



Cisco TelePresence Server 7010 and MSE 8710

V3.0

Locally Managed Mode
Deployment Guide

D14963.02

February 2013

Contents

Introduction	4
Audience	4
Scope	4
TelePresence Server Operation mode	5
Background	6
TelePresence Server overview	6
Conference initiation	6
Scheduled conferences	6
Network topology	6
Baseline configuration	7
Security	8
Which deployment?	9
TelePresence Server with VCS deployment model	9
Scalability and redundancy	10
Known limitations	10
TelePresence Server with CUCM deployment model	10
Scalability and redundancy	11
Known limitations	11
Deploying the TelePresence Server using Cisco VCS	12
Deployment overview	12
Prerequisites	12
Document List	12
Summary of the process	13
Step 1: Configuring the Cisco VCS	13
Step 2: Configuring the TelePresence Server	14
Step 3: Configuring Cisco TMS	23
Checking the TelePresence Server is registered to the VCS	24
Deploying the TelePresence Server using CUCM	26
Deployment overview	26

Prerequisites	26
Document List	26
Summary of the process	26
Step 1: Configuring a SIP trunk on CUCM	26
Step 2: Configuring a route pattern to the TelePresence Server	29
Step 3: Configuring the TelePresence Server	30
Verifying the implementation	32
Testing the implementation	35
Appendix A Clustering	37
Appendix B Option keys and screen licenses	39

Introduction

There are several ways to deploy a Cisco TelePresence Server and configure it to allow video calling. This deployment guide provides a description of the two recommended configuration options. This guide only applies to V3.0 TelePresence Server software when operating in Locally Managed mode.

Audience

This document is prepared for partners and technical sales people who have a good technical understanding of Cisco video infrastructure products and how they function in a video architecture. As a minimum, you are expected to be able to install and configure Cisco Unified Communications Manager (hereafter referred to as CUCM), Cisco Video Communication Server (VCS), Cisco TelePresence Management Suite (TMS), and the TelePresence Server as individual products. It is expected that all the components of the solution are already installed and on the network, ready for configuration. Therefore, this document is not a complete architecture installation manual for an end-customer, but a manual specifically developed for integrating the TelePresence Server into the video architecture.

Scope

This document provides step-by-step instructions for deploying the appliance model 7010 and the chassis-based MSE 8710 in the following deployments using Cisco infrastructure:

- ▶ TelePresence Server registered to a VCS. Optionally, the VCS can have a trunk to CUCM.
- ▶ TelePresence Server trunked to CUCM.

Each deployment is covered in a separate section. For example, the “Deploying the TelePresence Server using VCS” scenario explains:

- ▶ VCS and CUCM configuration requirements for TelePresence Server registration and conference call routing.
- ▶ How to set up and configure the TelePresence Server 7010 and MSE 8710 blade(s).
- ▶ How to configure TMS for conference booking and management. (This is optional.)

Administrator guides are referenced for setup that is outside of the scope of this guide.

Software versions used

This guide has been tested against the following software revisions:

Table 1: Software Revisions

Device	Software Revision
CUCM	9.0.1
VCS	X7.2
TelePresence Server	3.0 (Locally managed mode)
TMS	13.2

TelePresence Server Operation mode

From version 3.0 onwards you can define the operation mode of the TelePresence Server, that is, whether to allow it to be locally managed or remotely managed by a device such as Cisco TelePresence Conductor.

In locally managed mode the TelePresence Server will manage all conferences. Locally managed mode is the default for the TelePresence Server. This Deployment Guide describes the TelePresence Server when operating in locally managed mode.

In remotely managed mode all conference create and participant management are managed externally to the TelePresence Server, by a device such as Cisco TelePresence Conductor and so resources will be optimized dynamically. This means that calls can connect and only use the resources they require, giving the most efficient use of blade resources across the different media types (i.e. audio, video, content) of different participants. For more information on remotely managed mode refer to the [TelePresence Server V3.0 Release Notes](#).

For help with configuring remotely managed mode with Conductor in a Cisco VCS deployment refer to [Cisco TelePresence Conductor with Cisco TelePresence Video Communication Server Deployment Guide](#).

For help with configuring remotely managed mode with Conductor in a Cisco Unified CM deployment refer to [Cisco TelePresence Conductor with Cisco Unified Communications Manager Deployment Guide](#).

For help on how to configure conferences within Conductor refer to [Cisco TelePresence Conductor Administrator Guide \(XC2.0\)](#).

Background

TelePresence Server overview

The TelePresence Server is a transcoding multipoint device that is available in two form factors: the 7010 appliance and the 8710 blade for the MSE 8000 chassis. The TelePresence Server can connect many video and audio devices using a variety of protocols (including SIP, H.323, and TIP), showing an ActivePresence™ layout. It supports both single- and multi-screen telepresence systems with a maximum of 12 screen licenses per appliance or blade.

For more information see <http://www.cisco.com/en/US/products/ps11453/index.html>

Conference initiation

The TelePresence Server can support both rendezvous and scheduled conferences, which can be invoked by the endpoint, Cisco TMS, CUCM or via the TelePresence Server web interface.

Rendezvous conferences are conferences that have been pre-configured on a TelePresence Server and that are always available; that is, a participant can join the conference at any time. Another common way of describing this type of conference is as a virtual meeting or conference room. These conferences can be configured for individual use or for communal first-come, first-served meetings. The TelePresence Server can register up to 96 rendezvous conferences to a VCS or can accept 200 trunked to CUCM.

Scheduled conferences

Scheduled conferences are pre-booked conferences with a start and end time and a pre-defined set of participants. Scheduled conferences are booked via TMS, either using TMS directly through TMS Scheduler, or by using an integration point such as Microsoft Exchange.

Scheduled conferences can also be configured directly through the TelePresence Server user interface, but Cisco highly recommends scheduling through TMS.

Note: A TelePresence Server used for scheduled conferences should not also be used for rendezvous conferences in order to guarantee port availability for scheduled calls. A separate TelePresence Server should be provided for this functionality.

Network topology

In planning the video network, remember that the TelePresence Server will cause a concentration of video traffic at its location because each port can have a video call connected to it at up to 6mbit/s, plus 20% overhead. Therefore, the TelePresence Server should be placed at a network

location that has enough bandwidth to host these calls. Cisco recommends that the TelePresence Server be placed on the internal network with firewall protection from external access. For external calling, use a VCS Expressway in conjunction with a VCS Control in order to allow video calls to traverse the firewall.

Baseline configuration

Some of the TelePresence Server local conference settings can affect the quality experienced during a conference. The following settings are the most important of these, and the values below are not only recommended but those assumed for the deployments discussed in this guide. To access these settings go to **Configuration > System settings and Configuration > Default endpoint settings**.

