Cisco TelePresence Server 4.4(1.20)

Release Notes

First Published: January 2018

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 4.4(1.20)

Version 4.4(1.20) is a maintenance release. For more information, see Resolved and Open Issues, page 6. It also introduces the following new features and changes:

Table 1 New feature support by TelePresence Server platform in 4.4(1.20)

Feature name	7010 & MSE 8710	Media 310/320	Virtual Machine	Media 820
Minimum TLS/DTLS Version Changes, page 1	Yes	Yes	Yes	Yes
H.323 Removed (8710 only), page 2	Yes	No	No	No

Minimum TLS/DTLS Version Changes

TLS versions 1.0 and 1.1 have been deprecated as insecure by the wider security community, and as a result TLS 1.2 or later is now recommended for all encrypted sessions. The previous TelePresence Server version 4.4(1.16) supported all TLS versions so could not enforce the recommended TLS version.

Therefore to support customers who require this level of security, the minimum version of TLS and DTLS is now set to 1.2 as default. If required (typically for compatibility reasons with legacy equipment) the minimum TLS and DTLS versions can be manually configured back to 1.0 via new drop-down options on the **Network Settings** page of the

Web user interface. Before upgrading, check that all browsers and other equipment which must connect to TelePresence Server supports TLS 1.2 (see Upgrading to 4.4(1.20), page 11 for details).

Note: Currently CTS, TX9000 and ix5000 endpoints do not support DTLS 1.2. If DTLS 1.2 is enforced on TelePresence Server then media will not be encrypted and there may be no video when entering the lobby screen. We recommend that TelePresence Server is configured to allow DTLS 1.0/1.1 when using secure mode with these endpoints.

In normal deployments, TelePresence Server and endpoints are connected via VCS or CUCM. However, if you want to use direct SIP TLS 1.2 calls between TelePresence Server and Cisco endpoints using CE 9 software, make sure to enable self-certificate option for SIP in the endpoint configuration. If this is not enabled then the endpoint only offers anonymous ciphers and will not be able to connect with TelePresence Server using TLS 1.2.

H.323 Removed (8710 only)

H.323 protocol support is removed from the 8710 in 4.4(1.20). (Other platforms have never had H.323 protocol support.)

H.323 protocol is used as an alternative for SIP. Other Cisco products can interwork H.323 to SIP so it is no longer required in most deployments. It has been removed to improve the stability of the 8710 platform as the software memory requirements to support H.323 could result in “out of memory” issues. **Do not upgrade to 4.4(1.20) if H.323 support is still required by your deployment.**

Support for ESXi 6.5

Telepresence Server now supports ESXi 6.5.

New Features in Version 4.4(1.16)

Version 4.4(1.16) was a maintenance release that also introduced the following new feature:

Table 2 New feature support by TelePresence Server platform introduced in Version 4.4(1.16)

Feature name	7010 & MSE 8710	Media 310/320	Virtual Machine	Media 820
Content Channel Improvements, page 2	Yes	Yes	Yes	Yes

Content Channel Improvements

This release introduced a new API parameter `mediaTxShaping` to control the transmission profile of the content channel.

For more information, see the Version 4.4(1.16) API Guide at
http://www.cisco.com/en/US/products/ps11339/products_programming_reference_guides_list.html

New Features introduced in Version 4.4(1.9)

Version 4.4(1.9) introduced some new features to extend and improve the conference experience. This release is available on all TelePresence Server platforms.

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

Table 3 New feature support by TelePresence Server platform in Version 4.4(1.9)

Feature name	7010 & MSE 8710	Media 310/320	Virtual Machine	Media 820
Cisco TelePresence Server on Virtual Machine Improvements				

Table 3 New feature support by TelePresence Server platform in Version 4.4(1.9) (continued)

Feature name	7010 & MSE 8710	Media 310/320	Virtual Machine	Media 820
New Platform for TelePresence Server – Cisco Meeting Server 1000, page 3	No	No	Yes	No
SIP URI Expansion on Cisco TelePresence Server on Virtual Machine for WebEx, page 3	No	No	Yes	No
User Experience Improvements				
Join/Leave Meeting Notifications, page 3	Yes	Yes	Yes	Yes
Active Speaker Notification, page 4	Yes	Yes	Yes	Yes
OnePlusN Screen Layout Family, page 4	Yes	Yes	Yes	Yes
Audio Avatar Improvements, page 5	Yes	Yes	Yes	Yes

Cisco TelePresence Server on Virtual Machine Improvements

New Platform for TelePresence Server – Cisco Meeting Server 1000

This release introduces a new platform for the TelePresence Server software: the Cisco Meeting Server 1000 (CMS 1000).4.4(1.9) is the first release to support this platform. This gives an increased port capacity of 84 HD ports at 720p30 video + 720p5 content. This increased port capacity configuration (70 Hyperthread Core Cisco TelePresence Server) 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: To achieve the maximum port capacity, Cisco TelePresence Server on Virtual Machine must be the only VM on the Cisco Meeting Server 1000. It cannot be co-resident with any other UC application.

