

Troubleshooting Guide TC 6.0

- Cisco TelePresence C Series
- Cisco TelePresence MX Series
- Cisco TelePresence SX Series
- Cisco TelePresence EX Series



How to use this guide

The entries in the Table of contents are all hyperlinks. You can click on them to go to the topic.

Your Cisco product has been designed to give you many years of safe, reliable operation.

Please visit the Cisco web site regularly for updated versions of this guide.

The user documentation can be found at <http://www.cisco.com/go/telepresence/docs>.

Contents

Introduction	4
Accessing the system using the web interface.....	5
Find IP address – Touch interface	5
Find IP address – remote control.....	5
New troubleshooting features in TC6	6
Video problems	6
Settings effecting video quality	7
Default call rate	7
Video protocol.....	7
Selecting when to use 60fps over 30fps.....	7
Hardware support for 1080p 60fps for C60 and C90.....	7
Network related issues.....	8
Packet loss.....	8
One way video or audio	9
Interoperability issues.....	9
Far-end problem.....	10
Codec – no self-view.....	10
Using a remote control (C Series, SX20).....	10
Using the Touch interface (C Series, SX20)	10
Web Interface	10
Monitor	11
Cabling.....	11
Presentation issues. Sending of images from attached computer	11
General	11
Input Source Selection	11

Using multiple screens	12
Menus – On Screen Display (OSD)	12
Some parts of images are off the edge of the screen (C Series and SX20)	13
Screen does not turn off in standby (HDMI – CEC).....	13
Video layout customization	13

Audio problems	14
No sound locally	14
No sound (DNAM) – Profile, T1 and T3 Systems.....	14
Echo issues (echo cancellation)	15
Using internal speakers on a modern TV.....	15
Pop noise after unexpected restart.....	15
Custom Audio TC Console (C40, C60, C90).....	15

Peripheral issues	16
Touch	16
Camera	16
Multiple cameras (daisy chaining).....	17
ISDN Link	18
Microphones.....	18
Remote control.....	19
Confirming the key presses are received.....	19

System.....	19
Backup and restore configuration	19
Backup configuration	19
Restore configuration	19
Maintenance mode.....	20
Swapping the software image	20
Upgrading and downgrading software	20
Cannot downgrade	20
Upgrading issues	20
Hardware compatibility	20

Security	21
Web Page (HTTP/HTTPS)	21
Default user account	21
Root user account	21
Menus – restricting access to configuration changes	21
Web page restrictions	21
Web Snapshots.....	22
Auto Answer.....	22

Certificates	22
CUCM CAPF	22
How to factory reset your device.....	22
Suggested methods	22
Factory reset using the Touch interface	23
Factory reset using the web interface.....	23
Factory reset using SSH, Telnet and serial connection.....	24
Factory reset – physical reset method for C20, EX60, EX90, MX200, MX300 and SX20 ..	24
Factory reset the Touch panel.....	26
Running temperature of systems	26
Release and option keys.....	27
Release keys.....	27
Option keys.....	27
Adding option keys	27
How to create a support ticket	28
Getting required log files from the system	28
Basic log capturing	28
SIP and H.323 call flow logging.....	29
Capturing SIP and H.323 signaling messages	29
Packet capture.....	29
Wireshark call analysis usage.....	30
Appendix A – Other sources of information.....	31
Access latest software	31
FAQ.....	31
Customer TelePresence forum.....	31
Documentation	31
Search known bugs	32
TC Console	32
System integrator	32
Video conferencing Room Setup Guide	32
ClearPath Whitepaper	32
Appendix B – Gaining root access to your system	33
Appendix C – Serial connections	33

Appendix D – Useful software.....	34
Windows.....	34
OS X (Mac)	34
Linux.....	34
Packet capturing via Cisco Switch	34
Appendix E – Web diagnostics and on screen error messages and warnings	35

Introduction

This guide covers troubleshooting of the following equipment with software version **TC6.0** installed:

- C Series Codecs (C20, C40, C60, C90)
- EX Series (EX60, EX90)*
- SX20 Codec
- Profiles Series (containing C Series Codecs)
- MX Series (MX200, MX300)

For **Cisco CTS** products please see *Cisco CTS Troubleshooting Guide* at ► http://www.cisco.com/en/US/docs/telepresence/cts_admin/cts_troubleshooting/CTS_Troubleshooting.html.

This guide deals with configuration and troubleshooting mainly using the **web interface** of the system. For details on how to access the web interface please see "Accessing the system using the web interface" on page 5.



Please read the ► [Release notes for TC6.0](#) on the Cisco web-page to see new features introduced and bugs that are resolved in this release.



A new release key is required for upgrading to a major release e.g., from TC5.1.0 to TC6.0. A new release key is not needed for minor release upgrades e.g., from TC6.0 to TC6.1.

Please see "Appendix A – Other sources of information" on page 31 for information regarding the customer forum and other sources of documentation.

If your problem persists after following the troubleshooting steps in this guide, you can create a service request ticket. For instructions see section "How to create a support ticket" on page 28.

We welcome feedback on this document. Please send comments or suggestions for improvements to telepresence-writers@cisco.com.

* EX60/90 can also run TE6.0 for testing purposes with CUCM. This guide deals with EX series running TC6 software. All TE6.0 features (CUCM) will be available in TC6.1 for the EX series in the near future.

Accessing the system using the web interface

This guide deals mainly with management of the system using the web interface.

To access the web interface you must first identify the IP address of the system. The different methods to find the IP address are shown in the **Find IP address** sections below.

When you have obtained the IP address, open a web browser and enter the system's IP address in the address bar. Enter your user name and password in the corresponding fields on the sign in page and click **Sign In**. The default user name is **admin** with no password set.

Sign In

Username:

Password:

System name:

Figure 1 - Web Page Administration Sign In

To effectively manage the system you need to login as admin. Please see "Security" on page 21 for more details on default passwords and information on how to secure your system.

Find IP address - Touch interface

If you have a Touch panel, press the system settings icon in the upper right corner of the screen (Figure 2). This opens the System information and you can find your system's IP address under the **System Information -> NETWORK heading** (Figure 3).



Figure 2 - Settings Icon on Touch Screen

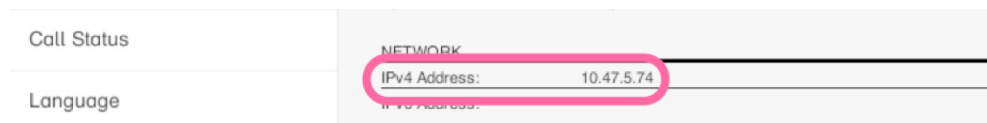


Figure 3 - System IP address - Touch Interface

Find IP address - remote control

Follow the steps below to get the IP address from the system.

- Press the Home button
- When you see menu choose **Settings**
- Then select **System Information**
- You will now see the IP address under **Network** (Figure 4)

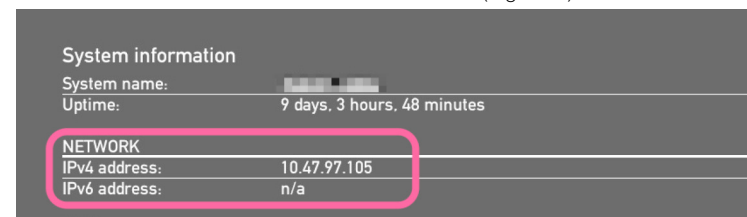


Figure 4 - IP Address shown under System Information

TIP There is a shortcut on the remote control to open the **System information**:

- Press the home button so that you see the menu
- Then press the fifth soft key at the top of the remote to open the System information and get the IP address (Figure 5)
- Another shortcut from the System Information screen is to press the fourth soft key to access the System configuration menus



Figure 5 - Soft Key Shortcut to System Information

New troubleshooting features in TC6

A Diagnostics section on the web interface was introduced in the software version TC6.0. If there is a problem with your system you will see a notification in the **Home** screen when you first login to the web interface. From here you can click on [Diagnostics -> Troubleshooting](#) to see the details of the problem (Figure 6).

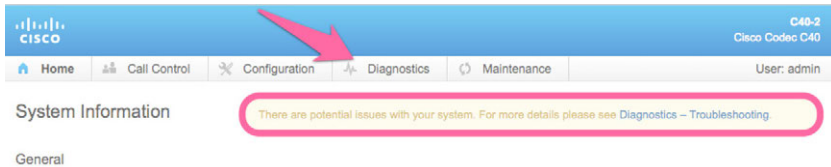


Figure 6 - Potential Problem with Your System

Once you have clicked this link or clicked [Diagnostics -> Troubleshooting](#) you will see a list of diagnostics run on the system with any error messages highlighted in red with **Error**. In the example below you can see that the system is set to use H.323 as the default call protocol, but H.323 has been disabled meaning all calls will fail by default.

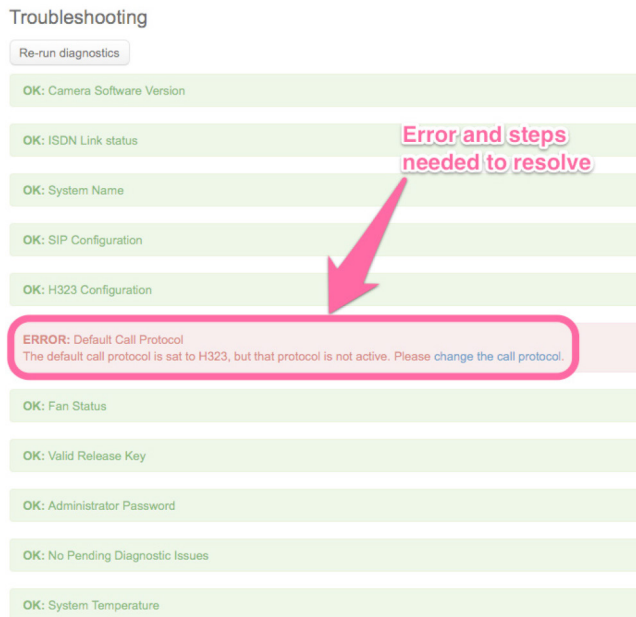


Figure 7 - Specific Problem on System

For descriptions about warning and error messages displayed on this screen in the web interface and possible methods to resolve these see "Appendix E - Web diagnostics and on screen error messages and warnings" on page 35.

Video problems

If you are having problems with the video quality there can be several reasons for this. The problem may be your equipment, but it can also be a fault from the far-end that you are seeing and issues can be related to multiple factors. It is important to identify the source of the problem and then troubleshoot from there.

One of the first questions to ask is are these problems only seen in a call. If you turn on self-view outside of a call, is the image quality stable and of good quality on your local system?

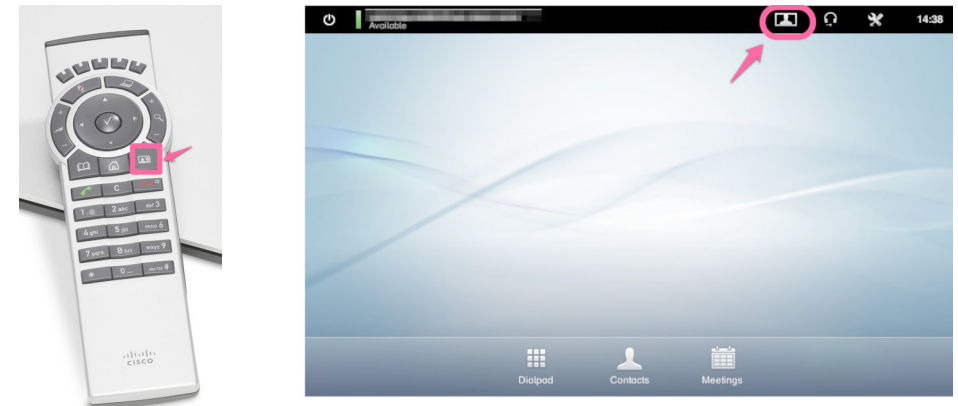


Figure 8 - Location of self-view button on Touch and remote control

If your self-view looks good, you can probably rule out hardware issues with your equipment and should investigate:

- "Settings effecting video quality" on page 7
- "Network related issues" on page 8
- "Interoperability issues" on page 9
- "Far-end problem" on page 10

If your self-view image has issues the problem is most likely with your system. Some possibilities are:

- "Camera" on page 16
- "Monitor" on page 11
- "Codec - no self-view" on page 10
- "Cabling" on page 11

Settings effecting video quality

Default call rate

The quality of the image will depend upon the bandwidth of the call as this limits the resolution of the images that will be sent and received. Generally from a system running TC software in order to have a call achieve 720p (HD) quality the call rate should be above 1152 kbps with 30 frame per second and 2560 kbps for 60 frame per second (if your codec supports 60fps). The quality you receive or send can be limited by the equipment you are calling at the far end site (see "Interoperability issues" on page 9).

Below are the minimum call rates you need in order that the system can achieve certain resolutions. The higher the bandwidth the greater the quality of the call should be.

Minimum Call Rates Needed for Various Resolutions						
Frame rate	Call rate					
	256 kbps	512 kbps	768 kbps	1152 kbps	2560 kbps	6000 kbps
30 fps	512x288	768x448	1024x576	1280x720	1920x1080	1920x1080
60 fps	256x144	512x288	512x288	768x448	1280x720	1920x1080

The default call rate can be set under [Configuration -> System Configuration -> Conference 1 -> Default Call -> Rate](#). You can change the call rate from the default when placing calls, if a different rate is required.

Video protocol

If the image quality is not what you expect, you can check that the video being transmitted/received using the H.264 video codec. It uses the bandwidth more efficiently and therefore the quality will be higher for a given bandwidth than when using a H.263 or H.261 video codec. You can check this in a call under the **Call Status** screen on the Touch panel and the **System Information** page using the remote control. On the web interface you can find this navigating to [Call Control -> Call Control -> Participants](#) and press the triangle symbol to expand the call detail. To see how to access these screens, please see the next section – Network Related Issues.

If the video is not being transmitted as H.264, check that the far-end system supports H.264.

Selecting when to use 60fps over 30fps

For each video input, this setting tells the system the lowest resolution where it should transmit 60fps. For all resolutions lower than this, the maximum transmitted framerate would be 30fps, while above this resolution 60fps would also be possible, if the available bandwidth is adequate.

To select when to use 60 fps rather than 30fps you can change the resolution under [Configuration -> System Configuration -> Video -> Input -> Source 1 -> Optimal Definition -> Threshold60fps](#).

For example if this is set to **1280_720** with a system that is not capable of 1080p 60fps (see next section) then from 1152 kbps you will get 1280x720 at 30fps. With a bandwidth of 2560 kbps and above, the resolution transmitted will be 1280x720 at 60fps, rather than 1920x1080 at 30fps. You cannot get a resolution of 1920x1080p in this case even at maximum call rate.

If set to **1280_720** with a system that is 1080p 60 fps compatible then you will get 1280 x 720 at 30fps at 1152 kbps, from 2560 kbps 1280 x 720 at 60 fps and from 6000 kbps 1920 x 1080 at 60fps. See the table under Optimal Definition Profile section for various resolutions and frame-rates supported.