Table 2: Conference Settings (Configuration > System settings)

TelePresence Server setting	Recommended
ClearVision	Enabled

ClearVision



Table 3: Conference Settings (Configuration > Default endpoint settings)

TelePresence Server setting	Recommended
Video format	NTSC – 30fps
Transmitted video resolutions	Allow all resolutions
Motion/Sharpness tradeoff	Balanced
Default bandwidth (both to and from the server)	6.00 Mbit/s
Maximum transmitted video packet size (MTU)	1400

Video

Video format

NTSC - 30 fps

Transmitted video resolutions

Allow all resolutions

Motion / sharpness tradeoff

Balanced

Network

Default bandwidth (both to and from the server)

6.00 Mbit/s

Maximum transmitted video packet size

1400

Security

If the TelePresence Server has the encryption feature key installed, then you can enable secure web access to the web interface using HTTPS and conduct encrypted conferences.

Whether encryption is Optional or Required for a conference is configurable on a per conference basis. If encryption is Required, only endpoints supporting encryption can join the conference.

By default, the TelePresence Server has a local certificate and private key pre-installed to authenticate against the browser. However, Cisco recommends uploading your own certificate and private key to ensure security because all TelePresence Servers shipped from Cisco have an identical default certificate and key.

Which deployment?

This section discusses the two deployment options (using VCS and TMS to manage the TelePresence Server, or using CUCM to manage the TelePresence Server), to help you decide which is suitable for your organization. Then follow the instructions in the appropriate deployment section.

TelePresence Server with VCS deployment model

This deployment uses VCS as the registration mechanism for the TelePresence Server, and scheduling using TMS (see the figure below). Endpoints registered to CUCM or VCS can join TelePresence Server calls through a SIP trunk between VCS and CUCM, if this exists but this is not shown.

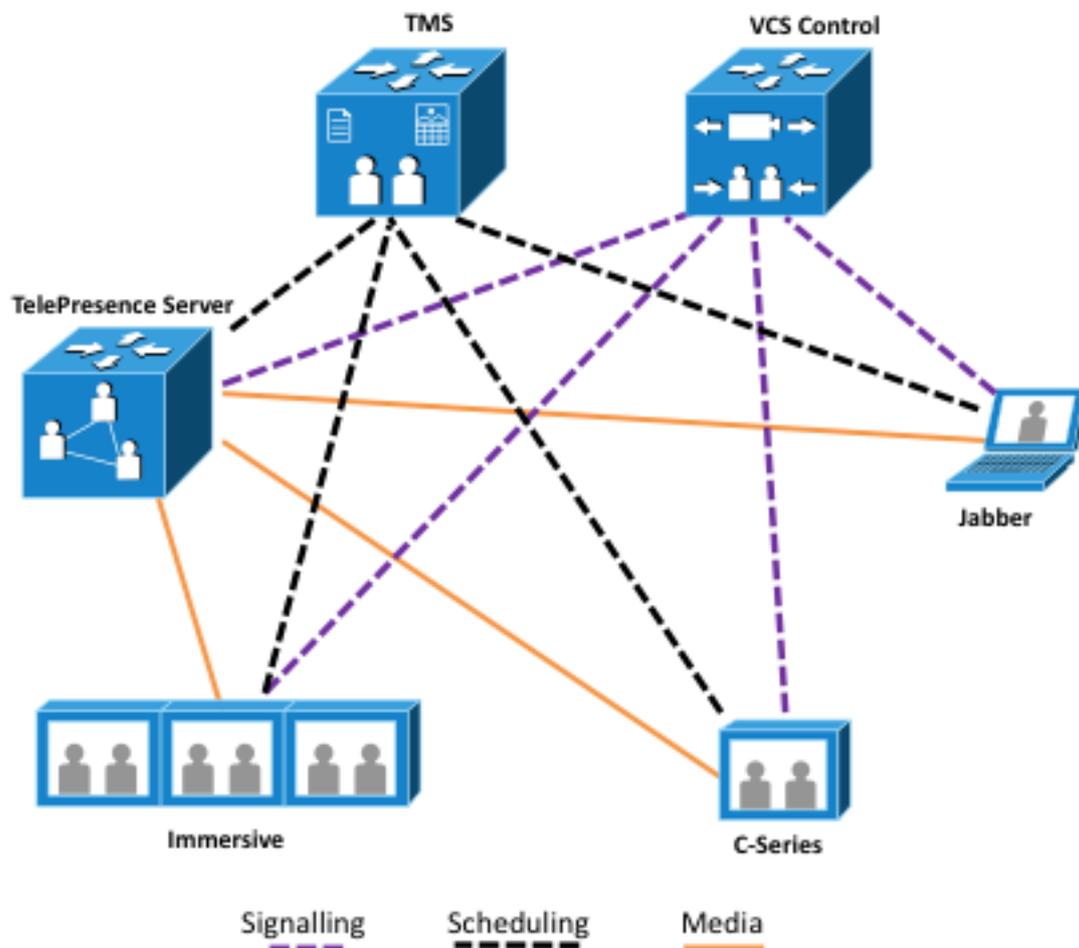


Figure 1 VCS deployment: media, signaling and scheduling overview

This deployment allows scheduled and rendezvous conferences as described in the following table:

Table 3: TelePresence Server with VCS deployment capability overview

Conference type	Options
Scheduled	Using TMS directly, via TMS Scheduler or via an integration point such as Microsoft Exchange.
Rendezvous	Static preconfigured conferences

Scalability and redundancy

For scalability and redundancy considerations, read the Clustering section in [Appendix A](#).

Known limitations

Known limitations are provided in the [TelePresence Server release notes](#).

TelePresence Server with CUCM deployment model

In this deployment model, TelePresence Server routes outbound calls through a trunk to CUCM (see the figure below) and there is no scheduling; only rendezvous conferences can be used, as detailed in the table below.

