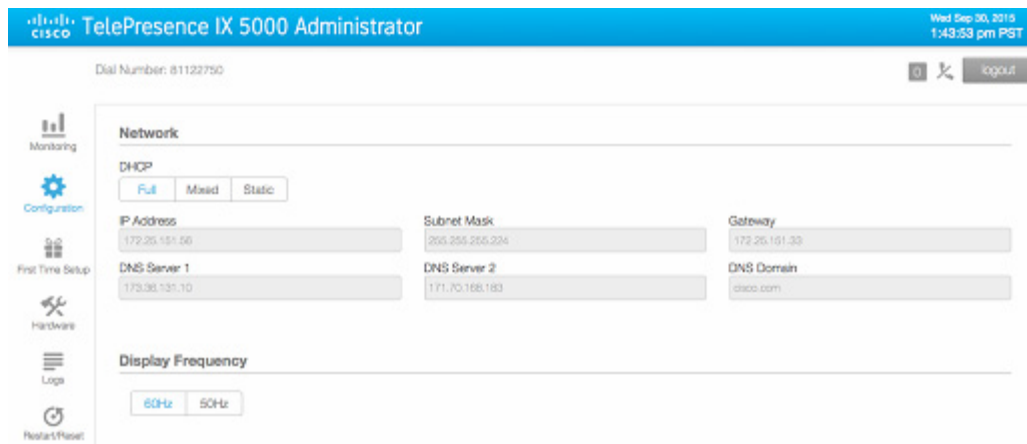


Figure 5-3 Configuration > Network Section - (no DHCP) Static

TelePresence IX 5000 Administrator Wed Sep 30, 2015
1:53:52 pm PST

Dial Number: 81122760 logout

Network

Monitoring
Configuration
First Time Setup
Hardware
Logs
Restart/Reset

DHCP
Full Mixed **Static**

IP Address: 172.25.151.56 Subnet Mask: 255.255.255.224 Gateway: 172.25.151.33

DNS Server 1: 173.38.131.10 DNS Server 2: 171.70.168.189 DNS Domain: cisco.com

Display Frequency
60Hz 50Hz

Step 2 Configure settings for the Cisco TelePresence System uplink to your network. The Cisco TelePresence System can be configured in the following ways:

- Full/Pure dynamic—Uses DHCP to determine all settings.
- Static/Pure static—Uses static settings to determine all settings.
- Mixed/Hybrid—Uses static settings for the IP Address, but uses DHCP to determine the rest of the settings.



Tip When you make any change to a **Configuration > Network** field, the **Restart** and **Apply** buttons at the bottom of the page are activated.

Step 3 Click **Restart** to restore the original settings.

Step 4 Click **Apply** to register new or modified settings.



Note All codecs on the system must be connected and enabled for the reset to complete.

Call Control Manager Settings

To specify TFTP server locations and view a list of available settings for the Cisco TelePresence IX System:

- Step 1** Choose **Configuration**, and scroll down to the **Call Control Manager** section shown in [Figure 5-4](#).

Figure 5-4 Configuration > Call Control Manager Section

- Step 2** Configure Unified CM TFTP server settings.



Note If you enter a new value for any of the TFTP Server fields, and the change does not persist, delete the Certificate Trust List (CTL) by clicking the **Delete Certificate Trust List** button and re-entering the TFTP server information.

The **Reset** and **Apply** buttons, located at the bottom of the **Configuration** page, become active when a value is entered in the TFTP Server fields.

- Step 3** Click **Apply** to register new or modified settings, or click **Reset** to restore the original settings.



Note All codecs on the system must be connected and enabled for the reset to complete.

Certificates Settings

The Certificates area is where you set up 802.1X authentication for your IX System. This section describes the steps you perform to set up 802.1X authentication, and includes the following topics:

- [Authenticating Your IX System Using a Security Certificate](#)
- [Examining the Security Certificate in Your IX System](#)



Note In order to complete 802.1X authentication, you must use a port that is not already enabled for 802.1X.

Authenticating Your IX System Using a Security Certificate

When the Cisco TelePresence IX System receives an authentication challenge from an Authenticator, the system responds with either the Manufacturing Installed Certificate (MIC) or the Locally Significant Certificate (LSC). When both the MIC and LSC are installed, the system uses the LSC to authenticate. If the LSC is not installed, Cisco TelePresence System uses the MIC, as the MIC is built into the system by the manufacturer. For more information on authentication, see the [“802.1X Authentication” section on page 8-1](#).

The LSC provides greater security because it creates a public key infrastructure (PKI) that is unique to each system. To authenticate the codec using the LSC, you must install it on your system manually by using the Certificate Authority Proxy Function (CAPF) in Unified CM. For more information, see [Installing the LSC](#).

Installing the LSC

To install the LSC, navigate to **Configuration > Certificates** and refer to information on the Certificate fields.

Examining the Security Certificate in Your IX System

You may want to examine the security certificate (MIC or LSC) on an 802.1X-authenticated system in order to verify that the certificates are valid, not expired, and issued by the CAPF.

To examine the security certificate in your IX System, you may download a copy of the certificate to your own system by using either of two methods:

- [Downloading a Security Certificate Using the CLI](#)
- [Downloading a Security Certificate Using the Administrator Interface](#)

Downloading a Security Certificate Using the CLI

To download the MIC or LSC using the CLI, complete the following steps:

-
- Step 1** Log in to the CLI.
- Step 2** Enter the following command: **file get cert** {*cert-type*} {*SCP-user*} {*SCP-password*} {*IP-address-or-hostname*} {*file-save-location*}
- See [Table 5-1](#) for syntax descriptions.