Hardware support for 1080p 60fps for C60 and C90

New to TC6 is the support for 1080 at 60 frames per second (previously 60fps was only available at lower resolutions) for C Series C60 and C90. Not all hardware is compatible with this. You can see if your system is 60fps capable from the **Home** section of the web interface under **General**. If it is not listed there, your system does not support 60fps.

To see if your system is capable of achieving this, please read the section **1080p60 support for SX20, newer C60s and C90s** in the [Release Notes for TC6.0](#): http://www.cisco.com/en/US/docs/telepresence/endpoint/software/tc6/release_notes/tc_software_release_notes_tc6.pdf

Optimal Definition Profile

Typical resolutions used for different optimal definition profiles, call rates and frame rates								
Frame rate	Optimal Definition Profile	Call rate						
		256 kbps	768 kbps	1152 kbps	1472 kbps	2560 kbps	4 Mbps	6 Mbps
30 fps	Normal	512x288	1024x576	1280x720	1280x720	1920x1080	1920x1080	1920x1080
	Medium	640x368	1280x720	1280x720	1280x720	1920x1080	1920x1080	1920x1080
	High	768x448	1280x720	1280x720	1920x1080	1920x1080	1920x1080	1920x1080
60 fps	Normal	256x144	512x288	768x448	1024x576	1280x720	1280x720	1920x1080
	Medium	256x144	768x448	1024x576	1024x576	1280x720	1920x1080	1920x1080
	High	512x288	1024x576	1280x720	1280x720	1920x1080	1920x1080	1920x1080

This setting controls at what bandwidth certain resolutions are transmitted (see table below). It is recommended to set this to normal. If you have a dedicated video room with very good lighting conditions, you can increase the profile to medium (or high in exceptional conditions) to transfer at a higher resolution for a lower bandwidth.

Network related issues

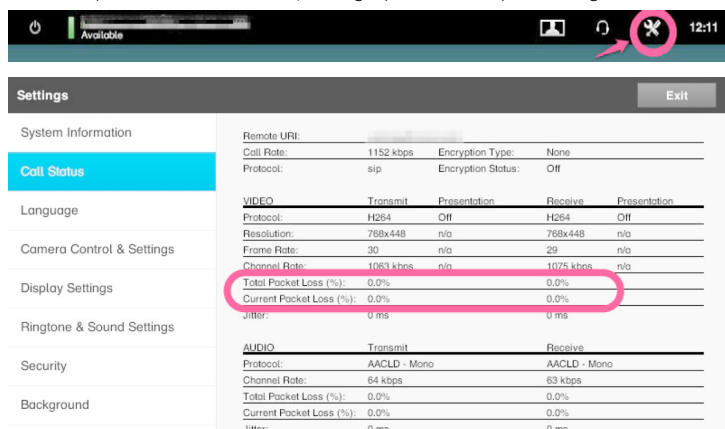
If you are experiencing bad video quality in calls with symptoms such as pixilation, smearing or pulsing of the image, the most likely cause for this is packet loss in the network.

Packet loss

You can check the packet loss information from the web interface, on the Touch panel if one is connected to your system, or on the **System Information** screen using a remote control.

Packet loss statistics – Touch panel

If you have a Touch panel connected, tap the [Settings](#) icon on the screen. Then tap [Call Status](#) and you will see the call status shown below. Here you can see the current packet loss statistics as well as the total packet loss statistic (average packet loss percentage over the whole call).



Packet loss statistics – remote control

Press the Home button on the remote control to open the on-screen menu. Navigate to [Settings](#) -> [System Information](#) to open the **System Information** screen. You can find the packet loss information under the **Video** heading.

VIDEO	Transmit	Presentation	Receive	Presentation
Protocol:	H264	Off	H264	Off
Resolution:	1280x720	n/a	1280x720	n/a
Frame rate:	30 fps	n/a	30 fps	n/a
Channel rate:	4434 kbps	n/a	717 kbps	n/a
Total packet loss (%):	0.0%		0.0%	
Current packet loss (%):	0.0%		0.0%	
Jitter:	0 ms		1 ms	

Packet loss statistics – web interface

To check the packet loss on the current call log in to the web interface. On the top navigation panel click [Call Control](#) -> [Call Control](#) and then under **Participants** select the symbol to expand the details visible. Now you can see the packet loss for the transmit and receive video and audio streams. As you can see below there is a constant 5% packet loss on both the transmit and receive streams which needs to be investigated. This is the loss percentage calculated over the entire call time frame.

On the web interface you can only see loss averaged for the duration of the call, meaning loss could have spiked higher during the call.

Participants		
Change layout		
Connected		
Protocol: Sip		
Transmit Call Rate: 1920 Kbps		
Receive Call Rate: 1920 Kbps		
Encryption: Aes-128		
Audio		
	Transmit	Receive
Protocol	AACLD	AACLD
Channel rate	61 kbps	57 kbps
Jitter	0 ms	0 ms
Loss	5 %	6 %
Video		
	Transmit	Receive
Protocol	H264	H264
Channel rate	1610 kbps	456 kbps
Resolution	1280x720@30Hz	1280x720@30Hz
Jitter	0 ms	3 ms
Loss	5 %	5 %

Packet loss – more information

Even a small amount of loss, for example 0.5%, can have noticeable effects on the image quality.

If you are calling another system running TC software directly (a point to point call), a technology called ClearPath will be used. This helps to mask the effects of packet loss and is enabled by default. When calling systems that do not support ClearPath, call quality will appear worse if there is packet loss, than a call to another TC based system with the same percentage loss. When ClearPath is not used the system will try and hide the loss when displaying the image (decoder concealment) and will down speed the bandwidth of the call. This results in the resolution being decreased thus lowering the amount of data being transmitted and thus hopefully reducing the packet loss. See "Appendix A – Other sources of information" on page 31 for information on the ClearPath whitepaper.

Packet loss can be caused by many issues and after making some basic checks on the endpoint you should start to investigate your network to see where the loss is occurring and take steps to eliminate this loss.

Network Port speed

It is worth checking the duplex/speed settings of the network port on the system and network switch to ensure they are set to the same settings. We recommend that both the network interface on the system and the interface port of the network switch both be set to **auto**. For example if one is set at a fixed rate 100/full and the other to **auto**, the port speed and duplex negotiation can fail and produce mismatched settings. To check the status of the port on the codec go to [Configuration](#) -> [System Status](#) and click on [Network 1](#) and look under the [Ethernet](#) section. Ensure the system is using full duplex and that the speed matches that in the network switch.

To check the configuration of the network port look under [Configuration](#) -> [System Configuration](#) and then click on [Network 1](#) and look under [General Settings](#).

If both the network switch and the system are set to **auto** and the port speed and duplex settings do not match, set both to manual values (e.g. 100/full), restart and retest.

ADSL broadband connection (Asymmetric network bandwidth)

If you have a system located in a home office or connected to an ADSL (Asymmetric Digital Subscriber Line), the bandwidth available for communication is different in each direction. Usually the downstream rate (data coming to you) is far greater than the upstream rate. On the system you can configure a lower upstream rate so your upstream link is not flooded with too much data causing packet loss.

To set this go to [Configuration -> System Configuration -> Conference 1 -> General Settings](#) and set [MaxTotalTransmitCallRate](#) to a value that will fit with your upstream rate. Enter the value in kbps. The value should be 20% less than the available upstream bandwidth as this figure is just for the video and audio traffic and does not account for call signaling and packetization data overheads.

Implementing QoS (Quality of Service)

Another way to deal with packet loss is to implement QoS in your network so that the video conferencing traffic is prioritized over other data. QoS has to be implemented throughout the entire network for this to be effective. Some suggested QoS values are shown below.

	PHB	DSCP (Diffserv Value)
Video and Audio Media	AF41	34
Signalling	CS3	24
Data	AF21	18
NTP	Best Effort	0
ICMPv6	Best Effort	0

You can enter the settings under [Configuration -> System Configuration -> Network 1 -> QoS](#).

One way video or audio

A common cause of video or audio being sent in only one direction (on systems that are known to work - cameras and microphones confirmed working at both ends) is that there is a firewall between the systems that is inspecting packets. Please raise a support case or involve your network technical team.

Interoperability issues

If the far-end system is from another manufacturer or a different generation of products, its capabilities may be less than what your system is capable of. Therefore the quality of images when calling these systems can be degraded compared to a normal call between similar systems.

When the two systems initially connect they exchange what their capabilities are so that unsupported media formats are not transmitted between them. If you are experiencing problems it is worth experimenting with calls at differing bandwidths and also perhaps try different call protocols (H.323 and SIP) to see if there are any differences.

The call status information is useful to see what is being sent and received. The easiest place to look is on the **Call Status** screen on the Touch panel and the **System Information** page using the remote. To see these statistics using the web interface go to [Call Control -> Call Control](#) and select the under the participant you are calling to expand the details. Now you can see information for the incoming and outgoing audio and video streams. As you can see in the image below, the system is transmitting video using H.264 at 720p (1280 x 720) resolution at 30 frames per seconds (30 Hz) and is receiving the same. The audio codec is AAC-LD. Using this information you can see what affects the different settings (call rate, protocol) have on calls.

The release notes for TC6.0 detail what equipment our systems have been tested with and any limitations known to exist - see "Appendix A - Other sources of information" on page 31.

There is a Cisco TelePresence Interoperability database where you can see what equipment has been tested against certain software releases. For more information see <http://www.cisco.com/go/tp-interop>.

Far-end problem

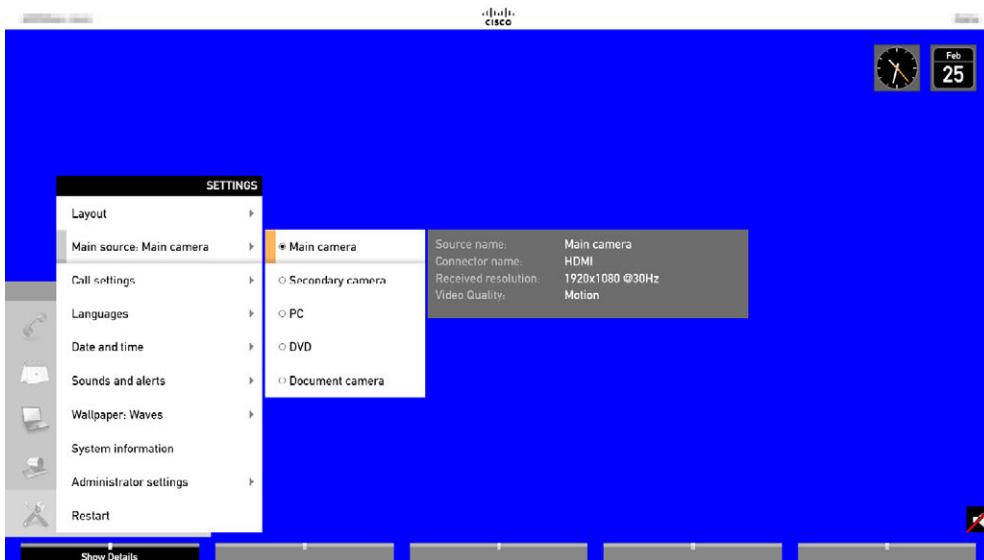
It is important to determine where the problem originates. Even though a problem manifests itself on your system it may be as a result of a problem with the other participants system (far-end). For example the remote site may be receiving video and audio with no problems at all from your system, but the local system cannot see any video from the remote site. This may well be related to a problem with the remote site camera and have nothing to do with the local system.

In situations like these it is worth getting the far end participant to ensure their system is operating correctly, as well as troubleshooting locally.

Codec – no self-view

If you are not seeing any image from the camera and have confirmed the camera is functioning (see "Camera" on page 16), make sure the main video source is set correctly and that there is a signal being received on this input. This can be done using multiple methods.

Using a remote control (C Series, SX20)

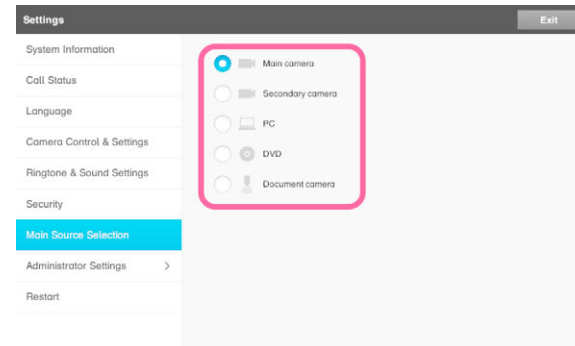


Open the [Settings](#) menu. Under [Main Source](#) check that the **Main Camera** is selected.

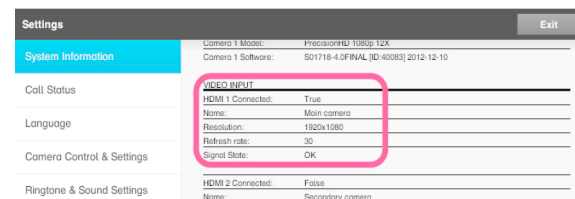
TIP You can check that a signal is being received on each input by selecting **Main Source** which then lists all the possible inputs. You can move up and down to each source and press the 1st soft key on the remote to display the input statistics for that input. This will show if there is anything connected and what the resolution and frame rate is.

Using the Touch interface (C Series, SX20)

Tap [Settings](#) icon (top right) then [Main Source Selection](#) and ensure the **Main camera** is selected.



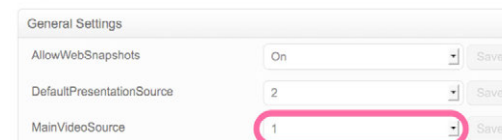
To check that the input chosen is receiving a video signal choose [Settings -> System information](#) on the Touch panel. Scroll down this page to the **Video input** section and you will see the various connected inputs.



Web Interface

From the web interface navigate to [Configuration -> System Configuration -> Video -> General Settings -> MainVideoSource](#)

Video



Default inputs for main video source (camera) are C Series and SX20 =1, EX60 and MX series =2, EX90=3

From the web interface you can also confirm that certain inputs are receiving a signal by navigating to [Configuration -> Peripherals](#)

Video Inputs

Input 1 – HDMI	Main camera – 1920x1080, 30Hz
Input 2 – HDSI	Secondary camera – 1920x1080, 30Hz
Input 3 – DVI	PC
Input 4 – HDMI	DVD
Input 5 – DVI	Document camera

Monitor

Checklist:

- Physical cabling – What output from the video system is being used and what input on the screen does it connect to. Swap the cable.
- Check that the input selected on the screen matches the connector the cable from the video system is plugged into (C Series, SX20 only).
- If you are using a digital connection (HDMI, DVI), the resolution of the screen should be detected and the correct resolution set on the video system. Check that the output resolution from the video system is a resolution supported by the screen by choosing [Configuration -> System Status -> Video -> Output](#).
- Confirm that another device connected to same input on the screen is displayed correctly.

Cabling

The easiest method of troubleshooting cable issues is to swap out the suspected cable with another standard cable. This one should be within the specifications for the type of cable used. If you are running cables at the limits of length specifications, try a cable that is well within the specifications and has no extenders, splitters or converters attached. Then restart all equipment.

