



# Cisco TelePresence Server 4.2(4.23)

Release Notes  
January 2016

## 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](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](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](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](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](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](http://www.cisco.com/en/US/products/ps11339/products_licensing_information_listing.html)

## New Features in Version 4.2

Version 4.2(4.23) is a maintenance release. For more information, see [Resolved and Open Issues, page 6](#).

Version 4.2(4.18) introduced some new features to extend and improve the conference experience.

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

**Table 1 New feature support by TelePresence Server platform**

| Feature name  | 7010 & MSE 8710 Locally Managed | 7010 & MSE 8710 Remotely Managed | Media 310/320 Remotely Managed | Virtual Machine Remotely Managed |
|---|---------------------------------|----------------------------------|--------------------------------|----------------------------------|
| Deployment improvements   |                                 |                                  |                                |                                  |
| <a href="#">Multiparty License Mode, page 2</a>                     | No                              | Yes                              | Yes                            | Yes                              |
| <a href="#">Conductor Support without an Encryption Key, page 2</a> | Yes                             | Yes                              | Yes                            | Yes                              |

**Table 1 New feature support by TelePresence Server platform (continued)**

| Feature name  | 7010 & MSE 8710 Locally Managed | 7010 & MSE 8710 Remotely Managed | Media 310/320 Remotely Managed | Virtual Machine Remotely Managed |
|---|---------------------------------|----------------------------------|--------------------------------|----------------------------------|
| Security improvements   |                                 |                                  |                                |                                  |
| <a href="#">Change Default Administrator Credentials on First Login, page 2</a> | Yes                             | Yes                              | Yes                            | Yes                              |
| User experience improvements  |                                 |                                  |                                |                                  |
| <a href="#">New Serial Command: reset_config_preserving_keys, page 3</a>        | Yes                             | Yes                              | Yes                            | Yes                              |

## Multiparty License Mode

This release introduces a Multiparty License mode for the TelePresence Server. This allows you to administer Multiparty licenses centrally on TelePresence Conductor instead of having to load screen licenses locally on each TelePresence Server.

The TelePresence Server connects to up to three clustered TelePresence Conductors. TelePresence Conductor will enforce the Multiparty licences and TelePresence Server will accept or place calls as instructed by TelePresence Conductor up until the hardware limit is met.

The TelePresence Server has two licensing modes: Multiparty license mode and Screen license mode. On start up the TelePresence Server is in Screen licensed mode by default. Previously only Screen licensed mode was supported

To enter Multiparty license mode the TelePresence Server must be:

- in remotely managed mode
- have no active calls
- connected to a TelePresence Conductor with multiparty license mode activated

You can query the current licensing mode using the Web user interface (**Status** page) or API `system.info` command.

## Conductor Support without an Encryption Key

This release introduces support for TelePresence Conductor without the need for an encryption feature key. TelePresence Conductor requires TLS for SIP communication with the TelePresence Server and as such the encryption feature key was needed to enable TLS. Now TLS for HTTP and SIP is available without the need for the encryption feature key.

Other points to note:

- HTTPS and SIP over TLS are available at all times without the need for the encryption feature key.
- HTTPS and SIP TLS services are available by default. Default ports remain 443 and 5061 respectively.
- HTTP and SIP TCP are enabled by default.
- The encryption key is still required for media encryption in either H.323 or SIP calls.

In this release Encryption key is now referred to as Media Encryption key on the Web user interface.

## Change Default Administrator Credentials on First Login

This release introduces the security improvement that requires the default administrator credentials to be changed on first login. No functionality or configuration is possible on the TelePresence Server until the default administrator

credentials have been changed.

The default administrator account is the 'immortal administrator user' that cannot be deleted and normally has the user name "admin" (although this can be changed by the API and Web interface). Other users can be created with 'administrator' privilege (mortal users), however, their passwords or lack of, are ignored by this feature unless they have the user name "admin".

When using the Web user interface for first login, if the immortal administrator's password corresponds to the default password, then a **Change password** Web page shows corresponding to the immortal admin. The **No administrator password configured** banner displays and no other Web pages/configuration/functionality are accessible until the default credentials have been changed.

When using the API for first login, if the immortal administrator's password corresponds to the default password, then all API commands except: `user.modify` (to change the password), and `user.enumerate` (to discover what users are at present), will fail. Once the `user.modify` command has been used to change the immortal administrator's password, the TelePresence Server will function as usual.

