Cisco TelePresence Management Suite

Product Support Reference Guide

Version 13 – Rev 01

D14990

Sept 2012

Contents

Introducing Cisco TMS interoperability

This document describes the level of support provided by the Cisco TelePresence Management Suite (Cisco TMS) for both Cisco and third party products. Full details of this interoperability are covered in two companion documents, which are intended to be used together:

- This document, which describes product configuration and network requirements.
- The Product Support Feature Matrix, which lists out individual feature compatibility for each product type.

This document is split into product categories, and then into specific product types. For each product type, information is provided on version compatibility, configuration requirements and network requirements. You must follow the listed requirements to use the product successfully with Cisco TMS.

Due to the nature of software release cycles across many different devices, this document will list the most recently tested combination of products. Please take special note of the Cisco TMS and device versions listed for each product type.

Management Models

When managing systems with Cisco TMS, there are several models and connectivity choices that impact the requirements, configuration, and features supported for managing a device. The different management models related to Cisco TMS are:

- Cisco TMS Managed
- Cisco TMS Managed with Behind Firewall Connectivity
- Cisco TMS Managed with Secure-Only Connectivity
- Cisco TMSPE Provisioned
- Cisco Unified Communications Manager Provisioned

Not all management models are supported by all product types. Where variations occur, they are listed in the relevant product section.

Cisco TMSPE Provisioned and Cisco Unified Communications Manager Provisioned are not covered in the scope of this document.

Refer to Appendix A for a description of the different models.

About the Product Sections

The following information is included for each product listed in this document:

Current status

Possible statuses are as follows:

- Active – New features and functionalities for this product type are evaluated for inclusion in Cisco TMS. Support for future releases of product software will be added to Cisco TMS development roadmaps.
- Maintain – New features and functionalities are no longer actively developed for this product type. Potential software changes are limited to compatibility topics or critical bug fixes.

- Deprecated – Not included in new features or functionalities of Cisco TMS. No guarantee of previous functionality and subject to removal from Cisco TMS. Products of this type in use should be migrated to later supported system types.

Supported and target software versions

Possible support statuses are as follows:

- Tested – When a product's software version is given as "tested" this indicates that the software version has been actively tested for use with the indicated version of Cisco TMS. The assumption in this document and in the Feature Support Matrix is that the indicated versions are in use.
- Target – When a product's software version is given as "target", Cisco intends these software versions to be compatible with the listed Cisco TMS release but does not guarantee compatibility. Incompatibilities may exist in target versions due to changes between product releases or later functionality that is not yet reflected in the Cisco TMS software release. The documentation provided here relates to the tested versions, not the target versions.

Configuration and network requirements

This section includes information such as:

- Configuration settings – settings on the device or in TMS that must be configured for Cisco TMS to successfully manage the device.
- Network ports and protocols – IP network settings that are required for proper communication between Cisco TMS and the managed device.
- Device notes/variations – additional information that does not fall into the above categories. This can include exceptions to the above information or specific notes related to the feature matrix for this device.

Endpoint Products

Cisco TelePresence System Endpoints running TC Software

At a glance

TMS version tested	13.2.1
Product status	Active
Product software versions - tested	TC4.2.1 TC5.1.3
Product software versions - target	TC4.x TC5.x

Cisco TelePresence Endpoints running TC Software represents all single codec Cisco TelePresence systems that run the TC line of software. This includes:

- Cisco TelePresence System Integrator C Series (C40, C60, C90)
- Cisco TelePresence System Quick Set Series (C20, SX20)
- Cisco TelePresence System Profile Series (C Series based)
- Cisco TelePresence System EX Series (EX60, EX90)
- Cisco TelePresence System MX Series (MX200, MX300)

Integrated systems or vertical products based on a single C20/SX20/C40/C60/C90 system are also included but may only be identified as a codec instead of a larger system and the functionality will be limited to the same as a standalone codec.