For video issues check the video input to ensure that the codec is getting a signal from that connector (see previous section). If there is no signal on the input where the equipment is connected and the equipment (camera, PC, Doc Cam) has been confirmed working separately, then the cabling could be the problem.

Presentation issues. Sending of images from attached computer

General

When you select to send a presentation, the information from the selected input will be transmitted to the far end as a separate data stream from the main video source (camera). If you are having presentation problems, first check that the presentation is seen locally. If it is not, check the input source selection below to ensure the video system is set to the correct input source.

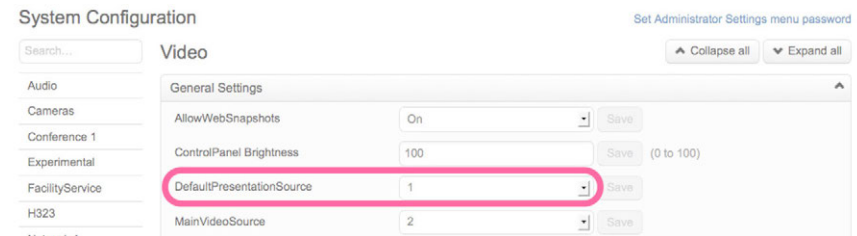
If you are sending a presentation but are having quality issues, please see the section below on settings that may affect presentation quality.

Input Source Selection

If you have connected a computer to the video system and are having problems with sending a presentation to the far-end, check to see if the presentation is visible on the video system locally. If you cannot see the presentation locally then check the following:

- Check that the cabling connected correctly and that the cables are working properly.
- Ensure that the computer is set to display its output on the external output connected to the video system.

- Check that the default presentation source is set correctly on the video system to the correct input. [Configuration -> System Configuration -> Video -> General Settings](#) (Default values are EX60=1, EX90=2, C Series=3, SX20=2). To determine what the numbers for the various inputs mean, scroll down the [Configuration -> System Configuration -> Video -> Input](#) and you can see what input corresponds to each number.



When starting a presentation using the Touch panel, you can see which input source is selected for the presentation and you can change the source by swiping left or right to see the alternate sources. Generally you should see something similar to the image below, where the PC is selected for presentation.



Presentation quality

You can check the resolution and codec used for the presentation from the **System Information/Call Status** screen on the Touch panel or remote control or look at the [Call Control -> Call Control -> Participants screen](#) in the web interface and press the small arrow to expand the information on the current call to show more detailed information. You should see that there is information under the **Presentation** section under **Transmit**.

Here you can see that a presentation is being sent using H.264 video codec at a resolution of 1024x576 at 15 fps.

Presentation	Transmit	Receive
Protocol	H264	-
Channel rate	291 kbps	-
Resolution	1024x576@15Hz	-
Jitter	0 ms	0 ms
Loss	0 %	-

Sharpness and motion settings

You can check this setting [Configuration -> System Configuration -> Video -> Input -> SourceX -> Quality](#) (X is the source number for the presentation source). For presentations this should be set to **Sharpness** rather than **Motion**. This prioritizes the video resolution over frame rate which is the default setting for presentation inputs and the preferred setting.

NOTE Camera sources should be set to motion.

Allocation of bandwidth for presentation

The available transmit video bandwidth (call rate) is distributed between the main channel (camera) and presentation channel according to **MainChannel Weight** and **PresentationChannel Weight** values. These can be changed under [Configuration -> System Configuration -> Conference 1 -> Video Bandwidth](#). The more bandwidth allocated to a channel, the better the image from that channel will be. This way you can prioritize your presentations over the camera video if needed.

For example if the presentation channel weight is set to 2 and the main channel weight is 1, then the presentation channel will use twice as much bandwidth as the main (camera) channel.

The [Configuration -> System Configuration -> Conference 1 -> Video Bandwidth -> Mode](#) can be set to **dynamic** or **static**. If set to **dynamic** (default setting) the system will use all the available call bandwidth until a presentation is started whereupon it will change the bandwidth to those defined above. If set to **static** the presentation bandwidth will be reserved even when no presentation is being shown. The recommendation is to set this to **dynamic** to utilize all bandwidth during the call.

Using multiple screens

To have output on a second screen on C20, C40, SX20 and EX90 dual display option key is needed. C60 and C90 do not need this key, as all outputs are enabled by default. Please see "Option keys" on page 27 for more information about the dual display option key and how to check which keys you have currently installed.

Menus - On Screen Display (OSD)

Cannot see the menus on current screen

On the C Series the menu is displayed on one monitor output only. On the other outputs you will only see the background image. To check the menu settings using web interface go to [Configuration -> System Configuration -> Video](#) and under **OSD** you can see the current settings.

OSD		
AutoSelectPresentationSource	Off	Save
EncryptionIndicator	Auto	Save
LoginRequired	Off	Save
MenuStartupMode	Home	Save
MissedCallsNotification	On	Save
Mode	On	Save
MyContactsExpanded	Off	Save
Output	1	Save
Today's Bookings	Off	Save
VirtualKeyboard	UserSelectable	Save

Figure 9 - Menu Settings

From here you can see if the menus are enabled (Mode - On) and which physical output the menus are sent to.

You can check which physical output the Output number is referencing by checking the [Configuration -> Peripherals](#) (see below) or checking the physical backplane of the system.

Video Outputs	
Output 1 - HDMI	1280x1024, 60Hz
Output 2 - DVI	1024x768, 60Hz
Output 3 - HDMI	1280x720, 60Hz
Output 4 - DVI	1024x768, 60Hz
Output 5 - Legacy	720x480, 60Hz

Figure 10 - Finding Physical Interface Numbers using Web Interface

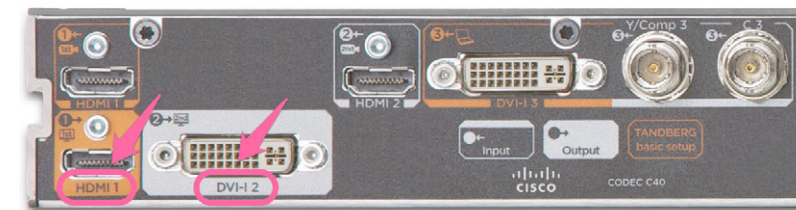


Figure 11 - Find Physical Interface Number

NOTE You will not see on screen menus when using a Touch panel that is correctly paired to the video system, they are only available for users using the remote control.

Some parts of images are off the edge of the screen (C Series and SX20)

Overscan means that on some parts of the image, menus and soft buttons may be off the edge of the screen. The recommended fix for this is to go into the menus of the monitor and turn off overscan if possible. This may be called 'just scan,' '1:1 pixel mapping,' 'dot by dot' or something else as name varies depending on the manufacturer.

If you cannot fix this using the menus on the actual monitor you can use the settings on the web interface. Go to [Configuration -> System Configuration -> Video -> Output](#) and change the overscan level for the interface being used.

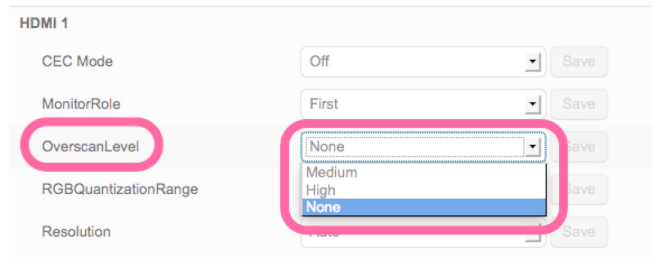


Figure 12 - Overscan Settings

Screen does not turn off in standby (HDMI - CEC)

By default the codecs will stop sending any signal when stand-by mode is activated. For some screens this is fine, they will register they have no signal and after a brief wait they too go into standby mode.

Some screens however will remain on. For HDMI connections you can enable CEC (Consumer Electronics Control). Depending on the monitor you are using this can also be called something else: Sony: BraviaLink, LG: Simplink, Sharp: Aquos Link, Pioneer: Kuro Link, Philips: EasyLink, and Samsung: AnyNet+.

To do this go to [Configuration -> System Configuration -> Video](#) and look under the output section to see the HDMI interfaces available. You should check that CEC is enabled on your display screens input as well from the screens menus.

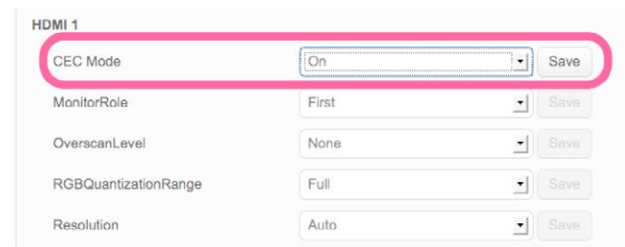


Figure 13 - Enable CEC

NOTE With some screen manufacturers we find their CEC implementation are non-standard and therefore even with this setting on the screen will not turn off. LG screens are known to use non-standard CEC and will not accept our standby signals. DVI connections use a difference signaling method thus screens connected by the DVI output on the codec to the DVI input on the screen should not have this problem.

Video layout customization

You can create new video layouts on the C60 and C90 codecs and change when to display the existing layouts on the C40. The easiest method to accomplish this is by using the TC Console tool. Please ensure you have the latest version of TC console by visiting <http://developer.cisco.com/web/telepresence-developer/home>

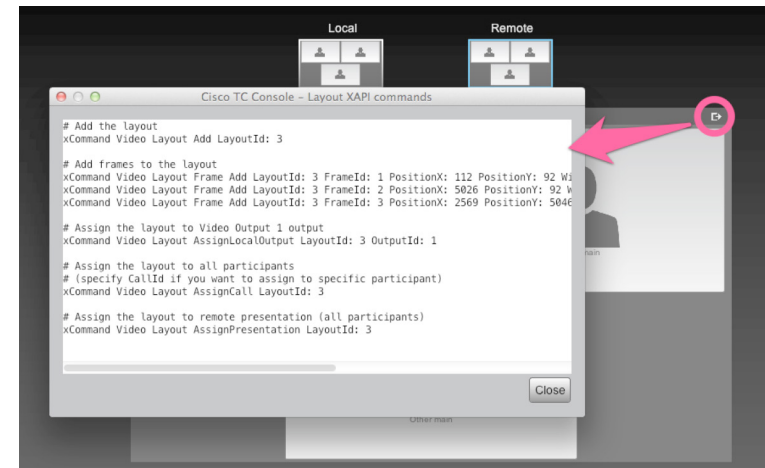
The Video Compositor allows you to modify the default video compositing behavior of the codec without the need for any programming. You can add new layouts, change the automatically selected layouts and control what will be shown to the user depending on the state of the codec.

New to TC6 is that the custom video layouts will be shown on the Touch interface.

TIP To see the affects of layout changes live on screen you can enable live layouts. To do this navigate to [Configure -> Live Layouts](#) and enable this option.

Settings are not saved onto the codec until the [Codec -> Synchronize settings menu](#) is selected. A file is then created on the system with the custom layouts and these API commands are executed upon startup of the video system.

To see the API commands for a specific video layout click on the button at the top right of the window.



Audio problems

No sound locally

In audio issues like video you need to determine which site is having the problem. If you are not hearing the far-end site it could be an issue locally with your speakers or audio output or the remote sites microphone.

- Check the cabling if you are using external speakers.

Audio

General Settings	
Microphones Mute	Off
SelectedOutputConnector	Headset
Volume	26

- Check if your systems output is set correctly to the desired output (headphone, speakers or handset). This can be checked under [Configuration -> System Status -> Audio](#).
- From the same screen you can check that **Volume** is set to a reasonable level. You can adjust the volume from the Touch panel, remote control or web interface.
- The far-end caller should check to ensure their microphone is not muted and check the physical connection of the microphone to ensure one is connected to their system. If your system or the far-end is muted you should see an onscreen graphic indicating this.
- You can test your system's audio output by changing the ringtone from the Touch panel at [Settings -> Ringtone & Sound Settings](#) or remote control at [Settings -> Sounds and alerts](#). You should hear the ringtone from your selected output device (headset, handset or speakers).

Settings	
System Information	Keytones
Call Status	Ringtone Volume (50)
Language	Ringtone
Camera Control & Settings	<div> <div>Polaris</div> <div>Drumset</div> <div>Jazz</div> <div>Bone</div> </div> <div> <div>IceCrystals</div> <div>Alert</div> <div>Fantasy</div> <div>Nordic</div> <div>Rhythmic</div> </div>
Display Settings	
Ringtone & Sound Settings	
Security	
Background	
Administrator Settings	
Restart	

- If you are using a system that uses a DNAM (Profile, T1, T3) ensure the audio cable is connected to the codecs audio output and that the DNAM is detected (see next section No sound (DNAM) – Profile, T1 and T3 Systems).

No sound (DNAM) – Profile, T1 and T3 Systems

The DNAM is a multichannel amplifier with digital signal processing built-in. It is a component specially designed for use with Cisco codecs.

- DNAM Short, used in Profile 65, T1 and T3
- DNAM II, used in Profile 42, Profile 52 and Profile 52 dual
- DNAM III, used in Profile 42 MKII, Profile 52 MKII and Profile 52 dual MKII

NOTE The T3 DNAM setup is special. If you experience any problems with it, please contact support.

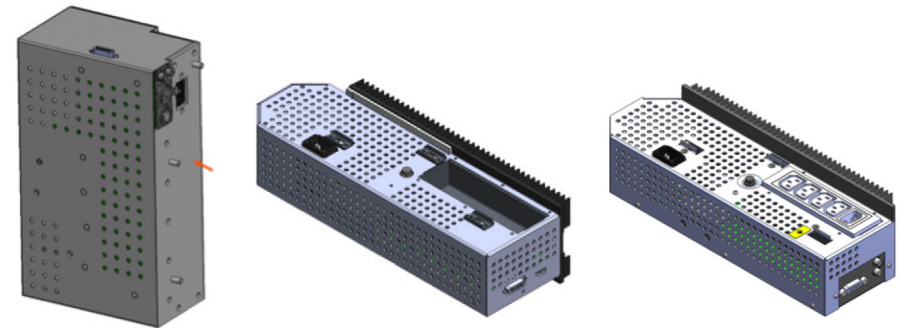


Figure 14 - Different DNAMs - Short, II and III

- Make sure all cables are properly and correctly connected. This includes the RCA cable from the codec audio output to the DNAM input, the cable(s) from the DNAM to the loudspeaker drivers or monitor assembly, and the power cable to the DNAM. On some systems some of these connections are not easily available, check those that are available. Verify that the DNAM is connected to **Line out 1** on the codec. Verify that the **Line out 1 Type** is set to **Auto**. You can find this in the audio part of the codec's advanced configuration settings.
- Power-cycle the complete system, including the codec, by pulling out and reinserting the mains plug from the wall socket. Wait for the system to boot completely and check the sound again. If cables and hardware are OK this will reset all software functions and re-establish codec-DNAM communication properly.
- If the problem persists, check the DNAM fuse. Make sure not to damage the fuse holder when removing the fuse for inspection. Push the fuse holder slightly inwards and turn counter-clockwise for release. On some systems this can be done with fingers only, on others a flat screwdriver is required. On some systems pulling the fuse holder out can be made easier by using a pair of pliers. If the fuse is blown it should be replaced with a **Littelfuse 215002**, which is a 2A 250V time-delay high-breaking capacity fuse. This should be readily available from electronics component warehouses. Some systems have an extra fuse kit in the column. Also inspect the fuse holder for damage. Take care also when reinserting the fuse and fuse holder. Push slightly inwards and turn the holder carefully clockwise until it locks in place. **NOTE** Using different fuses may easily lead to repeated failures or more serious hardware malfunction.
- Problem in codec, check settings and output signal, make sure there is sound.
- Try connecting external source to DNAM input.
- Check [Configuration -> System Status -> Audio -> Module 0](#) to see that the DNAM is detected – Type=DigitalNAM. If the DNAM is detected, there may be errors with speaker ID and cabling, contact support for assistance.