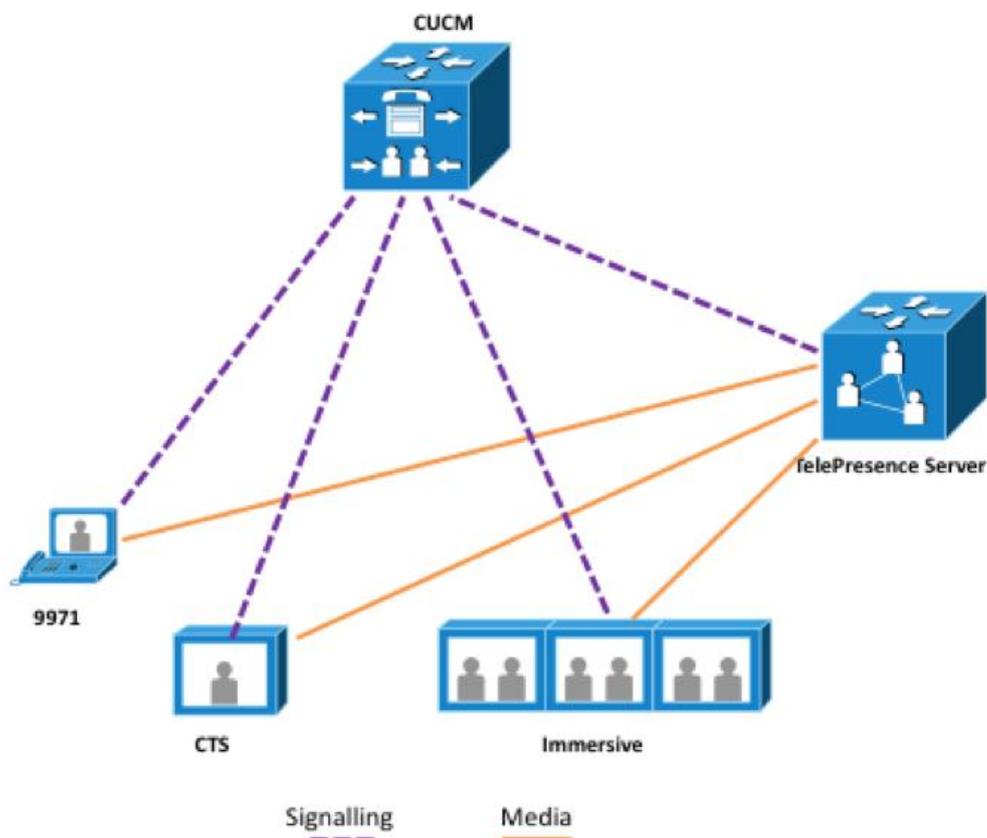


Figure 2 CUCM deployment: media and signaling overview

Table 4: TelePresence Server with CUCM deployment capability overview

Conference type	Options
Rendezvous	Static preconfigured conferences

Scalability and redundancy

For scalability and redundancy considerations, read the Clustering section in [Appendix A](#).

Known limitations

H.323 is not fully supported in the TelePresence Server with CUCM deployment model. For scenarios requiring H.323 support, the TelePresence Server with VCS deployment model is recommended.

Deploying the TelePresence Server using Cisco VCS

Deployment overview

This deployment uses VCS as the registration mechanism for the TelePresence Server, and conferences are scheduled using TMS. Endpoints registered to VCS can join TelePresence Server calls (as can endpoints registered to a CUCM that is trunked to the VCS, but this is not discussed further).

Follow the instructions in this section in the order provided.

Prerequisites

Before starting any configuration of the devices in this deployment, ensure that the following prerequisites are fulfilled:

- ▶ Cisco VCS is running X6.0 software or later.
- ▶ Cisco TelePresence Server 7010/MSE 8710 is running 3.0 software in locally managed mode.
- ▶ Cisco TMS is running 13.2 software, if used.
- ▶ Cisco CTS endpoints are running 1.7.4 software or later.
- ▶ Cisco VCS and TMS are installed and configured for base operation using their deployment guides.
- ▶ TelePresence Server has the factory default settings, as described [earlier](#).
- ▶ Cisco TMS has enough system licenses to add the relevant number of TelePresence Servers.

Document List

Have the following reference documentation available when configuring this deployment:

- ▶ [Cisco VCS Basic Configuration](#)
- ▶ [VCS Control with VCS Expressway Deployment Guide](#)
- ▶ [Cisco TelePresence Server 7010 Getting Started Guide](#)
- ▶ [Cisco TelePresence Server 8710 Getting Started Guide](#)
- ▶ [CUCM with VCS Deployment Guide](#) if deploying a CUCM trunked to the VCS

Summary of the process

Configuration consists of the following steps:

1. Configuring Cisco VCS
2. Configuring the TelePresence Server
3. Configuring Cisco TMS

Step 1: Configuring the Cisco VCS

The VCS Control should be deployed according to the recommendations of the [Cisco VCS Basic Configuration](#) or the [CUCM with VCS Deployment Guide](#), as appropriate to your installation.

Also, if you are using VCS Expressway, check that the prerequisites in the [VCS Control with VCS Expressway Deployment Guide](#) are fulfilled.

Configuring the VCS for the TelePresence Server requires the following steps, as described in the sections below:

1. Configuring the SIP domain
2. Verifying that SIP is enabled

Configuring the SIP domain

The TelePresence Server must be configured with a SIP domain name that matches the VCS sub-domain; otherwise the Cisco VCS will reject the SIP registration request from the TelePresence Server.

To configure a SIP domain on the VCS:

1. Go to **VCS configuration > Protocols > SIP > Domains**.
2. Click **New**.
3. Enter the domain name in the **Name** field:

Table 5: Settings for SIP domain

VCS setting	Value	Comment
Name	Fully qualified SIP domain name (FQDN)	Example: lab.cisco.com

4. Click **Create domain**.

Create domain

Configuration

Name

Verifying that SIP is enabled

On the VCS, ensure that the SIP protocol is enabled and the parameters are correct as follows.

1. Go to **VCS configuration > Protocols > SIP > Configuration**.
2. Verify that SIP Mode is On. If not, turn it on.

SIP

Configuration

SIP mode

3. Click **Save**.

Step 2: Configuring the TelePresence Server

The following steps required to configure the TelePresence Server are described in this section.

1. Installing feature keys
2. Configuring network settings
3. Configuring H.323 gatekeeper settings
4. Verifying H.323 gatekeeper registration
5. Optional: Adding TIP endpoints
6. Optional: Pre-configuring conferences

Installing feature keys

To install TelePresence Server feature keys:

1. Go to **Configuration > Upgrade**.
2. Ensure that the following keys are present or install them. (Screen licenses are added in **Configuration > Upgrade** if you are using a TelePresence Server 7010: on a TelePresence Server 8710 they are added using the Supervisor blade.)

Table 6: Required option keys

Key	Name	Usage
Activation	Activation key (required)	Required to activate TelePresence Server
Screen licenses	TelePresence Server screen licenses (required)	Supported number of screens
Encryption	Encryption key (optional)	HTTPs and Encrypted calls
Third party interop	Interop key (optional)	Multi-screen interoperability option for third-party endpoints
Backplane cluster	Clustering key (optional)	To cluster up to four 8710 blades

Feature management

The screenshot shows a web interface for feature management. On the left, there are sections for 'Activated features', 'License keys', and 'Activation code'. On the right, the following features are listed with their respective keys and 'remove' links:

- TelePresence Server 7010 activation** (MQV55-YWMHK-X8EKN-972EW)
- Encryption** (VX8G5-Y5LJR-T8WKY-C692A) [remove](#)
- Third party interop** (VXKG5-YRVV0-CWUQY-5A3C0) [remove](#)
- TS screen licenses x 16** (L7Y8H-UTP5A-X11GC-BPDU7-6B8F8)

Below the list is an empty text input field and an 'Update features' button.

3. Click **Update features**.

The example above shows for a TelePresence Server 7010. For more information on Option keys and Screen licenses see [Appendix B](#).

Configuring network settings

A number of network settings must be set on the TelePresence Server, and this is divided into groups.