Configuration Requirements

The following configuration requirements must be met for the device to be managed by Cisco TMS in the traditional ‘Managed by Cisco TMS’ mode:

- Cisco TMS must use the *admin* user account on the device and must have the password for that account.
- **NetworkServices SNMP Mode -** set to at *ReadOnly* or *ReadWrite* for full functionality
- **NetworkServices SNMP CommunityName** - set to a value listed in Cisco TMS’s list of SNMP community names
- Network Services for HTTP and/or HTTPS must be enabled in the managed device.
- **Provisioning Mode** – set to *TMS*

The following settings are required, but can be configured automatically by Cisco TMS after the device is added to Cisco TMS if **Enforce Management Settings** is enabled (recommended)

- **Phonebook Server Type** – set to *TMS*
- **Phonebook Server URL** – set to point at the HTTP phonebook web service in TMS
- **Provisioning ExternalManager Address** – set to the network address of the TMS server. Can be set automatically via DHCP Option 242 if using DHCP.
- **Provisioning ExternalManager Path** – set to the management web service path in TMS

- **Provisioning ExternalManager Protocol** – set to *HTTP* (will be set to HTTPS if Secure-Only mode is enabled in Cisco TMS)

Network Requirements

To be managed by Cisco TMS in the traditional 'Managed by Cisco TMS' mode, a system requires full bi-directional communication over the IP network to Cisco TMS with the following ports and protocols.

Service	Protocol	Port Number	Allows Connections (relative to system)
HTTP Or HTTPS	TCP TCP	80 443	Inbound
HTTP Or HTTPS*	TCP TCP	80 443	Outbound
SNMP	UDP	161	Inbound

***** Only used when Secure-Only Management is enabled, otherwise provisioning/feedback/phonebooks must use HTTP for connections to Cisco TMS and HTTP *must not be blocked on the network*.

Note: Network systems that rewrite source addresses will interfere with communications to Cisco TMS and proxies that require authentication may also hinder communications from systems to Cisco TMS.

Cisco TMS Behind Firewall mode

Supported	Yes
Changes to Requirements	When configured for Behind Firewall connectivity, the network requirements change to only require outbound connectivity via HTTP (TCP Port 80) or HTTPS (TCP Port 443) to Cisco TMS. The managed device can also be behind a NAT device.

Cisco TMS Secure-Only mode

Supported	Yes
Changes to Requirements	The network requirements change in that HTTP and SNMP will not be used and no longer are required. All connectivity to the system will be via HTTPS (TCP Port 443) inbound and outbound with the system. This mode can also be combined with Behind Firewall Connectivity to require only HTTPS (TCP Port 443) outbound from the system. When enabled, protocol and URL settings in the managed systems will be changed to HTTPS instead of HTTP.

Device Notes/Limitations

- The enhanced security rules settings of the system can be used, but the admin user account must be available for TMS to use, and must retain an admin level privilege. Using the 'strong security' or JITC policy settings in the managed system will block some functionality from Cisco TMS including software upgrades.
- To use pre-registration features, the **Provisioning ExternalManager** settings must be configured in the device for it to announce itself to Cisco TMS. The values can be set in the endpoint by an administrator, through the setup wizard on the endpoint, or automatically via DHCP options.

- Cisco TMS does not automatically make endpoints answer calls. If Auto Answer is disabled, a user must manually answer scheduled calls placed to the endpoint. Calls dialed out from the endpoint are handled automatically.
- This section does not describe TC endpoints being managed by Cisco Unified CM. Devices managed by Cisco Unified CM will be treated as a separate product category in this documentation.

Cisco IP Video Phone E20

At a glance

TMS version tested	13.1.2
Product status	Maintain
Product software versions - tested	TE4.1
Product software versions - target	TE4.x TE2.2.x

This category applies specifically to the Cisco IP Video Phone E20 model (E20).

Configuration Requirements

The following configuration requirements must be met for the device to be managed by Cisco TMS in the traditional 'Managed by Cisco TMS' mode:

- Cisco TMS must use the *admin* user account on the device and must have the password for that account.
- **NetworkServices SNMP Mode -** set to at *ReadOnly* or *ReadWrite* for full functionality.
- **NetworkServices SNMP CommunityName** - set to a value listed in Cisco TMS's list of SNMP community names
- Network Services for HTTP and/or HTTPS must be enabled in the managed device.
- **Provisioning Mode** – set to *TMS.*

The following settings are required, but can be configured automatically by Cisco TMS after the device is added to Cisco TMS if **Enforce Management Settings** is enabled (recommended)

- **Phonebook Server Type** – set to *TMS.*
- **Phonebook Server URL** – set to point at the HTTP phonebook web service in TMS.
- **Provisioning ExternalManager Address** – set to the network address of the TMS server. Can be set automatically via DHCP Option 242 if using DHCP.
- **Provisioning ExternalManager Path** – set to the management web service path in TMS.
- **Provisioning ExternalManager Protocol** – set to *HTTP* (will be set to HTTPS if Secure-Only mode is enabled in Cisco TMS).