Echo issues (echo cancellation)

The cause of echo problems can be:

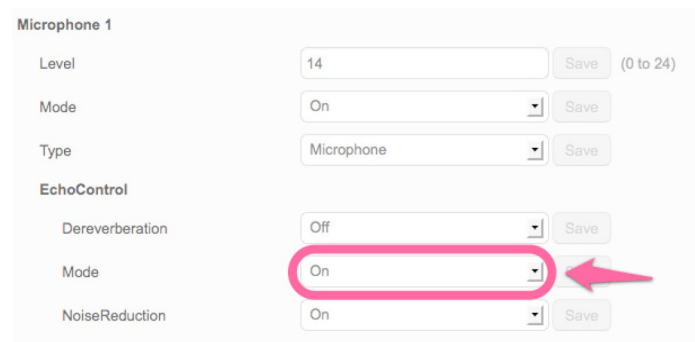
- Using internal speakers on a modern consumer TV. See below for explanation and techniques to fix this.
- Echo issues may occur immediately after restarting the system.
- Movement of the microphones or speakers during a call.
- Double-talk – both parties in the call speaking simultaneously.
- Very high noise levels
- Having the microphone too close to the speakers. Try moving the microphone further away.
- Having echo cancellation disabled.

You can see more information regarding room setup recommendations in the *Video Conferencing Room Primer guide*: http://www.cisco.com/en/US/docs/telepresence/endpoint/misc/user_guide/video_conferencing_room_primer_ver02.pdf.

NOTE The most likely cause for an echo heard locally is a problem with the far-end system.

General checks

Check that the input for each microphone you have connected to the system has echo control turned on. This is the default setting. If it is turned off the far-end will hear themselves. Echo control should only be turned off when using an external echo cancellation.



Microphone 1

Level: 14 [Save (0 to 24)]

Mode: On [Save]

Type: Microphone [Save]

EchoControl

Dereverberation: Off [Save]

Mode: On [Save] (highlighted with a red circle and a red arrow)


NoiseReduction: On [Save]

Using internal speakers on a modern TV

If you are using the internal speakers on a modern TV the various picture enhancing modes on the TV delay the audio whilst the image is being processed. This can result in the audio being outside the acceptable window for echo cancellation thus causing the far end to hear an echo.

There are various workarounds to try if you are experiencing this problem:

- Try and experiment on the TV with various picture modes looking for the one that processes the image the least. This can be called for example **Game mode** on some TVs.
- Rather than trying to use the internal speakers on the TV, use an external amplifier and speakers or powered speakers and see if this resolves the problem.
- You can experiment with the experimental setting **ECReferenceDelay** and try changing this from 0 to a higher value. The setting is located under [Configuration -> System Configuration -> Experimental -> Audio](#) and look under **ExReferenceDelay**.



Audio

EcReferenceDelay: 0 [Save (0 to 300)]

Figure 15 - EcReferenceDelay Value

Pop noise after unexpected restart

If the system restarts unexpectedly, and occasionally even during a controlled restart, you might hear a popping noise from the systems audio speakers. This is a normal operation and is not considered a fault.

Custom Audio TC Console (C40, C60, C90)

You can use the TC Console to configure advanced audio settings on the C40, C60 and C90 codecs. For more detail on TC Console please see the developer forum at <http://developer.cisco.com/web/telepresence-developer/tools/integrators/tc-console>. Documentation can be found within the application.

You should be aware that once these settings are synced to the codec a script is executed at startup and these settings are persistent.

You can also use this application to check the microphones. For more information on this see "Microphones" on page 18.

Peripheral issues

Touch

General information

The Touch Interface panel has two methods of connection, it can be plugged directly to supported systems or paired with a system over Ethernet. EX and MX systems are shipped as standard with the touch panel and with these systems the touch panel plugs directly into the codec. For other codecs (C series, SX) the Touch panel plugs into a power injector which in turn plugs into your network allowing pairing over the network or in some cases directly into the Ethernet 2 interface (C90, C60, C40).

Touch Panel

Name:	Cisco TelePresence Touch
Id:	██████████
Status:	Connected
Hardware Version:	101650
Software Version:	TT6.0.0 876266
Network Address:	169.254.1.30

When a Touch interface connects to a codec it will check to ensure it has the correct software for that release. If not the Touch will be upgraded to the current release and will restart.

You can find out if the video system is paired with a Touch panel from the web interface. Navigate to: [Configuration -> Peripherals](#).

Problems pairing Touch to system (Connecting...)

If you are having connection issues you should confirm that

- The Touch is physically connected to the codec directly or that it is plugged into the LAN or Ethernet 2 port of a C40, C60 or C90
- If you are using the LAN connection and power injector, check the LED on the power supply block to ensure it is green
- If you are using LAN, check the switch port to ensure there is a connection LED and check the network switch configuration
- If connecting directly to a C40, C60 or C90 check that the second Ethernet port is set to **DirectPairing** (see below)
- Try restarting the video system
- If the Touch is powered via the power brick, unplug it and replug to restart the Touch panel

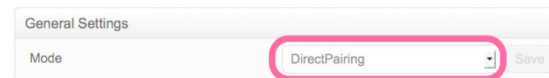
Factory reset

If you are having persistent problems, the last resort is to factory reset the Touch panel. For information on this, please see "Factory reset the Touch panel" on page 26.

Connect Touch to C40, C60, C90 Directly

To connect a Touch panel directly to the secondary Ethernet port on a C40 C60 or C90 codec, you must enable this port from [Configuration -> System Configuration -> NetworkPort2](#) and change the setting from **Inactive** to **DirectPairing**.

NetworkPort 2



General Settings

Mode: DirectPairing Save

NOTE Once **Direct pairing** is enabled you must restart the codec to start the pairing process.

WARNING Do not connect LAN to the secondary Ethernet port. When enabled, the secondary Ethernet port will run a DHCP server that can create conflicts with DHCP servers already present in the network.

Camera

No image seen when self-view enabled

To check the camera firstly enable self-view on the system to see if you can see your camera image.

If you cannot see anything in self-view then:

- Ensure that the privacy cover is not closed (EX series).
- If you are not using a built in camera check the physical cabling. Confirm that the camera is attached to the system and to which input it is connected (C Series, SX20).
- Check that the camera is operational. If you are not using a built in camera you can connect the camera into a standard screen with a HDMI input to check if there is an image from the camera (C Series, SX20).
- Confirm that the correct input source is selected for the main video source.
- Confirm the number of the input the camera is connected to.
- Check in [Configuration -> Video -> General Settings -> MainVideoSource](#) that the value here matches the number of the input the camera is connected to. You can check the default camera input from [Configuration -> Peripherals](#). Below you can see the output from a C90 showing that the camera is using input 1 so the **MainVideoSource** should be set to **1**.

Peripherals

Cameras

Camera 1 Cisco PrecisionHD 1080p 12X S01718-4.0FINAL [ID:40083] 2012-12-10

Video Inputs

Input 1 - HDMI	Main camera - 1920x1080, 30Hz
Input 2 - HDMI	Secondary camera - 1920x1080, 30Hz
Input 3 - DVI	PC
Input 4 - HDMI	DVD
Input 5 - DVI	Document camera

- In the above image you can see that the system is receiving a video signal as it displays a signal after the words **Main camera**. In this case the signal being received is 1920x1080, 30Hz. If there is no value here check the HDMI connection and ensure that the camera has power (SX20, C Series). If your system has a built in camera contact support for further diagnostics.

No camera control (Pan, tilt, zoom and software upgrade issues)

If the image from the camera is working but you cannot control the camera check that the video system can detect the camera. This can happen because the camera control is via a separate communication.

You can check the status of the attached camera from the web interface. If there is a problem you should see this reported on the home screen. You can also go to [Configuration -> Peripherals](#) to confirm the camera is detected by the codec. As you can see below the camera is not detected but the codec is receiving a video signal on the HDMI 1 interface.

Peripherals



This problem can also be confirmed in the [Diagnostics -> Troubleshooting](#) section of the web interface.

Troubleshooting

Diagnostics check of the most common system misconfigurations that may

Re-run diagnostics

ERROR: Camera Detection
No cameras found.

If you see that no camera is connected, there is an issue with either the camera control cable or the camera itself.

Far-end camera control

In order to control the camera of a far-end system in a call the system needs to have a moveable camera and have this option enabled. In TC6 you can set if you want to allow a far-end system to have the ability to control your camera. This setting is under [Configuration -> Conference 1 -> FarEndControl](#), both **Mode** and **SignalCapability** need to be enabled for a far-end system to be able to move the camera and to change input sources.

Multiple cameras (daisy chaining)

If you have multiple cameras note that only the first camera in the chain is upgraded. If the cameras are on different software versions there is a possibility of strange behavior, for example that only zoom works. To upgrade the other cameras in the chain connect these directly to the codec as the first camera in the chain and they will be upgraded. You can reposition the cameras after this. It is possible to upgrade the cameras if they are connected to Ethernet.

You will see a warning under [Diagnostics -> Troubleshooting](#) if there are multiple cameras attached that are not on the current camera software version.

You should see the message below if all of the cameras are on the correct software version.

OK: Camera Software Version
All cameras are running the same software version.

Camera Frequency 50Hz/60Hz

You can check the camera's frequency to ensure it matches the frequency of the lighting for the country you are in. You can find this under [Configuration -> System Configuration -> Cameras -> General Settings -> PowerLine Frequency](#).

Cameras



Camera not functioning - amber light

If you see your PrecisionHD 1080p4x Camera (CTS-PHD-1080P4XS1) in a similar state to this **outside a call** then you may have a problem where the software image on the camera has been corrupted.



Symptoms include:

- LED located on the top of the camera is on solid orange even though camera is not in a call. If orange LED is flashing and you have symptoms below, please contact support.
- Camera does not respond to controls nor does it send video.
- Video system does not detect the camera. Check [Diagnostics -> Troubleshooting](#) on the web interface to see if there are any problems detected.

The recovery method outlined below is available from TC5.1.5 onwards.

1. Start the procedure by typing the using SSH to access your system.
2. Login as **admin**.
3. Enter the command: `systemtools camerarescue`.
4. Your SSH session is terminated and a script runs to try and recover the camera. The script to upgrade the camera can take up to 15 minutes to complete, but normally this should take around 7 minutes.
5. The system reboots and the camera should be recovered. Should the recovery fail, there is a message in the logs saying "Failed to upgrade the camera, exiting..."

For more information, please see the field notice for PrecisionHD 1080p4x <http://www.cisco.com/en/US/ts/fn/635/fn63534.html>.

Contact support for further help should you experience this problem or if you are unable to recover the camera.

ISDN Link

ISDN Link is used in conjunction with a **single** endpoint to allow inbound and outbound ISDN calls. With TC6.0 and IL1.1 you can use the video systems web interface to pair the ISDN Link with a codec. You can also use the web interface to manage and upgrade the ISDN Link.

When you access the web interface of a TC6 system, you can easily see if it is paired and configured with an ISDN Link. On the **System information** screen, you can find a H320 section under the SIP/H323 sections. In addition, **Diagnostics** will indicate if an ISDN Link is detected.

If there are any configuration issues on the ISDN Link, you will see a red LED on the ISDN Link and a warning on the **System information** screen on the web interface of the paired TC6 system. In the example below there is an error on the PRI interface. Red alarm and L2 indicate a low level ISDN issue. In this case the cable was physically unplugged from the ISDN Link.

To manage the system, change the configuration, check the status or upgrade the ISDN Link you can do this from [Configuration -> Peripherals](#) and click [Manage ISDN Link](#).

Common Issues

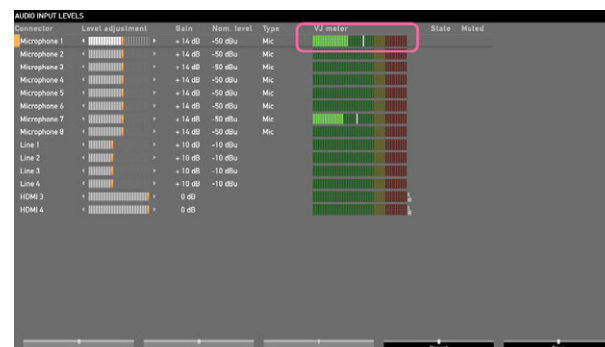
If you see the error message “Not SIP-registered to H320 peripheral” ensure that SIP is enabled. On the web interface select [Configuration -> System Configuration -> Network Services -> SIP Mode -> ON](#). Check that SIP outbound is not enabled either on the ISDN Link or the video system you are pairing the ISDN Link to.

Microphones

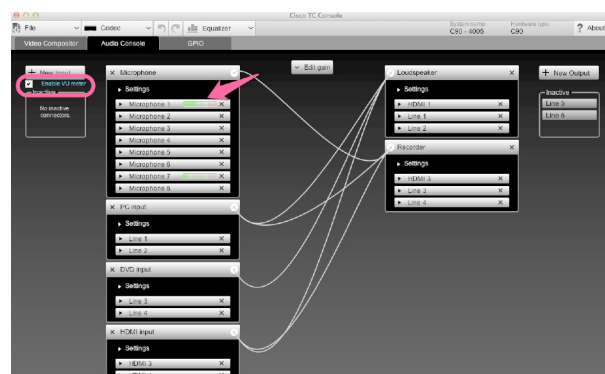
By default all microphone inputs are enabled and mixed on the C Series, MX Series and SX20. The EX Series has more selection of inputs and you can choose to use the handset, headset, Bluetooth or the built-in microphone on the system.

If the far-end cannot hear you, you should check the following:

- Microphone is not muted. MX, C20, SX20 can be muted and unmuted from a button on the microphone or Touch panel. You can see the microphone status on the [Call Control -> Call Control](#) section of the web interface.
- Microphone is physically connected to the system (C Series, SX, MX).
- Correct input is selected: phone, headset, built-in, Bluetooth (EX Series).
- Try another microphone and cable (C Series, SX, MX), or headset/headset/Bluetooth device (EX series).
- If you are using the remote control, you can check the audio input levels and see if the microphones are picking up sound. To do this go to [Settings -> Administrator Settings -> Audio input levels](#). Under the VU you will see a meter showing activity on the microphones.



