Cisco TelePresence Server 4.0(2.8)

Software Release Notes
Revised July 2014

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 4.0(2.8)

Table 1: New feature support by TelePresence Server platform

Feature name		7010 & MSE 8710	Media 310/320	Virtual Machine
Resilience and diagnostics improvements				
	Cisco Call Home support [p.2]	Yes	Yes	Yes
Cisco TelePresence Server on Virtual Machine improvements				
	New platform for TelePresence Server [p.3]	Not applicable	Not applicable	Yes
	Hypervisor version ESXi 5.5 support [p.3]	Not applicable	Not applicable	Yes
	User Interface changes [p.3]	Not applicable	Not applicable	Yes

Cisco Call Home support

This release enables the TelePresence Server to send diagnostic logs to the Cisco Call Home service. This feature can be configured to enable logs to be submitted automatically (disabled by default) or logs can be submitted manually.

Note: The TelePresence Server currently only supports anonymous reporting.

Logs are only sent via encrypted HTTPS connections. This requires the TelePresence Server to have an encryption feature key. Without this, you can view the Call Home web settings but the functionality will not be available.

Call Home messages are sent to **`https://tools.cisco.com/its/service/oddce/services/DDCEService`**. At that point, you may need to update your firewall to allow the reports through, by adding the domain **`tools.cisco.com`** and opening port 443 for outbound TCP traffic.

The TelePresence Server can send 'inventory' data (i.e. basic system information such as serial number, hardware platform and software version) to the Call Home service. If automatic reporting is enabled, inventory data is sent each time the device starts up.

Device inventory reports are always available. Media resource or unit-wide diagnostic logs may also be available depending on whether an unexpected shutdown or media resource restart has occurred.

Note: If you have any questions about a Call Home report please contact Cisco TAC.

The user interface has a new Call Home settings page (**Logs > Call Home**) to allow the TelePresence Server to be configured to send diagnostic logs automatically in the event of an unexpected restart. Logs can also be submitted manually from this page.

Cisco TelePresence Server on Virtual Machine improvements

New platform for TelePresence Server

This release introduces a new platform for the TelePresence Server software: the Cisco Multiparty Media 400v. This gives an increased port capacity of 28 HD ports at 720p30 video + 720p5 content.

This increased port capacity is enabled via the configuration dialog on the Deploy OVF Template wizard, see the **Deploying OVA to host** section of the latest Cisco TelePresence Server on Virtual Machine Installation Guide http://www.cisco.com/c/en/us/support/conferencing/telepresence-server/products-installation-guides-list.html

Note: This maintenance release enables extra capacity. However, the additional port capacity needs to be licensed separately to achieve this support.

Note: To achieve the maximum port capacity, Cisco TelePresence Server on Virtual Machine must be the only VM on the Multiparty Media 400v. It cannot be co-resident with any other UC application.

Hypervisor version ESXi 5.5 support

In this release, Cisco TelePresence Server on Virtual Machine now supports Hypervisor version ESXi 5.5.

Note: The Cisco Multiparty Media 400v requires Hypervisor version ESXi 5.5.

User Interface changes

The **System status** page on the user interface now provides information on **Platform status**, i.e. processor type, number of cores allocated for the Cisco TelePresence Server on Virtual Machine, clock speed of the system.

New features introduced in 4.0(1.57)

Table 2: New feature support by TelePresence Server platform

Feature name	7010 & MSE 8710	Media 310/320	Virtual Machine
User experience improvements			
Segment-switched display of telepresence rooms [p.4]	Yes	Yes	Yes
Video announce [p.7]	Yes	Yes	Yes
PiP strip and name label improvements [p.7]	Yes	Yes	Yes
*6 mute control [p.8]	Yes	Yes	Yes
Notification banner changes [p.9]	Yes	Yes	Yes
New technology			
Support for mixed IP scheme networks [p.9]	Yes	Yes	Yes
API improvements [p.9]	Yes	Yes	Yes
Third Party Interop feature key requirement lifted [p.10]	Yes	Yes	Yes

Table 2: New feature support by TelePresence Server platform (continued)

Feature name	7010 & MSE 8710	Media 310/320	Virtual Machine
Scalability improvements			
Increased calls per unit [p.10]	Remotely managed only	Yes	Yes
Dynamic resource optimization improvements [p.10]	Remotely managed only	Yes	Yes
OVA and specification changes for Cisco TelePresence Server on Virtual Machine [p.15]	Not applicable	Not applicable	Yes
Support for cascaded conferences [p.17]*	Remotely managed only	Yes	Yes
Security improvements			
Console password [p.17]	Yes	Yes	Yes
Static ARP and NDP [p.17]	Yes	Yes	Yes
Netstat [p.17]	Yes	Yes	Yes
Ephemeral port range [p.18]	Yes	Yes	Yes
Resilience and diagnostics improvements			
Intelligent flow control of incoming streams [p.18]	Yes	Yes	Yes
Resilience to media processor restart [p.18]	Yes	Yes	Yes

* This feature is controlled via the API but it is not supported by Cisco TelePresence Conductor XC2.3.

User experience improvements

Segment-switched display of telepresence rooms

In remotely managed mode, and on Media 310/320 and Virtual Machine, the display switching behavior is configurable via the API and is supported by TelePresence Conductor XC2.3.

In locally managed mode, the display switching mode can be changed via the TelePresence Server web interface.

On Cisco CTS or TX Series endpoints, you can change between room switching and segment switching via the touch controller .

The TelePresence Server now defaults to 'segment-switched' mode (may also be called 'panel-switched') for displaying speakers from telepresence rooms. In this mode, the TelePresence Server independently switches the display of individual cameras from a multiple camera system.

This is a change in display switching behavior; previously, the TelePresence Server would simultaneously switch all of the streams from that room into the display on another multiscreen endpoint. The older behavior is now called 'room-switched' mode.

In room-switched mode, when the loudest speaker is someone from a multiple camera system, the TelePresence Server displays, where possible, the whole room as the loudest speaker (all cameras). That is, all streams from the room's cameras are shown on multiscreen endpoints (if they have enough screens). If

the loudest speaker is *not* in the telepresence room, then the TelePresence Server shows no panels from that room in a large pane.

For example, consider the following conference that has two three-screen endpoints and three single-screen endpoints:

Figure 1: Top view of conference for display switching behavior description

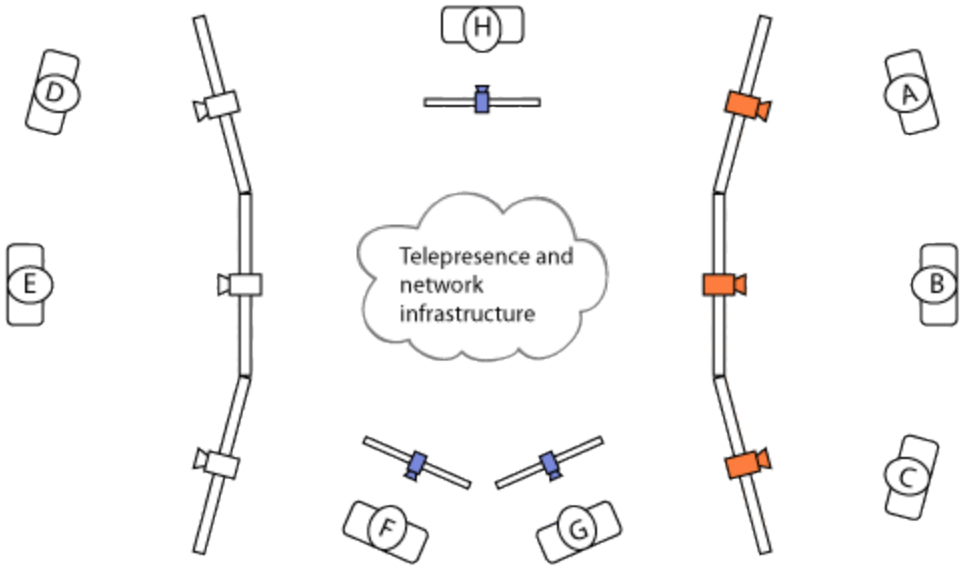
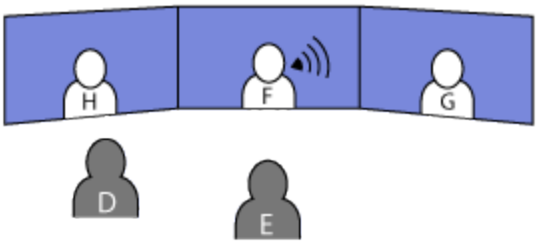


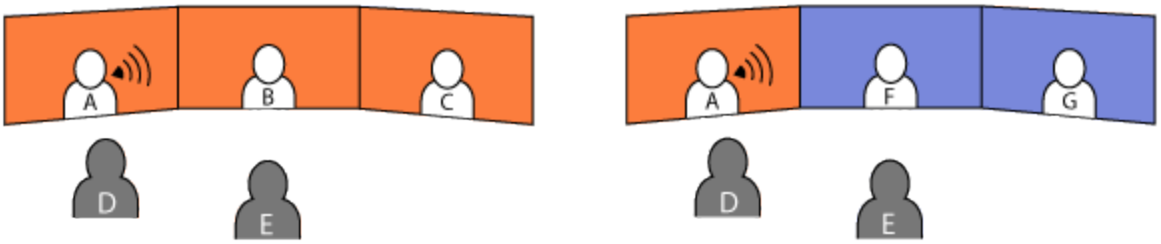
Figure 2: The display seen by participants D and E, while participant F is the active speaker



The following two diagrams show the same display after participant A becomes the loudest speaker, for the two display switching modes.

Figure 3: The room-switched display after A becomes loudest

Figure 4: The segment-switched display after A becomes loudest



Changes to endpoint group layout

When you are using the segment-switched display feature, grouped endpoints are composed differently than they were in the previous release. This change also applies to multi-camera endpoints that cannot reveal which camera is associated with the loudest speaker ("loudest pane information").

Grouped endpoints are now composed into a single pane so as not to disrupt segment-switching. Segment-switching isn't possible with these endpoints because the TelePresence Server doesn't know which of the segments actually shows the speaker. The benefit of this approach is that single-screen endpoints are no longer forced into the Equal layout (NxN grid) when the group is in the conference; they will see the group in a row, and in the correct order.

If the display of grouped endpoints on multi-screen systems is more important for your environment than segment-switching or the single-screen experience, use the room-switching display mode to have the conference layouts for groups behave as they did in the previous release.

Table 3: Example ActivePresence layouts when a group of four endpoints is active speaker

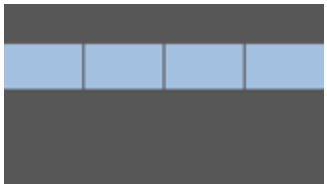
Display switching mode	Layout on single-screen endpoint	Layout on three-screen endpoint
Room-switched mode	 (Layout forced to Equal)	 (Layout forced to custom so that group switches in across screens)
Segment-switched mode	 (Group composed into single pane)	 (Other speakers remain in other screens when group switches in)

Endpoint group indicators

When a grouped endpoint is shown in the ActivePresence or Prominent layout, the endpoint must be placed in the PiP strip but, because of the lack of loudest pane information, the TelePresence Server cannot determine which pane of the group to place in the PiP strip. Also, now that the group is composed into a single pane, the live video of the group members is too small to be useful in these layouts.

In segment-switched mode, the PiP strip contains a static pictorial representation of the endpoint group instead of a live video stream, as follows:

Table 4: Endpoint group indicators

Two-screen group	Three-screen group	Four-screen group
		

Video announce

This feature shows new participants as they join, irrespective of how many other participants are already in the conference and who is currently the active speaker.

Video announce is not used in the Active Speaker layout (single), to avoid disruption, but the feature applies to all other layouts, allowing everyone to see people as they join.

In the ActivePresence and Prominent layouts: As video participants join, their video is shown to everyone else by the appearance of new PiPs (pictures in picture) at the right end of the row of PiPs. As more people join, the least active speakers are eventually removed from the PiP strip while new entrants are added.

In the Equal layout: New participants are announced by appearing in the next open position, typically at the right end of the bottom row (they're added in left-to-right reading order). If all the grid positions are full (16 participants) then the next participant to be announced appears in place of the least active speaker, and so on. In previous releases, participants joining after the grid was full would not necessarily have been shown until they had spoken.

PiP strip and name label improvements

In this release the behavior of the row of PiPs (PiP strip) at the bottom of the conference display has been improved to make the experience more consistent for all participants. New arrivals or recent speakers are shown at the right of the strip, and the strip moves left to accommodate the newly placed PiPs.

When someone is speaking their PiP is not shown; instead, a gap is left in the PiP strip to show their place (like an empty seat).

This provides a more consistent layout experience and helps participants to find each other more easily than in previous releases.

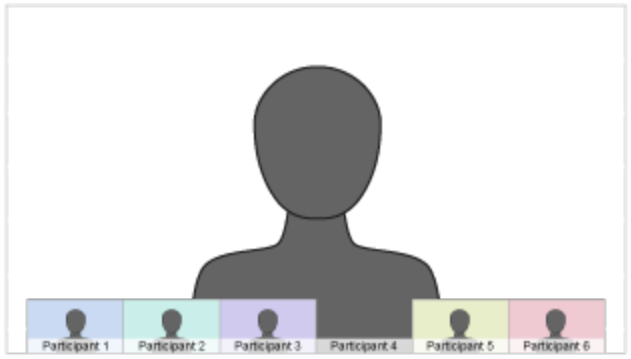
Figure 5: PiP strip showing the active speaker's place (gap)

The active speaker gap applies only to the ActivePresence layout. It is also not available on multiscreen endpoints that are in room-switched display mode.

Note: Future improvements to the PiP strip feature may include reducing the maximum number of PiPs and increasing their size, to make the feature more consistent across endpoints and to allow for better recognition of changes to facial expression. We cannot guarantee that this feature will remain as it is in the current release.

The name labels have been restyled and are now displayed below the participants. They are available in all layouts but are off by default.

Figure 6: ActivePresence layout showing name labels



The Cisco TelePresence Conductor XC2.3 user interface does not have a direct method for controlling the display of the name labels. You can toggle them using the **`displayShowEndpointNames`** call attribute in the template's advanced parameters section. For example, add the custom parameter **`{"callAttributes":{"displayShowEndpointNames":true}}`**. See the Cisco TelePresence Conductor's help for more details of editing templates.

*6 mute control

Users are now able to mute or unmute themselves using the *6 combination on a DTMF keypad.