Table 5-1 Syntax Descriptions

Argument	Description
<i>cert-type</i>	Type of certificate to retrieve (either MIC or LSC)
<i>SCP-user</i>	Username of Secure Copy (SCP) user
<i>SCP-password</i>	Password for SCP user
<i>IP-address-or-hostname</i>	Hostname or IP address of target system
<i>file-save-location</i>	Location to save file on target system

If you select the MIC as the type of certificate to retrieve when entering the command, the security certificate will save on the target system in the designated file-save location:

```
file get cert MIC username password 10.1.1.1 /home/user
Uploading MIC to 10.1.1.1...DONE
```

If you select the LSC as the type of certificate to retrieve, but the LSC is not installed on the Cisco TelePresence System, the command line will read as follows:

```
admin:file get cert LSC username password 10.1.1.1 /home/user
Uploading LSC to 10.1.1.1...LSC does not exist
Executed command unsuccessfully
```

If the LSC command is unsuccessful, you need to install the LSC on the codec. See [Installing the LSC](#). If the command is successful, continue to the next step.

- Step 3** Go to the designated file-save location, and click the file to view the certificate.
-

Downloading a Security Certificate Using the Administrator Interface

To download an MIC or an LSC from the Administrator interface, complete the following steps:

- Step 1** Log into the Administrator interface, and navigate to **Configuration > Certificates**.
- Step 2** Click **Download** at the right of the certificate row to download and view a certificate. A dimmed **Download** button indicates the lack of a given certificate.
-

Troubleshooting Your Configuration

For information about troubleshooting your configuration, refer to the “[Verifying and Troubleshooting the IX System Configuration](#)” section of the *Configuring Cisco Unified Communications Manager for the IX System* document.

Resetting Your IX Codec Password

This section contains the following information about managing and troubleshooting password issues on the Cisco TelePresence IX System:



Note

You must be in the Cisco TelePresence room to read the newly requested passcode that shows on the main display. At each point where the **pwrecovery** account requires input, the program will wait up to 60 seconds. If nothing is entered, the system will inform you that the entry took too long and will exit.

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.

Before You Begin

Make sure that the IX System is not in a call, and that there is only one instance of someone trying to reset the password. If either of these conditions exist, the session will abort.

The codec password is normally set from the Unified CM. If the Unified CM is not available, and the password is unknown, complete the steps in the following procedure.

Procedure

To reset your IX System codec password:

Step 1 Using a Secure Shell (SSH) or other secure host client, log in to the Cisco TelePresence System GUI:

Step 2 Log in with the following:

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

The following message appears in the SSH client window:

Example 5-1 Welcome to Password Reset

```
dhcp-249:~ $ ssh pwrecovery@10.00.00.100
pwrecovery@10.00.00.100's password:

*****
*****
**                               **
**      Welcome to password reset  **
**                               **
*****
*****

Do you want to continue ? (y/n):y
Preparing the system...
Please enter the passcode:
```

Step 3 The system will ask if you want to continue. Type **Y**, and then **return** to continue



Note If desired, type any other key, and then **return** to exit.

This system will now prepare for password reset and prompt you for a passcode. The new passcode is displayed on the IX System main display (See the following example.):

```
Password reset is now being run
Passcode: 919175
```



Note The passcode is a randomly generated number and will be different for each login attempt. If you enter the wrong passcode, the system will inform you that the passcode was incorrect and will exit, as shown in the following example. If this happens, repeat [Step 1](#) and [Step 2](#) from above.

Example 5-2 Invalid Password Reset Request

```
Do you want to continue ? (y/n):y
Preparing the system...
Please enter the passcode:12345
Sorry that was an invalid passcode...
Logging off
Connection to 10.00.00.100 closed.
dhcp-249:~ $
```

When you enter the correct passcode, the IX will then reset the administration account name and password to the system defaults.

**Note**

The top right of the screen could still show the previous, non-default user name. Do not use this user name, and continue to use the default user name and password.

The following example shows successful password reset information:

Example 5-3 Successful Password Reset Request

```
Please enter the passcode:507530
resetting admin name and password
stopping any existing admin session
admin account and password reset to default
success in applying security rules
Logging off
Connection to 10.00.00.100 closed.
dhcp-249:~ $
```

**Note**

If you are using the IX System with Unified CM, the next time you perform a “Refresh” or “Reset” from Unified CM, the administration account name and password will be reconfigured to the values specified in the Unified CM device page.

Troubleshooting Your IX System Components

For information about troubleshooting your IX System components, refer to the [First Time Setup](#) section of this administration guide.



Monitoring the System

Revised: May 11, 2017

Contents

This chapter contains the following Monitoring page sections:

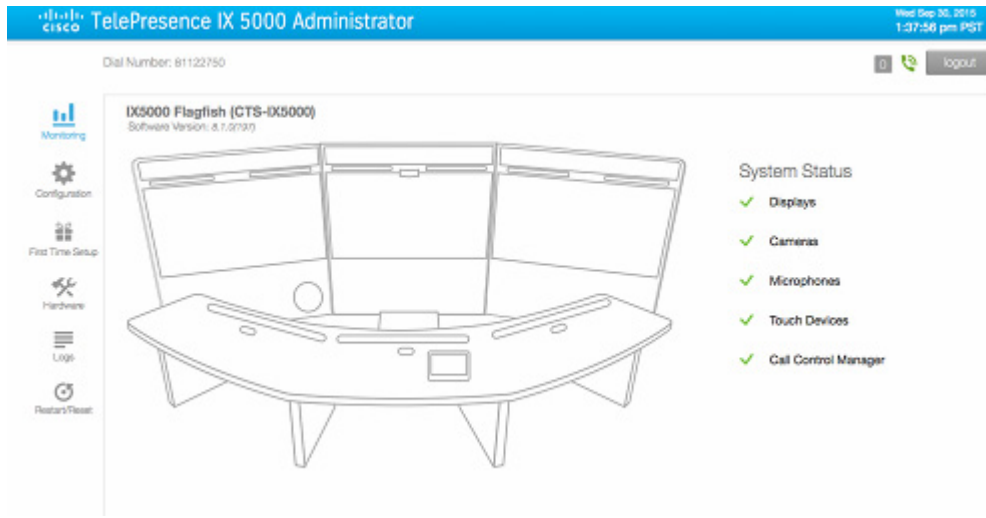
- [System Status, page 6-1](#)
- [Call Statistics, page 6-2](#)
- [Network Data, page 6-4](#)
- [Using SNMP Traps to Monitor the System, page 6-4](#)

System Status

Use the System Status section to view the current operating statuses of the IX system hardware components. Colored icons next to each component indicate whether that component is connected and functional (green checkmark) or not connected or nonfunctional (red x).