- If you have a C40, C60 or C90 you can download the TC Console application. Under the audio section enable the VU meter to check the microphone inputs live.



Remote control

The systems that do not have a Touch panel are controlled with a remote control. The remote control's IR codes are picked up by the IR sensor in the camera. The codecs do have IR sensors, but these are set to **Off** if a camera is detected (control signal).

If you are having problems with the remote control, check the following.

- Replace the batteries.
- Check the short range/long range -switch inside the battery compartment. If the remote only works when held within a few centimeters or an inch of the camera, it is set to short range.
- Check that there is no Touch panel paired to the system. If a Touch is paired, the remote control will be disabled. You can check if there is a Touch paired by going to [Configuration -> Peripherals](#). If you see the information below, the system is paired with a Touch panel.
- Check that the camera is detected by the system.
- Check the [Configuration -> Cameras](#) and check that the **IRSensor** is set to **On**.
- Check [Configuration -> System Unit](#) and check that the **IRSensor** is set to **Auto**.

Touch Panel

Name:	Cisco TelePresence Touch
Id:	██████████
Status:	Connected
Hardware Version:	101650
Software Version:	TT6.0.0 876266
Network Address:	169.254.1.30

Figure 16 - Touch Panel Pairing Information

Confirming the key presses are received

You can confirm that key presses are being received by the codec in the system by using the command line interface. Login as **admin** using SSH and enter the command: `xfeedback register /event`

Result:

```
xfeedback register /event
** end
```

When a key is pressed you will now see an event generated in the SSH session output. The actual key presses are masked by "*" for privacy, but this output will confirm that input is received from the remote control.

```
OK
*e KeyDown Key: "*"
** end
*e KeyRelease Key: "*"
** end
*e KeyDown Key: "*"
** end
```

System

Backup and restore configuration

Backup configuration

To take a backup of the system configuration go to [Maintenance -> Backup and Restore](#) and press on [Take backup](#).

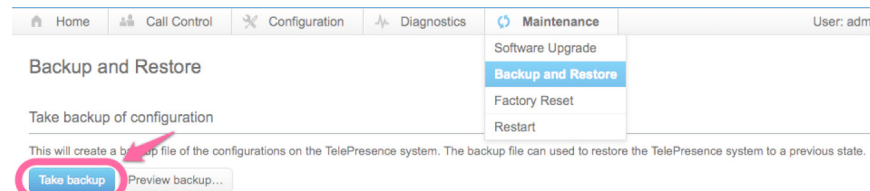


Figure 17 - Taking a Backup of System Configuration

You will now be asked where to save the configuration file. It is named **configuration.tsh** by default, but it can be renamed. This file is a text file.

You can press the [Preview backup...](#) button if you want to see the configuration that will be backed up when you press [Take backup](#).

Restore configuration

If you are having a problem with the system and choose to factory reset it, restoring a previously taken backup may re-introduce the problem. It may be worth reconfiguring the system by using the backup configuration.

To restore a backup go to [Maintenance -> Backup and Restore](#) and press [Browse...](#) and locate the backup file taken previously (default name - **configuration.tsh**). Select this file and press [Restore](#).



Figure 18 - Browse for Backup File

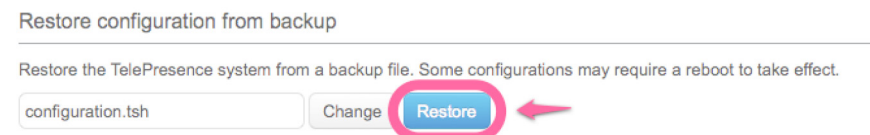


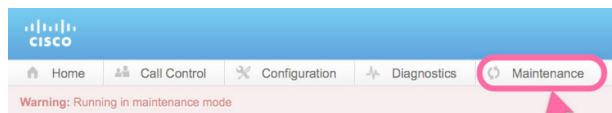
Figure 19 - Restore Configuration

NOTE Currently the web snapshot setting will not be restored for security reasons.

Maintenance mode

If a video system has a major problem starting it will enter maintenance mode. In this mode you should see a message on screen or Touch panel showing the IP address of the video system. You can access the system using a web browser to perform some maintenance tasks.

When you access a system in this state you will see a warning.



Maintenance Mode

The codec is currently not responding. Possible reasons for this includes:

- A reboot is in progress.
- One or more of the required services has crashed.

Now you can select Maintenance where you have the options to:

- Perform a software upgrade
- Factory reset the system
- Restart

NOTE If you attempt a factory reset please obtain the logs from the system **first**. A factory reset deletes all logging information. Should you involve support they will need the logs from the system. Go to [Diagnostics](#) -> [Log Files](#) and download all the current and historical logs (see "Basic log capturing" on page 28)

Swapping the software image

In maintenance mode you can also SSH into the system where you have some additional options, such as to swap software banks and get logs files. The codec has two locations for software. Using the command below you can change back to the previous version of software installed. This hopefully clears the problem and you can then upgrade back to the current release.

1. To see which memory bank is being used enter the command: `selectsw`
2. The result shows that the active software image is image2.:

```
image1
image2 [ACTIVE] [SELECTED]
```
3. To swap to the alternate bank (previous version prior to upgrade) enter the command:

```
selectsw image1
```
4. Result: Switching to image1
5. To complete the swap you have to reboot the system by entering the command: `reboot`

Your system may have **Image1** as [ACTIVE] [SELECTED]. In this case you would use **selectsw image2**.

You can also retrieve logs from the system by ensuring the SSH session is being captured to file and entering: `log`. You will then see all the logs being output onto the screen.

Upgrading and downgrading software

To upgrade the system manually use the web interface. From TC6.0 this is a two step process. First upload the image and then apply the upgrade to the system. Alternatively you can check **Upgrade automatically after upload** for the upgrade to be applied immediately

WARNING Release keys are needed for major upgrades. See "Release and option keys" on page 27 for more details.

Cannot downgrade

Please see the **Hardware compatibility** section below if you are having issues with your system not downgrading.

Upgrading issues

Ensure you are using the correct image for your system. We offer two versions of the software TC and TCNC. TCNC is a version with media encryption disabled. If you have a version of TC and mistakenly upgrade to TCNC software, you will get a message saying you need a new release key even though you have entered a valid TC6 release key. To solve this obtain the correct software file and go through the upgrade process again.

- For TC6.0 on C Series, EX and MX the normal software is file is s52000tc6_0_0.pkg. The non-crypto version that requires a different release key is s52001tcnc6_0_0.pkg.
- For the SX20 the normal file is s52010tc6_0_0.pkg and the non-crypto version is s52011tcnc6_0_0.pkg.
- For CUCM users software upgrades are usually applied automatically to the system.

If you have a Touch interface and cannot upgrade your system, check the following field alert:
<http://www.cisco.com/en/US/ts/fn/634/fn63448.html>

To read more about release and option keys, see "Release and option keys" on page 27.

Hardware compatibility

Due to replacement of hardware components there are some constraints on running older software on newly manufactured endpoints. This is due to end of life of some components and introduction of new components that require support in the software.


To see a hardware compatibility guide please review the [Release Notes for TC6.0](#) on the Cisco web site.

Security

Web Page (HTTP/HTTPS)

Access to the web management of the system is enabled on HTTP and HTTPS as default. HTTP access can be disabled from [Configuration -> System Configuration -> NetworkServices -> General Settings -> HTTP Mode](#) and set it to **Off**.

Default user account

 The video system is delivered with a default user account with full credentials. The user name is **admin**, and initially, no password is set for the default user.

We strongly recommend that you set a password for the admin user, and to any other user with similar credentials, to restrict access to system configurations.

Make sure to keep a copy of the password in a safe place. You have to factory reset the unit if you have forgotten the password.

Root user account

The root user account is disabled by default in TC6 and should not be enabled unless you are instructed to do so by support. For details on checking the status of root account, disabling and enabling it please see "Appendix B – Gaining root access to your system" on page 33.

Menus – restricting access to configuration changes

To restrict access to the available menus, you can set a menu password on the system. This affects the on-screen menus for remote control users and the Touch interface for those using a Touch Panel.

Currently this is only possible from the command line. SSH to the system. Log in as **admin** and enter the command:

```
xCommand SystemUnit MenuPassword Set Password: "ABC"
```

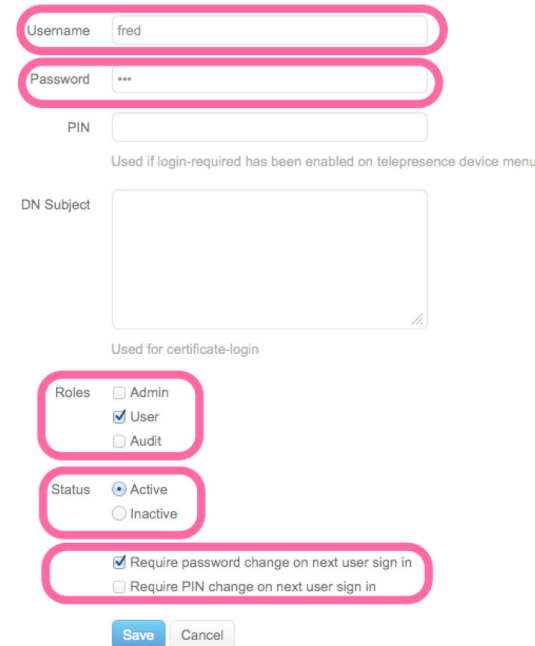
Where **ABC** is the password that must be entered in order to be able to access the configuration settings on the GUI interfaces.

Once enabled you will be asked for this password to access the configuration areas of the interface.

Web page restrictions

Web access can be restricted as well. To do this go to [Configuration -> User Administration -> Add New User](#). The new user will have access to the configuration page, but will not have the ability to save any changes to the configuration.

Add new user

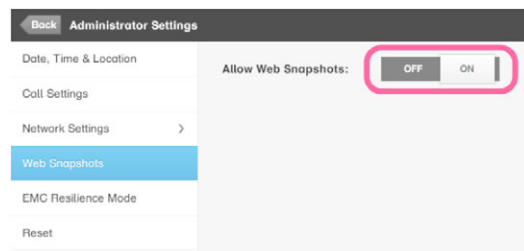


The screenshot shows the 'Add new user' form with the following fields and options highlighted in pink:

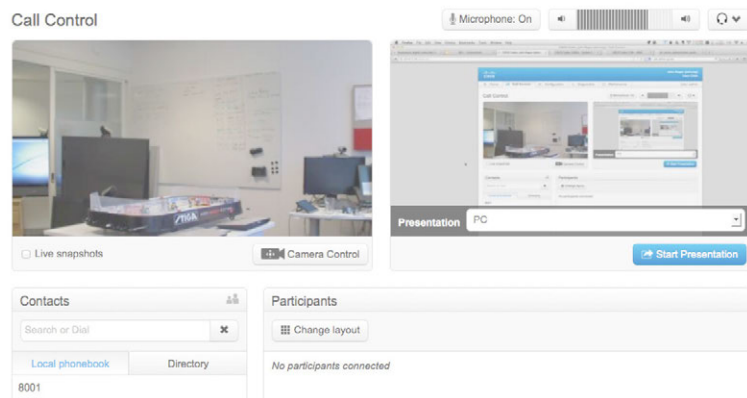
- Username:** fred
- Password:** ***
- PIN:** (empty field)
- Used if login-required has been enabled on telepresence device menu:** (checkbox, unchecked)
- DN Subject:** (empty text area)
- Used for certificate-login:** (checkbox, unchecked)
- Roles:**
 - ☐ Admin
 - ☒ User
 - ☐ Audit
- Status:**
 - ☒ Active
 - ☐ Inactive
- Password Change Options:**
 - ☒ Require password change on next user sign in
 - ☐ Require PIN change on next user sign in
- Buttons:** Save, Cancel

Web Snapshots

Web snapshots will allow the capture of images from the camera and connected computer even when not in a call and these can be seen in the web interface. For security reasons web snapshots can only be enabled with physical access to the system (Touch interface or remote control) and cannot be enabled remotely.



Once enabled, you can see snapshots captured every few seconds in the [Call Control -> Call Control](#) section of the web interface.



Auto Answer

If enabled auto answer will automatically answer any incoming calls even if you are not present. You can choose to have the microphone muted or unmuted when autoanswer is enabled.

Certificates

For more information regarding security and certificate installation under the section Managing the video system's certificates in the TC6.0 Administrator Guides for [C90](#), [C60/C40](#), [C20](#), [SX20](#), [MX Series](#) and [EX Series](#) on our web site.

CUCM CAPF

For more information about CUCM, CAPF and trust lists, read the [Administering TC Endpoints on CUCM guide](#) available on the Cisco web site.

How to factory reset your device

NOTE A factory reset will wipe all logging information from the system. PLEASE DOWNLOAD ALL CURRENT AND HISTORICAL LOGS FROM THE SYSTEM BEFORE PERFORMING A RESET.

Factory reset resets the TelePresence device to factory default settings, followed by an automatic reboot of the device.

- The call logs will be deleted.
- All system parameters will be reset to default values.
- All files that have been uploaded to the TelePresence device will be deleted. This includes, but is not limited to, custom backgrounds, ring tones, certificates, and the local phonebook.
- Release keys and option keys will **not** be affected.

WARNING A factory reset cannot be undone.

Suggested methods

In order to factory reset a system, choose the method available to you from the list below. The various methods are listed in order of ease of use.

1. If the system is attached to a Touch panel that is working, see "Factory reset using the Touch interface" on page 23.
2. If you can access the web interface of the system, see "Factory reset using the web interface" on page 23.
3. If you haven't the IP access to the system and can login as **admin** using SSH, see "Method 1 – If you can login as admin" on page 24.
4. If you can get access as **root** (has to have been previously enabled "Appendix B – Gaining root access to your system" on page 33), see "Method 2 – If can login as root" on page 24.
5. If the system has a standard serial connection, see "Factory reset using SSH, Telnet and serial connection" on page 24.
6. If you have no IP or serial access, see "—" on page 24.

Factory reset using the Touch interface

Using the Touch panel to factory reset your system is the recommended and easiest method to reset the system. Follow the steps below.

- Enter the Settings screen by tapping the Settings icon in the upper right corner of the screen.

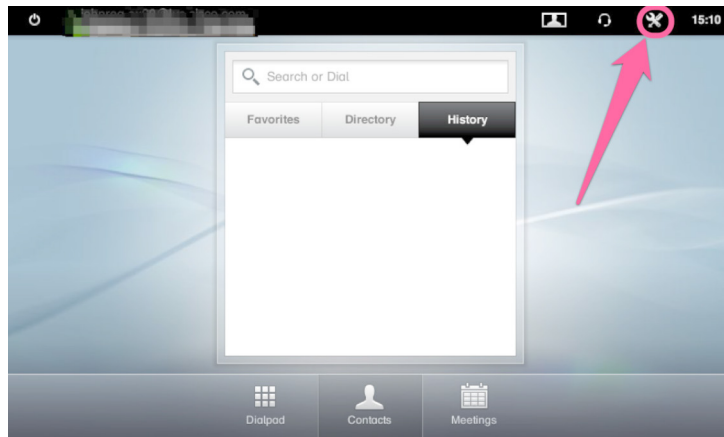


Figure 20 - Settings Icon Touch Screen

- Tap [Administrator Settings](#).
- Tap [Reset](#).
- Then [Factory Reset](#).
- A confirmation message appears.
- Tap [Do Factory Reset](#).