Network Requirements

To be managed by Cisco TMS in the traditional 'Managed by Cisco TMS' mode, a system requires full bi-directional communication over the IP network to Cisco TMS with the following ports and protocols.

Service	Protocol	Port Number	Allows Connections (relative to system)
HTTP Or HTTPS	TCP TCP	80 443	Inbound
HTTP	TCP	80	Outbound
SNMP	UDP	161	Inbound

Note: Network systems that rewrite source addresses will interfere with communications to Cisco TMS and proxies that require authentication may also hinder communications from systems to Cisco TMS.

Cisco TMS Behind Firewall mode

Supported	Yes
Changes to Requirements	When configured for Behind Firewall connectivity, the network requirements change to only require outbound connectivity via HTTP (TCP Port 80) or HTTPS (TCP Port 443) to Cisco TMS. The managed device can also be behind a NAT device.

Cisco TMS Secure-Only mode

Supported	No
Changes to Requirements	This system type is not supported by secure-only mode, so its configuration and network requirements do not change.

Device Notes/Limitations

- Cisco TMS does not automatically make endpoints answer calls. If Auto Answer is disabled, a user must manually answer scheduled calls placed to the endpoint. Calls dialed out from the endpoint are handled automatically.
- TE 4 and later support multiple lines/identities on the system, but Cisco TMS will only interact with SIP Profile 1 of the system. Identities on other lines will not be used and will not resolve to this system in features such as reporting or conference monitoring.
- Cisco TMS does not currently support the H323 interface for E20.
- To use pre-registration features, the **Provisioning ExternalManager** settings must be configured in the device for it to announce itself to Cisco TMS. The values can be set in the endpoint by an administrator, through the setup wizard on the endpoint, or automatically via DHCP options.

TANDBERG T150 MXP

At a glance

TMS version tested	13.1.2
Product status	Maintain
Product software versions – tested	L6.1
Product software versions – target	L6.x

This section applies exclusively to the TANDBERG T150MXP which runs L series software. The Cisco 7985 product while similar to the TANDBERG T150MXP is not equivalent and not supported in TMS.

Configuration Requirements

The following configuration requirements must be met for the device to be managed by Cisco TMS in the traditional 'Managed by Cisco TMS' mode:

- Cisco TMS must use the *admin* user account on the device and must have the password for that account.
- **SNMP Mode** – set to On for full functionality.
- **SNMP CommunityName** - set to a value listed in Cisco TMS's list of SNMP community names.
- **FTP Mode** – set to On for full functionality.

The following settings are required, but can be configured automatically by Cisco TMS after the device is added to Cisco TMS if **Enforce Management Settings** is enabled (recommended)

- **SNMP HostIPAddr** – one entry set to the network address of the Cisco TMS server.
- **CorporateDirectory Mode** - set to On.
- **CorporateDirectory Protocol** - set to *HTTP.*
- **CorporateDirectory Address** - set to the network address of Cisco TMS.
- **ExternalManager Address** - set to the network address of the TMS server. Can be set automatically via DHCP Option 242 if using DHCP.
- **ExternalManager Path** - set to the management web service path for Cisco TMS.
- **ExternalManager Protocol** - set to *HTTP.*

Network Requirements

To be managed by Cisco TMS in the traditional 'Managed by Cisco TMS' mode, a system requires full bi-directional communication over the IP network to Cisco TMS with the following ports and protocols.

Service	Protocol	Port Number	Allows Connections (relative to system)
HTTP Or HTTPS	TCP TCP	80 443	Inbound

Service	Protocol	Port Number	Allows Connections (relative to system)
HTTP	TCP	80	Outbound
SNMP	UDP	161	Inbound
SNMP Trap	UDP	162	Outbound
FTP	TCP	21	Inbound
FTP (data)	TCP	22	Outbound
Telnet*	TCP	23	Inbound

* Recommended, but not required for Cisco TMS management of system.

Note: Network systems that rewrite source addresses will interfere with communications to Cisco TMS and proxies that require authentication may also hinder communications from systems to Cisco TMS.

Cisco TMS Behind Firewall mode

Supported	Yes
Changes to Requirements	When configured for Behind Firewall connectivity, the network requirements change to only require outbound connectivity via HTTP (TCP Port 80) or HTTPS (TCP Port 443) to Cisco TMS. The managed device can also be behind a NAT device.