[Figure 6-1](#) shows a sample Monitoring page with the System Status section positioned on the right.

Figure 6-1 Monitoring > System Status Section



Call Statistics

Use the **Call Statistics** section to view audio and video call statistics collected by the codecs. Scroll down the **Monitoring** page to access this section.

Special Note for Statistics for HD Presentations

If you are sharing an HD presentation, the call statistics will appear in different places depending on whether the call is a point-to-point or multipoint call.

- For a point-to-point call, view the presentation statistics under **Monitoring > Call Statistics > General**.
- For a multipoint call, view the presentation statistics under **Monitoring > Call Statistics > AV Call Video**, **AV Call Audio**, or **Audio Only**.

Viewing Call Statistics

To view Call Statistics:

-
- Step 1** Navigate to **Monitoring > Call Statistics** to view tabs for the following IX system call statistics:
- **General**—Historical information about all system calls. See the sample Data Types and Values in [Figure 6-2](#).
 - **AV Call Video**—Video stream statistics of an in-progress TelePresence call for the Right, Center, or Left display. See sample statistics in [Figure 6-3](#).
 - **AV Call Audio**—Audio stream statistics of an in-progress TelePresence call.
 - **Audio Only**—Audio add-in data for the in-progress TelePresence call.

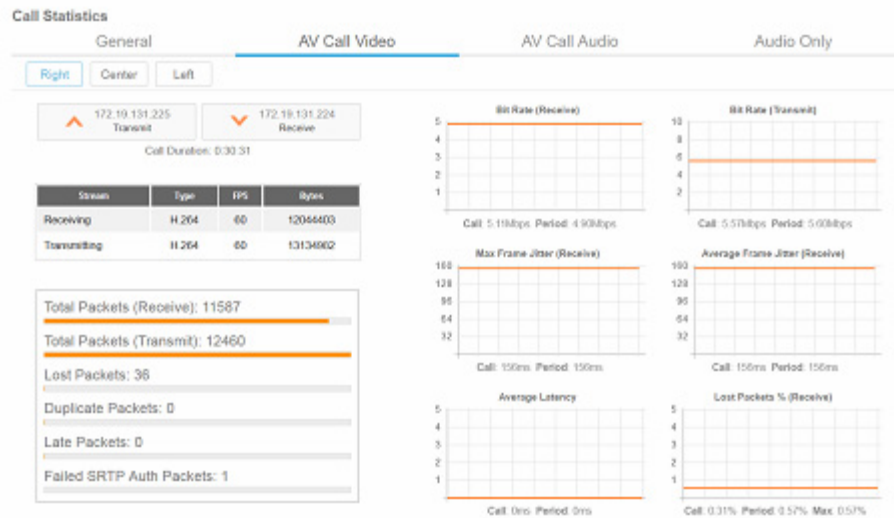
Step 2 Click a tab for a desired statistics selection.

Figure 6-2 General Call Statistics

Call Statistics	
General	AV Call Video
Data Type	Value
Total Calls in System Lifetime	6
Total Call Duration in System Lifetime	22:06:16
Last Call Duration	0:27:09
Total Call Duration Since Reboot	0:27:09
Last Call Start Time	Tue Sep 23 08:58:10 2014
Total Calls Since Last Reboot	1
Time Call Stats Were Last Cleared	Thu Sep 11 14:07:51 2014

Click any of the three AV stream selections to get their specific statistics as in [Figure 6-3](#).

Figure 6-3 AV Call Video Stream Statistics



Note that in the AV Call Video tab you view statistics for either the Right, Center, or Left system displays. View either transmit or receive statistics by clicking either the Transmit or the Receive button.

Note

For more information about jitter and packet loss, see the [“Understanding Jitter and Defining Jitter Thresholds”](#) section on page 1-2.

Continue to scroll down the **Monitoring** page to the Network Data section to view your system’s transmission data.

Network Data

Use the Network Data section to view packet transmission statistics collected from the network. Data is listed in columns labeled as if you were looking at the back of the system. For example, on an IX5000, the labels would indicate statistics from the left, center, and right codecs.

To monitor network statistics:

- Step 1** In the **Monitoring** page, scroll down to **Network Data**. Your network data appears as in [Figure 6-4](#).

Figure 6-4 Network Data Section

Network Data			
Call Control Manager: 10.22.146.31	MAC Address: 00:0b:ab:61:a8:76	Hostname: ts1	Domain Name: ts1.local
DHCP Setting: static	IP Address: 10.22.185.111	Gateway: 10.22.185.1	Subnet: 255.255.255.128
DNS Server 1: 173.36.131.10	DNS Server 2:	Operational VLAN:	

Service Status			
Admin Web UI Service	Running	Studio Service	Running
Virtual Canvas Manager Service	Stopped	Media Agent Service	Running
Media Relay Service	Running	Snapshot Stream Service	Running
SSIM Service	Running	Back-end Library service	Running
System Status Collection	Running	TBCSC Service	Running
Whiteboard Mgr Service	Running	Call Control Service	Stopped
Conference Control Service	Running	Calendar Service	Running

- Step 2** View your Network Data information.