To configure IP settings on the TelePresence Server:

1. Go to **Network > Network settings**.
2. Configure the fields as follows:

Table 7: IP settings for the TelePresence Server

TelePresence Server setting	Value	Comment
IP configuration	Manual	Example: 10.1.1.100
Manual configuration	Ipv4 or Ipv6 address, subnet mask, default gateway	Example: 255.255.255.0 Example: 10.1.1.1

Network settings

Port A IP configuration

IPv4 configuration

IP configuration Manual

Manual configuration

IP address

Subnet mask

Default gateway

3. Click **Update IP configuration**.

To configure the **DNS settings** on the TelePresence Server:

1. Go to **Network > DNS**.
2. Configure the fields as follows:

Table 8: DNS settings for the TelePresence Server

TelePresence Server setting	Value	Comment
DNS configuration	Manual	
Host name	TS hostname	Example: ts1
Name server	IP of DNS server	Example: 4.2.2.2
Secondary name server	IP of DNS server	Example: 8.8.4.4
Domain name (DNS suffix)	Domain	Example: cisco.com

DNS

DNS configuration

DNS configuration Manual

Host name

Name server

Secondary name server

Domain name (DNS suffix)

3. Click **Update DNS configuration**.

To configure network services on the TelePresence Server:

1. Go to **Network > Services**.
2. Configure the fields as follows:

Table 9: Services settings for the TelePresence Server

TelePresence Server setting	Value	Comment
Secure web	Enabled port 443	Enable/disable secure (HTTPS) web access (Encryption feature key required)

TelePresence Server setting	Value	Comment
Encrypted SIP (TLS)	Enabled port 5061	Allow/reject incoming encrypted SIP calls to the TelePresence Server using SIP over TLS
SIP (UDP)	Enabled port 5060	Allow/deny incoming and outgoing calls to the TelePresence Server using SIP over UDP

Services

		Port A
TCP service		IPv4
Web	<input checked="" type="checkbox"/>	80
Secure web	<input checked="" type="checkbox"/>	443
Incoming H.323	<input checked="" type="checkbox"/>	1720
SIP (TCP)	<input checked="" type="checkbox"/>	5060
Encrypted SIP (TLS)	<input checked="" type="checkbox"/>	5061
FTP	<input checked="" type="checkbox"/>	21

		Port A
UDP service		IPv4
SIP (UDP)	<input checked="" type="checkbox"/>	5060

3. Click **Apply changes**.

Configure H.323 gatekeeper settings

To configure H.323 gatekeeper settings go to **Configuration > H.323 settings**:

Table 10: H.323 settings on the TelePresence Server

TelePresence Server setting	Value	Comment
Use gatekeeper	Enabled	
H.323 Gatekeeper Address	FQDN of the VCS or VCS cluster	DNS A record must resolve to the VCS IP address Example: vcsc1.lab.cisco.com
H.323 ID to register	URI	Example: ts1@lab.cisco.com Note: The domain must match the FQDN configured in the VCS under SIP domains
Password		If the configured gatekeeper requires password authentication from registrants, enter the password

H.323 settings

H.323 gatekeeper

Use gatekeeper

Address

H.323 ID to register

Password

4. To configure **SIP settings** go to **Configuration > SIP settings**:

Table 11: SIP settings on the TelePresence Server

TelePresence Server setting	Value	Comment
Outbound call configuration	Use registrar, Use trunk or Call Direct	This setting affects outgoing SIP calls and registration.
Outbound address	Hostname or IP address of SIP registrar	The hostname or IP address of the SIP registrar or trunk destination. Example: vcsc1
Outbound domain	String	The domain of the SIP registrar or trunk destination. Example: cisco.com
Username	String	The TelePresence Server uses this name to authenticate with the SIP device (registrar, trunk destination, or endpoint) if that device requires authentication.

TelePresence Server setting	Value	Comment
Password	None	The TelePresence Server uses this password to authenticate with the SIP device (registrar, trunk destination, or endpoint) if that device requires authentication.
Outbound transport	TLS	Select the protocol that the TelePresence Server will use for outbound calls (and registrations, if enabled). One of TCP, UDP, or TLS.
Negotiate SRTP using SDES	For secure transports (TLS) only	The TelePresence Server will negotiate SRTP using SDES for whichever value is set.
Use local certificate for outgoing connections and registrations	Enabled (recommended)	Forces the TelePresence Server to present its local certificate when registering with the SIP registrar (via TLS) or making outgoing TLS calls.

SIP settings

SIP

Outbound call configuration	Use registrar ▼
Outbound address	vcsc1
Outbound domain	cisco.com
Username	admin
Password	•••••
Outbound transport	TLS ▼
Negotiate SRTP using SDES	For secure transports (TLS) only ▼
Use local certificate for outgoing connections and registrations	<input type="checkbox"/>

5. Click **Apply changes**.

Verifying H.323 gatekeeper registration

1. Go to **Status > Status**.
2. In the Status section, ensure that the TelePresence Server has registered to the VCS successfully.

H.323 gatekeeper status	1 TelePresence Server successfully registered
SIP registrar status	1 TelePresence Server successfully registered

Optional: Adding TIP endpoints

CTS endpoints running versions 1.6.x or 1.7.x (up to and including 1.7.3) must be added to the TelePresence Server on the Add Legacy TIP endpoint page as described in this section. (Legacy

TANDBERG systems and CTS endpoints running software version 1.7.4 or later are supported automatically and must not be added using this step. (Information for CTS endpoints running 1.7.4 or later is passed as a part of the TIP negotiation and used by the TelePresence Server to identify the CTS endpoint.)

If the third-party interop key is installed, TelePresence Server also supports interworking with Polycom RPX and TPX telepresence systems.

To manually add a legacy TIP endpoint, follow these steps:

1. Go to **Endpoints > Add legacy TIP endpoint**
2. Configure the following on the TelePresence Server:

Table 12: Add legacy TIP endpoint

TelePresence Server setting	Value	Comment
Name	Endpoint name	Example: CTS 3010
Call-out Address	String	Directory number of CTS IP address/hostname of the CUCM. The TelePresence Server uses this to place outgoing calls to the endpoint. Example: 881239876

3. Click **Add new endpoint**.
4. Go to the **Endpoints Configuration** page. (**Endpoints > [Your legacy TIP endpoint] > Configuration**) and configure the fields as follows to match the dial string.

Note: The TelePresence Server will match the fields below with a Boolean "OR". Therefore Cisco highly recommends only configuring one of the Call-in match parameters.

Table 13: Endpoint configuration – Call-in match parameters

TelePresence Server setting	Value	Comment
Name	String	Remote Party ID in SIP INVITE Example: Alexander
Address	IP address/FQDN	The originating IP address or hostname of the SIP INVITE Note: Using this call-in match

TelePresence Server setting	Value	Comment
		parameter is not recommended because it can be too generic.
E.164	E.164 number	The directory number assigned in CUCM Example: 881239876

Call-in match parameters	
Name	Alexander
Address	10.10.10.100
E.164	881239876

- Click **Update endpoint**.

Optional: Preconfiguring conferences

Setting up a preconfigured conference through the web interface creates a virtual conference that maintains a consistent configuration and can be dialed directly from endpoints so long as the TelePresence Server has free resources.

Note: Optionally, a preconfigured conference can be scheduled with a start and end time. However this is not the recommended scheduling method because TMS offers more functionality and ease of use.

To preconfigure a conference:

- Go to the **Conferences > Add new conferences** page
- Configure the fields as follows for the conference:

Table 14: Preconfiguring a conference

TelePresence Server Setting	Value	Comment
Name	Name of conference	Example: All Hands Meeting
Numeric ID	Unique numeric identifier from address plan	Used for dialing into the conference. This ID should be taken from the range in the address plan allocated to preconfigured conferences Example: 411
PIN	Unique PIN for the conference	Up to 40 digits. Can be entered via DTMF
Register with H.323 gatekeeper	Enabled	
Register with SIP registrar	Enabled	

TelePresence Server Setting	Value	Comment
Conference Locked	Default is disabled (unchecked).	Check to lock the conference. No participants can join (call-in) when the conference is active.

