Cisco TelePresence Server 4.1(1.85)

Software Release Notes
March 2015

Contents

Product documentation

The following sites contain documents covering installation, initial configuration, and operation of the product:

- Release notes: http://www.cisco.com/en/US/products/ps11339/prod_release_notes_list.html
- Install guides: http://www.cisco.com/en/US/products/ps11339/prod_installation_guides_list.html
- Configuration guides: http://www.cisco.com/en/US/products/ps11339/products_installation_and_configuration_guides_list.html
- API reference guides: http://www.cisco.com/en/US/products/ps11339/products_programming_reference_guides_list.html
- Maintain and operate guides: http://www.cisco.com/en/US/products/ps11339/prod_maintenance_guides_list.html
- Licensing information: http://www.cisco.com/en/US/products/ps11339/products_licensing_information_listing.html

New features in Version 4.1(1.79)

Version 4.1(1.79) introduces some new features to extend and improve the conference experience.

The user interface and API have been updated as required to support these new features.

Table 1: New feature support by TelePresence Server platform

Feature name	7010 & MSE 8710 Locally Managed	7010 & MSE 8710 Remotely Managed	Media 310/320 Remotely Managed	Virtual Machine Remotely Managed
User experience improvements				
Layout changes [p.3]	Yes	Yes	Yes	Yes
Message background [p.3]	Yes	Yes	Yes	Yes
Participant overflow icon [p.3]	Yes	Yes	Yes	Yes
Audio avatar [p.4]	Yes	Yes	Yes	Yes
ActiveControl enabled by default [p.4]	No	Yes	Yes	Yes
Name label changes [p.4]	Yes	Yes	Yes	Yes
Improved content [p.5]	Yes	Yes	Yes	Yes
Enhanced layout experience [p.5]	No	No	Yes	Yes
Resilience and diagnostics improvements				
Remote logging of protocols log [p.8]	Yes	Yes	Yes	Yes
TIP messages logged in event log [p.8]	Yes	Yes	Yes	Yes
Event log message on packet loss [p.8]	Yes	Yes	Yes	Yes
Network packet capture controls on web interface [p.9]	Yes	Yes	Yes	Yes
'Bad video' event log message [p.9]	Yes	Yes	Yes	Yes
Improvements to participant media summary CDR entry [p.9]	Yes	Yes	Yes	Yes
Scalability improvements				
Capacity improvements [p.9]	No	No	Yes	Yes
General improvements				
One conference URI with separate guest/chair PINs [p.10]	No	Yes	Yes	Yes
Cisco Sans font [p.10]	Yes	Yes	Yes	Yes

User experience improvements

Layout changes

The existing layouts on TelePresence Server have been adjusted slightly so the PiP strip remains at an appropriate size and the maximum number of PiPs is now six on Active Presence layout.

Prominent layout now has the same size and behavior as the PiP strip in the Active Presence layout and a small amount of space between the main pane and the PiP strip.

This change ensures peoples' facial expressions are visible in the PiPs and provides consistency across the layouts.

The TelePresence Server's four layouts are:

- Single for when you want to focus on the active speaker.
- Active Presence and Prominent for when you want to focus on the active speaker but also want to see other participants.
- Equal for when you want to see as many participants as possible and do not want to focus on the active speaker.

Message background

Text messages can be rendered by the TelePresence Server in the main video pane sent to an endpoint.

In this release, the following improvements have been made to the message background of text messages rendered by the TelePresence Server in the main video pane sent to an endpoint:

- The default location is changed to closer to the top of the screen.
- A semi-transparent dark grey background, rectangular in shape with rounded corners, has been added.
- The text font size is 26pt for 1080p video, and is scaled appropriately at other resolutions.
- The color of the text remains white, but the slight shadow from version 4.0 is removed.
- The width of the message should be approximately one quarter of the screen for short messages. This switches to three quarters if the smaller size would mean displaying more than three lines.

In version 4.0 release, the message had white text and no background, and occurred in the centre of the pane making it hard to read if the main video at that location was also a pale colour. It could also obscure participants’ faces.

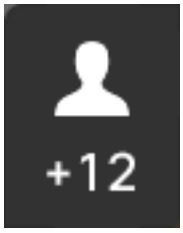
Participant overflow icon

This release introduces a participant overflow icon (on by default) to indicate when more participants are present in a conference than can be displayed on a given endpoint's layout. This icon will appear showing the number of participants not being displayed. This number includes both video and audio-only participants. Grouped endpoints are counted as a single endpoint.

Limitation

Cascaded conferences where the number of remote participants are unknown will count as a single participant.

Figure 1: Participant overflow icon example



In Remotely managed mode the participant overflow icon can be turned off via the API using the **`indicateAudioOnlyParticipants`** command . In Locally managed mode the icon can be turned off on the user interface via **System settings > Indicate presence of additional participants**.

In previous releases there was an “audio-only” icon—a telephone with a number indicating the number of audio-only participants—appearing in the top left-hand corner of the screen. This icon is now replaced by a combination of the audio avatar and the participant overflow icon.

Audio avatar

This release introduces an audio avatar which is used when there is no video for the participant. So instead of having no visual presence, audio-only participants, or a participant that has muted their video, are represented by a static picture: an “audio avatar”. Avatars will behave identically to video from video endpoints. Their inclusion in a layout is determined by the pre-existing voice switching behavior.