Other points to note:

- An event log message is printed if an action (Web page request or API command) is requested but not fulfilled because the immortal admin password has not been changed.
- The `user.modify` API command, **Change password** and **Modify user** Web pages prevent the immortal administrator user's password from being modified to the default password.
- The API and Web interface prevent a mortal user from being created or modified to have username 'admin' and a blank password.

## New Serial Command: `reset_config_preserving_keys`

This release introduces a new serial command: `reset_config_preserving_keys` to simplify and speed up the process of restoring a unit to its factory settings. This new command acts exactly the same as the previous `reset_config` command, with the exception that any feature keys and screen license keys found in the configuration file are preserved.

Previously when restoring a unit to its factory settings you would need a copy of any feature keys and screen license keys to reinstate them once the unit was returned to its factory settings.

## Advance Notice of Deprecation

TelePresence Server 4.2 will be the last release to support Locally managed mode. Future releases will not support this mode. Remotely managed mode, which requires TelePresence Conductor, will be required to support the latest TelePresence Server releases and features.

Cisco has not announced or started the end of life process for the TelePresence Server 4.x software, when it does it will follow the standard process for maintenance releases and TAC support.

## 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.

**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](http://docwiki.cisco.com/wiki/Advanced_Resource_Optimization_on_TelePresence_Server).

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

| Call type description |              |               | Screen licenses required per call |
|-----------------------|--------------|---------------|-----------------------------------|
| Main video            | Audio        | Content       |                                   |
| -                     | Mono         | -             | 1/52                              |
| 360p30 <sup>†</sup>   | Mono         | In main video | 1/8                               |
| 360p30 <sup>†</sup>   | Stereo       | 720p5         | 1/4                               |
| 480p30                | Stereo       | In main video | 1/4                               |
| 480p30                | Stereo       | 720p5         | 1/3                               |
| 720p30                | Stereo       | 720p5         | 1/2                               |
| 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                                 |

<sup>†</sup> Requires TelePresence Conductor XC2.2 or later.

**Table 3 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 <sup>‡</sup> | Media 320 or MCU 5320 | Two appliance cluster | Media 410v <sup>‡</sup> (46 vCPU) | Media 820          | Four blade cluster with 8710/8510 | Two blade cluster with Media 820 |
|                                   | 5 screen licenses  | 6 screen licenses     | 10 screen licenses      | 12 screen licenses    | 24 screen licenses    | 27 screen licenses                | 30 screen licenses | 48 screen licenses                | 60 screen licenses               |
| 1/52                              | 200*   | 200*                  | 200*                    | 200*                  | 200*                  | 200*                              | 200*               | 200*                              | 200*                             |
| 1/8                               | 41   | 49                    | 81                      | 97                    | 195                   | 145 <sup>†</sup>                  | 200*               | 200*                              | 200*                             |
| 1/4                               | 20   | 24                    | 40                      | 48                    | 97                    | 108                               | 120                | 195                               | 200*                             |
| 1/3                               | 15   | 18                    | 30                      | 36                    | 73                    | 81                                | 90                 | 146                               | 180                              |
| 1/2                               | 10   | 12                    | 20                      | 24                    | 48                    | 54                                | 60                 | 97                                | 120                              |
| 1                                 | 5  | 6                     | 10                      | 12                    | 24                    | 27                                | 30                 | 48                                | 60                               |
| 1 1/2                             | 3  | 4                     | 6                       | 8                     | 16                    | 18                                | 20                 | 32                                | 40                               |
| 2                                 | 2  | 3                     | 5                       | 6                     | 12                    | 13                                | 15                 | 24                                | 30                               |
| 3                                 | 1  | 2                     | 3                       | 4                     | 8                     | 9                                 | 10                 | 16                                | 20                               |
| 4                                 | 1  | 1                     | 2                       | 3                     | 6                     | 6                                 | 7                  | 12                                | 15                               |

\* 200 is the maximum number of calls on a TelePresence Server. Requires Cisco TelePresence Conductor XC2.3 or later.

<sup>†</sup> If you place more than 145 calls of this screen license fraction on the device it may result in degraded performance.

<sup>‡</sup> To achieve the maximum number of calls, Cisco TelePresence Server on Virtual Machine must be the only VM hosted on the Multiparty Media 400v, 410v 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:** The following have not had any capacity changes since 4.1(1.79): BE6K, Media 400v.