Add new conference

Conference

Name

Numeric ID

PIN

Register numeric ID with H.323 gatekeeper

Register numeric ID with SIP registrar

Conference locked

3. Select **Schedule** button to create the conference immediately.

Scheduling

Schedule

Start time 06:32 Date: 1 May 2012

4. Optional: If you are logged in to the TelePresence Server as an administrator you can limit the number of video and audio participants in the conference; by default the check boxes are clear which means "unlimited". An example of 10 video and 6 audio participants is shown below.

Port limits

Video

Audio only

5. Optional: If you are using the TelePresence Server web interface to schedule conferences (which is not recommended) you can have the TelePresence Server dial out to participants at the conference start time by adding preconfigured participants to the Conference. (If you are scheduling using any other alternative, skip this step.)

Pre-configured participants

Note: The TelePresence Server can register 100 unique H.323 and 100 unique SIP aliases but four of those aliases are reserved for the system, making 96 available for each protocol.

6. Click **Add new conference**.

Step 3: Configuring Cisco TMS

Configuring Cisco TMS requires the following steps:

1. Adding the TelePresence Server to TMS
2. Editing extended settings
3. Setting the preferred MCU type in TMS

Refer to the [TMS Administration Guide](#) for specific steps and more details: only notes are included here.

Adding the TelePresence Server to TMS

When adding the TelePresence Server to Cisco TMS, In TMS select **Discover Non-SNMP Systems** In **Advanced settings**.

Discovery Options

Use the following SNMP community names (new community names is only a one time setting):

Discover Non-SNMP Systems. WARNING: Will significantly increase time required for discovery

Editing extended settings

1. Log in to TMS as an administrator.
2. Select the new TelePresence Server that you just added.
3. Click **Edit Settings**.
4. Scroll down to the **TMS Scheduling Settings** section.
5. To allow the TelePresence Server to be used for booking through TMS (the recommended approach), select the Allow bookings check box. (If you do not want TMS to be used for scheduling, leave the check box clear.)

Table 15: Allow bookings for scheduled TelePresence Server on TMS

TMS Setting	Value	Comment
Allow bookings	Enabled	



6. To set the scheduled conference number range for the TelePresence Server on TMS, on TMS go to **System > Navigator > TS > Settings**.
7. Configure the following:

Table 16: Extended settings for scheduled TelePresence Server on TMS

TMS Setting	Value	Comment
First meeting id	Start of the number range for scheduled conferences	This is the first number in a sequence sent to conference participants from TMS. Example: If the address plan has five digit short numbers and the TelePresence Server prefix is 71, then use 71000
Meeting id Step	1	TMS will consecutively add this number to the First meeting ID to avoid duplication of the meeting ID.

The screenshot shows the 'Settings' tab in the TMS interface. Under the 'Extended Settings' section, the 'First Meeting Id' is configured to 8300 and the 'Meeting Id Step' is configured to 1.

- Click **Save**.

Setting the preferred type MCU usage

Some endpoints can support small conferences if they have the Multisite feature key installed. To have TMS schedule a TelePresence Server to host the conference rather than the endpoint's on-board MultiSite feature, complete the following steps on TMS:

- Go to **Administrative Tools > Configuration > Conference Settings**.
- Configure the field as follows:

Table 17: Settings for preferred MCU type usage

TMS Setting	Value	Comment
Preferred MCU Type in Routing	TANDBERG Codian MCU	Default (TANDBERG Codian MCU is the correct choice for the TelePresence Server.)

- Click **Save**.

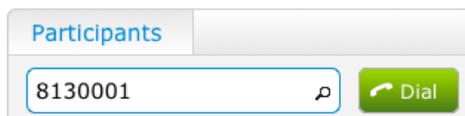
Checking the TelePresence Server is registered to the VCS

To test this, use an endpoint (e.g. EX90) to dial into the TelePresence Server conference.

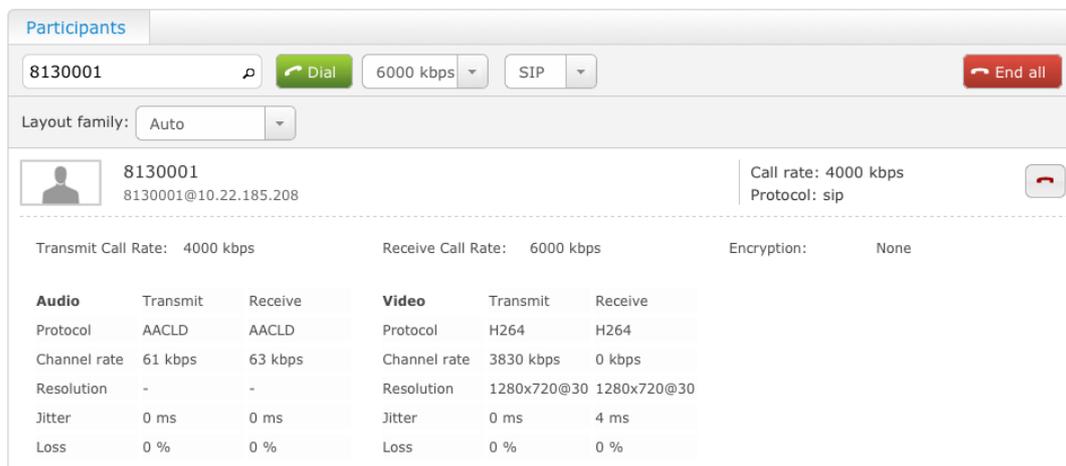
First set up a preconfigured conference with 8130001 as the alias.

- On the endpoint's web interface, click **Call Control**.

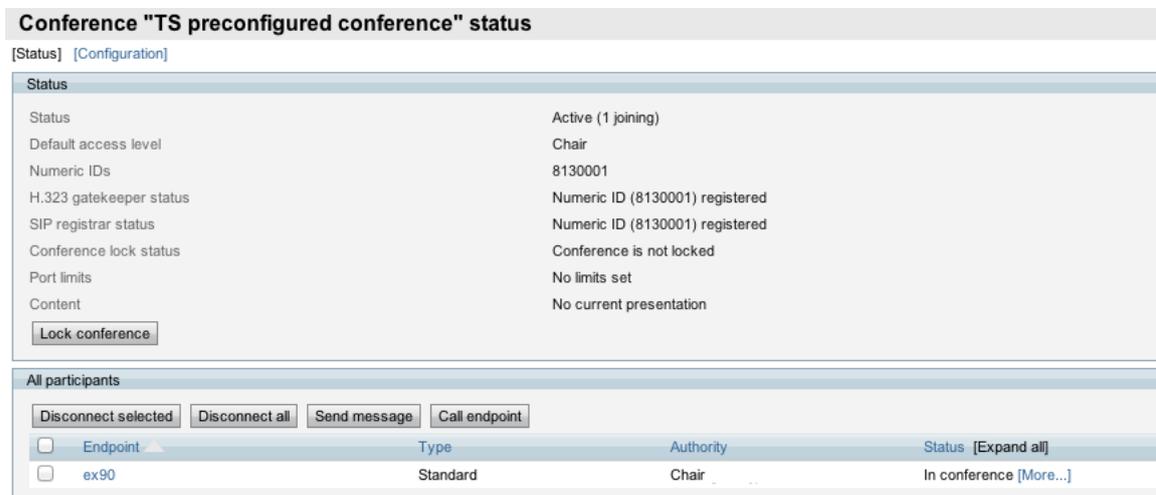
2. Enter 8130001.
3. Click **Dial**.