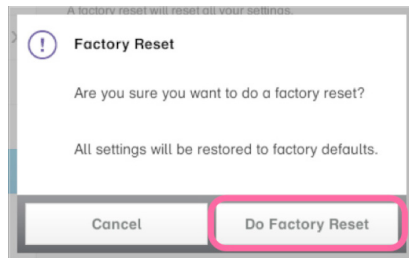


Figure 21 - Factory Reset Dialogue Box

Factory reset using the web interface

Access the web interface of the system using http://<ip_address_of_system>.

- Login as **admin**.

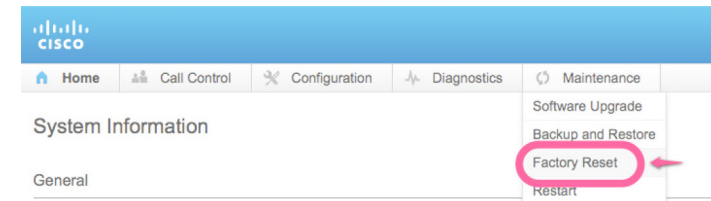


Figure 22 - Factory Reset via Web Interface

- Click on [Maintenance](#) -> [Factory Reset](#).
- A warning screen opens.
- Click [Perform a Factory Reset](#).

Factory Reset

This will reset the TelePresence device to factory default settings, followed by an automatic reboot of the TelePresence device.

- The call logs will be deleted.
- All system parameters will be reset to default values.
- All files that have been uploaded to the TelePresence device will be deleted. This includes, but are not limited to, custom backgrounds, ring tones, certificates, and the local phonebook.
- Release keys and option keys will not be affected.



Figure 23 - Factory Reset Warning

Factory reset using SSH, Telnet and serial connection

i Only the C40, C60 and C90 codecs have standard serial port interfaces. Please see "Appendix C – Serial connections" on page 33 for more information regarding serial connection setup. The EX, MX, SX and C20 systems require a special cable to access these systems via serial port.

Details on SSH and Telnet clients and their use is documented in "Appendix D – Useful software" on page 34.

Method 1 – If you can login as admin

- Login as **admin**.
- Enter the command: `xCommand SystemUnit FactoryReset Confirm: Yes`
- You will see the text:

```
*r FactoryResetResult:
** end
OK
```
- If connected by SSH or Telnet, the session will shut down.
- System restarts and a message on screen confirms the factory reset.

Method 2 – If can login as root

- Login as **root** using SSH, Telnet or connect via serial port.
- Enter the command `rm /mnt/base/active/config.db -`
- Restart the codec using the command `reboot`.

This will remove all the settings from the system, but is not a full factory reset and there may be some settings remaining e.g., local phonebook. It is recommended once the system is recovered to login as **admin** and use Method 1 above to do a proper factory reset if a complete reset of the system is required.

Factory reset – physical reset method for C20, EX60, EX90, MX200, MX300 and SX20

Before trying to perform factory reset with the physical method, you should first see if you can use one of the other methods. See "Suggested methods" on page 22 for alternative methods of factory reset.

C20

- Turn off the C20 by holding down the physical power button on the rear of the codec until you see the shutdown message on your screen. Release the button and wait for the system to shut down.



Figure 24 – C20 Power Button

- Once the system has completely shut down, press and hold the power button (approximately 8 to 10 seconds) until the green LED on the front panel of the codec starts blinking slowly.

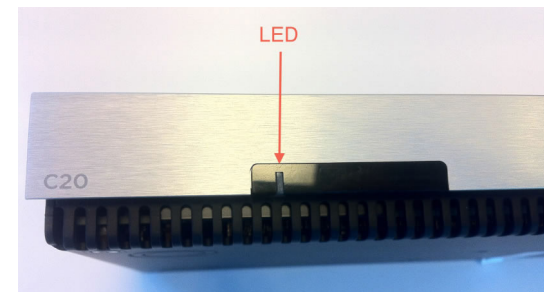


Figure 25 – C20 LED

- Release the power button and push it twice in quick succession within the next 5 seconds.
- You will now see the green LED flash more quickly.
- The codec should now factory reset and restart. This can take a few minutes.
- When the system starts up, you will briefly see a message on the screen confirming the system was successfully factory reset and all settings have been removed.

EX60 and EX90

Please see "Suggested methods" on page 22 for alternative methods of factory reset.

- Turn the off the EX60 or EX90 by holding down the physical power button on the front of the unit until you see the shutdown message on your screen. Release the button when you see the message. Wait for the system and Touch panel to turn off.
- Once the system has completely shut down, press and hold the power button (approximately 8 to 10 seconds) until the LED on front of system starts blinking slowly.
- Now release the power button and push it twice in succession within the next 5 seconds.
- The system should now factory reset and restart. This can take a few minutes.
- When the system starts up you will briefly see a message on the screen confirming the system was successfully factory reset and all settings have been removed.

MX 200 and MX300

Please see "Suggested methods" on page 22 for alternative methods of factory reset.

- Remove the back cover of the MX200 or MX300. The system can be running during this procedure.
- Press and hold for the recessed reset button (see picture below) for approximately 10-12 seconds until the screen and Touch panel go black and the system restarts.



Figure 26 - MX200/300 - Reset Button Location

- When the system starts up you will briefly see a message on the screen confirming the system was successfully factory reset and all settings have been removed.

The recessed button can be hard to locate. You should feel the physical button go down when you push it.

SX20

Please "Suggested methods" on page 22 for alternate factory reset methods.

- Turn off the codec by pressing the physical power button until the unit shuts down.



Figure 27 - SX20 Power Button

- Hold the power button down for approximately 10 seconds until it starts blinking slowly.
- Now press the button twice (two deliberate presses with a slight pause)
- The codec should now factory reset and restart.
- When the system starts up you will briefly see a message on the screen confirming the system was successfully factory reset and all settings have been removed.

C40, C60 and C90

- These systems cannot be reset by using physical button presses, but they have standard serial interfaces.
- Please see "Factory reset using SSH, Telnet and serial connection" on page 24 and "Appendix C - Serial connections" on page 33 for more information on configuration parameters for the serial interface.

Factory reset the Touch panel

1. The Touch panel can be factory reset by pressing the exclamation mark button in the bottom right corner. Press the button for 10 seconds until it lights up .
2. Once the exclamation button is lit, press the mute button in the upper right corner twice.
3. The Touch panel should reboot after a couple of seconds with factory settings.

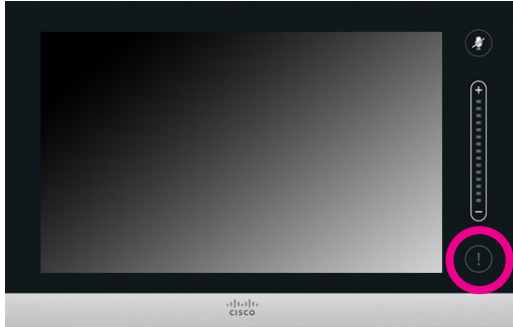


Figure 28 - Factory Reset Touch Panel

The exclamation button is not visible in normal operation. Please refer to the picture above to see its location.



On the TelePresence support forum you can watch a short video outlining the factory reset procedure ▶ <https://supportforums.cisco.com/videos/4166>.

Running temperature of systems



The C20 and SX20 may appear to be running very hot but this is normal and part of their design. Their casings are proving heat dissipation due to the small form factor of these units.

You may get a fan error reported in the web interface immediately following the start of a system. Please see [Diagnostics -> Troubleshooting](#) and click the [Re-Run diagnostics](#) button to see if the issue is still reported.

You can check the general temperature and fan status of your device on the web interface of the system. You can find this information on the [System Information](#) page under [General](#). If there is a problem with the temperature or the fans, you will see an alarm under [Diagnostics -> Troubleshooting](#).

System Information

General

System name:	C20	Installed options:	NaturalPresenter, HighDefinition, DualDisplay
Software version:	TC6.0.0	Temperature:	58.5°C / 137.3°F
Product:	Cisco Codec C20	Fans:	Fan 1 - locked on 5120 rpm Fan 2 - locked on 5120 rpm
Serial number:			
IPv4 address:			
MAC address:			
Valid release key:	Yes		

Figure 29 - Check Fan Speeds and Temperature

OK: System Temperature

The system is running at an acceptable temperature.

Figure 30 - From Diagnostics -> Troubleshooting

The system shuts down if the internal hardware temperature gets too hot (over 85°C/185°F). If you think this is happening:

- Wait for the system to cool down.
- Restart it.
- Collect the historical logs (see "Basic log capturing" on page 28).
- Create a support case (see "How to create a support ticket" on page 28)

Release and option keys

Release keys

A release key is needed to upgrade between major releases, for example when upgrading from TC5.1.5 to TC6.0.0. A new release key is not needed when upgrading between minor releases, for example from TC5.1.4 to TC5.1.5.

You can check if you have a valid release key for the current software from the web interface. You will be notified on screen or the Touch device if you have no valid release key (Figure 32). You can check which release keys have been installed to the system the web interface. You can find this information at [Maintenance -> Software Upgrade](#). Next to the release key field you can see all release keys currently installed on the system (Figure 31).

You can read more about the release keys in the [Activation Key Process Guide](#): http://www.cisco.com/en/US/services/ps10436/ps11105/activation_key_process_guide_services.pdf

To contact Cisco regarding keys, you can e-mail licensing@cisco.com.



Please install the new release key prior to upgrading.

Software Upgrade

Software package:

Current software version is TC6.0.0

☐ Upgrade automatically after upload

Release key: The system has valid release keys for TC4, TC6 and TC5

Option key:

Figure 31 - Check All Release Keys Entered on System

System Information

General	
System name:	C40-2
Software version:	TC6.0.0
Product:	Cisco Codec C40
Serial number:	
IPv4 address:	
Valid release key:	Yes

Installed options:	
NaturalPresenter,	PremiumResolution
Temperature:	72.5°C / 162.5°F
Fans:	Fan 1 - locked on 3946 rpm
	Fan 2 - locked on 3946 rpm
	Fan 3 - locked on 3946 rpm
	Fan 4 - locked on 3946 rpm

Figure 32 - Web Interface - Check for valid release key

Option keys

Product options are ordered through normal sales channels and processes. These options must be activated by installing option keys. Note that this process only applies for options purchased after initial product purchase. Options purchased with the initial product purchase are shipped pre-activated.

You can read more about the option keys in the [Activation Key Process Guide](#): http://www.cisco.com/en/US/services/ps10436/ps11105/activation_key_process_guide_services.pdf

The available option keys are:

- **Presentation** This allows systems to send a presentation and is now supplied by default on all new systems. On the EX series you will not see this option listed -it is available by default in these systems.
- **Dual display** Dual display option is needed for C20, C40 and EX90 to use a second screen. **NOTE** On C40 both HMDI and DVI outputs work in mirrored mode without a key. The EX90 will only display far-end presentation or local presentation/PC-input on the second screen.
- **Multisite** To allow your video system to call multiple video systems on C40, C60, C90, EX90 and SX20 without the use of infrastructure such as an MCU/Bridge. Without this option we support a single video call and one audio call.
- **HD** Allows 720p at 30fps encode/decode
- **Premium resolution** Allows encode/decode resolution of 1920x1080 and 60fps support and allowing some higher presentation resolutions.

System Information

General	
System name:	EX90
Software version:	TC6.0.0
Product:	Cisco EX90
Serial number:	
Installed options:	MultiSite, PremiumResolution, DualDisplay
Fans:	Fan 1 - locked on 1600 rpm
	Fan 2 - locked on 1600 rpm

Adding option keys

You can add option keys on the web interface of your system. Navigate to [Maintenance -> Software Upgrade](#). Here you can find a field to add in new options keys

Software Upgrade

Software package:

Current software version is TC6.0.0 Beta9

☐ Upgrade automatically after upload

Release key: The system has valid release keys for TC3, TC4, TC5 and TC6

Option key:

Add the key you have and press [Add](#). If the key was added successfully, you can see the message below. If the key is not accepted, check that you are entering it to the correct system as keys are tied to serial numbers. In addition, check the keys that are already installed. If the key is already there, it will not be accepted.

Release key: The system has valid release keys for TC3, TC4, TC5 and TC6

Option key: Option key added. Please restart for changes to take effect.

How to create a support ticket

Recommended steps:

- Read this document to do some basic troubleshooting and collect logs.
- Check known bugs. See "Search known bugs" on page 32.
- Create a support ticket (see below).

If you cannot resolve your issue after reading this guide, you can raise a support ticket with TAC (Technical Assistance Centre). Registered Cisco users can request help from the Cisco Technical Assistance Center by going to: <http://tools.cisco.com/ServiceRequestTool/create/>

Before opening a support ticket you should have the following information available:

- Complete description of the problem.
- Details on how to reproduce the problem.
- Versions of software involved in all devices involved.
- Serial numbers from equipment.
- Basic status and configuration information from endpoint and other equipment involved, the `xStatus` and `xConfiguration` logs. See "Basic log capturing" on page 28 on how to retrieve these.
- Logs or packet captures from the systems involved. See "SIP and H.323 call flow logging" on page 29.

A complete description of the problem and steps taken already to try and resolve early on in a case will help support resolve the problem more efficiently.

Getting required log files from the system

Basic log capturing

Capturing the systems configuration and status information

It is useful to enter and capture the output of these two commands when raising a support case:

- `xStatus`
- `xConfiguration`

The `xStatus` provides information on the current status of the system, e.g. is it registered or in a call etc, and the `xConfiguration` will show all the configuration values set on the systems.

This information is obtained via the command line. To get this information:

- Use an SSH client to login with the systems IP address (see "Appendix A - Other sources of information" on page 31).
- Enter username of `admin`.
- Enter the password configured on the system - by default the password is blank.
- You now have access to the command line interface. Type in:
 - `xStatus`
 - `xConfiguration`

NOTE This produces a lot of text output. Please ensure you capture ALL of this and forward it to support as a text (.txt) file.