Using SNMP Traps to Monitor the System

Cisco provides management information base (MIB) files that monitor your system using the Simple Network Management Protocol (SNMP). For more detail, refer to the “MIBs, RFCs, and SNMP Trap Messages for the Cisco TelePresence System” chapter of the *Cisco TelePresence System Message Guide*.

Where to Go Next

For more information about system statistics and messages, including System Operations (Sysops) Log messages, see the *Cisco TelePresence System Message Guide* at Cisco.com.



IX System Ports and Protocols

Revised: May 11, 2017

Contents

This chapter contains the following sections:

- [Overview, page 7-1](#)
- [Ports and Protocols Used by the IX System, page 7-2](#)
- [Ports and Protocols Used by the Cisco Unified Communications Manager, page 7-4](#)
- [Ports and Protocols Used by the Cisco TelePresence Management Suite, page 7-4](#)
- [Ports and Protocols Used by Cisco TelePresence Server, page 7-4](#)
- [Ports and Protocols Used by Cisco TelePresence Multipoint Switch \(CTMS\), page 7-5](#)
- [Ports and Protocols Used for Cisco IOS IP Service Level Agreements \(IPSLA\), page 7-6](#)

Overview

Immersive Cisco TelePresence Systems are designed to be deployed on a converged IP network. Many enterprise customers rely on firewalls and/or Access Control Lists (ACLs) to protect the systems registered to Cisco Unified Communications Manager (Unified CM) from various sorts of malicious threats. ACLs are also frequently used to enforce Quality of Service (QoS) settings, including marking, shaping and policing traffic at various places in the network, such as at the access edge of a local area network (LAN), or at the intersection of a LAN and wide area network (WAN).

There are three key considerations for using Firewalls and/or Access Control Lists with Cisco TelePresence:

1. The specific TCP and UDP ports that need to be permitted between each component of the solution.
2. The bandwidth required for the audio and video media streams of a Cisco TelePresence meeting is significantly higher and far less tolerant to latency, jitter and loss than a typical voice call and should be taken into consideration when considering specific router, switch, firewall, and intrusion prevention (IPS) platforms and their performance characteristics.
3. Firewalls that rely on Application Layer Inspection in order to dynamically open/close certain UDP ports may not support the specific SIP protocol implementation of Cisco TelePresence, or may not be able to inspect the contents of the application layer protocol because it is encrypted.

This document only addresses the first of the above three considerations. It provides the list of TCP and UDP ports used by Cisco TelePresence. It does not provide guidance on which router, firewall or IPS platforms or configurations customers should use. For more information about network design, refer to the Solution Reference Network Design (SRND) guides at <https://www.cisco.com/go/ucsrnd>. Use this document along with the information in the SRND guide for your Unified CM release.

**Note**

Customers are advised to thoroughly test Cisco TelePresence against their specific firewall, ACL, and IPS configurations before deploying them in production.

Ports and Protocols Used by the IX System

This chapter contains information about ports used by IX systems that are relevant to a firewall or ACL administrator. Ports used for internal system communication are not included in this appendix.

Table 7-1 Protocols and Ports Used by the IX System

Protocol	TCP or UDP	Source Device: Port	Destination Device: Port	Description and Use
CDP	N/A	IX codec: N/A	Switch: N/A	Advertises its existence to the upstream Cisco Catalyst Ethernet Switch to which it is attached and learn what Virtual LAN (VLAN) it should tag its packets with. Note CDP is a layer-2 protocol and hence does not use TCP or UDP for transport.
DHCP	UDP	0.0.0.0: 68 IX codec: 68	Broadcast: 67	Requests an IP address from the DHCP server. Note It is recommended to use static IP addressing instead of DHCP on every CTS endpoint.
	UDP	0.0.0.0: 67 DHCP: 67	Broadcast: 68	Sent by the DHCP server in response to a request for an IP address.
ICMP	N/A	ANY: N/A	ANY: N/A	ICMP may sometimes to be used to determine whether a device is reachable (for example, ICMP echo request and response). ICMP unreachable may sometimes be sent by a device to indicate that a device or port is no longer reachable. ICMP time-exceeded may be sent by a device to indicate that the Time to Live (TTL) of a packet was exceeded.
NTP	UDP	IX codec: 123	NTP: 123	Synchronizes the hardware clock on the CTS with an NTP server.
DNS	UDP	IX codec: Ephemeral	DNS: 53	Resolves hostnames to IP addresses.
HTTP	TCP	ANY: Ephemeral	IX codec: 80, 443	Accesses the administrative web interface of the IX codec. Port 80 is automatically redirected to port 443.

Table 7-1 Protocols and Ports Used by the IX System (continued)