4. Verify connectivity on the endpoint (an example is shown below).



5. Verify connectivity on the TelePresence Server by going to **Conferences > Conferences** and selecting the conference. (An example is shown below.)



Deploying the TelePresence Server using CUCM

Deployment overview

From TelePresence Server release 2.2 a direct SIP trunk to CUCM is supported. This functionality allows existing CUCM customers that do not have a Cisco VCS to deploy the TelePresence Server with CUCM. Note that this deployment does not support H.323 and scheduling through TMS.

Prerequisites

Before starting the configuration process, ensure that the following prerequisites are fulfilled:

- ▶ CUCM running is version 8.5.1 or later.
- ▶ Cisco TelePresence Server 7010 or MSE 8710 is running 3.0 software locally managed mode.
- ▶ Cisco CTS endpoints are running 1.7.4 software or later.
- ▶ CUCM is installed and configured for base operation using the relevant Cisco deployment guides.
- ▶ Cisco TelePresence Server is set to factory default settings.

Document List

Have the following documentation available for reference during this deployment.

- ▶ Information about SIP and configuring SIP trunks
- ▶ Route Pattern configuration

Summary of the process

Deploying the TelePresence Server consists of the following steps:

1. Configuring a SIP trunk on CUCM.
2. Configuring a Route Pattern to the TelePresence Server.
3. Configuring the TelePresence Server.

Step 1: Configuring a SIP trunk on CUCM

To add a SIP trunk between CUCM and the TelePresence Server follow these steps on CUCM:

1. Go to **Device** -> **Trunk**.
2. Select **Add New**.
3. Configure the following:

Table 18: Trunk configuration

UCM setting	Value	Comment
Trunk Type	SIP Trunk	
Device Protocol	SIP	Default
Trunk Service Type	None	Default

Status

i Status: Ready

Trunk Information

Trunk Type * SIP Trunk

Device Protocol * SIP

Trunk Service Type * None(Default)

Next

4. Click **Next**.
5. Configure the following:

Table 19: Trunk configuration – Device information

UCM setting	Value	Comment
Device Name	String	Unique identifier for the trunk.
Device Pool	Drop-down	Appropriate device pool for the trunk.
Call Classification	Use System Default	Default value for Call Classification is Use System Default.
SRTP allowed	Disabled	Disables the use of SRTP on the trunk; all media will use RTP.

Device Information

Product:	SIP Trunk
Device Protocol:	SIP
Trunk Service Type	None(Default)
Device Name*	TS1_Trunk
Description	Trunk to Telepresence Server 1
Device Pool*	Default
Common Device Configuration	< None >
Call Classification*	Use System Default
Media Resource Group List	< None >

SRTP Allowed - When this flag is checked, Encrypted TLS needs to be configured in the network to provide end to end security.

Table 20: Trunk configuration – SIP Information

CUCM setting	Value	Comment
Destination Address	IP address	Destination Address represents the remote SIP peer with which this trunk will communicate. Example: 10.22.185.181
Destination Port	5060	Default 5060 indicates the SIP port.
Presence Group	Standard Presence group	
SIP Trunk Security Profile	Non Secure SIP Trunk Profile	
SIP Profile	Standard SIP Profile	

SIP Information

Destination

Destination Address is an SRV

	Destination Address	Destination Address IPv6	Destination Port
1*	10.22.185.181		5060

MTP Preferred Originating Codec* 711ulaw

Presence Group* Standard Presence group

SIP Trunk Security Profile* Non Secure SIP Trunk Profile

Rerouting Calling Search Space < None >

Out-Of-Dialog Refer Calling Search Space < None >

SUBSCRIBE Calling Search Space < None >

SIP Profile* Standard SIP Profile

6. Click **Save**.
7. Reset the Trunk by clicking **Reset**.
8. Click **Close** to return to the trunk configuration page.

Step 2: Configuring a route pattern to the TelePresence Server

CUCM uses route patterns to route or block internal and external calls. A route pattern comprises a string of digits (the address) and a set of associated digit manipulations that route calls to a Route list or to a gateway. Route patterns provide flexibility in network design and work in conjunction with Route filters and Route lists to direct calls to specific devices. These functions can include, exclude, or modify any digit patterns.

To set up a new Route pattern to the TelePresence Server complete the following steps:

1. Go to **Call Routing > Route/Hunt > Route Pattern**.
2. Click **Add New**.
3. Configure the fields as following:

Table 21: Route Pattern Configuration

UCM setting	Value	Comment
Route Pattern	String	Enter the route pattern, including numbers and wildcards (do not use spaces); for example, for typical local access or 8XXX for a typical private network numbering plan. Example: 813xxxx
Description	String	Enter a description of the route pattern.
MLPP Precedence	Default	
Route Class	Default	The Default setting uses the existing route class of the incoming call.
Gateway/Route List	Select configured SIP trunk from drop down list.	Choose the gateway or route list.
Route Option	Route this pattern.	
Call Classification	OffNet	Call Classification indicates whether the call that is routed through this route pattern is considered either off (OffNet) or on (OnNet) the local network. The default value specifies OffNet.

Pattern Definition

Route Pattern*	813XXXX
Route Partition	< None >
Description	Route Pattern for 813xxxx to TS1
Numbering Plan	-- Not Selected --
Route Filter	< None >
MLPP Precedence*	Default
<input type="checkbox"/> Apply Call Blocking Percentage	
Resource Priority Namespace Network Domain	< None >
Route Class*	Default
Gateway/Route List*	TS1_Trunk
Route Option	<input checked="" type="radio"/> Route this pattern <input type="radio"/> Block this pattern
Call Classification*	OffNet

4. Click **Save**.

Step 3: Configuring the TelePresence Server

Configuring the TelePresence Server involves the followings steps:

1. Installing feature keys
2. Configuring network settings
3. Configuring system settings

Installing feature keys

Refer to [Step 2](#) – Installing feature keys – in Deploying the TelePresence Server with VCS.

Configuring network settings

Refer to [Step 2](#) – Configuring network settings – in Deploying the TelePresence Server with VCS.

Configuring SIP settings

To configure outbound SIP on the TelePresence Server:

1. Go to **Configuration > SIP Settings**.
2. In the SIP section, configure the following:

Table 22: SIP Settings

TelePresence Server settings	Value	Comment
Outbound call configuration	Use trunk	
Outbound address	UCM_IP_Address	Address to CUCM server

TelePresence Server settings	Value	Comment
		configured with SIP trunk. Example: 10.22.185.208
Outbound domain	Domain	The domain of the trunk destination. Either use the IP address of CUCM or the host name of the CUCM as listed on the System > Server page.
Username		Not required
Password		Not required
Outbound transport	TCP	
Negotiate SRTP using SDES	For secure transports (TLS) only	The TelePresence Server will negotiate SRTP using SDES for whichever value is set.
Use local certificate for outgoing connections and registrations	Enabled.	Forces the TelePresence Server to present its local certificate when registering with the SIP registrar (via TLS) or making outgoing TLS calls. This option should be checked if TLS is in use.