This new mute/unmute control complements the ability to mute a participant from the TelePresence Server end. The feature is particularly important for usability of endpoints that can be muted by means that they don't support.

Figure 7: The TelePresence Server's "you are muted" icon

Participants will see this icon when their audio contributions are muted from the TelePresence Server side. This mute can be applied by the participants themselves, using *6, or by another authorized party. Participants may also see a message about having been muted.

This icon does not appear when the participant uses the endpoint's own mute control.

Note: The TelePresence Server places its conference status icons on the left hand edge of the display, near the top. In some cases the endpoint's own icons will also be visible but these are usually in a different region of the display.

Notification banner changes

This release includes new or updated notification banners for the following important conditions:

- Unexpected media resource restart
- Unexpected device restart
- Font file missing

The banners provide suggestions or links to help you resolve the noted conditions and will disappear when the condition is resolved.

Note: If you are upgrading a TelePresence Server MSE 8710, you will probably see the banner about the missing font file. If this is the case, it is the *notification* that is new, and not the absence of the font file. You can download the font file from the Software download page for 3.0(2.48). There are more detailed instructions for Upgrading the font (optional) [p.34] later in this document.

New technology

Support for mixed IP scheme networks

The TelePresence Server can now negotiate IPv4 and IPv6 destinations for media in SIP, whether IPv4 or IPv6 is being used as the transport.

The TelePresence Server now supports the ANAT semantics (Alternative Network Address Types) to establish media streams to both IPv4 and IPv6 addresses within a SIP call. The ANAT semantics are also used by Cisco Unified Communications Manager.

API improvements

The XML-RPC API has been extended in this release to support the new features. There are also improvements to the data returned in some API methods, and better coverage for licensing features that were previously only available via the web interface.

The API maintains backward compatibility with version 3.1. See the Cisco TelePresence Server API reference for details of the following changes:

- Reporting on the state of conferences and participants has been improved as follows:
  - Participant deletions can be requested per conference
  - Connection state of enumerated participants is reported
  - Current presenter is reported
  - A new participant enumeration has been added. The new method returns more detailed information on each connected participant, for example the participant's encryption status and media status.
- New methods have been added to control the feature keys and license keys on the TelePresence Server. An API user can now query, add, and delete these keys.

Third Party Interop feature key requirement lifted

In this release, the TelePresence Server no longer requires the *Third Party Interop* feature key to host conferences with multi-screen endpoints that are not third party interoperable.

In previous releases, the TelePresence Server would have required this key to host conferences with all multi-screen endpoints *except*:

- Cisco TelePresence System T3
- TIP-compatible endpoints (eg. CTS).

In previous releases, the TelePresence Server would also have required the *Third Party Interop* key to host multi-call participants, most notably participants using PSTN audio with the WebEx Enabled TelePresence solution. The key is no longer required for such multi-call participants.

Scalability improvements

Increased calls per unit

Note: This feature is only available in the remotely managed mode of TelePresence Server operation. It is not available in the locally managed mode.

Note: This feature requires Cisco TelePresence Conductor XC2.3.

The maximum number of calls that a TelePresence Server - or cluster of TelePresence Servers - can concurrently process has been raised from 104 to 200. The maximum number of participants in a conference is still 104, although this can be extended by cascading the conference.

The higher call limit does not imply changes to media processing or licensing limits; rather, it makes the TelePresence Server adaptable to scenarios that scale the number of low-resource calls (eg. one blade for 200 audio calls) as well as those that scale the number of higher-resource calls (eg. 200 360p calls on a three-blade cluster).

When hosting resource-intensive calls, the 200 calls limit will not be reached. For example, either the media processing limit or the licensing limit will be reached first if you try to connect 200 720p calls.

Dynamic resource optimization improvements

Note: This feature is only available in the remotely managed mode of TelePresence Server operation. It is not available in the locally managed mode.

This feature requires a management system that controls the TelePresence Server via its API. This discussion refers to the Cisco TelePresence Conductor and its user interface.

Cisco TelePresence Conductor allocates screen licenses to calls based on the TelePresence Server's reports of what the endpoints require.

The reports are affected by several factors:

- The **Participant quality** setting of the Conductor's conference template, provides an upper limit to the number of screen licenses that can be allocated to a participant for video and audio
- The **Content quality** setting of the Conductor's conference template, which provides an upper limit to the number of screen licenses that can be allocated to a participant for content (also known as 'extended video'). TelePresence Server honors this limit when calculating the screen license requirement, so that content quality does not suffer if the call is optimized down.
- The endpoint's advertized maximum resolution (behavior in previous releases; TelePresence Server's response to this factor is not configurable)
- The endpoint's advertized receive bandwidth (new in this release; TelePresence Server's response to this factor is now configurable via API)

You can define the participant quality and content quality settings in the conference template. When an endpoint is joining the conference, the TelePresence Server negotiates with endpoints to calculate how many screen licenses are required to fulfil the endpoint's request, within the limits provided by Conductor. The TelePresence Conductor then grants those resources to the call.

Prior to this release, the TelePresence Server only considered the maximum resolution advertized by the endpoints when doing this calculation. In this release, TelePresence Server calculates the resources required for a particular call based on two aspects of the endpoint's advertized capabilities; the maximum resolution (as previously) and the receive bandwidth. The TelePresence Server then chooses the lower of the two resulting screen license requirements to report to Cisco TelePresence Conductor.

The benefit is more concurrent calls for the same number of screen licenses. The management system can reclaim resources if a call does not have enough bandwidth to support the requested resolution.

In addition to limiting the Participant quality and Content quality, you can now choose how aggressively the TelePresence Server pursues resource efficiency when considering the receive bandwidth, by setting the *optimizationProfile*.

There are five settings for optimizationProfile; one that disables the feature, causing the TelePresence Server to behave as it did in previous releases, and then four levels that control the balance between quality of experience and efficiency of resources. The optimizationProfile parameter, which is passed to the API during conference creation, takes one of the following values:

Table 5: Optimization profiles enumerated type

`optimizationProfile` value	Description
`maximizeEfficiency`	Screen licenses are conserved aggressively. This value gives the most calls for the available resources.
`favorEfficiency`	This is a balance of efficiency and experience that favors conserving screen licenses over attempting to grant the requested resolution.
`favorExperience`	Default. This is a balance of efficiency and experience that favors granting the requested resolution over conserving screen licenses.

Table 5: Optimization profiles enumerated type (continued)

`optimizationProfile` value	Description
`maximizeExperience`	Screen licenses are more readily allocated. This value gives the best experience of the four profiles. If you disable the optimization by bandwidth (by setting `optimizationProfile` to `capabilitySetOnly`), calls will be capable of higher resolutions at lower bandwidths but the inefficency in allocation could well outweigh the benefit.
`capabilitySetOnly`	This is the behavior of TelePresence Server 3.1. The TelePresence Server only considers the endpoint's maximum advertized resolution when reporting its screen license requirement to the managing system; it does not attempt to report resources based on the endpoint's advertized receive bandwidth.

The following diagram illustrates how the TelePresence Server will report requirements for the different optimization profiles and the different bandwidths. The diagram assumes that the conference's Participant quality is set to the maximum possible (1080p30 or 720p60). There are two horizontal bars for each profile, representing two of Conductor's possible Content quality limits. The upper bar represents the maximum Content quality (1080p30) and the lower represents a more commonly used Content quality (720p5).