**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.

## Resolved and Open Issues

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

### Resolved Issues

[https://tools.cisco.com/bugsearch/search?kw=\\*&pf=prdNm&pfVal=283613665&rls=4.2%284.23%29&sb=fr&sts=fd&svr=5nH&srtBy=byRel&bt=empCustV](https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283613665&rls=4.2%284.23%29&sb=fr&sts=fd&svr=5nH&srtBy=byRel&bt=empCustV)

### Open Issues

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

## Limitations

### Flow Control Disabled for Endpoints that Negotiate TIP/MUX

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

### The TelePresence Server Does Not Support Sender-Side Flow Control

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

### Video Issues with Earlier Versions of TX Endpoint Software



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

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

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

### Call Transfer is Disabled

The TelePresence Server does not support call transfer.

### DTLS and Custom Certificates

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

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

## HD Quality Indicators on CTS Endpoints

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

## Encryption Required Causes Issues with Some Endpoints

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

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

## Clustering Limitations

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

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

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

## Firefox 14 is Not Supported for use with the Cisco TelePresence Server

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

## TIP Calls and Encryption Required Conferences

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

## Recommended VCS Version X7.2 or Later

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

## Limited Support for some VM Operations

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

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

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

## Alarm Encryption Key is Missing Warning (on Conductor)

If you are using a TelePresence Conductor older than XC4.0 and do not have the media encryption key installed, TelePresence Conductor will display a warning that the encryption key is required. This warning is erroneous.

## 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 4.2(4.23)

### 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\_4.2\_4.23.zip** for the Media 310/320 platforms. You must unzip this file before you can use it.
  - For the virtual machine platform, the initial install file has a **.ova** extension but the upgrade package has a **.tgz** extension, for example, **Cisco\_tsVirtualMachine\_4.2\_4.23.ova** and **Cisco\_tsVirtualMachine\_4.2\_4.23.tgz**. You do not need to unzip either of those packages before you use them.
- Current software image file (in case you need to reverse the upgrade).
- Backup of the configuration (the **configuration.xml** file).
- You will require the administrator user name and password for the configuration backup file if you ever need to use the backup. If you attempt to downgrade / restore the software and you cannot load an appropriate configuration file, you may be unable to log in to the device.
- If using Call Detail Records (CDRs), or any other logs, for billing, auditing or other purposes, you must download and save your logged data. When the device reboots as part of the upgrade, all existing CDRs will be deleted.
- Administrative access to all units to be upgraded.
- The model numbers and serial numbers of your devices in case you need to contact Cisco Technical Support.

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

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

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

#### Backing Up Your Configuration

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

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

## Upgrading the Cisco TelePresence Server on Virtual Machine

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

**Note:** If upgrading from TelePresence Server 4.0 to 4.1 or later on a 16 vCPU machine (high capacity) you need to carry out the additional step of reconfiguring the VM with 30 vCPUs to take advantage of the increased capacity on existing hardware otherwise the upgrade will result in reduced capacity on some virtual platforms. If upgrading an 8 vCPU you only need to change the RAM. (See [Table 4 Upgrade paths for Cisco TelePresence Server on Virtual Machine, page 10.](#))

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 9](#), unless an item is explicitly excluded from the Virtual Machine platform.

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

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

**Note:** Upgrades to 4.2(4.23) will stay at the previous 8 GB RAM value and need to be manually changed in the VM settings via vSphere. Likewise downgrades to earlier versions will retain the 12 GB value.