		IX codec: Ephemeral	CUCM: 6970	Downloads configuration and firmware files from the Cisco Unified CM TFTP service. Note The IX codec uses HTTP instead of TFTP for accessing these files.
		IX codec: Ephemeral	CUCM: 8080	Used by the Directories feature on the CTS Cisco Unified IP Phone user interface to search the Cisco Unified CM LDAP directory.
		<ul style="list-style-type: none"> IX codec: Ephemeral CTS-Manager: Ephemeral 	<ul style="list-style-type: none"> CTS-Manager: 8080, 8444 IX codec: 8081, 9501 	<p>Uses XML/SOAP to coordinate meeting schedule and system operational status with CTS-Manager:</p> <ul style="list-style-type: none"> When security is enabled, the CTS uses port 8444 and CTS-Manager uses port 9501 on the CTS (recommended). When security is not enabled, CTS uses port 8080 on CTS-Manager and CTS-Manager uses port 8081 on the CTS.
		IX codec: Ephemeral	CTMS: 9501	Uses XML between each CTS and the CTMS for in-meeting controls such as Site/Segment Switching and Meeting Lock/Unlock.
SSH	TCP	ANY: Ephemeral	IX codec: 22	Accesses the IX codec administrative command-line interface (CLI).
SNMP	UDP	ANY: Ephemeral	IX codec: 161	Receives SNMP queries from a management station.
		IX codec: Ephemeral	SNMP: 162	Sends SNMP traps to a management station.
CAPF	TCP	IX codec: Ephemeral	CUCM: 3804	Registers its Manufacturing Installed Certificate (MIC), or obtains a Locally Significant Certificate (LSC) from the Cisco Unified CM Certificate Authority Proxy Function (CAPF) service.
CTL	TCP	IX codec: Ephemeral	CUCM: 6970 and 2444 (see notes)	Downloads the Certificate Trust List (CTL) from the Cisco Unified CM Certificate Trust List (CTL) Provider service. When downloading the CTL, port 2444 is used.
SIP	UDP	IX codec: Ephemeral	CUCM: 5060	Used for registration and call signaling between the CTS and Cisco Unified CM. Can be one of the following: <ul style="list-style-type: none"> UDP port 5060 TCP port 5060 TCP port 5061 if SIP over TLS is enabled (recommended).
	TCP		CUCM: 5060, 5061	
RTP	UDP	IX codec: 16384 – 32768	ANY: ANY	Sends and receives audio and video media.
XML-R PC	TCP	IX codec: Ephemeral	Phone: 61456	Autostarts the MIDlet phone user interface (UI).
		Phone: Ephemeral	IX codec: 61457	Sends notifications to the MIDlet phone UI.
		Phone: Ephemeral	IX codec: 61458	Receives notifications from the MIDlet phone UI.

Ports and Protocols Used by the Cisco Unified Communications Manager

For a comprehensive list of all ports used by Cisco Unified Communications Manager (Unified CM) release 10, refer to the *TCP and UDP Port Usage Guide for Cisco Unified Communications Manager, Release 10.0(1)* at the following URL:

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/port/10_0_1/CUCM_BK_T537717B_00_tcp-port-usage-guide-100.html

For a comprehensive list of all ports used by Cisco Unified Communications Manager (Unified CM) for release 11.0 and later, see the *System Configuration Guide for Cisco Unified Communications Manager* for your release at the following URL:

<https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-call-manager/products-installation-and-configuration-guides-list.html>

Ports and Protocols Used by the Cisco TelePresence Management Suite

For a list of the ports and protocols used for the Cisco TelePresence Management Suite, refer to the “Port used by Cisco TMS” section of the *Cisco TelePresence Management Suite Installation and Upgrade Guide* for your release at the following URL:

<https://www.cisco.com/c/en/us/support/conferencing/telepresence-management-suite-tms/products-installation-guides-list.html>



Note

Starting with TMS 15.8, IX communicates with TMS via HTTPS over port 9501. To support this, IX5000 needs a Locally Significant Certificate (LSC) installed.

Ports and Protocols Used by Cisco TelePresence Server

Table 7-2 provides you with a list of the ports used by the Cisco TelePresence Server.



Note

This table provides the default list for a Cisco TelePresence Server MSE 8710. The following TelePresence Server products do not use the FTP or H.323 ports:

- Cisco TelePresence Server on Multiparty Media 3x0
- Cisco TelePresence Server on Virtual Machine

Table 7-2 Protocols and Ports Used for Cisco TelePresence Server

Protocol	TCP or UDP	Port	Description and Use
HTTP	TCP	80	HTTP port

Table 7-2 Protocols and Ports Used for Cisco TelePresence Server (continued)

HTTPS	TCP	443	HTTPS port
H.323	TCP	1720	Incoming port for H.323
SIP (TCP)	TCP	5060	SIP port
Encrypted SIP (TLS)	TCP	5061	Encrypted SIP port
FTP	TCP	21	FTP port
SIP (UDP)	UDP	5060	Encrypted SIP port
N/A	N/A	49152-65535	Ephemeral ports

Ports and Protocols Used by Cisco TelePresence Multipoint Switch (CTMS)

Table 7-3 contains information about the Cisco TelePresence Multipoint Switch.

Table 7-3 Cisco TelePresence Multipoint Switch

Protocol	TCP or UDP	Source Device: Port	Destination Device: Port	Description and Use
CDP	N/A	N/A	N/A	Advertises its existence to the upstream Cisco Catalyst Ethernet Switch to which it is attached. Note CDP is a layer-2 management protocol and hence does not use TCP or UDP.
DHCP	UDP	0.0.0.0: 68 CTMS: 68	Broadcast: 67	Requests an IP address from the DHCP server. Note It is recommended to use static IP addressing instead of DHCP.
		0.0.0.0: 67 DHCP: 67	Broadcast: 68	Sent by the DHCP server in response to a request for an IP address.
ICMP	N/A	ANY: N/A	ANY: N/A	ICMP may sometimes be used to determine whether a device is reachable (for example, ICMP echo request and response). ICMP unreachable may sometimes be sent by a device to indicate that a device or port is no longer reachable. ICMP time-exceeded may be sent by a device to indicate that the Time to Live (TTL) of a packet was exceeded.
NTP	UDP	CTMS: 123	NTP: 123	Synchronizes the hardware clock on the CTMS with an NTP server.
DNS	UDP	CTMS: Ephemeral	DNS: 53	Resolves hostnames to IP addresses.