Figure 8: Screen license requirements by advertized receive bandwidth, for different optimization profiles and content quality

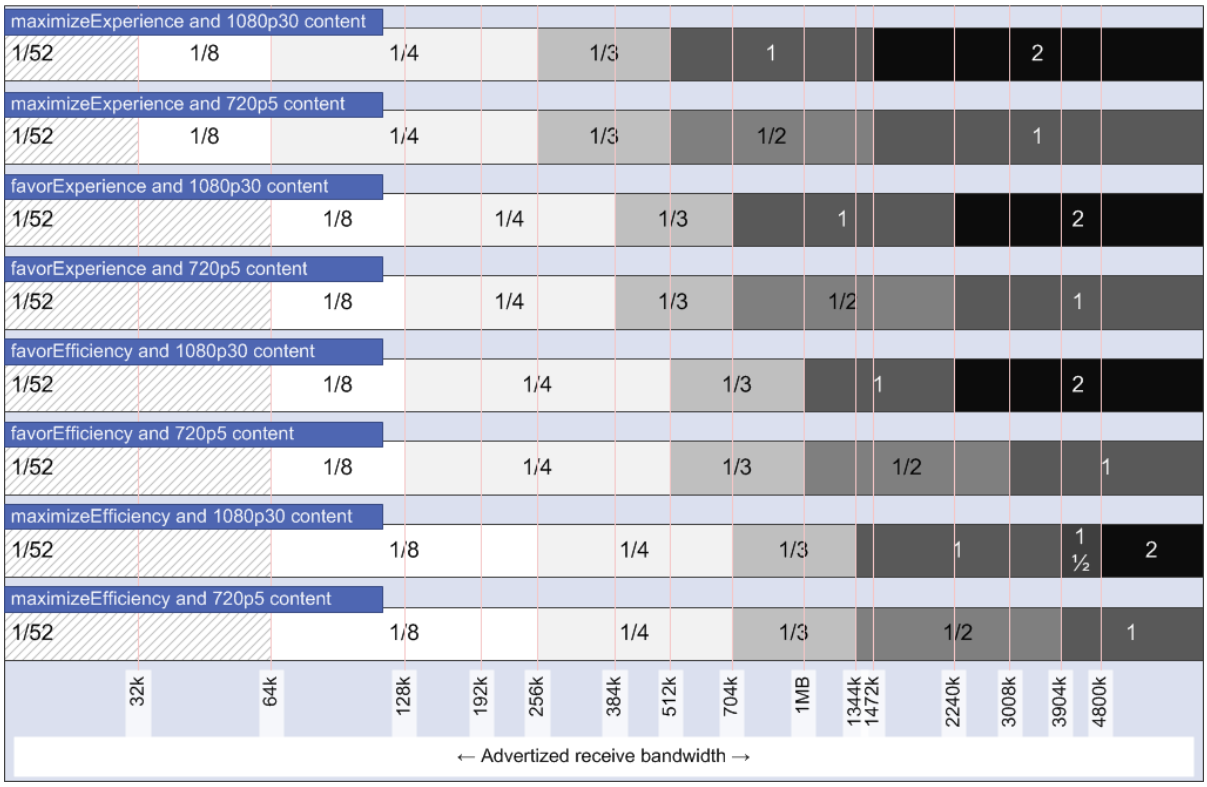


Figure 9: Key to the previous chart

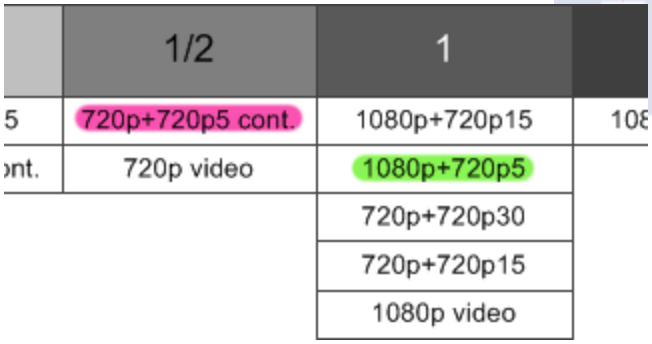
1/52 license	1/8 license	¼ license	1/3 license	½ license	1 license	1 ½ licenses	2 licenses
Audio-only	360p video	480p	480p+720p7.5	720p+720p5 cont.	1080p+720p15	1080p+720p30	1080p+1080p
		360p+720p5 cont.	480p+720p5 cont.	720p video	1080p+720p5		
					720p+720p30		
					720p+720p15		
					1080p video		

How to read the chart:

The shading levels on the chart represent the fractions/multiples of screen licenses that the TelePresence Server reports to the managing system for the given bandwidth ranges and content quality limits. The key relates types of calls to each of those levels.

There are two horizontal bars for each profile; the upper bar shows the reported licenses when the conference content quality is set to 1080p30 on the Conductor; the lower bar shows the reported licenses when the Conductor limits the conference content quality to 720p5. The Conductor has two intermediate content quality levels that are not shown.

Table 6: Example of how to read this chart

On Conductor: Content quality is set to 720p5, Participant quality is set to 1080p30 The endpoint: Requests 1080p30 video with 720p5 content, at 2048kBps. The key shows that this type of call requires 1 screen license. The bandwidth of the call is limited to 2MBps (2048kBps), so we're looking at the region between 1472kBps and 2240kBps on the chart. Maximum content is 720p5, which means we should consider the lower of the two bars for each profile.	
On the chart, the only profile that allows 1 screen license in the 2048k bandwidth region, in the 720p5 bar, is maximizeExperience. So, if the conference is configured to max 720p5 content and maximizeExperience (green highlight on the diagram to the right), the TelePresence Server tells Conductor that this call requires one screen license and the endpoint will get the requested experience.	
However, if the conference is configured to any of the other three profiles (pink highlights on the diagram), the TelePresence Server will report that this call should only receive half a screen license. On the key we can read that with half a screen license, the endpoint will actually receive 720p30 video with 720p5 content (see below). The benefit is that half a screen license is reclaimed.	

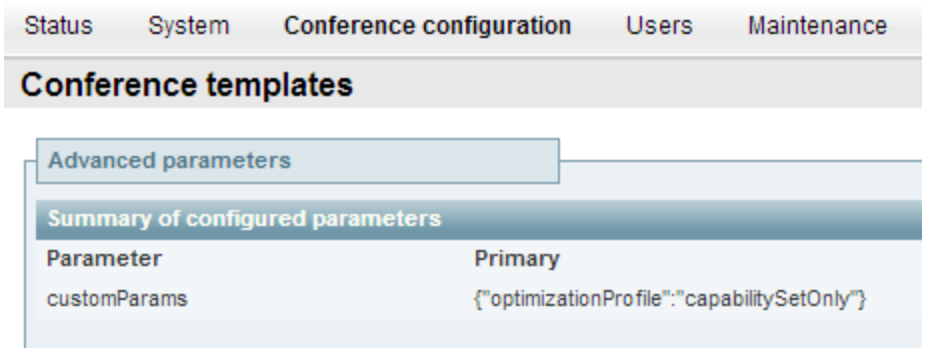
Conductor support

The Cisco TelePresence Conductor supports changing the optimization profile by adding a custom parameter to the TelePresence Server template. You will need to specify the custom parameter if you want Conductor to use a profile other than the TelePresence Server's default, which is *favorExperience*.