Figure 2: Audio avatar

Each audio participant in a conference has its own avatar. All audio avatars are identical, however, each one has a name or number associated with it. If name labels are turned off then the avatar no longer has a unique identifier. We therefore recommend that users leave the name labels on (default setting) for the best user experience.

In previous releases there was an “audio-only” icon—a telephone with a number indicating the number of audio-only participants—appearing in the top left-hand corner of the screen. This icon is now replaced by a combination of the audio avatar and the participant overflow icon.

Name label changes

The audio avatar feature introduced in this release uses the same image for all audio-only participants. They will not be distinguishable from each other without a name label. For this reason, name labels are enabled by default in this release.

Additionally, the name labels are now white text on a dark background, to be in line with the on-screen messages. Previously they were dark text on a white background.

ActiveControl enabled by default

In this release the iX protocol, necessary for ActiveControl, is now enabled by default (does not apply to locally managed mode). In previous releases it was disabled by default.

ActiveControl provides conference control functions and conference information for endpoints running software version TC6.2 or later (provided they have Touch controllers). From the touchpad users can see a

list of participants and other information during a conference. On certain endpoints they can change the conference layout displayed locally, and disconnect other participants. Having ActiveControl enabled by default fully optimizes the user experience.

To deploy ActiveControl you need the following prerequisites:

- TelePresence Server 3.1 or later in remotely managed operation mode. TelePresence Server must be behind a Conductor (XC2.2 or later), not directly registered to VCS or Cisco Unified CM.
- Cisco Unified CM version 9.1.2 or later.
- VCS Control/Expressway version X7.2 or later.
- TC6.2 or later on EX60, EX90, Quick Set C20, SX20, C Series C40, C60, and C90, MX200, MX300 or Profile Series.
- TelePresence Touch 8 (remote control does not support ActiveControl).
- In TC6.2, UDP port 5170 is used for ActiveControl. If a firewall or access list is denying traffic on this port, it must be opened up to accommodate the iX protocol.

For more information on using ActiveControl in optimized conferencing with Unified CM, see:

http://www.cisco.com/c/en/us/support/conferencing/telepresence-conductor/products-installation-and-configuration-guides-list.html

Improved content

This release implements improvements to the user experience around content video:

- H.264 will always be the preferred codec for content video.
- Sharpness is prioritized over motion:
  - The highest spatial resolution possible is used between source and destination—this eliminates unnecessary scale adjustments, and preserves aspect ratios and resolution.
  - Video encoders are made aware when they are encoding video for content instead of main video; this results in encoding techniques that render frames at good quality, and reduces the encoded frame rate where necessary.

These improvements mean that, for example, it is possible to get 1080p/WUXGA resolution for content at a low frame rate when the conference has been configured to 720p5 for content.

Enhanced layout experience

This release introduces a new default behavior on the TelePresence Server—support for multistream video.

Note: This is an experimental feature and is disabled by default in endpoint software TC 7.3.

This means that a multistream-capable endpoint can compose the video streams locally into a conference layout resulting in an enhanced user experience. However, all endpoints continue to be supported with the best experience available to them.

To achieve this, the TelePresence Server advertises the ability to send multiple streams, and allows a multistream-capable endpoint to subscribe to the streams that it requires.

The TelePresence Server can receive up to four main video streams from a multistream-capable endpoint—of the same video source at different resolutions and frame rates, for example, the endpoint could send both 1080p30 and 720p60, or 720p30 and 480p30.

The TelePresence Server can transmit up to sixteen video streams to an endpoint, also at different resolutions and frame rates. A multistream-capable endpoint will then compose the video streams locally into a conference layout.

Some key points to note about this feature:

- Only supported in remotely managed mode on Cisco TelePresence Server on Virtual Machine and Cisco Multiparty Media 310/320.
- The TelePresence Server supports conferences featuring both multistream and single stream endpoints.
- Provides encryption for switched media streams.
- Provides resilience for multistream calls using Forward Error Correction and rate control.
- Multistream is supported via SIP only (not H.323 or TIP).
- It is enabled by default. However, it can be disabled using the API **`multistreamMode`** parameter.
- The TelePresence Server provides support using an H.264 SVC channel to receive and transmit video streams to and from a multistream-capable endpoint.
- Multistream is not supported over cascade links.
- Multistream is supported for all token levels. However, the main video bit rate must be 500kbps minimum.

Supported multistream-capable endpoints

The supported multistream-capable endpoints are (note that Multistream support is experimental and is disabled by default in TC 7.3):

- Cisco TelePresence MX200 G2
- Cisco TelePresence MX300 G2
- Cisco TelePresence MX700
- Cisco TelePresence MX800
- Cisco TelePresence SX20
- Cisco TelePresence SX80

Infrastructure products—minimum requirements

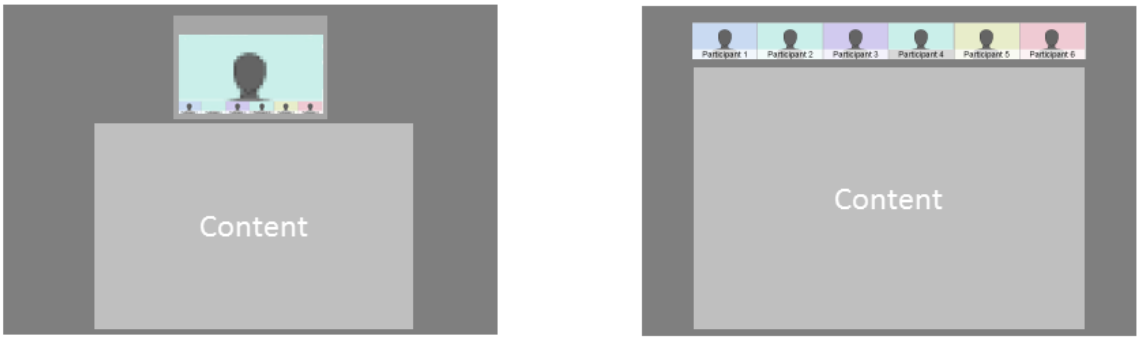
To support enhanced layout experience the following infrastructure products need to be running these minimum software versions:

- Cisco TelePresence Conductor XC3.0
- Cisco Unified Communications Manager 10.5(2)

Conference examples

The figure below shows a single-screen endpoint (Prominent layout). On the left, the endpoint is in a transcoded call. The example on the right belongs to the same endpoint in a multistream call and demonstrates how enhanced layout experience maximizes the use of the screen display when composing the video and content layout.

Figure 3: Single-screen endpoint conference example



The figure below shows a two-screen endpoint system. On the left, the two-screen endpoint is in a transcoded call. The two screen example on the right belongs to the same endpoint in a multistream call—it is using both screens for video when no content is being shared.

Figure 4: Two-screen endpoint conference example

Feature limitations

- TIP endpoints are displayed on multistream-capable endpoints by displaying only the active speaker segment.
- All endpoints will be switched to transcoded mode when a grouped endpoint is in a conference.

Bandwidth requirements

Below are the recommended call bandwidths required for multistream calls.

- Single screen multistream endpoints:

  1128kbps < SD <1664kbps

  1664kbps< 720p30 <2432kbps

  >2432kbps 1080p30

- Dual Screen multistream endpoints

  3200kbps <720p30 <4736kbps

  >4736kbps 1080p30

If at any point the call bandwidth falls below 1128kbps then the call will be transcoded.

Resilience and diagnostics improvements

Remote logging of protocols log

In this release the protocols log is available over HTTP or HTTPS. A client can make an HTTP POST request to a specific URL. The protocols log is then streamed back to the client along this TCP connection. The log stream continues until the client breaks the TCP connection. A maximum of two simultaneous log streams are available at any time. This improves troubleshooting as it is now easier to obtain and archive logs.

If you wish to start logging protocols messages to a remote device:

1. Send an HTTP POST request from the remote device to **`http[s]://<ip address>/protocols_log_stream`**. This POST request must include the following valid user and password parameters: **`authenticationUser=<username>&authenticationPassword=<password>`**

   The following is an example using wget (for a Linux system):
   `wget https://<IP address>/protocols_log_stream --post-data='authenticationUser=<username>&authenticationPassword=<password>'`

   (Users with API-only permissions are considered valid.)
2. The entire contents of the protocols log is then streamed back to the remote device using this TCP connection. The log stream continues until the remote device breaks the TCP connection.

TIP messages logged in event log

TIP is a signaling protocol. In previous TelePresence Server releases, TIP messages were not logged —the only way to troubleshoot them was to obtain a network packet capture which could be difficult for customers to achieve.

This release introduces a new feature so each TIP message sent or received generates an event log message at TRACE level.

Note: We recommend that you do not change the log level unless under the guidance of Cisco TAC.

Event log message on packet loss

In previous releases, real-time information about packet loss was only available for active calls. This made it difficult to troubleshoot video quality problems.

This release introduces an event log message that is generated when a particular threshold rate* of packet loss is exceeded (default is 5). This applies to both incoming media streams (where TelePresence Server can detect packet loss directly) and to outgoing media streams (where RTCP reports are used to gather data). The event log message clearly indicates the numbers of packets lost and expected.

To avoid flooding the event log, the event log message is only printed a maximum of once every ten minutes for any given participant and direction combination.

*The threshold rate is user-specified, either by **Configuration > System settings > Packet loss threshold** (locally managed mode) or by **`callAttributes member packetLossThreshold`** (remotely managed mode).

Network packet capture controls on web interface

This release introduces the ability to control a packet capture from the web interface. The packet capture has the same options and settings as the console version. In previous releases you could only obtain a packet capture from the device using console access to the device.

Note: this feature requires the TelePresence Server to have an Advanced Diagnostics feature key.

'Bad video' event log message

This release introduces an event log message that is generated when a video decoder has lost synchronization with a remote encoder. A further event log message is printed when synchronization is regained. The message includes a Call ID to identify the participant that the TelePresence Server could not decode and assists troubleshooting once the call has ended.

Improvements to participant media summary CDR entry

In this release the following information is added to the **`participant media summary`** CDR log message to assist troubleshooting:

- Number of packets lost for all video streams both sent and received for a participant.
- Total video frame count for all video streams both sent and received for a participant.
- Frame error count for all video streams received from a participant.
- Fast Update Request count for all video streams both sent and received for a participant.

Scalability improvements

Capacity improvements

This release offers increased capacity, for detail see Platform licensing comparison [p.11]. The TelePresence Server now allows up to 2.5MB for HD calls (previously 4MB), thereby increasing the total number of calls possible without reducing the call quality. This is achieved as current endpoints are more efficient and do not need such a high allocation of bandwidth as previously required.