Table 7-3 Cisco TelePresence Multipoint Switch (continued)

HTTP	TCP	<ul style="list-style-type: none"> CTMS: Ephemeral CTS-Manager: Ephemeral 	<ul style="list-style-type: none"> CTS-Manager: 8080, 8444 CTMS: 8080, 8444 	<p>Uses XML/SOAP over HTTP or HTTPS to coordinate meeting schedule and system operational status between CTS-Manager and the CTMS.</p> <ul style="list-style-type: none"> When security is enabled, the CTMS uses port 8444 on CTS-Manager and CTS-Manager uses port 8444 on the CTMS (recommended). When security is not enabled, CTMS uses port 8080 on CTS-Manager, and CTS-Manager uses port 8080 on the CTMS.
		ANY: Ephemeral	CTMS: 80,443	Accesses the CTMS administrative web interface. Port 80 is automatically redirected to port 443.
		IX codec: Ephemeral	CTMS: 9501	Uses XML between each CTS and the CTMS for in-meeting controls such as Site/Segment Switching and Meeting Lock/Unlock. This port is the same for both secure and non-secure modes.
SSH	TCP	ANY: Ephemeral	CTMS: 22	Accesses the CTMS administrative command-line interface (CLI).
SNMP	UDP	ANY: Ephemeral	CTMS: 161	Receives SNMP queries from a management station.
		CTMS: Ephemeral	SNMP: 162	Sends SNMP traps to a management station.
SIP	UDP	CTMS: Ephemeral	CUCM: 5060, 5061	<p>Used for call signaling with Cisco Unified CM.</p> <ul style="list-style-type: none"> When security is not enabled, use UDP or TCP port 5060. When security is enabled, use UDP or TCP. <p>Note Unlike the CTS endpoints which always initiate the SIP TCP socket to Cisco Unified CM, in the case of CTMS either side can initiate the connection.</p>
		CUCM: Ephemeral	CTMS: 5060, 5061	
	TCP	CTMS: Ephemeral	CUCM: 5060, 5061	
		CUCM: Ephemeral	CTMS: 5060, 5061	
RTP	UDP	CTMS: 16384 – 32768	ANY: ANY	Send and receives audio and video media.

Ports and Protocols Used for Cisco IOS IP Service Level Agreements (IPSLA)

Cisco IOS IP Service Level Agreements (IPSLA) is commonly used prior to the installation of Cisco TelePresence to measure and assess the network path.

Table 7-4 lists the specific ports relevant for the IPSLA UDP Jitter probe operation used to conduct Cisco TelePresence Network Path Assessment (NPA) testing. The term “Agent” refers to the router who generates the IPSLA test packets, and “Responder” refers to the router which replies to those requests. “Both” means that either the Agent or the Responder could generate such a packet.



Note

Table 7-4 provides the ports most commonly used by IPSLA Agent and IPSLA Responder routers. Because IPSLA runs on Cisco IOS, there may be other ports used for communications by those routers.

Table 7-4 Cisco IOS IP Service IPSLA Support

Protocol	TCP or UDP	Source Device: Port	Destination Device: Port	Description and Use
CDP	N/A	N/A	N/A	Advertises its existence to the upstream Cisco Catalyst Ethernet Switch to which it is attached. Note CDP is a layer-2 management protocol and hence does not use TCP or UDP.
ICMP	N/A	ANY: N/A	ANY: N/A	ICMP may sometimes be used to determine whether a device is reachable (for example, ICMP echo request and response). ICMP unreachable may sometimes be sent by a device to indicate that a device or port is no longer reachable. ICMP time-exceeded may be sent by a device to indicate that the Time to Live (TTL) of a packet was exceeded.
NTP	UDP	Both: 123	NTP: 123	Synchronizes the hardware clock on the Cisco IOS IPSLA router with an NTP server.
DNS	UDP	Both: Ephemeral	DNS: 53	Resolves hostnames to IP addresses.
SSH	TCP	ANY: Ephemeral	Both: 22	Accesses the Cisco IOS IPSLA router administrative command-line interface (CLI).
SNMP	UDP	ANY: Ephemeral	Both: 161	Receives SNMP queries from a management station.
		Both: Ephemeral	ANY: 162	Sends SNMP traps to a management station.
IPSLA	UDP	Agent: Ephemeral	Responder: 1967	Signals a new IPSLA operation between the Agent and the Responder.
RTP	UDP	Agent: Ephemeral	Responder: 16384 – 32768 (configurable)	Sends and receives audio and video media from the Agent to the Responder. The Responder then returns these packets back to the Agent. The specific destination UDP ports can be defined in the IPSLA Agent configuration.



802.1X Authentication

Revised: May 11, 2017

- [IEEE 802.1X Authentication Overview, page 8-1](#)
- [Checking IX 802.1X Authentication Status, page 8-2](#)
- [Troubleshooting 802.1X Authentication Issues, page 8-4](#)

IEEE 802.1X Authentication Overview

This section describes how to monitor and troubleshoot 802.1X authentication in the Cisco TelePresence System. 802.1X is an IEEE standard for port-based network access control. It offers the capability to permit or deny network connectivity, control Virtual LAN (VLAN) access, and apply traffic policy, based on user or machine identity.

802.1X permits or denies device access to the network by using authentication. Ethernet switch ports can be enabled dynamically based on the identity of the device that connects to it. Devices which are not authenticated cannot gain access to the network.

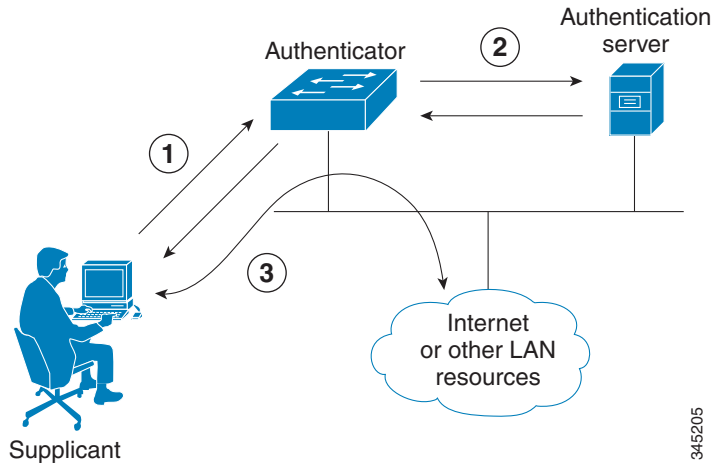
802.1X Authentication Components

802.1X authentication involves the following three network devices:

- A **supplicant**: a client device (such as a laptop or endpoint) that attempts to access a LAN/Wireless LAN (WLAN), or the software that runs on this device and that provides credentials to the authenticator.
- An **authenticator**: a network device (such as an Ethernet switch or wireless access point) that acts as an access point to a protected network. For 802.1X authentication, the supplicant provides network credentials, such as username, password, digital security certificate, or a combination of these, to the authenticator. The authenticator then forwards the credentials to the authentication server for verification.