For example, to revert the template to use the previous TelePresence Server behavior:

1. Go to **Conference configuration > Conference templates** and select the appropriate template
2. In the template's **Advanced parameters**, click **Edit**
3. Add the custom parameter and value pair **`{"optimizationProfile":"capabilitySetOnly"}`**

Figure 10: **Advanced parameters** section of template configuration, showing the custom **`optimizationProfile`** parameter



OVA and specification changes for Cisco TelePresence Server on Virtual Machine

The Cisco TelePresence Server on Virtual Machine deployment configurations have changed in this release, allowing the application to run on a variety of different hardware platforms. There are now two OVA configurations supporting deployment to virtual machines using 8 or 16 CPUs. The number of vCPUs must be mapped 1:1 with the number of physical CPUs.

These changes improve co-residency with other UC applications. For example, the TelePresence Server can now be deployed on a virtual machine with 8 CPUs so that it can be bundled with Cisco Business Edition 6000.

Note: We no longer support the 20 vCPU (10 physical CPUs) configuration from previous releases. This configuration is now replaced by the 16 Cores configuration (16 physical CPUs).

The upgrade to version 4.0(2.8) will work on a 20 vCPU VM running version 3.1, but the new configuration requires 16 dedicated physical CPUs. The new 16 Cores configuration can also support more screen licenses than the previous 20 vCPU configuration, so you may wish to acquire more screen licenses. See Upgrading the Cisco TelePresence Server on Virtual Machine [p.31].

Recommended platforms

The following physical hosts are tested and officially supported in this release, although the TelePresence Server should run on VMware machines on any physical hosts that meet the minimum specifications:

- C220 M3S (SFF) TRC#3 (supported for Business Edition 6000 bundle - BE6000 HD Server)
- C240 M3S (SFF) TRC#1 (previously introduced)
- C220 M3S (SFF) TRC#2 (supported for Business Edition 6000 bundle - BE6000 MD Server)

See http://docwiki.cisco.com/wiki/UC_Virtualization_Supported_Hardware for details of these configurations.

Specifications-based platform

The specifications for a host that is not one of the tested reference configurations have improved in this release; the new specifications are:

- 2 x Intel Xeon processor E5-2600 series with 2.4GHz or faster processor
- At least 8 GB RAM to be dedicated to Cisco TelePresence Server on Virtual Machine
- At least 53 GB of local or SAN storage
- IOPS (input/output operations per second) and storage perfomance must meet or exceed the following requirements:

  Table 7: Storage performance requirements

Mean # IOPS	Mean read latency	Mean write latency	Peak read latency	Peak write latency
6	4ms	10ms	15ms	15ms

- 1 GigE NIC
- The OVA is pre-configured to have 8GB of RAM, and 8 or 16 CPUs
- No oversubscription of resources is allowed, even if hyperthreading is enabled
- Hypervisor version ESXi 5.0 Update 1, or ESXi 5.1
- VMware client to access Hypervisor directly or through Virtual Center to deploy the OVA

Conferencing capacity changes

Table 8: Cisco TelePresence Server on Virtual Machine capacity by release version and number of vCPUs

Number of CPUs	Capacity in 3.1 (1.82)	Capacity in 3.1 (1.96)	Capacity in 4.0(2.8)
8 (16 vCPU)	Not supported	8 HD calls	Not supported
10 (20 vCPU)	12 HD calls	12 HD calls	Not supported. We recommend upgrading software and changing VM configuration, see Upgrading the Cisco TelePresence Server on Virtual Machine [p.31]
8 (8 vCPU) (BE6k)	Not supported	Not supported	8 HD calls (New configuration)
16 (16 vCPU)	Not supported	Not supported	16 HD calls (New configuration)

For example, on an 8 CPU virtual machine, the TelePresence Server can use 4 screen licenses and this capacity can be used to process up to 8 HD (720p30) calls, or a larger number of lower resource calls. See the Platform licensing comparison [p.20] for more examples of how screen licenses translate into conferencing capacity.

Virtual machines with intermediate numbers of vCPUs are treated as the lower of the supported levels for the purpose of running TelePresence Server. That is, if there are between 8 and 15 vCPUs, the TelePresence Server can only use 4 screen licenses. If there are 16 or more vCPUs, the TelePresence Server can use up to 8 screen licenses. For example, after upgrading a VM with 20 vCPUs to this version, and changing the number of vCPUs to 16, the TelePresence Server can use up to 8 screen licenses. You must have a 1:1 mapping from vCPUs to physical cores.

Note: Adding more vCPUs will not increase the TelePresence Server's ability to use screen licenses beyond the supported levels.

Support for cascaded conferences

Note: This feature is only available in the remotely managed mode of TelePresence Server operation. It is not available in the locally managed mode.

Note: This feature is not supported on Cisco TelePresence Conductor XC2.3.

The TelePresence Server software now supports cascading, which is the ability for one TelePresence Server to invite another TelePresence Server into a conference.

The cascading feature allows for up to 500 participants in a single conference. This is a nominal limit for testing and support purposes - as it is the maximum number supported by the roster list - but there is no fixed limit applied by the software. You may be able to achieve higher numbers but we cannot guarantee support beyond the nominal limit.

The audio, video, and content contribution from an endpoint connected to one of the linked TelePresence Servers will be shown to all participants in the cascade. There can only be one master and one slave in each cascade link, but you can configure multiple links to create a star (hub and spoke) topology.

Cascade links must be configured via the TelePresence Server's remotely managed mode API.

Cascading is supported on all TelePresence Server platforms, although it is not supported in locally managed mode. Cascading is not supported between a TelePresence Server and other conference bridges, eg. Cisco TelePresence MCU Series.

Security improvements

Console password

Password protection has been added to the TelePresence Server console (the serial console on physical hardware or the virtual machine console). When the feature is enabled, the console does not respond until the user logs in with TelePresence Server administrator credentials.

The feature is disabled by default, to prevent locking out users who upgrade to this version, but we recommend enabling it immediately after upgrade. You can toggle the password protection via the web interface but this feature is not exposed via the API.

Static ARP and NDP

Static ARP (Address Resolution Protocol) and NDP (Neighbor Discovery Protocol) enable administrators to manually bind MAC addresses to IPv4 or IPv6 addresses respectively. This feature enhances security by giving administrators certainty over the binding, which can potentially be compromised if it is automatically resolved.

On the TelePresence Server console, administrators can manually create, edit, and delete static ARP or NDP entries, or show a list of current entries. When resolving an IP address to a MAC address, the TelePresence Server first tries to do so using the static binding table, but will fall back on ARP (or NDP) if there is no entry for the requested IP address.

You can only access the static bindings feature via the console.

Netstat

The TelePresence Server now provides a real time list of all its network connections. This information is available via the **`netstat`** command on the console or on the **Network > Netstat** page of the web interface.

For each connection, the netstat list contains the following information about each end:

- The IP address or hostname (requires external DNS)
- The port or service
- Whether the connection uses TCP or UDP, and the associated internet protocol address scheme (4 or 6)

Ephemeral port range

The TelePresence Server now gives the administrator control over the range of ephemeral ports used for media connections. This is configurable on the **Network > Services** page of the web interface.

The configurable range defaults to its previous value (49152 - 65535), so that upgraded TelePresence Servers do not experience an unexpected restriction. The ephemeral port range may not start at a value lower than your highest configured service port, and the maximum range is 10000 - 65535. We recommend a range of at least 5000 ports to adequately provide for the theoretical limit on connections to the TelePresence Server.