This increased capacity improvement introduces changes to the bandwidth of four common resolutions as shown in the table below:

Resolution	Previous rx bandwidth (kbps)	New rx bandwidth (kbps)	Previous tx bandwidth (kbps)	New tx bandwidth (kbps)
360p30	1000	675	1000	675
480p30	2000	1000	2000	1000
720p30	4000	2500	4000	2500
1080p30	4000	3250	4000	3250

General improvements

One conference URI with separate guest/chair PINs

In this release, a conference URI can support multiple PINs, with important participant settings (such as chair or guest privilege levels, or different token levels) determined by the PIN entered by the endpoint.

In previous releases, each conference URI supported only a single PIN.

Note: This feature can only be configured via the TelePresence Server's remotely managed mode API. It is not supported on Cisco TelePresence Conductor XC2.4 or earlier.

Cisco Sans font

This release introduces the Cisco Sans font. This font provides consistency with other TelePresence products and displays in conferences. The Cisco Sans font is the default font for this release, however, if upgrading to this release the existing font file will remain, so it can still be used after a downgrade.

In this release the web interface font upload mechanism and the warning banner to indicate the font is not present have been removed.

Platform licensing comparison

The following table compares the number of TelePresence Server screen licenses that each of the platforms can accept and how they translate into conferencing capacity. The table does not display information about licensing for the locally managed mode of operation, as this is only possible on the 7010 and MSE 8710 platforms. Refer to the online help or administrator documentation for details of licensing in locally managed mode.

Table 2: TelePresence Server screen licenses per call for each call type

Call type description			Screen licenses required per call
Main video	**Audio**	**Content**	
-	Mono	-	1/52
360p30†	Mono	In main video	⅛
360p30†	Stereo	720p5	¼
480p30	Stereo	In main video	¼
480p30	Stereo	720p5	⅓
720p30	Stereo	720p5	½
720p30	Stereo	720p30	1
1080p30	Stereo	720p15	1
720p60	Stereo	720p15	1
1080p30	Stereo	720p30	1½
Three-screen 720p30	Multichannel	720p5	1½
Three-screen 720p30	Multichannel	720p30	2
1080p30	Stereo	1080p30	2
Dual-screen 1080p30	Stereo	720p30	2
Three-screen 1080p	Multichannel	720p30	3
Three-screen 1080p	Multichannel	1080p30	4
Four-screen 1080p	Stereo	1080p30	4

Table 3: TelePresence Server conferencing capacity on various platforms

Screen licenses required per call	Maximum calls by hardware type (with licenses to provide 100% of capacity)								
	8 Cores VM MD	8 Cores VM HD	Media 310 or MCU 5310	30 vCPU / High Density VM ‡	Media 320 or MCU 5320	7010, MSE 8710 or MCU MSE 8510	Media 400v ‡ (30 vCPU) ‡‡	Biggest appliance cluster (two appliances)	Biggest blade cluster (four blades)
	4 screen licenses	5 screen licenses	6 screen licenses	10 screen licenses	12 screen licenses	12 screen licenses	18 screen licenses	24 screen licenses	48 screen licenses
1/52	200*	200*	200*	200*	200*	200*	200*	200*	200*
⅛	33	41	49	81	97	97	145	195	200*
¼	16	20	24	40	48	48	72	97	195
⅓	12	15	18	30	36	36	54	73	146
½	8	10	12	20	24	24	36	48	97
1	4	5	6	10	12	12	18	24	48
1½	2	3	4	6	8	8	12	16	32
2	2	2	3	5	6	6	9	12	24
3	1	1	2	3	4	4	6	8	16
4	1	1	1	2	3	3	4	6	12

* 200 is the maximum number of calls that is possible on a TelePresence Server. Requires Cisco TelePresence Conductor XC2.3.

† Requires TelePresence Conductor XC2.2 or later.

‡ To achieve the maximum number of calls, Cisco TelePresence Server on Virtual Machine must be the only VM hosted on the Multiparty Media 400v or 30 vCPU / High Density VM. It cannot be co-resident with any other UC application (unlike the 8-core option that runs at 2.4GHz minimum and can be co-resident).

‡‡ Media 400v is configured with 30 vCPUs as per the High Density configuration but it has a higher capacity.

Note: The table above assumes that calls of one type are being used to reach these maximum values. To calculate the total number of licenses required for a variety of concurrent calls, sum the screen licenses required for each concurrent call.

Resolved and open issues

Use the links below to find up-to-date information about this release in the Cisco Bug Search tool.

Resolved issues

https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283613665&rls=4.1%281.22%29,4.1%281.42%29,4.1%281.61%29,4.1%281.67%29,4.1%281.79%29,4.1%281.85%29&sb=fr&srtBy=byRel&bt=empCustV

Open Issues

https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283613665&sb=afr&sts=open&svr=5nH&srtBy=byRel&bt=empCustV

Limitations

Flow control disabled for endpoints that negotiate TIP/MUX

Endpoints that negotiate TIP/MUX, including the CTS series, would have been negatively impacted by the new flow control algorithm introduced in TelePresence Server 4.0. Flow control requests have thus deliberately been disabled for TelePresence Server 4.0 or later when it is in calls with these endpoints. This also means that the **Received video: flow control on video errors** setting will have no effect if it is enabled for these endpoints.

The TelePresence Server does not support sender-side flow control

The TelePresence Server does not currently support sender-side media flow control. This can create problems when calls are made over low bandwidth pipes to endpoints that do not support receive-side flow control. In such calls, flow control is not possible for the media from the TelePresence Server to the endpoint. Issue identifier CSCun86953.

Video issues with earlier versions of TX endpoint software

Note: We strongly recommend that you use TX6.0.5 or later software on these endpoints when they interoperate with TelePresence Server 3.1(1.95) or later.