Note: Cisco Meeting Server 1000 requires ESXi 6.0 and virtual machine version 11.

SIP URI Expansion on Cisco TelePresence Server on Virtual Machine for WebEx

Cisco TelePresence Server on Virtual Machine can now handle SIP URIs up to 1024 characters. In previous releases this limit was 80 characters. Note that for all other TelePresence Server platforms the limit remains at 80 characters.

User Experience Improvements

This release features the following User Experience improvement:

Join/Leave Meeting Notifications

This release introduces an audio notification whenever anyone joins or leaves a video conference. Previously it was not always obvious that someone had joined, especially to audio participants who cannot see new participants arriving in the video layout.

The notifications are configurable on a per-conference level via the API. The default is for no notifications to be played. You can enable join and leave notifications separately. This feature can only be configured on TelePresence Conductor using Conductor's Advanced Parameters on a conference template.

To enable audio notifications to be played for a conference using the API:

1. On TelePresence Conductor, go to **Conference Configuration > Conference Templates** and find the template for the conference.
2. Go to **Advanced Parameters**, click **Edit**.
3. In the **Custom parameters** text box, enter the following text:
   `"audioJoinNotification":"all","audioLeaveNotification":"all"`
4. Click **Save**.

These parameters go in `flex.conference.create` or `flex.conference.modify`, and are reported in `flex.conference.query` on the TelePresence Server.

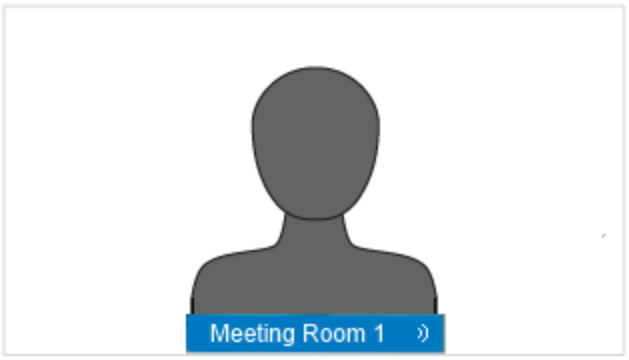
Any other Flex API controller can include these parameters at conference creation or by modifying an ongoing conference. See the Cisco TelePresence Server API 4.4 Reference Guide for more information.

Active Speaker Notification

This release introduces new active speaker notification:

- the name label of the active speaker was grey and is now blue, without animation.
- the "wave pulse" icon was blue and is now white, without animation.

Figure 1 New active speaker label



OnePlusN Screen Layout Family

This release introduces the new OnePlusN layout family. This new layout family can be configured as the default by Administrators via Conductor's Advanced Parameters. It can be selected by a conference participant cycling through all the layout families using DTMF 2 or 8. It can also be set as the default single-screen layout for a conference by using the Flex API.

The layout starts as “single” then automatically grows to onePlus5, onePlus7, onePlus9, and onePlus12 based on the number of participants, as follows:

- Full screen if there are 2 participants
- onePlus5 if there are 3, 4, 5, 6 or 7 participants
- onePlus7 if there are 8 or 9 participants
- onePlus9 if there are 10 or 11 participants
- onePlus12 if there are more than 11 participants

Figure 2 OnePlusN family layouts

To set this layout family as the default single-screen layout for a conference using the API:

1. On TelePresence Conductor, go to **Conference Configuration > Conference Templates** and find the template for the conference.
2. Go to **Advanced Parameters**, click **Edit**.
3. In the **Custom parameters** text box, enter the following text:
   `{"callAttributes": {"displayDefaultLayoutSingleScreen": "layoutOnePlusN"}}`
4. Click **Save**.

Audio Avatar Improvements

This release introduces changes to the audio avatar feature.

Audio avatars are static pictures used to give visual presence to participants that are audio only, or that have muted their video. This avatar provides a place to display a name label and indicate when the participant is speaking. Previously, if there were several such participants, large amounts of the screen could be taken up with avatars, instead of live video.

In this release, any video participants take priority and the TelePresence Server reduces the number of avatars (typically to just one) to maximize the screen space available for participants with video. This behavior is enabled by default.

Also, when one audio avatar stops speaking in favor of another, only the name label of the avatar changes. This behavior is enabled by default.