Resilience and diagnostics improvements

Intelligent flow control of incoming streams

A new rate adaption algorithm is now being used to respond to network conditions that could affect video quality. These conditions include limited bandwidth, known packet loss level, and burstiness in packet loss.

The TelePresence Server uses the algorithm to recommend a bandwidth restriction to the stream's source, based on the recent performance of that stream with respect to the network conditions. The TelePresence Server continues to respond to changes if the chosen level does not improve the experience or is unnecessarily restrictive on the incoming stream.

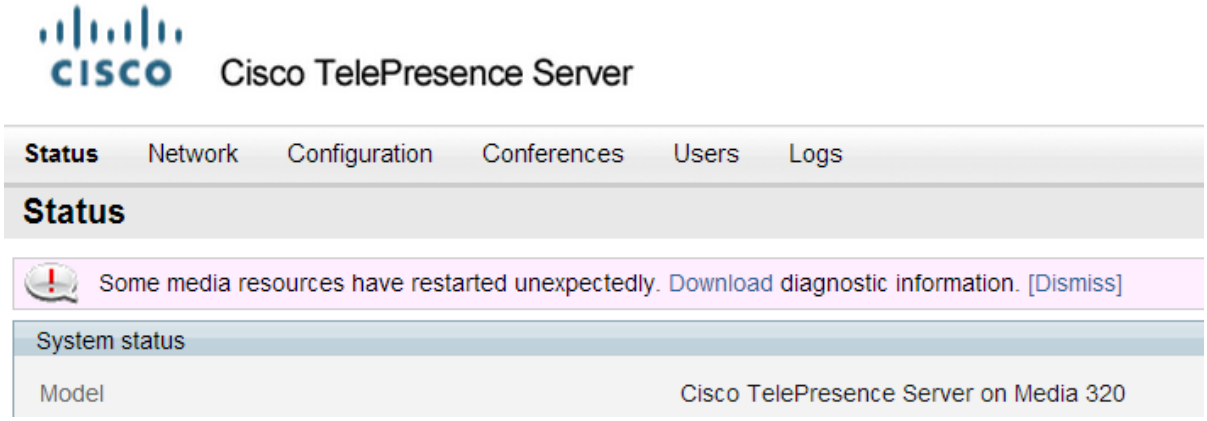
Resilience to media processor restart

Resilience to individual media processor restart was partially introduced in TelePresence Server version 3.1 for the Multiparty Media 310/320 models. This feature is now improved and also available on the TelePresence Server MSE 8710, TelePresence Server 7010, and Cisco TelePresence Server on Virtual Machine platforms.

All TelePresence Server platforms are now more resilient in the unusual circumstances of an individual media processor failure. If a single media processor restarts it will not cause the whole device to restart. This means that the other parts of the device software can maintain the state of the conferences—except for the tasks performed by that particular processor—while recovering the processor gracefully.

A notification on the web interface alerts the administrator to the restart, as follows:

Figure 11: The media resource restart notification banner



Note: Some participants may experience a loss of media in the unlikely event of a media processor restart, although it should come back after a pause of about 30 seconds.

On a virtual machine, a media processor restart will affect all participants but should take less than 5 seconds to recover.

If a media processor restarts repeatedly, it may still cause the TelePresence Server to restart.

In the case of a media processor restart, the TelePresence Server isolates the processor as well as it can, while rebooting the processor, as follows:

- The TelePresence Server tries to reallocate tasks from the restarting processor to other media resources if available. Participants may see a glitch while the tasks are recovered
- If there are no spare media resources available, the affected participants will experience a loss of video but the calls will stay up while the affected processor reboots
- The processor recovers and video to the affected participants will resume

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 9: TelePresence Server conferencing capacity on various platforms

Call type description			Screen licenses required per call	Maximum calls by hardware type (with licenses to provide 100% of capacity)								
Main video	**Audio**	**Content**		**8 Cores VM**	**Media 310 or MCU 5310**	**16 Cores VM**	**Media 320 or MCU 5320**	**7010**	**MSE 8710 or MCU MSE 8510**	**Media 400v‡**	**Biggest appliance cluster (two appliances)**	**Biggest blade cluster (four blades)**
				4 screen licenses	**5 screen licenses**	**8 screen licenses**	**10 screen licenses**	**12 screen licenses**	**12 screen licenses**	**14 screen licenses**	**20 screen licenses**	**48 screen licenses**
-	Mono	-	1/52	200*	200*	200*	200*	200*	200*	200*	200*	200*
360p30†	Mono	In main video	⅛	33	41	65	81	97	97	113	163	200*
360p30†	Stereo	720p5	¼	16	20	32	40	48	48	56	81	195
480p30	Stereo	In main video	¼	16	20	32	40	48	48	56	81	195
480p30	Stereo	720p5	⅓	12	15	24	30	36	36	42	61	146
720p30	Stereo	720p5	½	8	10	16	20	24	24	28	40	97
720p30	Stereo	720p30	1	4	5	8	10	12	12	14	20	48
1080p30	Stereo	720p15	1	4	5	8	10	12	12	14	20	48
720p60	Stereo	720p15	1	4	5	8	10	12	12	14	20	48
1080p30	Stereo	720p30	1 ½	2	3	5	6	8	8	9	13	32

Table 9: TelePresence Server conferencing capacity on various platforms (continued)

Call type description			Screen licenses required per call	Maximum calls by hardware type (with licenses to provide 100% of capacity)								
Main video	**Audio**	**Content**		**8 Cores VM**	**Media 310 or MCU 5310**	**16 Cores VM**	**Media 320 or MCU 5320**	**7010**	**MSE 8710 or MCU MSE 8510**	**Media 400v‡**	**Biggest appliance cluster (two appliances)**	**Biggest blade cluster (four blades)**
				4 screen licenses	**5 screen licenses**	**8 screen licenses**	**10 screen licenses**	**12 screen licenses**	**12 screen licenses**	**14 screen licenses**	**20 screen licenses**	**48 screen licenses**
Three-screen 720p30	Multichannel	720p5	1½	2	3	5	6	8	8	9	13	32
Three-screen 720p30	Multichannel	720p30	2	2	2	4	5	6	6	7	10	24
1080p30	Stereo	1080p30	2	2	2	4	5	6	6	7	10	24
Dual-screen 1080p30	Stereo	720p30	2	2	2	4	5	6	6	7	10	24
Three-screen 1080p	Multichannel	720p30	3	1	1	2	3	4	4	4	6	16
Three-screen 1080p	Multichannel	1080p30	4	1	1	2	2	3	3	3	5	12
Four-screen 1080p	Stereo	1080p30	4	1	1	2	2	3	3	3	5	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. It cannot be co-resident with any other UC application (unlike the 8-core and 16-core VMs that run at 2.4GHz minimum and can be co-resident).

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 issues

The following issues were found in previous releases and are resolved in 4.0(2.8).

Resolved since version 4.0(1.57)

Identifier	Description
CSCup45147	When using a CTS or TX endpoint to connect an audio add-in participant, it was possible that a TelePresence Server could unexpectedly restart. This issue is now resolved.
CSCun60259	In some instances it was possible to disable IPv4 over an IPv4 connection, and disable an IPv6 over an IPv6 connection. This issue is now resolved.