**To upgrade Cisco TelePresence Server on Virtual Machine:**

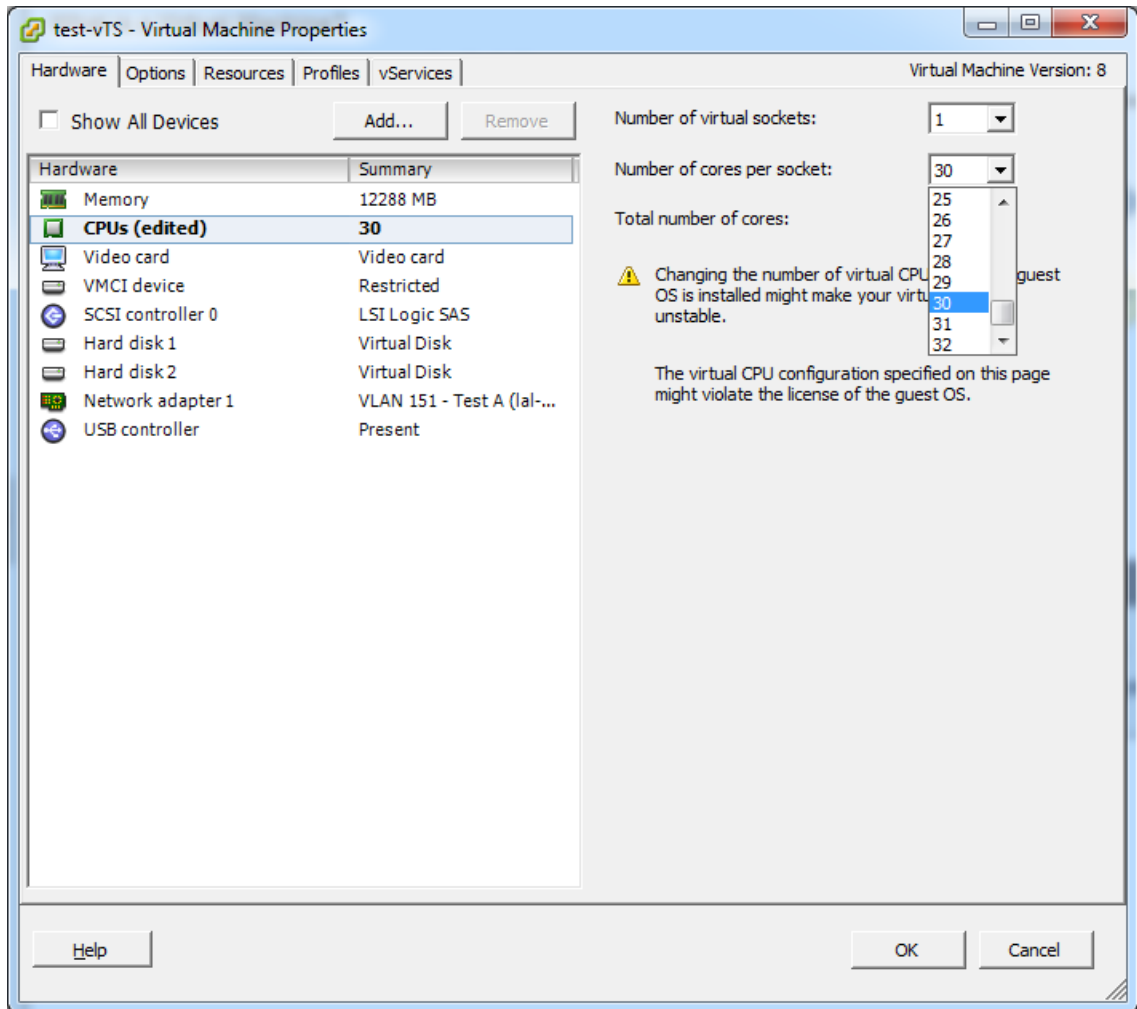
**Table 4 Upgrade paths for Cisco TelePresence Server on Virtual Machine**

| Upgrade                 | Media 400v |           | 16 Cores VM |           | 8 Cores VM (8vCPU) |           |
|-------------------------|------------|-----------|-------------|-----------|--------------------|-----------|
|                         | From this  | To this   | From this   | To this   | From this          | To this   |
| Software version        | 4.0(2.8)   | 4.2(4.23) | 4.0(2.8)    | 4.2(4.23) | 4.0(2.8)           | 4.2(4.23) |
| Physical CPUs           | 16         | 16        | 16          | 16        | 8                  | 8         |
| Virtual CPUs            | 30         | 30        | 16          | 30        | 8                  | 8         |
| RAM                     | 8 GB       | 12 GB     | 8 GB        | 12 GB     | 8 GB               | 12 GB     |
| Maximum screen licenses | 14         | 18        | 8           | 10        | 4                  | 5         |

**Note:** The maximum number of screen licenses that some Virtual Machine configurations can use have increased since their initial release. You may wish to purchase more licenses to take advantage of the increased capacity. See [Platform Licensing Comparison, page 4](#) for details of the capacity given by any new configurations.