Cisco TMS Secure-Only mode

Supported	No
Changes to Requirements	This system type is not supported by secure-only mode, so its configuration and network requirements do not change.

Device Notes/Limitations

- Cisco TMS does not automatically make endpoints answer calls. If Auto Answer is disabled, a user must manually answer scheduled calls placed to the endpoint. Calls dialed out from the endpoint are handled automatically.
- To use pre-registration features, the **ExternalManager Address** setting must be configured in the device for it to announce itself to Cisco TMS. The value can be set in the endpoint by an administrator, through the setup wizard on the endpoint, or automatically via DHCP options.

Cisco TelePresence System MXP Series

At a glance

TMS version tested	13.1.2
Product status	Maintain
Product software versions - tested	F9.1
Product software versions - target	F9.x

Cisco TelePresence System MXP Series represents all single codec Cisco TelePresence Systems based on the MXP family of codecs that that run the F line of software. This includes room, integrator, and personal systems such as:

- Cisco TelePresence System 1000 MXP
- Cisco TelePresence System 1700 MXP
- Cisco TelePresence System Profile 3000 MXP/6000 MXP
- Cisco TelePresence System Codec 3000 MXP/6000 MXP
- Cisco TelePresence Set-top 770/880/990
- Cisco TelePresence System Edge 75 MXP/85 MXP/95 MXP

Integrated systems or vertical products based on 3000 MXP or 6000 MXP systems are also included but may only be identified as a codec instead of a larger system and the functionality will be limited to the same as a standalone codec.

Configuration Requirements

The following configuration requirements must be met for the device to be managed by Cisco TMS in the traditional 'Managed by Cisco TMS' mode:

- Cisco TMS must use the *admin* user account on the device and must have the password for that account.
- **SNMP Mode** – set to On for full functionality.
- **SNMP CommunityName** - set to a value listed in Cisco TMS's list of SNMP community names.
- **FTP Mode** – set to On for full functionality.

The following settings are required, but can be configured automatically by Cisco TMS after the device is added to Cisco TMS if **Enforce Management Settings** is enabled (recommended)

- **SNMP HostIPAddr** – one entry set to the network address of the Cisco TMS server.
- **CorporateDirectory Mode** - set to On.
- **CorporateDirectory Protocol** - set to *HTTP.*
- **CorporateDirectory Address** - set to the network address of Cisco TMS.
- **ExternalManager Address** - set to the network address of the TMS server. Can be set automatically via DHCP Option 242 if using DHCP.
- **ExternalManager Path** - set to the management web service path for Cisco TMS.
- **ExternalManager Protocol** - set to *HTTP.*

Network Requirements when Cisco TMS managed

To be managed by Cisco TMS in the traditional ‘Managed by Cisco TMS’ mode, a system requires full bi-directional communication over the IP network to Cisco TMS with the following ports and protocols.

Service	Protocol	Port Number	Allows Connections (relative to system)
HTTP Or HTTPS	TCP TCP	80 443	Inbound
HTTP Or HTTPS*	TCP TCP	80 443	Outbound
SNMP	UDP	161	Inbound
SNMP Trap	UDP	162	Outbound
FTP	TCP	21	Inbound
FTP (data)	TCP	22	Outbound
Telnet**	TCP	23	Inbound

***** Only used when Secure-Only Management is enabled, otherwise provisioning/feedback/phonebooks must use HTTP for connections to Cisco TMS and HTTP *must not be blocked on the network*.

** Recommended, but not required for Cisco TMS management of system.

Note: Network systems that rewrite source addresses will interfere with communications to Cisco TMS and proxies that require authentication may also hinder communications from systems to Cisco TMS.

Cisco TMS Behind Firewall mode

Supported	Yes
Changes to Requirements	When configured for Behind Firewall connectivity, the network requirements change to only require outbound connectivity via HTTP (TCP Port 80) or HTTPS (TCP Port 443) to Cisco TMS. The managed device can also be behind a NAT device.

Cisco TMS Secure-Only mode

Supported	Yes
Changes to Requirements	The network requirements change in that HTTP, FTP and SNMP will not be used and no longer are required. All connectivity to the system will be via HTTPS (TCP Port 443) inbound and outbound with the system. This mode can also be combined with Behind Firewall Connectivity to require only HTTPS (TCP Port 443) outbound from the system. When enabled, protocol and URL settings in the managed systems will be changed to HTTPS instead of HTTP.