Identifier	Description
CSCup22629	**Symptom:** The following Cisco products: Cisco TelePresence Server 8710 / 7010 Cisco TelePresence Server on Media 3x0 Cisco TelePresence Server on Virtual Machine include a version of openssl that is affected by the vulnerabilities identified by the Common Vulnerability and Exposures (CVE) IDs: CVE-2014-0195 - DTLS invalid fragment vulnerability CVE-2014-0221 - DTLS recursion flaw CVE-2014-0224 - SSL/TLS MITM vulnerability CVE-2014-3470 - Anonymous ECDH denial of service This bug has been opened to address the potential impact on this product. **Conditions:** HTTPS or SIP/TLS in use. For CVE-2014-3470 to apply, certificate verification for outbound connections must not have been enabled. **Workaround:** Only CVE-2014-3470 can be avoided by setting up trust stores and enabling certificate verification for outbound connections, this will disable anonymous ciphers. Workaround to other vulnerabilites are not available. **Further Problem Description:** Affected TS versions: 2.3(1.55), 2.3(1.57), 2.3(1.58), 3.0(2.24), 3.0(2.46), 3.0(2.48), 3.0(2.49), 3.1(1.80), 3.1(1.82), 3.1(1.95), 3.1(1.96), 3.1(1.97), 3.1(1.98), 4.0(1.57) **PSIRT Evaluation:** The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 10/9.5: https://intellishield.cisco.com/security/alertmanager/cvss?target=new&version=2.0&vector=AV:N/AC:L/Au:N/C:C/I:C/A:C/E:F/RL:U/RC:C The Cisco PSIRT has assigned this score based on information obtained from multiple sources. This includes the CVSS score assigned by the third-party vendor when available. The CVSS score assigned may not reflect the actual impact on the Cisco Product. Additional information on Cisco's security vulnerability policy can be found at the following URL: http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html
CSCuo85864	In previous releases of the virtual TelePresence Server it was possible to upload a configuration file which would disable the need for administrator login. This issue is now resolved.
CSCuo93120	In calls between a remotely managed Cisco TelePresence Server and a Cisco TelePresence endpoint running TC software that was registered to Cisco Unified Communications Manager via collaboration edge, Far End Camera control (FECC) did not work after the endpoint performs a hold and resume. This issue is now resolved.

Resolved since version 3.1(1.97)

Identifier	Description
CSCuo21468	**Symptom:** The following Cisco Telepresence products: Cisco TelePresence Server 8710, 7010 Cisco TelePresence Server on Multiparty Media 310, 320 Cisco TelePresence Server on Virtual Machine include a version of openssl that is affected by the vulnerability identified by the Common Vulnerability and Exposures (CVE) ID CVE-2014-0160. This bug has been opened to address the potential impact on this product. **Conditions:** Device with default configuration and running TelePresence server software 2.3(x), 3.0(x) or 3.1(x) **Workaround:** Not currently available. Customers that do not require of the new functionality present on TelePresence server software 2.3(x), 3.0(x) or 3.1(x) may evaluate the possibility to downgrade affected devices to TelePresence server release 2.2, which is not affected by this vulnerability. **Further Problem Description:** Additional details about this vulnerability can be found at http://cve.mitre.org/cve/cve.html **PSIRT Evaluation:** The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 5/5: https://intellishield.cisco.com/security/alertmanager/cvss?target=new&version=2.0&vector=AV:N/AC:L/Au:N/C:P/I:N/A:N/E:H/RL:U/RC:C The Cisco PSIRT has assigned this score based on information obtained from multiple sources. This includes the CVSS score assigned by the third-party vendor when available. The CVSS score assigned may not reflect the actual impact on the Cisco Product. CVE-2014-0160 has been assigned to document this issue. Additional information on Cisco's security vulnerability policy can be found at the following URL: http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html
CSCui23212	The TelePresence Server's maximum packet size restriction did not behave as expected. This issue is now resolved.
CSCun27820	The TelePresence Server could previously request flow control on the received video stream based on the size at which the stream was viewed by others. This behavior was considered too aggressive when used with more recent flow control features. This has been resolved by applying the flow control request only when the stream is not being viewed at all, rather than when it is viewed at small resolutions.
CSCun27995	In some circumstances the following error messages could display: **`DSP xxxx, object 00000000: DSP xxxx vs_surface store alloc x failures in last five seconds`** (where **`x`** represents a number, such as **`DSP 8496, object 00000000: DSP 2130 vs_surface store alloc 2 failures in last five seconds`**). This issue is now resolved.
CSCun68517	In some rare circumstances, a TelePresence Server could restart while trying to encode a JPEG snapshot image with an invalid size.

Identifier	Description
CSCun70776	The TelePresence Server event log was recording many messages of the form "`RTCP : Info : call 1615, RTP session 2: message failed validity checks (invalid payload)`". This issue is now resolved by reducing the severity of invalid messages.
CSCuj26833	On 7010 and MSE 8710 TelePresence Server platforms, the application's CDR log was not properly recording remote teardown of H.323 calls. This issue is now resolved.
CSCul55216	In some rare circumstances, a TelePresence Server could restart after receiving an unexpected internal packet. This issue is now resolved.
CSCum07100	When a CTS endpoint tried to join a TelePresence Server conference that had only audio ports available, the CTS would join the conference without hearing any audio. This issue is now resolved.
CSCun86369	The TelePresence Server would retransmit video received from Lync in the incorrect aspect ratio, but only when significant horizontal motion was recorded by Lync. This issue is now resolved.
CSCue88488	The TelePresence Server was too aggressively flow controlling the video from TC series endpoints while there was a constant packet loss on the line. This issue is now resolved.
CSCul94805	The TelePresence Server could unexpectedly restart during combinations of call defer and automatic reconnection of dropped calls. This issue is now resolved.

Open issues

The following issues apply to this version of Cisco TelePresence Server.

Identifier	Description
CSCup59735	Cisco TelePresence Server on Virtual Machine requires 2.4 GHz or higher processors. If the processor speed is too low, there is no warning to indicate that the processor is not supported and that video calls cannot be made.
CSCup49756	On an 8 vCPU Cisco TelePresence Server on Virtual Machine the recommended maximum 360p call participant capacity is 32. If a 33rd endpoint joins, call quality issues may occur.

Identifier	Description
CSCuo72774	**Symptom:** If a new trust store is uploaded to a TelePresence Server, it will not take effect until after a system reboot. This means that certificates will continue to be checked and verified against the old trust store and undesired connections may still be established. **Conditions:** This issue will be encountered any time the trust store is updated without a reboot. **Workaround:** Reboot the system to ensure the new trust store is used and that the correct set of CAs are being used for certificate verification (if enabled).
CSCun21354	When calls on a SIP trunk between Cisco Unified Communications Manager and TelePresence Server experience a glare condition, the calls may fail because Unified CM does not respond properly to the SIP 491 message (Request Pending).
CSCun53448	A TelePresence Server may become inaccessible if the network port speeds are specifically configured to 10 Mbit/s. We recommend that you do not configure the Ethernet port speed to 10 Mbit/s.
CSCun62590	Attempting to clone a virtual machine that is running Cisco TelePresence Server on Virtual Machine while it is powered on causes the virtual machine to stop responding. This type of cloning is not currently supported and we recommend that you power off the virtual machine before you clone it.
CSCun53487	When it starts up, Cisco TelePresence Server on Virtual Machine synchronizes its time with the time of the ESX host. This behavior causes system logs to be unsynchronized between the host and the TelePresence Server if you configure a different offset on TelePresence Server. You can mitigate this issue by setting the TelePresence Server time to the same time as that of the host; for example, by setting them both to UTC.