The following endpoints display significant orange or green flashes when they are using software versions between TX6.0.0 and TX6.0.4 in calls with TelePresence Server 3.1(1.95) or later:

- Cisco TelePresence System 500-32
- Cisco TelePresence TX1300 Series
- Cisco TelePresence TX9000 Series
- Cisco TelePresence TX9200 Series

Resource optimization causes brief video interruptions

When TelePresence Conductor optimizes the resources used for a call, that endpoint's video contribution is very briefly interrupted. This can be visible to others as a flicker of black in the otherwise continuous stream. Issue identifier CSCuj53830.

Call transfer is disabled

The TelePresence Server does not support call transfer.

DTLS and custom certificates

DTLS is used to negotiate encryption parameters with TIP endpoints. This requires a certificate to be used. There are some limitations when using DTLS with customer-supplied certificates:

- Opportunistic DTLS, as supported in release 2.2, always uses the default certificate for DTLS negotiation, even if a customer-supplied certificate is uploaded. This is due to technical limitations.
- Release 2.3 and later supports a new improved DTLS type — 'negotiated DTLS'. When using 'negotiated DTLS', the TelePresence Server uses the customer-supplied certificate if they have uploaded one (which is the preferred procedure). If 'negotiated DTLS' is used in a call to a CTS endpoint combined with some custom certificates, DTLS may fail on these calls. This is due to defect CSCts24503. The call may still connect but without encryption. As a workaround, use a smaller custom certificate such as a certificate with a 1024 byte key or use the default certificate on the TelePresence Server.

HD quality indicators on CTS endpoints

The lobby screen is a static image that is designed for HD mode, that is, 720 pixels high. When a CTS endpoint displays the lobby screen, it may go on to incorrectly report the quality of the received video stream. The quality indicator may show four bars – for 720p video – even though the endpoint is actually receiving 1080p video and should display five bars.

Encryption required causes issues with some endpoints

Some endpoints such as the Sony XG-80 and HG-90, and the TANDBERG Classic 6000s are unable to join conferences in which encryption is required, even when encryption is enabled on the endpoint. (TANDBERG is now part of Cisco.)

Setting these conferences to have optional encryption allows these endpoints to join using encryption.

Clustering limitations

Slot 10 of the Cisco TelePresence MSE 8000 chassis does not support clustering in this TelePresence Server software release. However, slot 10 in the same chassis as a cluster can be used for a standalone blade of any type.

Calls from Microsoft Lync which do not use Advanced Media Gateway may fail

For direct calls from Microsoft Lync or OCS you must use the VCS B2BUA. Calls may no longer work if configured through a VCS zone with profile "Microsoft Office Communication Server". For more information on configuring the VCS, refer to the VCS Administrator documentation.

Firefox 14 is not supported for use with the Cisco TelePresence Server

We strongly recommend that you do not use Firefox 14 to access the TelePresence Server's web interface. This version of the browser causes an issue that was not present in previous Firefox versions and has been fixed in Firefox 15. This issue also affected previous versions of the TelePresence Server software.

TIP calls and encryption required conferences

TIP calls can only join conferences with the Encryption setting configured to *Required* when TLS encrypted signaling is used throughout the call signaling path. This ensures that the call is fully secure.

Recommended VCS version X7.2 or later

On calls to CTS endpoints in certain network configurations, calls may fail or become audio-only with earlier versions of VCS. In order to avoid this, upgrade VCS to X7.2. If using a custom zone profile on VCS for the Cisco Unified Communications Manager zone, ensure that **SIP UPDATE strip** mode is disabled on this zone.

Limited support for some VM operations

Snapshotting a Cisco TelePresence Server on Virtual Machine is not recommended and should only be undertaken when no calls are active and only when following the best practice guidelines from VMware. Cisco recommends that customers check for any automated snapshotting processes and disable them for any Cisco TelePresence Server on Virtual Machines.

Cloning of a Cisco TelePresence Server on Virtual Machine is not supported—any cloned machines will require new licenses.

Unless otherwise stated, Cisco supports only those VMware features recommended in this and other Cisco TelePresence Server on Virtual Machine guides.

Interoperability

The interoperability test results for this product are posted to http://www.cisco.com/go/tp-interop, where you can also find interoperability test results for other Cisco TelePresence products.

Upgrading to 4.1(1.85)

Prerequisites and software dependencies

Software dependencies

In the case of the TelePresence Server MSE 8710 blade(s), the Cisco TelePresence Supervisor MSE 8050 blade must be running Supervisor software version 2.2 or later.

Prerequisites

The software upgrade process requires a hardware restart. Schedule a downtime window and notify users of when the service will be unavailable. The duration of an upgrade can be up to 25 minutes. Have the following available and complete the backup processes described before you proceed to upgrade the software:

- New software package.
  - For hardware platforms, this will be a file with a **.zip** extension, for example **cisco_ts_media_300_4.1_1.85.zip** for the Media 310/320 platforms. You must unzip this file before you can use it.
  - For the virtual machine platform, the initial install file has a **.ova** extension but the upgrade package has a **.tgz** extension, for example, **Cisco_tsVirtualMachine_4.1_1.85.ova** and **Cisco_tsVirtualMachine_4.1_1.85.tgz**. You do not need to unzip either of those packages before you use them.
- Current software image file (in case you need to reverse the upgrade).
- Backup of the configuration (the **configuration.xml** file).
- You will require the administrator user name and password for the configuration backup file if you ever need to use the backup. If you attempt to downgrade / restore the software and you cannot load an appropriate configuration file, you may be unable to log in to the device.
- If using Call Detail Records (CDRs), or any other logs, for billing, auditing or other purposes, you must download and save your logged data. When the device reboots as part of the upgrade, all existing CDRs will be deleted.
- Administrative access to all units to be upgraded.
- The model numbers and serial numbers of your devices in case you need to contact Cisco Technical Support.