If you prefer the previous experience (as found in TelePresence Server 4.3, 4.2 and 4.1) where audio avatars are treated with equal importance to video participants, then you can configure the behavior for a conference using the API:

1. On TelePresence Conductor, go to **Conference Configuration > Conference Templates** and find the template for the conference.
2. Go to **Advanced Parameters**, click **Edit**.
3. In the **Custom parameters** text box, enter the following text: `{"displayAudioAvatarMode": "all"}`
4. Click **Save**.

Changes and Minor Enhancements

4.4(1.20) introduces the following changes:

3DES and IDEA Ciphers Removed

To align with security best practice and deprecation of less secure encryption standards, support for all remaining 3DES and IDEA ciphers has been removed in this release.

ECDHE Ciphers Added

ECDHE ciphers have been added to increase the range of secure algorithms available.

Cisco TelePresence Server on Virtual Machine User Interface Change

The **Disable serial console input during startup** checkbox on the vTS user interface is now removed.

Change to Multistream Default Setting

Version 4.4(1.16) introduced a change to the multistream default setting. Multistream support is now off by default, previously it was on by default.

To set multistream mode to “on” for a conference using the API:

1. On TelePresence Conductor, go to **Conference Configuration > Conference Templates** and find the template for the conference.
2. Go to **Advanced Parameters**, click **Edit**.
3. In the **Custom parameters** text box, enter the following text: `{"callAttributes": {"multistreamMode": "multistreamOn"}}`
4. Click **Save**.

Advance Notice of Deprecation

TelePresence Server 4.4(1.20) will be the final release to support MSE 8710 platform.

Resolved and Open Issues

Resolved Issues

Issues seen in previous releases that are fixed in 4.4(1.20):

https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283613665&rls=4.4(1.20)&sb=fr&bt=custV

Open Issues

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

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.

Note: These are the recommended combinations for configuration via TelePresence Conductor. Other combinations are possible but are likely to cost more than expected. For further information see http://docwiki.cisco.com/wiki/Advanced_Resource_Optimization_on_TelePresence_Server.

Table 4 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

† Requires TelePresence Conductor XC2.2 or later.

Table 5 TelePresence Server conferencing capacity on various platforms for current products

Screen licenses required per call	Maximum calls by hardware type (with licenses to provide 100% of capacity)								
	8 Cores VM (8 vCPU)	Media 310 or MCU 5310	30 vCPU VM ‡	Media 320 or MCU 5320	Two appliance cluster	Media 820	Media 410v ‡ (46 vCPU)	CMS 1000 ‡ (70 vCPU)	Two blade cluster with Media 820
	5 screen licenses	6 screen licenses	10 screen licenses	12 screen licenses	24 screen licenses	30 screen licenses	32 screen licenses	42 screen licenses	60 screen licenses
1/52	200*	200*	200*	200*	200*	200*	200*	200*	200*
⅛	41	49	81	97	195	200*	200*	200*	200*
¼	20	24	40	48	97	120	128	168	200*
⅓	15	18	30	36	73	90	96	126	180
½	10	12	20	24	48	60	64	84	120
1	5	6	10	12	24	30	32	42	60
1½	3	4	6	8	16	20	21	28	40
2	2	3	5	6	12	15	16	21	30
3	1	2	3	4	8	10	10	14	20
4	1	1	2	3	6	7	8	10	15

* 200 is the maximum number of calls on a TelePresence Server. Requires Cisco TelePresence Conductor XC2.3 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 410v, CMS 1000, or 30 vCPU 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).

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.

Note: BE6K has not had any capacity changes since 4.1(1.79).

Note: This table is for current products only. For a comprehensive list including older products please see the licensing capacity table in the online help.

Limitations

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.

Flow Control Disabled for Endpoints that Negotiate TIP/MUX

Flow control requests are disabled for TelePresence Server 4.0 or later when it is in calls with CTS endpoints. This means that the **Received video: flow control on video errors** setting will have no effect if it is enabled for these endpoints.

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.

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. 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.

HD Quality Indicators on CTS Endpoints

When a CTS or IX5000 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.

Clustering Limitations

Slot 10 of the Cisco TelePresence MSE 8000 chassis does not support clustering for 8710 blades in this TelePresence Server software release. However, slot 10 in the same chassis as a cluster can be used for clustering Media 820 blades, or for standalone blades of any type.

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.

TelePresence Server Prioritizes Sharpness over Motion in Content Channels

TelePresence Server prioritizes sharpness over motion in content channels in TelePresence Server software 4.1 or later. See issue identifier CSCuy09938 for details.