- An **authentication server**: a server (such as Cisco Secure Access Control Server) that guards the protected network. For 802.1X authentication, the authentication server receives the supplicant's network credentials from the authenticator and verifies the supplicant's identity. Then the supplicant is able to access the resources located on the network.

Figure 8-1 Diagram of 802.1X Authentication Process



Authenticating Your IX System

Your Cisco TelePresence IX system is equipped to function as an 802.1X-compliant supplicant. 802.1X authentication is enabled by default.



Note

Cisco recommends that you configure your switch port (or authenticator) for multi-domain mode.

Checking IX 802.1X Authentication Status

To check 802.1X authentication status in the Cisco TelePresence System, use either of the following options:

- View the IX main display screen during system bootup (see [Checking 802.1X Authentication Status on the Main Display Screen, page 8-2](#))
- Enter the CLI command **show dot1x status** (see [Checking 802.1X Authentication Status with a CLI Command, page 8-4](#))

Checking 802.1X Authentication Status on the Main Display Screen

To check the 802.1X authentication status on the Cisco TelePresence IX system main display screen, complete the following steps:

-
- Step 1 Power off the Cisco TelePresence IX system.
 - Step 2 Power on the Cisco TelePresence IX system.

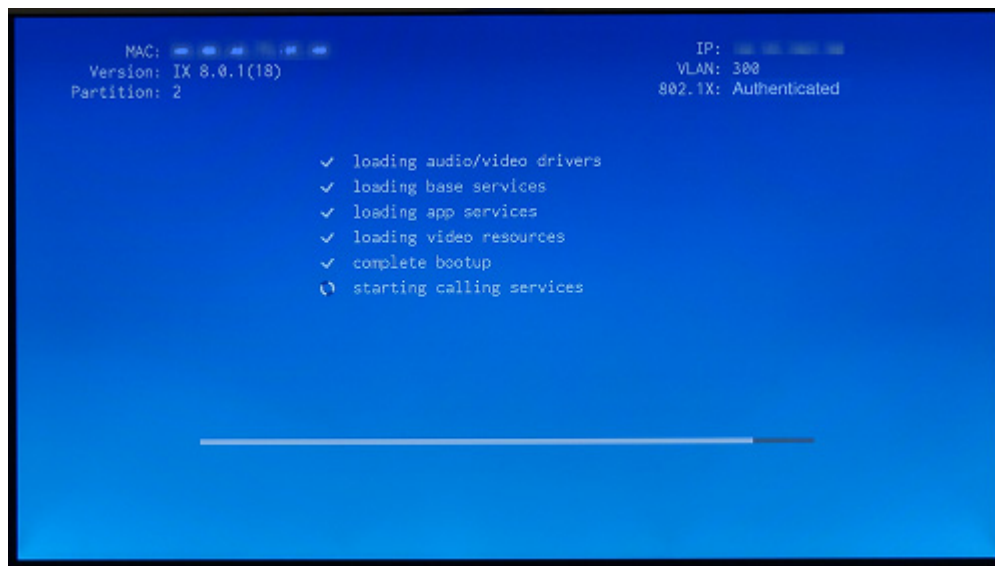
- Step 3** View the bottom right of the main display screen. In a three-screen system, view the bottom-right of the center screen. Text will display to indicate whether 802.1X is authenticated, not authenticated, or not required on your system.

Example:

```
802.1X: Connecting...
802.1X: Not Authenticated
```

This text, as viewed on the Cisco TelePresence System main display screen, indicates the success or failure of 802.1X authentication on that system. If the status line reads “Not Required,” 802.1X authentication is not required for that system.

Figure 8-2 Screenshot of Cisco TelePresence System Boot-Up Screen



See [Table 8-1](#) for a summary of 802.1X authentication status displays for enabled and non-enabled networks.

Table 8-1 802.1X Authentication Status Display Summary

Status	802.1X-Enabled Network	Non-802.1X-Enabled Network
In Progress	Connecting / Authenticating	Connecting
Success	Authenticated	Not Required
Failure	Not Authenticated	Not Required



Note

The 802.1X authentication status can only be viewed on your Cisco TelePresence System primary screen, not on a secondary screen (for example, a presentation screen, or in a three-screen system, the left or right screen). If the 802.1X authentication status does not show on the primary screen, follow the steps below listed under the [“Checking 802.1X Authentication Status with a CLI Command”](#) section on [page 8-4](#)

Checking 802.1X Authentication Status with a CLI Command

To check the 802.1X authentication status with a CLI command, complete the following steps:

-
- Step 1** Log into the CLI.
 - Step 2** Input the following command: **show dot1x status**
 - Step 3** View resulting text. Text will display indicating whether 802.1X is authenticated, not authenticated, or not required on your system.

Example:

```
admin:show dot1x status
Authenticated
```

Troubleshooting 802.1X Authentication Issues

When 802.1X does not authenticate properly, review the following sections:

- [Troubleshooting Issues in 802.1X Authentication](#)
- [Viewing the Security Certificate](#)

Troubleshooting Issues in 802.1X Authentication

[Table 8-2](#) summarizes some issues that may appear during 802.1X authentication, as well as potential resolutions.

Table 8-2 Troubleshooting Issues in 802.1X Authentication

Symptom	Possible Root Causes	Resolution
Cisco Secure ACS authentication server rejects security certificate from the Cisco TelePresence System supplicant.	The security certificate is invalid, expired, or not issued by CAPF.	Install a valid, non-expired security certificate using the CAPF. See Viewing the Security Certificate .
Cisco TelePresence System fails 802.1X authentication.	Errors may be present in the system's most recent log files.	Use the file list log dot1x command in the CLI to check logs for error or failure messages.