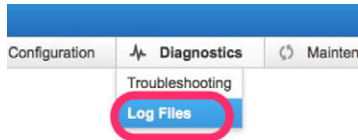
```
*s Video Input Source 2 Resolution RefreshRate: 0
*s Video Input Source 2 Resolution FormatType: Unknown
*s Video Input Source 2 Resolution FormatStatus: Unknown
*s Video Input Source 3 Resolution Height: 0
*s Video Input Source 3 Resolution Width: 0
*s Video Input Source 3 Resolution RefreshRate: 0
*s Video Input Source 3 Resolution FormatType: Unknown
*s Video Input Source 3 Resolution FormatStatus: Unknown
*s Video Input HDMI 1 Connected: True
*s Video Input HDMI 1 SignalState: OK
*s Video Input HDMI 2 Connected: False
*s Video Input HDMI 2 SignalState: Unknown
*s Video Input DVI 3 Connected: False
*s Video Input DVI 3 SignalState: Unknown
*s Video Input Legacy 3 Connected: False
*s Video Input Legacy 3 SignalState: Unknown
*s Video Output HDMI 1 Resolution Height: 720
*s Video Output HDMI 1 Resolution Width: 1280
*s Video Output HDMI 1 Resolution RefreshRate: 60
*s Video Output DVI 2 Resolution Height: 768
*s Video Output DVI 2 Resolution Width: 1024
*s Video Output DVI 2 Resolution RefreshRate: 60
** end

OK
xconfig
*c xConfiguration Audio Microphones Mute Enabled: True
*c xConfiguration Audio Volume: 45
*c xConfiguration Audio SoundsAndAlerts RingVolume: 50
*c xConfiguration Audio SoundsAndAlerts RingTone: Marbles
*c xConfiguration Audio SoundsAndAlerts KeyTones Mode: On
*c xConfiguration Audio Input Microphone 1 Type: Microphone
*c xConfiguration Audio Input Microphone 1 Mode: On
*c xConfiguration Audio Input Microphone 1 Level: 14
*c xConfiguration Audio Input Microphone 1 EchoControl Mode: On
*c xConfiguration Audio Input Microphone 1 EchoControl NoiseReduction: On
*c xConfiguration Audio Input Microphone 1 EchoControl Dereverberation: Off
*c xConfiguration Audio Input Microphone 1 Equalizer Mode: Off
*c xConfiguration Audio Input Microphone 1 Equalizer ID: 1
*c xConfiguration Audio Input Microphone 1 VideoAssociation MuteOnInactiveVideo: Off
*c xConfiguration Audio Input Microphone 1 VideoAssociation VideoInputSource: 1
*c xConfiguration Audio Input Microphone 2 Type: Microphone
*c xConfiguration Audio Input Microphone 2 Mode: On
```

Capturing system logs

To capture the system logs you can do this from the web interface, see “Accessing the system using the web interface” on page 5:

- Login as **admin**.



- First click [Diagnostics](#) on the upper navigation bar and then [Log Files](#).
- You will now see a list of **Current Log Files** and **Historical Log Files**. All Current logs can be downloaded as a single compressed file. Scroll to the end of the **Current logs** section for this button. The same is applicable to the **Historical Logs**. Scroll to the end to see the **Download all log files** button.



Log Files

Current logs

All current system log files are listed here and can be opened by clicking on them. Most useful are the all.log and main.log

File Name	Size	Last Modified
arm0-system.log	10 KB	2010-04-16 13:58
arm1-system.log	10 KB	2010-04-16 13:58
arm2-system.log	10 KB	2010-04-16 13:58
messages.log	10 KB	2010-04-16 06:33
rsync.log	1 KB	2010-04-16 14:22
wtmp	17 KB	2010-04-16 17:45

Click Here to download all current logs into one file

Download all log files as .tar.gz bundle

Historical logs

These are the logs for HISTORICAL activity on the system

File Name	Size	Last Modified
log.0.tar.gz	354 KB	2010-03-05 12:45
log.1.tar.gz	53 KB	2010-03-05 15:44
log.2.tar.gz	113 KB	2010-04-16 13:57
log.3.tar.gz	57 KB	2012-05-31 09:01
log.4.tar.gz	395 KB	2010-01-14 12:01
log.5.tar.gz	226 KB	2010-02-10 15:15
log.6.tar.gz	53 KB	2010-02-26 18:35
log.7.tar.gz	55 KB	2012-05-31 07:16
log.8.tar.gz	57 KB	2012-05-31 07:23
log.9.tar.gz	58 KB	2012-05-31 07:39
log.tar.gz	113 KB	2010-04-16 13:57
log.tar.gz	131 KB	2010-03-02 12:26

Click Here to download all historical logs into one file

Download all log files as .tar.gz bundle

SIP and H.323 call flow logging

You can capture log information on calls in two different methods on the video system. The first is to enable either SIP or H.323 logging commands to capture the signaling messages you are interested in. The advantage of this method is that, it works with encrypted calls and is easy to setup. The other method is to collect a packet capture from the system so that all call signaling, media and all other interactions with any external system (TMS/CUCM), HTTP etc. is captured. This method is takes a little more effort but will capture more information in non-encrypted call scenarios. This can be useful when diagnosing media issues.

Capturing SIP and H.323 signaling messages

- Restart your codec. This will ensure that the log files are empty when you start logging.
- Login using SSH to your system as **admin**.
- For SIP enter the command: `log ctx sippacket debug 9`.
- For H.323 enter the command: `log ctx h323packet debug 9`.
- All log message output will now be sent into the **application.log** file under current logs.
- Now place the call and re-create the problem.
- Hang up the call.
- Turn off the logging you enabled, by either `log ctx sippacket debug off` or `log ctx h323packet debug off`. **TIP** You can press up arrow to repeat last command and delete the 9 and add off.
- From the web interface navigate to [Diagnostics](#) -> [Log Files](#). Under **Current logs** select **eventlog/application.log** to see the logging messages.

Packet capture

You can capture the traffic from using port spanning on your switch (or use a hub), or directly from the video system. The latter is in many cases easier, although there are some limitations.

To capture directly from the system requires root access (see “Appendix B – Gaining root access to your system” on page 33) and will use tcpdump to capture all information entering and leaving the system. The advantage of this method is that, if you capture a complete call it can be opened in Wireshark and analyzed graphically. There are however a few limitations to watch for when using this method.

If you are using SIP, set the default transport to **TCP**. Otherwise the call signaling might be encrypted and you will not be able to see the call signaling. If you are having media issues, place calls without encryption so that the media can later be analyzed.

Logging can be captured for around a maximum of 10 minutes before the internal memory is filled and the logging stops, so if you are interested in capturing long calls use port spanning on your switch instead and Wireshark on a PC to capture.

In order to later analyze the call in Wireshark, it is recommended to capture the complete call. Start the capture before the call is made and stop it after the call has been disconnected.

Capture the call with the above limitations in mind:

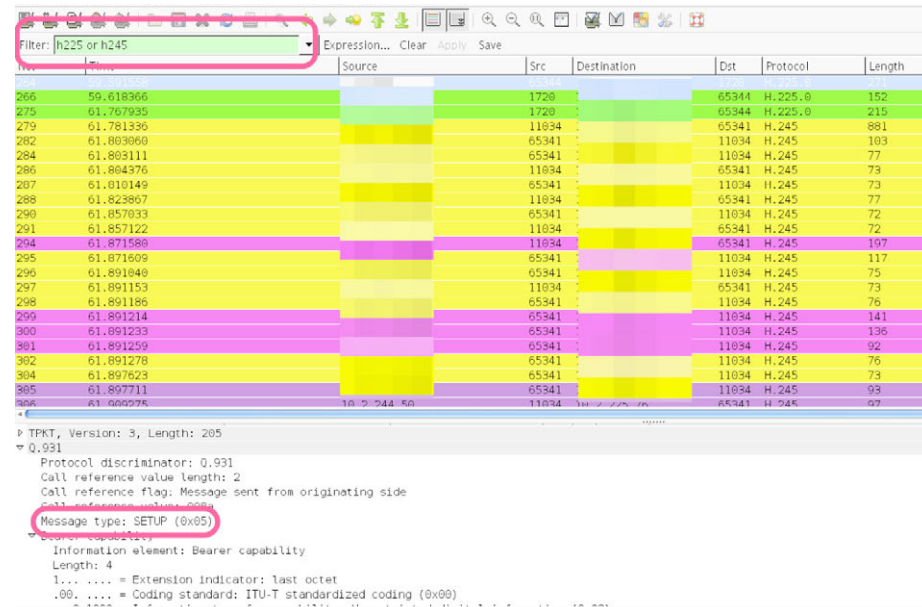
- Login as **root**
- Enter the command: `tcpdump -s0 -w /tmp/filename.pcap`
- Place a call or perform the action you want recorded (e.g. phonebook lookup). **NOTE** If you have a video issue please make an unencrypted call. This way support can decode the media.
- Replicate the issue.
- Hang up the call (if you are in a call).
- **Ctrl + C** to stop the capture.
- Use WinSCP on windows or scp on Linux/OS X to login as **root** and navigate to **/tmp** and download the **log.pcap** file (e.g. `scp root@<Ip-Address-System>:/tmp/*.pcap` will copy all **.pcap** files from system to the current directory).
- To analyze the resulting file you can use Wireshark – see next section.

Wireshark call analysis usage

First download and install Wireshark for your system ▶ <http://www.wireshark.org/download.html>. There are some requirements for OS X (x11 or Xquartz) that may require some additional downloads.

Once you have Wireshark installed and working and have captured a file (see Packet capture above), simply double clicking the file should open it in Wireshark.

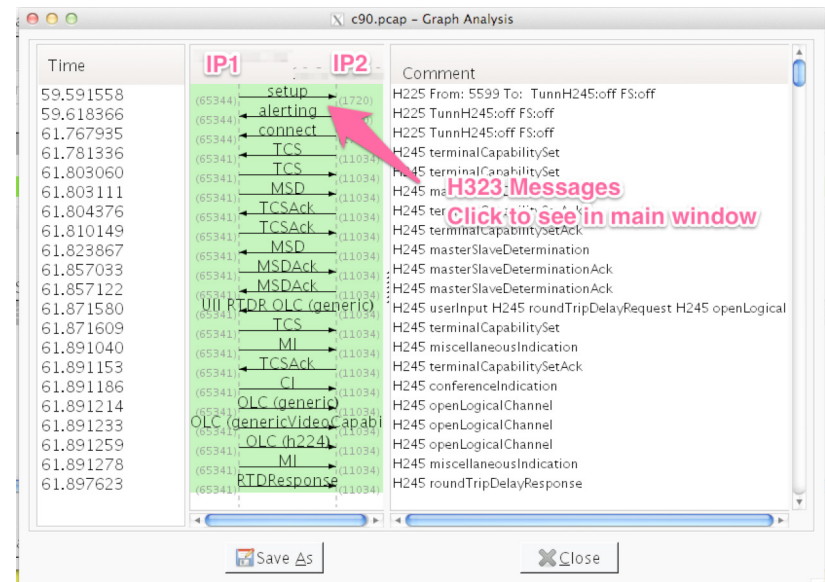
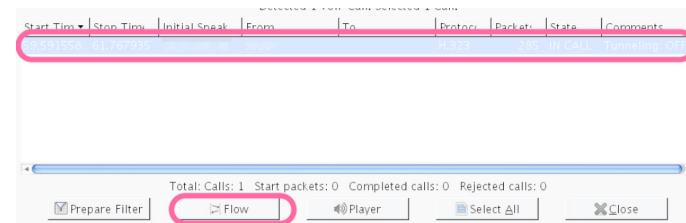
You will now see all the packets sent and received by the system. This is useful, but you may want to filter so that you can see the call setup.



H.323

There are various methods to create a filter to show only the appropriate packets from the capture. For H.323 calls you can enter a filter just to see the call signalling of **"h225 or h245"**.

- Now you can see all the gatekeeper messages, call setup messages and the opening of the media channels. You can investigate them further by opening the packets you are interested in to see their Q.931 and H.225 information.
- You can also see a graphic representation of the call by using **Telephony -> VOIP Call**. All detected calls will be shown. You need the complete call for this to work: Capture started before the call started and stopped after the call was terminated. Highlight the call you are interested in and click on **Flow**. Clicking on the various messages you will be taken to that packet in the capture.



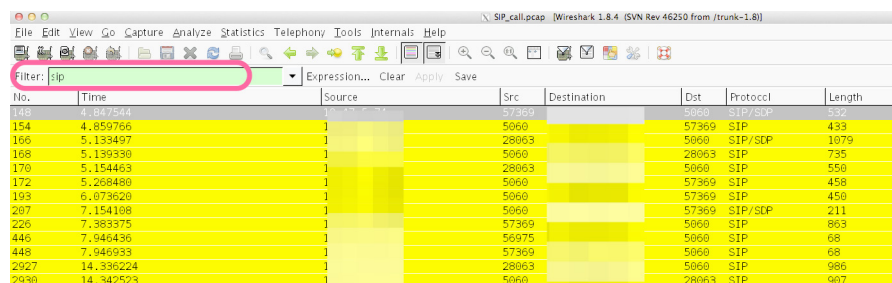
SIP

With SIP there are a few extra considerations as the call signalling can be encrypted. If you want to see this, the easiest way is to set the **SIP DefaultTransport** to **TCP**. Remember to set this back to previous setting when you have finished collecting the logs.

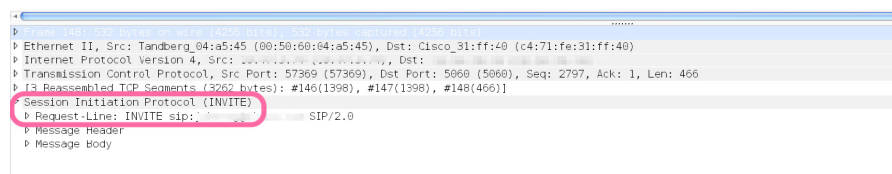
To see the call setup you can filter on **sip** to see the SIP call signalling. Again you can click on each packet and drill down into the detail.

You can also see a graphical representation of the call by using **Telephony -> VOIP Call**. All detected calls will be shown. You need the complete call for this to work: Capture started before the call started and stopped after the call was terminated. Highlight the call you are interested in and click on **Flow**. Clicking on the various messages you will be taken to that packet in the capture to investigate its contents further.

Filtering using "sip" will only show the call signalling. You can see the media packets as well if you remove the filter.



No.	Time	Source	Src	Destination	Dst	Protocol	Length
154	4.859756		5060		57369	SIP	433
166	5.133497		28063		5060	SIP/SDP	1079
168	5.139330		5060		28063	SIP	735
170	5.154463		28063		5060	SIP	550
172	5.268480		5060		57369	SIP	458
193	6.073620		5060		57369	SIP	450
207	7.154108		5060		57369	SIP/SDP	211
226	7.383375		57369		5060	SIP	863
446	7.946436		56975		5060	SIP	68
448	7.946933		57369		5060	SIP	68
2927	14.336224		28063		5060	SIP	986
2930	14.342523		5060		28063	SIP	907



```

Ethernet II, Src: Tandberg_04:a5:45 (00:50:60:04:a5:45), Dst: Cisco_31:ff:40 (c4:71:fe:31:ff:40)
Internet Protocol Version 4, Src: ..., Dst: ...
Transmission Control Protocol, Src Port: 57369 (57369), Dst Port: 5060 (5060), Seq: 2797, Ack: 1, Len: 466
[3 Reassembled TCP Segments (3262 bytes): #146(1398), #147(1398), #148(466)]
Session Initiation Protocol (INVITE)
Request-Line: INVITE sip: ... SIP/2.0
Message Header
Message Body
  
```

Appendix A - Other sources of information

Access latest software

You can download the software for your product from the Cisco web site, go to: <http://software.cisco.com/download/navigator.html?mdfid=283661039&i=rm>

FAQ

You can find further information on the TC endpoints in the FAQ guide on the Cisco web site, go to: [Cisco TelePresence Endpoints Knowledge Base Articles](#)

Customer TelePresence forum

On the Cisco TelePresence support forum you can discuss problems you are experiencing and see common issues and how to resolve them <https://supportforums.cisco.com/community/netpro/collaboration-voice-video/telepresence>

Documentation

The user documentation for the Cisco TelePresence systems running TC software includes several guides suitable for various systems and user groups.