Device Notes/Limitations

- Cisco TMS does not automatically make endpoints answer calls. If Auto Answer is disabled, a user must manually answer scheduled calls placed to the endpoint. Calls dialed out from the endpoint are handled automatically.

- To use pre-registration features, the **ExternalManager Address** setting must be configured in the device for it to announce itself to Cisco TMS. The value can be set in the endpoint by an administrator, through the setup wizard on the endpoint, or automatically via DHCP options.

Polycom HDX Series Systems

At a glance

TMS version tested	13.1.2
Product status	Active
Product software versions - tested	v3.0.3.1 v2.6.0.2
Product software versions - target	v3.0.x v2.6.x

Polycom HDX Series represents all single codec Polycom systems based on the HDX family of codecs family of codecs that that run the same HDX system software. This includes room, integrator, and personal systems from the:

- Polycom HDX 6000 Series
- Polycom HDX 7000 Series
- Polycom HDX 8000 Series
- Polycom HDX 9000 Series
- Polycom HDX 4000 Series

Integrated systems or vertical products based on a single HDX codec are also included but may only be identified as a codec instead of a larger system and the functionality will be limited to the same as a standalone codec.

Cisco does not validate all product variations of the HDX product line, but tests with key system types in the HDX product line. Cisco tests with HDX 9004, HDX 8006, and HDX4000 systems. Other HDX variants should be compatible, but compatibility is not explicitly tested or guaranteed.

Configuration Requirements

The following configuration requirements must be met for the device to be managed by Cisco TMS in the traditional 'Managed by Cisco TMS' mode:

- Cisco TMS must use the *admin* user account, the account must have administrative privileges on the device and must have the password for that account.
- **SNMP Community Name** - set to a value listed in Cisco TMS's list of SNMP community names.
- **Console IP Address** – set to the network address of Cisco TMS.
- **Enable Remote Access** must be enabled for **Web**, **Telnet**, and **SNMP.**
- **Call Detail Report** option under **System Settings** > **Call Settings** must be enabled for full functionality.
- **Allow Video Display on Web** under **System Settings** > **Security** must be enabled for full functionality.
- **Polycom GDS** directory setting must be enabled.

The following settings are required, but can be configured automatically by Cisco TMS after the device is added to Cisco TMS if **Enforce Management Settings** is enabled (recommended)

- **Global Directory (GDS) Server address** set to network address of Cisco TMS and **register** checkbox enabled.
- **Management Server URL** – set to the feedback handler on Cisco TMS (Ex: `http://10.10.10.2/pwx/nx_status.asp`).

Network Requirements

To be managed by Cisco TMS in the traditional 'Managed by Cisco TMS' mode, a system requires full bi-directional communication over the IP network to Cisco TMS with the following ports and protocols.

Service	Protocol	Port Number	Allows Connections (relative to system)
HTTP	TCP	80	Inbound
HTTPS	TCP	443	Inbound
HTTP	TCP	80	Outbound
SNMP	UDP	161	Inbound
API	TCP	24	Inbound

Note: Network systems that rewrite source addresses will interfere with communications to Cisco TMS and proxies that require authentication may also hinder communications from systems to Cisco TMS.

Cisco TMS Behind Firewall mode

Supported	No
Changes to Requirements	This system type is not supported by behind firewall mode, so its configuration and network requirements do not change.

Cisco TMS Secure-Only mode

Supported	No
Changes to Requirements	This system type is not supported by secure-only mode, so its configuration and network requirements do not change.

Device Notes/Limitations

- **Secure Mode** must not be enabled (it makes the system read-only for settings), **Security Profile** must be set to Medium or lower, and **Enable Sessions List** must not be enabled.
- The system should not be managed by another Management System (such as Polycom CMA) if the device is being managed by Cisco TMS.
- The **Management Servers** setting is not configurable via the Polycom user interfaces and can only be set by the management system.
- Cisco TMS does not automatically make endpoints answer calls. If Auto Answer is disabled, a user must manually answer scheduled calls placed to the endpoint. Calls dialed out from the endpoint are handled automatically.
- Call preference cannot be set to *manual* if both ISDN and ISDN Gateway call profiles are enabled on the endpoint as the endpoint cannot dial API initiated ISDN calls automatically in this configuration. Change Call Preference to *Auto*, or disable the ISDN Gateway call profile in the endpoint.
- The default telnet and web ports must not be changed from their default values to work with Cisco TMS.
- Use of the Polycom Touch Panel control for HDX systems impacts the controls and behavior of the HDX system. Cisco TMS does not support the Touch Panel and it's use may cause configuration mismatches.