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 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 should only be undertaken when following the best practice guidelines from VMware. 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 4.0(2.8)

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_4.0_2.8.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 file has a **.ova** extension but the upgrade package has a **.tgz** extension, for example, **Cisco_tsVirtualMachine_4.0_2.8.ova** and **Cisco_tsVirtualMachine_4.0_2.8.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 blades in 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.

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.30], 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 TelePresence Server web interface, you need to adjust the number of physical cores dedicated to the virtual machine and may need to adjust the RAM. These changes require that you power off the VM.

To upgrade Cisco TelePresence Server on Virtual Machine:

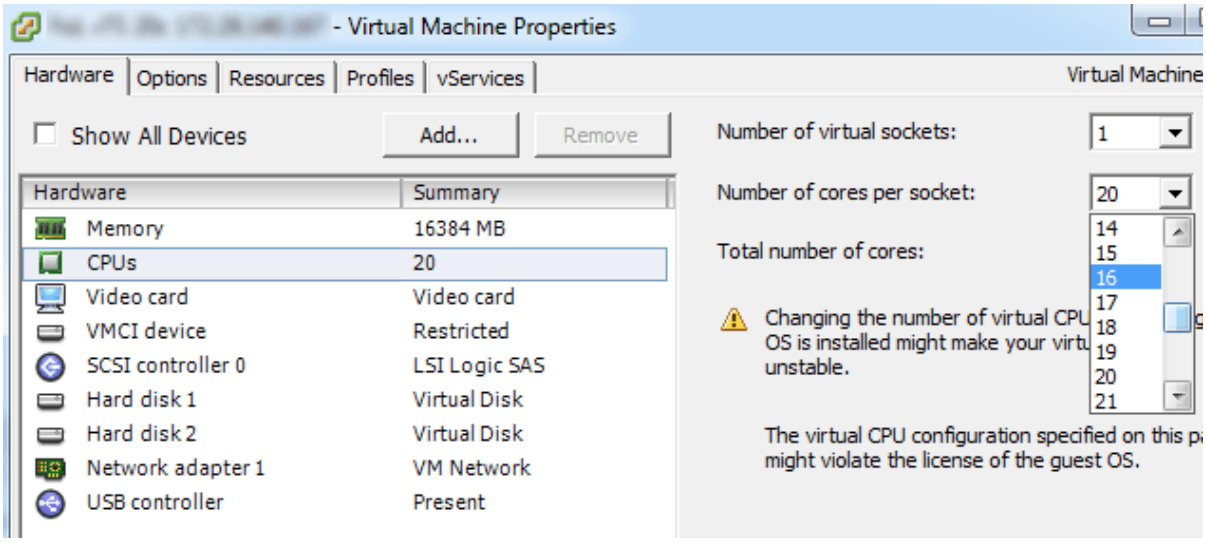
Table 10: Upgrade paths for Cisco TelePresence Server on Virtual Machine

	Higher spec. configuration		Lower spec. configuration	
Upgrade	**From this**	**To this**	**From this**	**To this**
Software version	3.1(1.96)	4.0(2.8)	3.1(1.96)	4.0(2.8)
Physical CPUs	10	16	8	8
Virtual CPUs	20	16	16	8
RAM	16	8	16	8
Maximum screen licenses	6	8	4	4

Note: The maximum number of screen licenses that the higher spec configuration 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.20] for details of the capacity given by the new configurations.

1. Follow the software Upgrade instructions [p.33], 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**

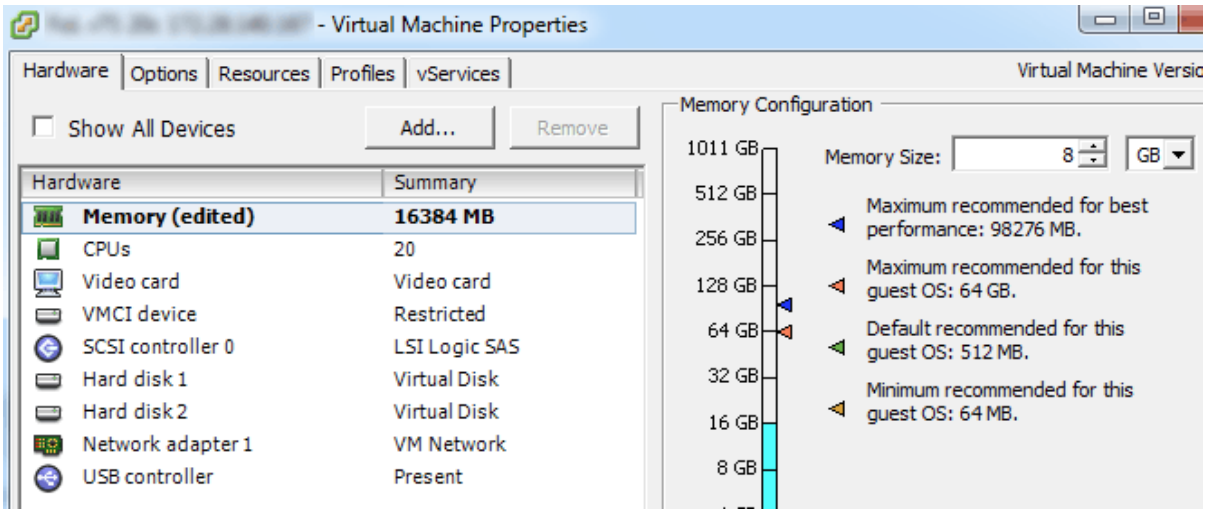
c. Right-click the TelePresence Server virtual machine and select **Edit Settings…**
d. On the **Hardware** tab, click **CPUs**
e. From the **Number of cores per socket** list, select the required number of virtual CPUs (vCPUs)



Note: 16 vCPUs should map to 16 physical CPUs since oversubscription is not supported.

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 16 GB to 8 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 8 GB



Note: 8 GB vRAM should map to 8 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.30] 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 4.0(2.8)

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.

Upgrading the font (optional)

Note: These instructions apply only to TelePresence Server 7010 and MSE 8710 platforms. The Media 310/320 platforms always have the font pre-installed and there is no way to replace or remove it.

Your device may be shipped with the TrueType font pre-installed. You can check this on the **Status** or **Configuration > Upgrade** page.

If the font is not present, and you want to use TrueType text rendering on your device instead of the default text rendering method, you must upload the font file. You can get this file, called **ts-font_3_0_2_49**, from the Software download page for 3.0(2.49).

Note: You should do this when the device is not heavily loaded. Also, you must use the supplied font; do not attempt to load a different font file.

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. Under **Font upgrade** at **New font file** browse to locate the downloaded font file.
5. Select the font file.
6. Click **Upload font**.
   After a short while, the **Font file status** changes to *Present*.

Removing the font

1. If you want to revert to the default text rendering, click **Delete font**.
2. Confirm that you want to remove the font file.
   The **Font file status** changes to *Not present*.

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 11: TelePresence Server release notes revisions

Date	Revision	Description
July 2014	09	Revised wording for snapshotting and cloning limitation
July 2014	08	Snapshotting and Cloning not supported added to Limitations
June 2014	07	4.0 Maintenance release
April 2014	06	Cisco TelePresence Server 4.0 release