- Video conference room primer
- Video conference room acoustics guidelines
- Installation guides for the TelePresence systems
- Software release notes for the TC software
- Getting started guide for the TelePresence systems
- User guides for the TelePresence systems
 - With a remote control
 - With a Touch panel
- Quick reference guides for the TelePresence systems
- Administrator guides for the TelePresence systems
- Camera user guide for the PrecisionHD cameras
- API reference guides for the Codec C Series
- TC Console user guide for the Codec C Series
- Physical interfaces guides for the Codec C Series
- Regulatory compliance and safety information guide
- Legal & licensing information for products using TC software

Documentation on www.cisco.com

EX Series (EX90, EX60): ▶ www.cisco.com/go/ex-docs

MX Series (MX200, MX300): ▶ www.cisco.com/go/mx-docs

SX20 Quick Set and Quick Set C20: ▶ www.cisco.com/go/quickset-docs

Codec C Series (C90, C60, C40): ▶ www.cisco.com/go/cseries-docs

Profile Series (Profile 42/52/55/65): ▶ www.cisco.com/go/profile-docs

Cisco TelePresence ISDN Link: ▶ www.cisco.com/go/isdnlink-docs

Search known bugs

To find out whether the problem you are experiencing with your video system is a known issue and has a known solution, please check the Cisco web site for known bugs. Go to: ▶ <https://www.cisco.com/cisco/psn/bssprt/bss>

To locate known bugs for your product and software version you can either search by product, by a keyword search or by selecting your product from the product category list. To locate your product from the list, do the following:

- Click [Search by product](#).
- Select [TelePresence](#) from **Product Category**.
- Select for example [Cisco Telepresence System Integrator C Series](#) from **Select Product**.
- You can enter a specific software version in the [Software Version](#) field, or if you are looking for a specific bug you can enter a keyword in the **Keyword** field.
- Click **Search**.
- You get a list of all bugs and can click on each to see more details.

TC Console

You can download the TC Console from ▶ <http://developer.cisco.com/web/telepresence-developer/home>

For the *TC Console user guide* go to: ▶ http://www.cisco.com/en/US/docs/telepresence/endpoint/codec-c-series/tc6/tc_console/codec-c-series_tc-console_tc60.pdf

System integrator

For the developer forum go to: ▶ <http://developer.cisco.com/web/telepresence-developer/forum>

Video conferencing Room Setup Guide

To get an optimized video conferencing experience, please check the *Video Conferencing Room Primer* for instructions on how to set up your room. Go to: ▶ http://www.cisco.com/en/US/docs/telepresence/endpoint/misc/user_guide/video_conferencing_room_primer_ver02.pdf

ClearPath Whitepaper

ClearPath is the technology in TC software that helps to conceal the visual effects of packet loss, for more details on this technology see the whitepaper. Go to: ▶ http://www.cisco.com/en/US/docs/telepresence/endpoint/software/clearpath/clearpath_whitepaper.pdf

Appendix B – Gaining root access to your system

Root access is disabled by default from TC4 onwards. However it can occasionally be useful to enable this for troubleshooting.



It is critical to always set a password when enabling root access.

To enable root access login as admin and use the command:

```
systemtools rootsettings on [password]
```

Replace **[password]** with the actual password you want to set for root access. When you enter this command, your telnet/SSH session will close. After this you are able to login as **root**.

To check if root is enabled you can login as **admin** and enter:

```
systemtools rootsettings get
```

The system returns:

```
systemtools rootsettings get
on
OK
```

To turn off root access (default state):

```
systemtools rootsettings off
```

Appendix C – Serial connections

The C40, C60 and C90 have standard serial port interfaces. Profile systems containing these codecs will also have standard serial connectors.

The EX, MX and SX series need non-standard cables to access their serial ports. These should be available to order in the near future, please contact your local Cisco representative for more details on orderability.

With a modern PC or laptop with no standard serial connector, you will need a USB to serial adaptor like the one illustrated here.



Model	Parameter	
<i>C Series, EX, MX, SX, Profile</i>	Baud Rate	38400
	Data Bits	8
	Parity	None
	Stop Bits	1
	Flow Control	None

The default baud rate is shown above. This can be changed on the system and it is worth checking other baud rates if you are having connection problems. The port can be disabled. You can check the serial port settings on the web interface by going to [Configuration -> System Configuration -> SerialPort](#).

SerialPort

General Settings		
BaudRate	38400	<input type="button" value="Save"/>
LoginRequired	On	<input type="button" value="Save"/>
Mode	On	<input type="button" value="Save"/>

Appendix D – Useful software

Most of this guide is concerned with the management of the system by the web interface. All configuration and troubleshooting can also be done via the command line as well as the checking of the system status. See the API reference guide for examples of commands that can be used: ▶ http://www.cisco.com/en/US/products/ps11422/prod_command_reference_list.html.

By default all systems have SSH enabled and you can connect to the systems command line using the appropriate SSH client for your computer. Telnet can be enabled if required, but it is not recommended, as it is less secure. Useful tools for various operating systems are listed below. SCP (Secure Copy) is used to retrieve files from the video system.

Windows

- **SSH access:** Windows does not come with a built in SSH client. One popular choice is PuTTY: ▶ <http://www.chiark.greenend.org.uk/~sgtatham/putty/>
- You can setup PuTTY to log all sessions to an output file by default which can be useful for gathering information to send to Cisco support. To do this you have to change the default settings. Open PuTTY and go to [Session -> Logging](#). Select all session output and specify a log file. You can specify something like: `c:\putty\&H-&Y&M&D-&T.log` which will create a unique file for every session. The parameters mean;
 - &H = hostname for the session
 - &Y = year
 - &M = month
 - &D = day
 - &T = time
- **SSH (alternative):** mRemoteNG which can be useful when managing multiple systems and can be downloaded here: ▶ <http://www.mremoteng.org/>
- **SCP:** WinSCP (▶ <http://winscp.net/eng/index.php>) can be used to download files from the system.
- **Wireshark:** ▶ <http://www.wireshark.org/download.html> is useful for decoding packet captures from the systems (see “Packet capture” on page 29)
- **Serial Access:** PuTTY can be enabled for serial connections as well.
- **Web Browsers:** To access the web interface any modern browser such as Firefox or Internet Explorer or Safari should work correctly.

OS X (Mac)

- **SSH/SCP:** OS X computers have command line SSH and SCP client installed by default. To access the command line you can use the command: `ssh admin@ip-address>`
- For transferring files from the system to your local computer, SCP from the command line is quite easy. If you have taken a packet capture directly from the system (see “Packet capture” on page 29) and want to copy that file from the system e.g. `capture.pcap` from `/tmp` on the video system, to the current directory on local computer (do not forget the space nd “.” at the end of the command line) `scp root@ip.address.of.system:/tmp/capture.pcap .`
- **SSH GUI:** ITerm 2 is a good SSH/Telnet client with bookmarking features and can be downloaded from ▶ <http://www.iterm2.com>
- **Wireshark:** ▶ <http://www.wireshark.org/download.html> is useful for decoding packet captures from systems (see “Packet capture” on page 29) If you are using Mountain Linon, you. will need to install Xquartz.
- **RS-232:** Zterm
- **Web Browsers:** The latest releases of Internet Explorer, Mozilla Firefox, Opera, Chrome or Safari are recommended

Linux

- **SSH/SCP:** As with OS X above you can use the built in SSH and SCP command lines tools to access the command line and download files.
- **SSH GUI:** A GUI utility for managing multiple hosts is called PAC (Pac manager) ▶ <http://sourceforge.net/projects/pacmanager/>
- **Wireshark:** ▶ <http://www.wireshark.org/download.html> is useful for decoding packet captures from systems (see “Packet capture” on page 29)
- **RS-232:** For serial access there are many utilities – some well known applications are minicom or GTKTerm
- **Web Browsers:** The latest releases of Internet Explorer, Mozilla Firefox, Opera, Chrome or Safari are recommended

Packet capturing via Cisco Switch

You can packet capture directly from the video system, but there are limitations to this, such as the amount of time you can capture for due to the limited internal space available for storage.

To get around this issue you can, if using a Cisco switch, enable port spanning which duplicates all traffic entering and leaving one port to another monitor port where you can attach a computer running Wireshark to capture traffic.

For some examples on how to achieve this on various switches, please see here: ▶ http://www.cisco.com/en/US/products/hw/switches/ps708/products_tech_note09186a008015c612.shtml or refer to the documentation for your switch model.

Appendix E – Web diagnostics and on screen error messages and warnings

Messages that may be displayed on screen or in the diagnostics section of the web page are listed below.

The **OK** state shows the message displayed when there is no diagnostic issue. The **Problem** message shows the message that is displayed upon an error or warning state. **Resolve** gives you suggestions to on how to fix the error.

Camera Detection	
OK	The system has X connected cameras.
Problem	No cameras found.
Resolve	This means that the camera control is not detected, but you may still be getting video from the camera. See “Camera” on page 16 for more information.

Camera Software Version	
OK	All cameras are running the same software version.
Problem	The system has several cameras with different software versions installed. Please upgrade your cameras.
Resolve	If you have multiple cameras connected to the system and daisy chained control, only the first camera in the chain will be upgraded when the system is upgraded. Connect the other cameras to the codec as first in the chain to obtain a software upgrade.

Camera Control Setup	
OK	Camera control for all inputs are configured correctly.
Problem	Input number X is configured with camera control using camera Y but there is no such camera. Please configure the input to use an existing camera, or turn off the camera control for that input.
Resolve	Disable camera control for that input.

ISDN Link status	
OK	The ISDN Link is connected.
Problem	The link status is ERR_MESSAGE.
Resolve	To troubleshoot this it depends what the error message is. Red Alarms generally indicate low level Physical ISDN Line Issues.

System Name	
OK	The device has a system name set.
Problem	The system has not been configured with a name. Please configure a system name
Resolve	Set a system name on the system to resolve this issue. From the web interface got to Configuration -> System Configuration -> General Settings -> Name .

SIP Status	
OK	SIP is configured correctly and is registered to the proxy.
Problem	The system is not registered to a SIP proxy. Please configure a SIP proxy.
Resolve	SIP protocol is turned on but there is no configuration. Check and complete the SIP configuration. If SIP not required, turn off SIP.

H.323 Status	
OK	H.323 is configured correctly and is registered to the gatekeeper.
Problem	The system is not registered to an H.323 gatekeeper. Please configure an H.323 gatekeeper.
Resolve	Check the H.323 configuration. If H.323 not required, turn off H.323.

SIP Registration	
OK	
Problem	Registration failed: Reason Please verify the SIP configuration.
Resolve	Check the reason for failure. Verify your SIP configuration and that the system is able to contact the SIP Registrar.

H323 Registration	
OK	No message displayed. This can be checked under System information on the web interface.
Problem	Registration failed: Reason. Please verify the H.323 configuration.
Resolve	Check the reason for failure. Verify your H.323 configuration and that the system is able to contact an H.323 Registrar.

Default Call Protocol	
OK	The default call protocol is set to a valid network service.
Problem	The default call protocol is set to [H323/SIP], but that protocol is not active.
Resolve	H.323 or SIP are set as the default protocol but that protocol is disabled meaning that all calls will fail. Either enable the protocol or change the default call protocol.

Fan Status	
OK	All fans are running.
Problem	There might be an issue with the fans. Please contact Cisco support for assistance.
Resolve	If you see this just after a reboot, please press Re-run Diagnostics to run the test again. If you constantly see this message, contact support.

CUCM CAPF	
OK	There are no outstanding CUCM provisioning operations.
Problem	There is a pending operation: OPERATION Please take action.
Resolve	There is a problem with the CAPF setup. Please refer to the CAPF setup here: ▶ http://www.cisco.com/en/US/docs/telepresence/endpoint/codec-c-series/tc6/administration_guide/administering_endpoints_running_tc6_on_ucm90.pdf

CUCM CAPF	
OK	No message.
Problem	WARNING - There was a notice with the last request.
Resolve	Follow link and check settings: ▶ http://www.cisco.com/en/US/docs/telepresence/endpoint/codec-c-series/tc6/administration_guide/administering_endpoints_running_tc6_on_ucm90.pdf

Valid Release Key	
OK	The system has a valid release key for the current software.
Problem	The system requires a valid release key. Please add a release key.
Resolve	The current release key is not valid for the software loaded. Check that the correct software is loaded – usually TC not TCNC (non-crypto version that requires new key) and that you have entered the key correctly.

Administrator Password	
OK	A password has been set on the administrator account.
Problem	The system requires an administrator password. Please configure the admin user.
Resolve	A password for admin user has not been set and system is using the default (no password). Set a password – login on web interface as admin , click User: admin and select Change Password .

Self-diagnostics	
OK	
Problem	Error while trying to run self-diagnostics.
Resolve	You may see this message shortly after starting a system. Try to Re-run the diagnostics to see if this is cleared.

System Temperature	
OK	The system is running at an acceptable temperature.
Problem	The system temperature is X°C, nearing the warning threshold of 85°C
Resolve	Ensure that the system has adequate ventilation and cooling. If the system temperature exceeds 85°C, it will shut down to prevent damage. If the environmental conditions are ok and you are still getting this message, please open a support ticket.

Echo Cancellation Configuration	
OK	No message.
Problem	The Echo Cancellation delay has been altered to X. Consider resetting it back to 0.
Resolve	This setting rarely needs changing. Echo cancellation should only be disabled if you are using an external echo cancellation device.

Multistream Configuration	
OK	No message.
Problem	Multistream has been enabled. Consider disabling it.
Resolve	This setting is experimental and should not be enabled for normal use. Currently it will cause you problems with SIP calls. Disable it.

Do not disturb mode	
OK	Do not disturb is turned off
Problem	Do not disturb is turned on. Until this is turned off, the system cannot accept calls.
Resolve	A warning that you have this enabled and therefore incoming calls will not be seen. Turn off to enable incoming calls.

Standby Control	
OK	The system goes into standby automatically after X minutes.
Problem	The automatic standby control is turned off. This will increase power usage and may cause burn-ins on plasma screens if left on for longer periods. Consider enabling standby.
Resolve	Enable standby. The video signal will stop being sent to the monitor as the video system goes into standby. CEC can also be enabled if your monitor supports it. As a result, the monitor is shutdown when the video system enters standby.

No issues found	
OK	The system appears to be in working order.
Problem	None
Resolve	None

Cisco contacts

On our web site you will find an overview of the worldwide Cisco contacts.

Go to: [▶http://www.cisco.com/web/siteassets/contacts](http://www.cisco.com/web/siteassets/contacts)

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Dr.
San Jose, CA 95134 USA

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

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

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

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

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

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

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

© 2012 Cisco Systems, Inc. All rights reserved.