Audio Prompts from a TelePresence Server may be Unexpectedly Cut Short

Audio prompts from a TelePresence Server that are being played at the time of an audio codec change may be unexpectedly cut short. For example, if the remote endpoint sends updated SDP offering a better audio codec.

If this is regularly affecting some calls, we recommend restricting the available audio codecs on affected endpoints to a single codec to prevent the TelePresence Server from being able to change the codec.

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 4.4(1.20)

Prerequisites and Software Dependencies

Note: 8710, 7010, Media 320, Media 310, Media 820 can be upgraded as standard using the .kupgrade or .zupgrade files. Back up your configuration file before upgrading.

Software Dependencies

- In the case of the TelePresence Server MSE 8710 blade(s) and the Media 820, the Cisco TelePresence Supervisor MSE 8050 blade must be running Supervisor software version 2.2 or later.
- Check that all your 3rd party software (including Browsers) supports TLS 1.2. If not, these will lose connectivity after the upgrade. After the upgrade you can change the minimum TLS version supported via new drop-down options on the **Network Settings** page of the Web user interface.

Table 6 TLS 1.2 support on other software

Other software and browsers	MinimumVersion	TLS 1.2 support	Notes
Chrome	30	yes	Previous to v30 only up to TLS 1.1 was supported.
Firefox	27	yes	Enables TLS 1.1 and 1.2 by default.
Internet Explorer	11	yes	Support for TLS 1.2 from Feb 2013.
Opera	17	yes	Versions 10-12 supported TLS 1.1 and 1.2 but disabled by default. Versions 14-16 supported TLS 1.1 but not 1.2.
Safari	5 on iOS and 7 on OS X	yes	Support for up to TLS 1.2.
Windows	Windows 7 and Windows Server 2008 R2	yes	TLS 1.1 and 1.2 support added but disabled by default; post Windows 8.1 they are enabledby default.
Windows	OS 2003	no	Does not support TLS 1.1 or 1.2.
Cisco TelePresence Management Suite	15.3 with Windows Server 2012 (Or the relevant TLS settings enabled on the Windows registry for 2008.)	yes	
CTS (first generation)	1.10.16	yes	
Cisco TelePresence TX9000 Series	TX 6.1.13	yes	
Cisco TelePresence IX5000 Series	8.2.1	yes	
Cisco TelePresence Video Communication Server/Cisco Expressway-E	X8.10	yes	
Cisco TelePresence Conductor	XC4.3.1	yes	

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_4.4_1.20.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 **.tar.xz** extension, for example, **Cisco_tsVirtualMachine_4.4_1.20.ova** and **Cisco_tsVirtualMachine_4.4_1.20.tar.xz**. 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. Log 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.

Using 4.4(1.20) on the Cisco TelePresence Server on Virtual Machine

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

Note: Version 4.3 can be upgraded to 4.4 in the normal way. However, if upgrading from 4.2 or earlier to 4.3 or later, Cisco TelePresence Server on Virtual Machine needs to be redeployed. For more information, please see "Migrating to TelePresence Server on Virtual Machine 4.3", at: http://www.cisco.com/c/en/us/support/conferencing/telepresence-server/products-installation-guides-list.html.

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, page 11, unless an item is explicitly excluded from the Virtual Machine platform.

Note that the upgrade file for Cisco TelePresence Server on Virtual Machine has a **.tar.xz** file extension.

Upgrade Instructions

1. In a web browser, navigate to the web interface of the device.
2. Log in as an administrator and configure a new password, if required.
   The username is *admin*
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, page 12 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.

Note: You can downgrade to 4.3 normally. However, to downgrade to 4.2 or earlier requires a redeploy. If you previously had that version deployed, you can turn that virtual machine back on after turning the one running 4.4 off, as described in the Cisco TelePresence Server on Virtual Machine Installation Guide under “Using 4.4 on the Cisco TelePresence Server on Virtual Machine”.

Downgrading from 4.4(1.20)

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.

Obtaining Documentation and Submitting a Service Request

Use the Cisco Notification Service to create customized flexible notification alerts to be sent to you via email or by RSS feed.

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation*.

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the What's New in Cisco Product Documentation RSS feed. The RSS feeds are a free service.

Document Revision History

Table 7 TelePresence Server release notes revisions

Date	Description
January 2018	Version 4.4(1.20)
October 2017	Version 4.4(1.20) second maintenance release
December 2016	Version 4.4(1.16) first maintenance release
August 2016	Version 4.4(1.9) First release

Cisco Legal Information

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

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

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

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

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

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

All printed copies and duplicate soft copies are considered un-Controlled copies and the original on-line version should be referred to for latest version.

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

Cisco Trademark

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)