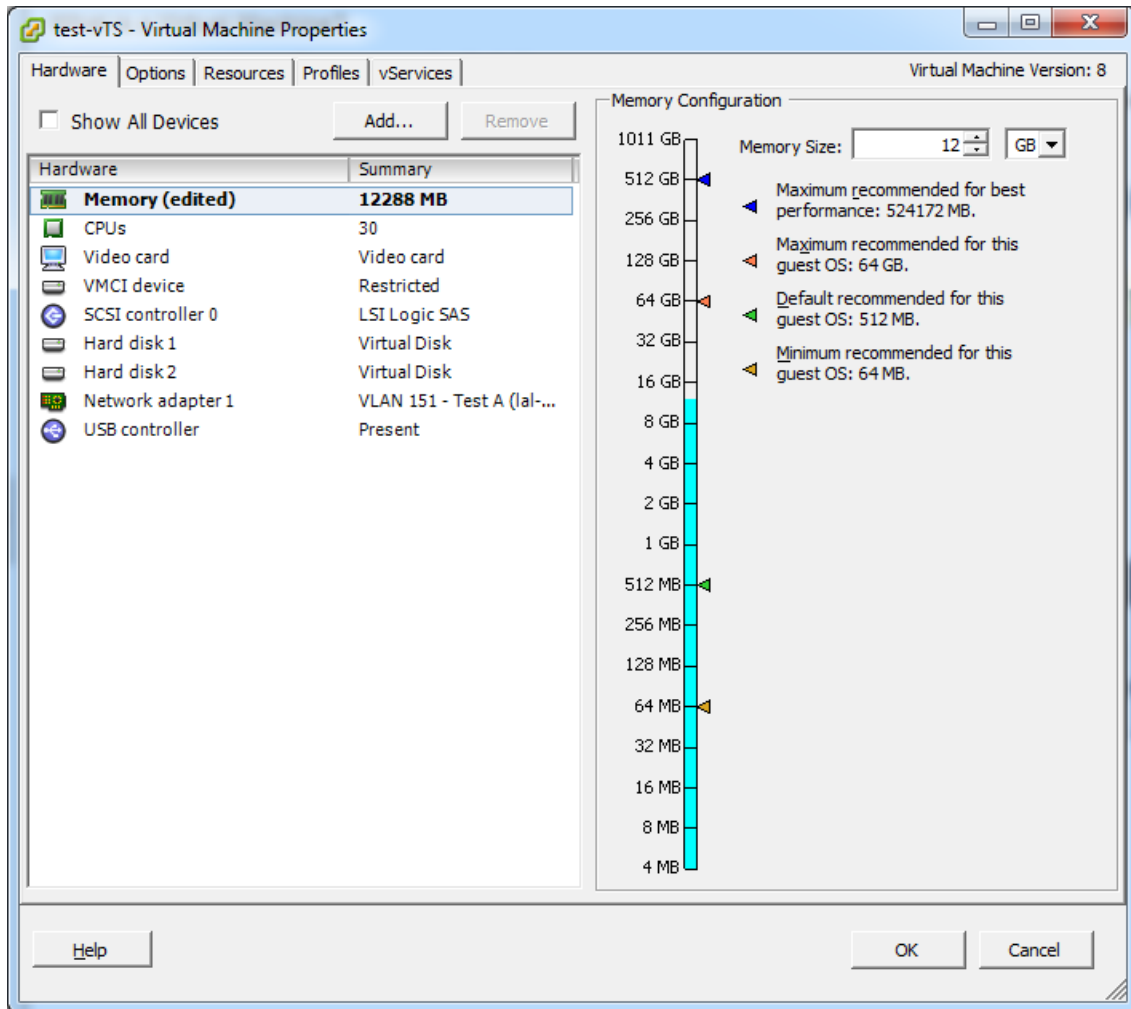
1. Follow the software [Upgrade Instructions, page 12](#), browsing to the **.tgz** file from the **Configuration > Upgrade** page.

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). Ensure that the **Number of virtual sockets** stays at 1.



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

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



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

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

## Upgrade Instructions

1. In a web browser, navigate to the web interface of the device.
2. Sign in as an administrator.  
The username is *admin* and there is no password on a new unit.
3. Go to **Configuration > Upgrade**.

4. In the **Main software image** section, locate the **New image file** field. Browse to and select the new image file.
5. Click **Upload software image**.

The web browser uploads the file to the device, which may take a few minutes.

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

A pop-up window displays to show upload progress. When complete, close the message. The web browser refreshes automatically and displays the message *Main image upload completed*.
6. Click **Shut down TelePresence Server**. This option will now change to **Confirm TelePresence Server shutdown**. Click to confirm.
7. Click **Restart TelePresence Server and upgrade**.

The unit will reboot and upgrade itself; this can take up to 25 minutes.

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

## Downgrade Instructions

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

**Caution:** Make sure that all relevant backup processes described in [Prerequisites, page 9](#) 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 4.2(4.23)

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

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

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

## Document Revision History

**Table 5** TelePresence Server release notes revisions

| Date         | Description  |
|--------------|--|
| January 2016 | Limitation added: Alarm Encryption Key is Missing Warning (on Conductor) |
| October 2015 | Version 4.2(4.23) MR1 release  |
| August 2015  | Version 4.2(4.18) Initial 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](http://www.cisco.com/go/offices).

© 2016 Cisco Systems, Inc. All rights reserved.

## 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](http://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)