SIP settings

SIP

Outbound call configuration	Use trunk <input type="button" value="v"/>
Outbound address	<input type="text" value="10.22.185.208"/>
Outbound domain	<input type="text" value="10.22.185.208"/>
Username	<input type="text" value="dt8b4"/>
Password	<input type="text"/>
Outbound transport	TCP <input type="button" value="v"/>
Negotiate SRTP using SDES	For secure transports (TLS) only <input type="button" value="v"/>
Use local certificate for outgoing connections and registrations	<input type="checkbox"/>

3. Click **Apply changes**.
4. Click **Conferences** and then **Add New Conference**.
5. Configure the following:

Table 23: Conference Settings

TelePresence Server settings	Value	Comment
Name	String	
Numeric ID	Conference number (8130001)	Conference number that is used by CUCM. For example an

TelePresence Server settings	Value	Comment
		813xxxx will be sent.

Conference	
Name	Trunk Conf 1
Numeric ID	8130001

6. Click **Add New Conference**.

Verifying the implementation

To verify the registration of an endpoint to CUCM follow the steps below. (An EX90 running TC5.1 software is used in the examples below.)

1. HTTP or HTTPS to the web interface of the EX90.
2. Click **Configuration** and then **Advanced Configuration**.
3. Click **SIP Profile 1**.
4. Configure the fields as follows clicking **OK** after entering each field.

Table 24: Endpoint Settings

TelePresence Server settings	Value	Comment
Default Transport	TCP	Use TCP to match the rest of the configuration guide.
URI 1	Sip:DN@IP_Address of CUCM Or sip:DN@FQDN of CUCM	Enter the DN number for the endpoint.
Proxy 1 address	IP_Address or FQDN of CUCM	Address of CUCM. This can be FQDN or IP address.
Proxy 1 Discovery	Manual	

SIP Profile 1	
DefaultTransport	TCP
DisplayName	<input type="text"/> ok
Outbound	Off
TlsVerify	Off
Type	Cisco
URI 1	p:1214@10.22.185.208 ok
Authentication 1	
LoginName	<input type="text"/> ok
Password	<input type="text"/> ok
Proxy 1	
Address	10.22.185.208 ok
Discovery	Manual

The endpoint will not be registered until it is configured as a device in CUCM.

5. On CUCM go to **Device > Phones**.
6. Select **Add New**.
7. Select the phone type. (For this example, an EX90 is used, so select EX90.)
8. Click **Next**.
9. In the SIP section, configure the following:

Table 25: System Settings

TelePresence Server settings	Value	Comment
MAC Address	String	Do not enter the colons
Description	String	
Device Pool	Default	
Phone Button Template	Standard Cisco TelePresence EX90	

TelePresence Server settings	Value	Comment
Common Phone Profile	Standard Common Phone Profile	
Presence Group	Standard Presence group	
Device Security Profile	Cisco TelePresence EX90 – Standard SIP Non-Secure	
Sip Profile	Standard Sip Profile	

Device Information

Device is trusted

MAC Address*

Description

Device Pool*

Common Device Configuration

Phone Button Template*

Common Phone Profile*

Protocol Specific Information

Presence Group*

MTP Preferred Originating Codec*

Device Security Profile*

Rerouting Calling Search Space

SUBSCRIBE Calling Search Space

SIP Profile*

- Click **Save**.
- Click **Line1 – Add new DN**.

Association Information

1

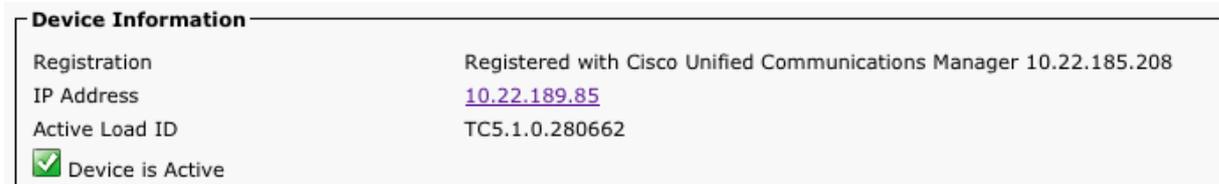
- Enter the DN in the **Directory Number** field, for example 1214.
- Click **Save** and then **Apply Config**.
- In the Related links field, click **Go** to return to the device.

Related Links:

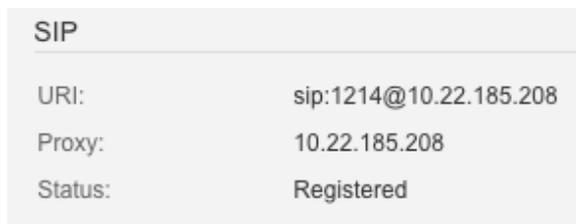
- Verify that the DN is added.



- Verify that the endpoint (EX90) is registered on CUCM.



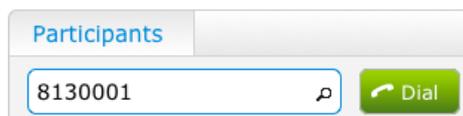
- On the endpoint (EX90) verify that it is registered by going to **Diagnostics > System Information**.



Testing the implementation

First setup a preconfigured conference as shown previously. For the example below 8130001 is used. To test the configuration, the endpoint (EX90) needs to dial 8130001 to access the TelePresence Server conference.

- On the endpoint's web interface, click **Call Control**.
- Enter 8130001.
- Click **Dial**.



- Verify connectivity on the endpoint.

Participants

8130001 Dial 6000 kbps SIP End all

Layout family: Auto

8130001
8130001@10.22.185.208 Call rate: 4000 kbps
Protocol: sip

Transmit Call Rate: 4000 kbps Receive Call Rate: 6000 kbps Encryption: None

Audio			Video		
	Transmit	Receive		Transmit	Receive
Protocol	AACLD	AACLD	Protocol	H264	H264
Channel rate	61 kbps	63 kbps	Channel rate	3830 kbps	0 kbps
Resolution	-	-	Resolution	1280x720@30	1280x720@30
Jitter	0 ms	0 ms	Jitter	0 ms	4 ms
Loss	0 %	0 %	Loss	0 %	0 %

5. Verify connectivity on the TelePresence Server by going to **Conference > Conferences** and selecting the trunk conference.