- Some configuration changes in Polycom HDX systems require the system reboot immediately for the change to take effect. This reboot may cause settings changes to take longer to complete or may cause the endpoint to appear unreachable temporarily. Examples include changes to SNMP or DNS settings.
- Cisco TMS does not support the use of analog telephone lines for HDX systems
- The call preference for **preferred speed** defined in the system will override bandwidths set in the Cisco TMS phonebooks sent to the system
- Cisco TMS Phonebooks do not support presence for Polycom GDS entries added to favorites groups
- The maximum IP bandwidth for all HDX endpoints is defined to be 4096 kbs
- The maximum IP bandwidth TMS can dial for HDX endpoints is 1920kbs.

Cisco TelePresence Systems (CTS Systems)

At a glance

TMS version tested	13.2.1
Product status	Active
Product software versions - tested	
Product software versions - target	1.7.x, 1.8.x, 1.9.x

This section is incomplete in this revision of the documentation and will be completed in an upcoming revision of this document.

Cisco TelePresence T3 (and TANDBERG TelePresence T1)

At a glance

TMS version tested	13.2.1
Product status	Active (not the T1)
Product software versions - tested	
Product software versions - target	4.x

This section is incomplete in this revision of the documentation and will be completed in an upcoming revision of this document.

Cisco SCCP Endpoints

At a glance

TMS version tested	13.2.1
Product status	Deprecated
Product software versions - tested	
Product software versions - target	M2.2

Cisco SCCP endpoints represent the TANDBERG MXP endpoints running the M-series of software for use with Cisco Unified Communications Manager.

This section is incomplete in this revision of the documentation and will be completed in an upcoming revision of this document.

TANDBERG Classic Endpoints

At a glance

TMS version tested	13.2.1
Product status	Deprecated
Product software versions - tested	
Product software versions - target	B10.3/E5.3

TANDBERG Classic endpoints represents the TANDBERG 500, 550, 770, 800, 880, 990, 1000, 2500, 6000, 7000, and 8000 systems. Classic systems run software from version A1.x through B10.x and E1.x through E5.x.

This section is incomplete in this revision of the documentation and will be completed in an upcoming revision of this document.

Polycom VSX Series

At a glance

TMS version tested	13.2.1
Product status	Deprecated
Product software versions - tested	
Product software versions - target	9.0.5.x

Polycom VSX series represents the Polycom 7000, VSX 8000, VSX 3000, VSX 500 endpoints and their variants.

This section is incomplete in this revision of the documentation and will be completed in an upcoming revision of this document.

Polycom Viewstation Series

At a glance

TMS version tested	13.2.1
Product status	Deprecated
Product software versions -	

tested	
Product software versions - target	7.5.x

Polycom Viewstations Series represents the Viewstation 128, SP, H323, 384, 512, and MP. The Viewstation DCP system is not included.

This section is incomplete in this revision of the documentation and will be completed in an upcoming revision of this document.

Polycom FX Series

At a glance

TMS version tested	13.2.1
Product status	Deprecated
Product software versions - tested	
Product software versions - target	6.0.x

Polycom FX series represents the Polycom Viewstation FX, VS4000, and EX endpoints and their variants.

This section is incomplete in this revision of the documentation and will be completed in an upcoming revision of this document.

Polycom iPower Endpoints

At a glance

TMS version tested	13.2.1
Product status	Deprecated
Product software versions - tested	
Product software versions - target	6.2.0

Polycom iPower Series Endpoints include all systems based on iPower, include the 900 Series, 600 Series, 9000 Series, and their packaged variants.

This section is incomplete in this revision of the documentation and will be completed in an upcoming revision of this document.

Polycom ViaVideo Endpoints

At a glance

TMS version tested	13.2.1
Product status	Deprecated
Product software versions - tested	
Product software versions - target	5.1.1

Polycom ViaVideo endpoints represent systems running the ViaVideo software with either revision of ViaVideo Camera. The Polycom PVX software is not included in this category.

This section is incomplete in this revision of the documentation and will be completed in an upcoming revision of this document.