CAUTION: Make sure that all the backup processes described in this section have been completed before you start the upgrade. Failure to do so could result in data loss.

CAUTION: If you are upgrading a cluster you must upgrade all members of the cluster to the same software version.

Note: While you are upgrading a cluster, or restarting it for another reason, the master cannot report the cluster's full capacity until the slaves have also restarted. Any devices that poll the master for such information should check that the slaves are back up before assuming that the capacity has permanently been reduced, or that there is some other fault in the cluster.

Backing up your configuration

1. In a web browser, navigate to the web interface of the device.
2. Sign in as an administrator.
3. Go to **Configuration > Upgrade**.
4. In the **Back up and restore** section, click **Save backup file**.
5. Copy the resulting **configuration.xml** file to a secure location.

CAUTION: You must remember the administrator user name and password for the configuration backup file in case you ever need to use the backup.

Upgrading the Cisco TelePresence Server on Virtual Machine

Note: This section is not applicable if you are upgrading a hardware platform TelePresence Server.

Note: If upgrading from TelePresence Server 4.0 to 4.1 on a 16 vCPU machine (high capacity) you need to carry out the additional step of reconfiguring the VM with 30 vCPUs to take advantage of the increased capacity on existing hardware otherwise the upgrade will result in reduced capacity on some virtual platforms. If upgrading an 8 vCPU you only need to change the RAM. (See Table 4: Upgrade paths for Cisco TelePresence Server on Virtual Machine [p.17].)

The upgrade process for a Cisco TelePresence Server on Virtual Machine is very similar to that of the hardware platforms, although there are some differences. You must comply with all the Prerequisites and software dependencies [p.15], unless an item is explicitly excluded from the Virtual Machine platform.

The main differences in the Virtual Machine upgrade are as follows:

- The upgrade file for Cisco TelePresence Server on Virtual Machine has a **.tgz** file extension.
- After doing the software upgrade via the Cisco TelePresence Server on Virtual Machine web interface, you may need to adjust the number of vCPUs dedicated to the virtual machine and may need to adjust the RAM. These changes require that you power off the VM.

Note:Upgrades to 4.1(1.85) will stay at the previous 8 GB RAM value and need to be manually changed in the VM settings via vSphere. Likewise downgrades to earlier versions will retain the 12 GB value.

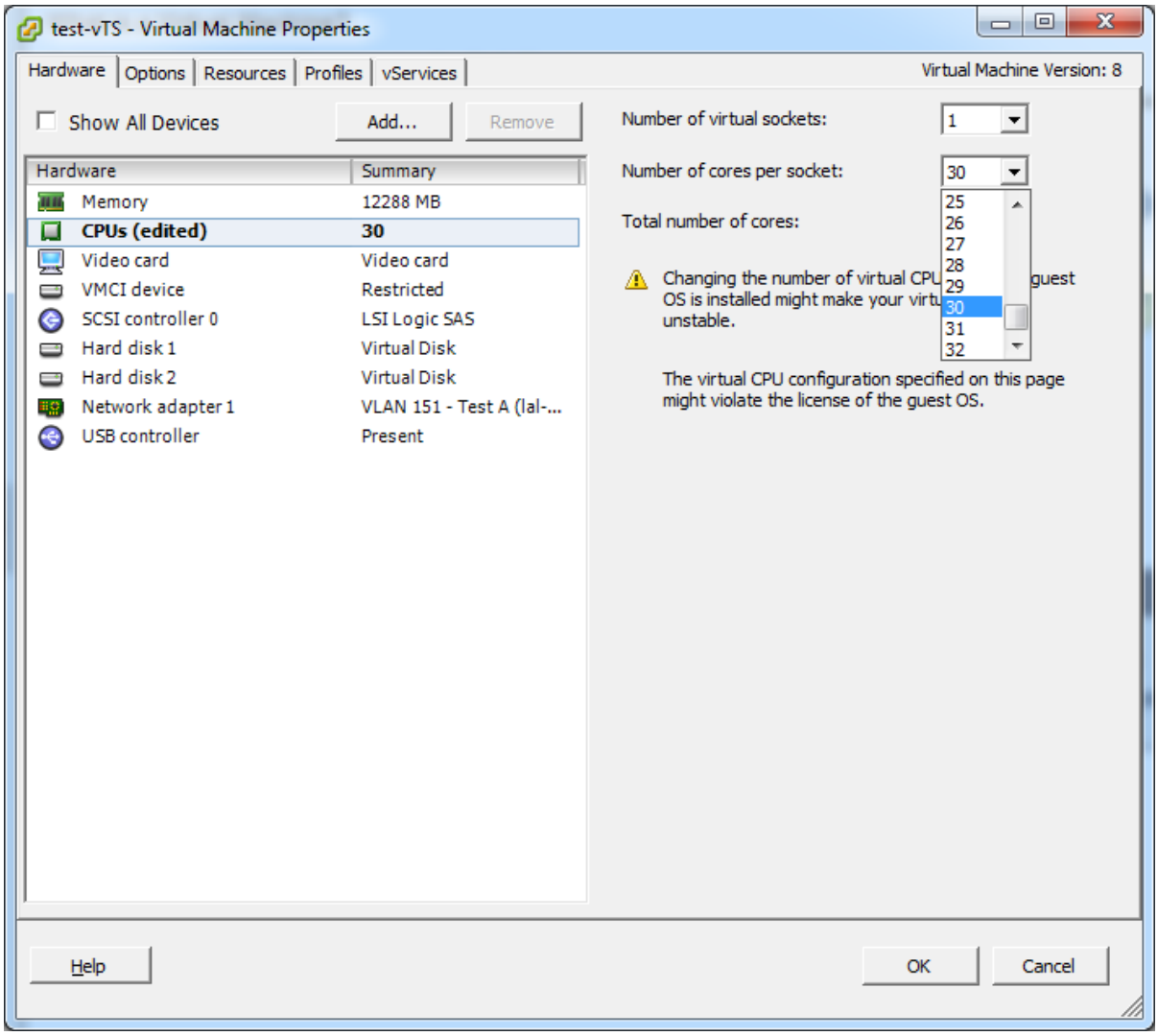
To upgrade Cisco TelePresence Server on Virtual Machine:

Table 4: Upgrade paths for Cisco TelePresence Server on Virtual Machine

	Media 400v		16 Cores VM		8 Cores VM HD	
Upgrade	**From this**	**To this**	**From this**	**To this**	**From this**	**To this**
Software version	4.0(2.8)	4.1(1.85)	4.0(2.8)	4.1(1.85)	4.0(2.8)	4.1(1.85)
Physical CPUs	16	16	16	16	8	8
Virtual CPUs	30	30	16	30	8	8
RAM	8 GB	12 GB	8 GB	12 GB	8 GB	12 GB
Maximum screen licenses	14	18	8	10	4	5

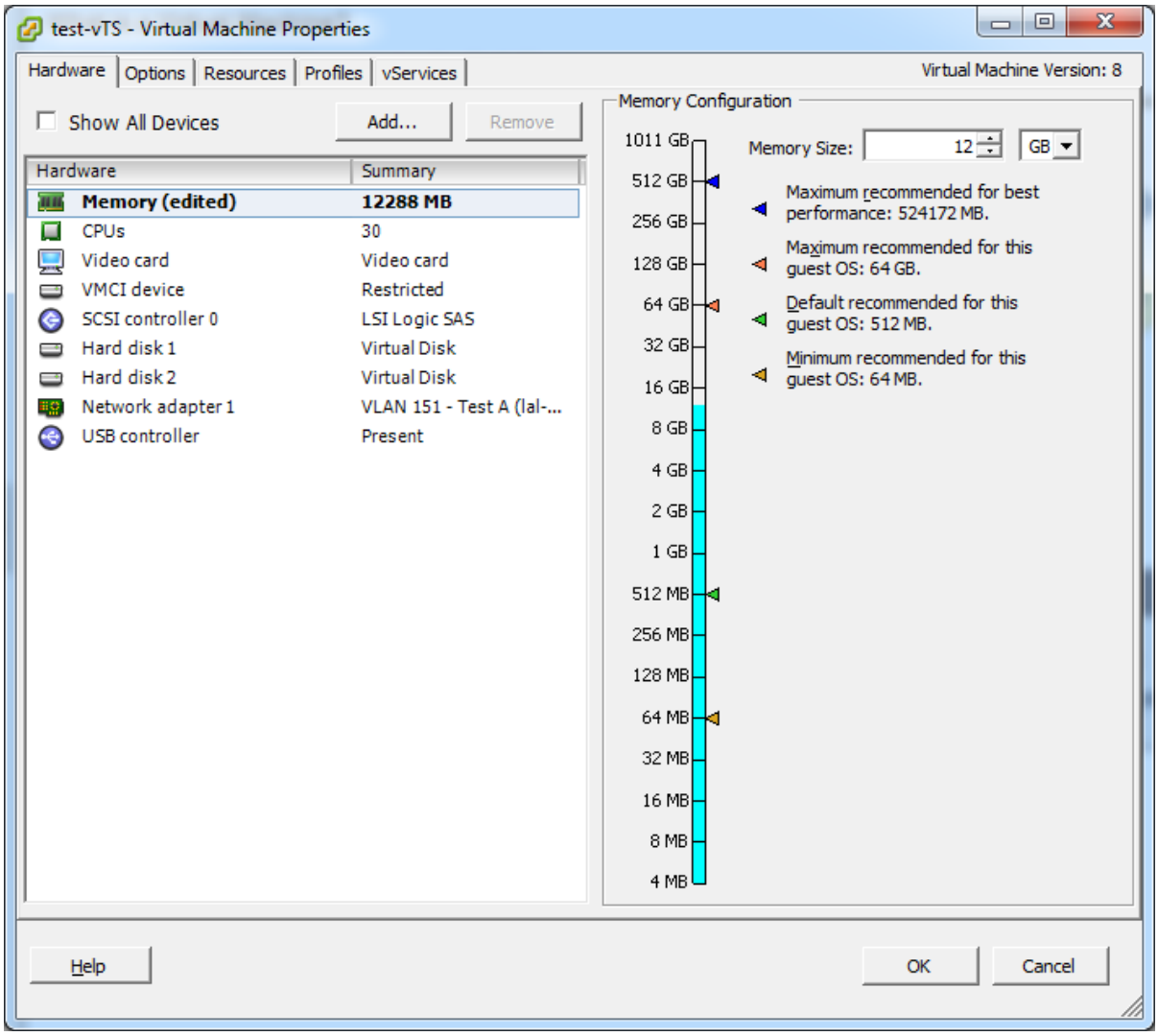
Note: The maximum number of screen licenses that most Virtual Machine configurations can use has increased in this release. You may wish to purchase more licenses to take advantage of the increased capacity. See Platform licensing comparison [p.11] for details of the capacity given by the new configurations.