Status

Connected to conference	Trunk Conf 1
Call status	Connected (called in)
Protocol	SIP
Call-in IP address	10.22.185.208
Call-in E.164	1214
Call-in name	1214
Endpoint advertised capabilities	Audio, Video, Unencrypted traffic
Video channels	Rx channel open, Tx channel open
Far end audio mute	off
Bandwidth	Rx: 4.00 Mbit/s Tx: 4.00 Mbit/s
Encryption check code	<none>
Preview	

Appendix A Clustering

Deployment concept for multiple TelePresence Servers

The TelePresence Server can be deployed in a cluster. To create a cluster of TelePresence Servers, one of the TelePresence Servers is the master or primary blade of the cluster and the other blades are the secondary or slave blades, of which there can be up to 3. For example, with TelePresence Server version 2.3 or later, four 8710 blades can be installed in a single MSE 8000 and clustered to make the TelePresence Server appear as one large TelePresence Server to all other devices.

A cluster is a group of blades hosted on the same TelePresence MSE 8000 chassis, which are linked together to behave as a single unit. The administrator can configure and manage clusters using the Supervisor MSE 8050.

A cluster provides the combined screen count of all the blades in the cluster. This larger screen count provides the flexibility to set up conferences with more participants or several smaller conferences.

For more information about screen licenses, see Understanding Screen Licenses of the online help and [Appendix B](#) in this document.

TelePresence Server 8710 cluster: TelePresence Server blades running software version 2.1 or later support clustering. Up to four blades can be clustered in version 2.2 or later (increased from three in version 2.1), with one blade acting as a Master and the other blades being slaves to this master. Clustering provides the administrator with the combined video port count of the blades in the cluster. For example, on an MSE 8710 cluster of four blades each with 12 screen licenses, the cluster has 96 HD (or 48 Full HD) video ports depending on the HD mode configured. The master can allocate the licenses to participants in conferences as necessary. This could be one large conference, or several smaller conferences.

Master blades: All of the port or screen licenses allocated to all the blades in a cluster are "inherited" by the master blade; the master controls all ports in the cluster. Therefore, after the administrator has configured a cluster, functionality is controlled through the master using either its web interface or through its API. All calls to the cluster are made to the master.

Slave blades: Slave blades do not display the full blade web interface. Only certain settings are available, such as network configuration, logging and upgrading. Similarly, a slave blade only responds to a subset of API methods. For more information, refer to the relevant [API documentation](#).

General points

Some points to note about clustering:

- ▶ The cluster support feature key is required on each blade going to be part of the cluster.
- ▶ The MSE 8000 Supervisor blade must be running software version 2.1 or above to configure clustering.
- ▶ The administrator cannot mix the type of blades in a cluster but can have both types of clusters in the same MSE chassis.
- ▶ All blades in a cluster must be running the same version of software.
- ▶ Blades that do not support clustering can be installed into an MSE chassis alongside a cluster.
- ▶ The administrator assigns the cluster roles (master/slave) to the slots in the chassis; if a blade fails, the blade can be replaced with one of the same type and the cluster configuration will persist; however, what happens to active calls and conferences varies, as described below.
- ▶ If the administrator restarts or removes the master, the slaves will also restart: all calls and conferences end.
- ▶ If the Supervisor restarts or is removed, the cluster continues to function, conferences continue, and the cluster does not restart when the Supervisor reappears.
- ▶ If the clustering configuration on the Supervisor and a blade disagree, then the Supervisor pushes the clustering configuration to the blade. (This might happen if the admin replaces a slave blade with another blade of the same type.) The clustering configuration only includes clustering information; it does not configure network settings or anything else on the blade. If the Supervisor has pushed a configuration change to a blade, the Supervisor will prompt the admin to restart the blade.
- ▶ Slave blades only have admin logins.

Always keep a recent backup of the Supervisor.

Appendix B Option keys and screen licenses

This section describes the option and feature keys that are available on the Cisco TelePresence Server. In addition, it describes the screen licenses that need to be purchased for the TelePresence Server.

Option keys

The TelePresence Server requires activation before its features can be used. (If the TelePresence Server has not been activated, the banner at the top of the web interface will show a prominent warning; in every other respect the web interface will look and behave normally.)

If this is a new TelePresence Server, the TelePresence Server should already be activated; if it is not, contact your partner, TAC, or Cisco account to obtain an appropriate activation code.

Activation codes are unique to a particular TelePresence Server and will require the MSE 8710 blade or appliance serial number to generate the activation key.

Regardless of whether the administrator is activating the TelePresence Server or enabling an advanced feature, the process is the same.

Activation keys:

Depending on the model number the activation key will have a different naming structure.

For the 7010 appliance: "TS 7010 activation"

For the 8710: "8510 activation key"

Encryption feature key:

This key is not shipped with the TelePresence Server by default. This key needs to be acquired from the appropriate Cisco contact to get HTTPS and encrypted call support on the TelePresence Server. This feature is the "Encryption" feature on the TelePresence Server.

Third party interop key:

This key is used to group multiple endpoints to act as a single endpoint in the TelePresence Server. In addition, this key is needed for all non-TIP enabled 1 or three-screen systems. This feature is the "Third Party Interop" feature on the TelePresence Server.

Cluster support key:

This key is used for the 8710 blades in the MSE 8000 chassis. It enables the clustering functionality of multiple TelePresence Server 8710 blades using the backplane. From TelePresence Server version 2.2, four 8710 blades are supported in a single cluster.

The following is an example of some of the licenses applied to a Cisco TelePresence Server 7010.

Feature management

Feature management	
Activated features	TelePresence Server 7010 activation (MQV55-YWMHK-X8EKN-972EW) Encryption (VX8G5-Y5LJR-T8WKY-C692A) remove Third party interop (VXKGS-YRVV0-CWUQY-5A3C0) remove TS screen licenses x 16 (L7Y8H-UTP5A-X11GC-BPDU7-6B8F8)
License keys	
Activation code	<input type="text"/> <input type="button" value="Update features"/>

To activate the TelePresence Server or enable an advanced feature:

1. Check the **Activated features** (TelePresence Server activation is shown in this same list) to confirm that the feature required is not already activated.
2. Enter the new feature code into the **Activation code** field exactly, including any dashes.
3. Click **Update features**. The browser window refreshes and lists the newly activated feature, showing the activation code. If the activation code is not valid, the TelePresence Server displays a prompt to re-enter it.

Activation codes may be timed and if this is the case, an expiration date or a warning that the feature has already expired is displayed. Expired activation codes remain listed, but the corresponding feature is not activated.

Successful TelePresence Server or feature activation has immediate effect and persists even if the TelePresence Server is restarted.

Screen licenses

Each TelePresence Server has a certain number of screen licenses, and each screen license effectively activates one FullHD or two HD video ports. If there are fewer screen licenses than the number of video ports provided, then not all of those video ports are available for calls between the TelePresence Server and endpoints. When all screen licenses are in use, the TelePresence Server uses audio-only ports for additional calls.

In a TelePresence Server cluster, activated screen licenses are effectively pooled and allocated to the master blade in the cluster so that the number of available screen licenses is the sum of available screen licenses in the cluster.

In order to activate screen licenses a screen license key is required. For TelePresence Server 8710 blades, the screen license keys are configured on the Supervisor blade and then allocated to the individual TelePresence Server 8710 blades through the Port Licensing page. On a TelePresence Server 7010 add the screen license keys in the same way as other feature keys (go to **Configuration > Upgrade** page and use the Feature Management section).

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

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

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

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

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

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

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

© 2013 Cisco Systems, Inc. All rights reserved.