Table 8-2 Troubleshooting Issues in 802.1X Authentication

Symptom	Possible Root Causes	Resolution
Cisco TelePresence System displays “802.1X: Not Required” on its boot-up screen.	The Ethernet switch is not configured to support 802.1X.	Check the 802.1X authentication status on the Ethernet switch by logging into the switch and using the CLI command show authentication sessions interface {FastEthernet GigabitEthernet} {Interface Number} . If the Ethernet switch is not 802.1X-enabled, enable it. Please refer to Identity-Based Networking Services: IP Telephony in IEEE 802.1X-Enabled Networks Deployment and Configuration Guide for instructions.
Cisco Secure ACS authentication server rejects security certificate from the Cisco TelePresence System supplicant.	Cisco Secure ACS is not configured to support 802.1X.	Configure Cisco Secure ACS (and all backend network configurations) to support 802.1X. Please refer to Identity-Based Networking Services: IP Telephony in IEEE 802.1X-Enabled Networks Deployment and Configuration Guide for instructions.
Cisco TelePresence System attempts authentication with the MIC instead of the LSC.	The LSC has not been exported from CAPF and imported into Cisco Secure ACS.	Check that the LSC is exported from CAPF and imported into Cisco Secure ACS. See Installing the LSC .
After moving to a different CAPF and Unified CM, Cisco TelePresence System fails 802.1X authentication.	The LSC no longer supports 802.1X authentication, since it was installed from the previous CAPF and Unified CM. Moving the Cisco TelePresence System to a different CAPF and Unified CM requires reinstalling the LSC and upgrading the system.	Reinstall the LSC from Cisco Unified CM and upgrade the Cisco TelePresence System. See Installing the LSC .

Viewing the Security Certificate

You may need to examine the security certificate (MIC or LSC) in order to verify that the certificates are valid, not expired, and issued by the CAPF. For more information on security certificates, see [Examining the Security Certificate in Your IX System, page 5-6](#).

You can use the CLI or a third-party tool to view the MIC or LSC.

- [Viewing the Security Certificate from the CLI](#)
- [Viewing the Security Certificate from a Third-Party Tool](#)

Viewing the Security Certificate from the CLI

To show the MIC or LSC from the CLI, complete the following steps:

-
- Step 1** Log in to the CLI.
 - Step 2** Enter the following command: **show cert {mic | lsc}**. You must enter either **mic** or **lsc**, not both.
 - Step 3** View the certificate that displays within the CLI. Verify that the certificate is valid, not expired, and issued by the CAPF.

Example:

```
> admin:show cert lsc
> Certificate:
Data:
Version: 3 (0x2)
Serial Number: 5 (0x5)
Signature Algorithm( sha1WithRSAEncryption
Issuer: C=US, O=organization, OU=department, CN=CAPF-1a234bcd, ST=CA, L=CH
Validity
Not Before: Mar 23 16:10:31 2012 GMT
Not After: Mar 22 16:10:30 2017 GMT
Subject: C=US, O=organization, OU=department, CN=SEPXXXXXXXXXXXXX
```

If you enter **show cert lsc** on a system where the LSC is not installed, the command line will read as follows:

```
show cert lsc
There is no certificate to display
```

If the security certificate is expired, invalid, or issued by a different source, install a new certificate using the CAPF.

Viewing the Security Certificate from a Third-Party Tool

You can also view the MIC or LSC using a third-party tool. Consult the documentation provided with the tool for instructions.



A

- About function [2-5](#)
- adapters, cable, supported [1-14](#)
- ad hoc conferencing [4-2](#)
- Apply button [2-5](#)
- audio
 - codec statistics [3-4, 6-2](#)

B

- bandwidth provisioning guidelines [1-5](#)
- bandwidth requirements [1-8](#)
- bandwidth resiliency mechanisms [1-4](#)
- bit rate, advertised and negotiated [3-4, 6-2](#)

C

- cable adapters, supported [1-14](#)
- Call Statistics window [3-4, 6-2](#)
- camera
 - monitoring [2-4](#)
- Cisco CallManager
 - monitoring [2-4](#)
- Cisco Unified Communications Manager
 - configuration file location [3-9, 5-5](#)
 - monitoring [2-4](#)
- Cisco Unified Communications Manager Settings window [3-9, 5-5](#)
- codec, statistics from [3-4, 6-2](#)

D

- DHCP configuration [5-3](#)
- display
 - monitoring [2-4](#)

E

- encoder pacing [1-5](#)

F

- field, data in [2-5](#)

G

- Gradual Decoder Refresh (GDR) [1-5](#)

H

- H.264 [4-3](#)
- H.265 Support [4-3](#)
- Help function [2-5](#)

I

- IP address
 - Cisco TelePresence [5-3](#)
 - dynamic [5-3](#)
 - static [5-3](#)
- IP phone
 - monitoring [2-4](#)
- IP Settings window [5-3](#)

L

Logout function [2-5](#)

M

MAC address

 Cisco TelePresence [5-3](#)

main display icons

 call connection status bars [1-12](#)

message

 validation [2-5](#)

P

Passwords

 resetting in CTS [5-7](#)

ports used by IX system [7-1](#)

protocols used by system [7-1](#)

R

Reset button [2-5](#)

S

system

 ports used [7-1](#)

 protocols used [7-1](#)

 status update [2-4](#)

System Status window [2-4](#)

T

TelePresence IX5000 Administrator home page [3-1](#)

TFTP server, configuring [3-9, 5-5](#)

TMMBR dynamic rate adaptation [4-3](#)

TMS Phone Books [4-2](#)

V

video

 codec statistics [3-4, 6-2](#)