1. Follow the software Upgrade instructions [p.19], browsing to the **.tgz** file from the **Configuration > Upgrade** page.
2. After the TelePresence Server has restarted, change the number of vCPUs dedicated to the Cisco TelePresence Server on Virtual Machine as follows:
   a. Open your VMware client and access the ESXi host.
   b. Right-click the TelePresence Server virtual machine and select **Power > Power Off**.
   c. Right-click the TelePresence Server virtual machine and select **Edit Settings…**.
   d. On the **Hardware** tab, click **CPUs**.
   e. From the **Number of cores per socket** list, select the required number of virtual CPUs (vCPUs).



f. Click **OK**.
g. Right-click the TelePresence Server virtual machine and select **Power > Power On**.

3. You should also change the memory allocation from 8 GB to 12 GB as follows:
   a. Open your VMware client and access the ESXi host.
   b. Right-click the TelePresence Server virtual machine and select **Power > Power Off**.
   c. Right-click the TelePresence Server virtual machine and select **Edit Settings…**.
   d. On the **Hardware** tab, click **Memory**.
   e. In the **Memory Size** field, select the required amount of memory; the minimum requirement is 12 GB.



Note: 12 GB vRAM should map to 12 GB physical RAM since oversubscription is not supported.

f. Click **OK**.
g. Right-click the TelePresence Server virtual machine and select **Power > Power On**.

Upgrade instructions

1. In a web browser, navigate to the web interface of the device.
2. Sign in as an administrator.
   The username is *admin* and there is no password on a new unit.
3. Go to **Configuration > Upgrade**.
4. In the **Main software image** section, locate the **New image file** field. Browse to and select the new image file.
5. Click **Upload software image**.
   The web browser uploads the file to the device, which may take a few minutes.

Note: Do not browse away from the **Upgrade** page, or refresh the page, during the upload process – this will cause the upload to fail.

A pop-up window displays to show upload progress. When complete, close the message. The web browser refreshes automatically and displays the message *Main image upload completed*.

6. Click **Shut down TelePresence Server**. This option will now change to **Confirm TelePresence Server shutdown**. Click to confirm.
7. Click **Restart TelePresence Server and upgrade**.
   The unit will reboot and upgrade itself; this can take up to 25 minutes.

   Note: You may be logged out due to inactivity. If this happens, log in again, go to **Configuration > Shutdown** and click **Restart TelePresence Server and upgrade**.
8. Go to the **Status** page to verify that your device is using the new version.
9. If necessary, restore your configuration; refer to the online help for details.

Downgrade instructions

If you need to reverse your upgrade, you can re-install the former version of the software. The downgrade procedure is the same as the upgrade procedure except you will use the earlier software image.

CAUTION: Make sure that all relevant backup processes described in Prerequisites [p.15] have been completed before you start the downgrade. Failure to do so could result in data loss.

Note: We recommend that you delete any custom certificate before downgrading on Media 310 and Media 320 platforms, and re-upload the certificate after downgrading.

Downgrading from 4.1(1.85)

You need the correct target version of the software and the corresponding saved configuration before you proceed.

1. Follow the upgrade procedure using the earlier software image.
2. Restart the hardware and check the status via the web interface.
   The status report indicates the software version.
3. Restore your configuration from the saved XML file; refer to the online help for details.

Using the Bug Search Tool

The Bug Search Tool contains information about open and resolved issues for this release and previous releases, including descriptions of the problems and available workarounds. The identifiers listed in these release notes will take you directly to a description of each issue.

To look for information about a specific problem mentioned in this document:

1. Using a web browser, go to the Bug Search Tool.
2. Sign in with a cisco.com username and password.
3. Enter the bug identifier in the **Search** field and click **Search**.

To look for information when you do not know the identifier:

1. Type the product name in the **Search** field and click **Search**.
2. From the list of bugs that appears, use the **Filter** drop-down list to filter on either *Keyword*, *Modified Date*, *Severity*, *Status*, or *Technology*.

Use **Advanced Search** on the Bug Search Tool home page to search on a specific software version.

The Bug Search Tool help pages have further information on using the Bug Search Tool.

Technical support

If you cannot find the answer you need in the documentation, check the website at www.cisco.com/cisco/web/support/index.html where you will be able to:

- Make sure that you are running the most up-to-date software.
- Get help from the Cisco Technical Support team.

Make sure you have the following information ready before raising a case:

- Identifying information for your product, such as model number, firmware version, and software version (where applicable).
- Your contact email address or telephone number.
- A full description of the problem.

To view a list of Cisco TelePresence products that are no longer being sold and might not be supported, visit: www.cisco.com/en/US/products/prod_end_of_life.html and scroll down to the TelePresence section.

Document revision history

Table 5: TelePresence Server release notes revisions

Date	Description
March 2015	Version 4.1 maintenance release to resolve PSIRT issue
January 2015	Version 4.1 initial release