Sony PCS Series

At a glance

TMS version tested	13.2.1
Product status	Deprecated
Product software versions - tested	
Product software versions - target	3.42

Sony PCS series represents the PCS-1600, PCS6000, TL-50, GL-70, and PCS-1 endpoints and their variants.

This section is incomplete in this revision of the documentation and will be completed in an upcoming revision of this document.

VTEL Galaxy Series

At a glance

TMS version tested	13.2.1
Product status	Deprecated
Product software versions - tested	
Product software versions - target	2.2.0.70

VTEL Galaxy Series represents the range of PC based endpoints running the Galaxy software.

This section is incomplete in this revision of the documentation and will be completed in an upcoming revision of this document.

Aethra VegaStar Series

At a glance

TMS version tested	13.2.1
Product status	Deprecated
Product software versions - tested	
Product software versions - target	6.0.49

Aethra VegaStar series represents the VegaStar Gold and Silver products and their variants.

This section is incomplete in this revision of the documentation and will be completed in an upcoming revision of this document.

Conferencing Products

Cisco TelePresence MCU 42xx/45xx/8420/8510

At a glance

TMS version tested	13.2.1
Product status	Active

Product software versions - tested	4.3(2.30)
	4.2(1.50)

Product software versions - target	4.3, 4.2

Cisco TelePresence MCU in this section refers to the 4200 and 4500 series of TelePresence MCUs and their model variants. The MSE blade versions of these MCU series, MSE8420 and MSE8510 are also covered by this section.

Configuration Requirements

The following configuration requirements must be met for the device to be managed by Cisco TMS in the traditional 'Managed by Cisco TMS' mode:

- Cisco TMS must be provided a username and password of an account on the MCU that has administrator privileges.
- HTTPS and/or HTTP service must be enabled on their default ports
- **SNMP Service** should be enabled on the default port for full functionality
- **SNMP RO Community Name** - set to a value listed in Cisco TMS's list of SNMP community names

The following settings are required, but can be configured automatically by Cisco TMS after the device is added to Cisco TMS if **Enforce Management Settings** is enabled (recommended)

- feedback receiver URL - must be set to point to the Cisco TMS server. This setting is not accessible via the device's web interface but will be configured automatically when the device is added to Cisco TMS

Conference Aliasing Setup

Note: It is important that aliases are configured prior to opening the MCU for scheduling by users. If you change the aliases used by Cisco TMS for the MCU, existing scheduled meetings that use that MCU will need to be rebooked by editing the existing conference to update the conference to the new aliases.

Aliases used for conferences created by Cisco TMS on the MCU are a combination of the MCU's prefix settings and the Meeting ID settings defined in System Navigator for the MCU. One alias is computed for each possible conference the MCU could host, up to the total number of ports in the MCU.

Meeting IDs are defined per MCU in **System Navigator** under **Extended Settings** for the system. The **First Meeting ID** value is used for the first alias, and each additional alias is created by incrementing the alias by the **Meeting ID step** value.

H.323 aliases are created by prefixing the Meeting IDs with the H.323 prefix value defined in the MCU. The MCU's prefix settings are found in the **Settings** > **H323** page of the MCU's web interface. The choice of MCU's prefix registration settings should be set based on your desired dial plan. The prefixes are optional, but it is recommended that **Prefix for MCU registrations** be used. Alternatively, the **MCU Service prefix** may be defined, or both prefixes may be defined; but if both prefixes are enabled they both must be set to the same value.

If **Prefix for MCU registrations** is used, and **MCU Service Prefix** is not, the MCU setting **Allow numeric ID registration for conferences** must be enabled in the MCU's H.323 configuration. (**Settings** > **H.323**). If using SIP, the MCU setting **Allow numeric ID registration for conferences** must be enabled in the MCU's SIP configuration. (**Settings** > **SIP**).

SIP aliases are created using the same Meeting ID settings in Cisco TMS, but the SIP registrar domain is suffixed to the Meeting ID to create the aliases rather than using the MCU's prefix settings. The MCU's SIP registar domain setting is found in **Settings** > **SIP** of the MCU's web interface.

The resulting computed aliases to be used by Cisco TMS are listed in the **View Settings** page for the MCU in **System Navigator**.

ISDN Calling

An MCU can be accessible for ISDN dial in and out if a gateway is configured for the IP Zone assigned to the MCU. Call routes will be via the gateway's call prefixes and DID number. If the setting **Enable ISDN Gateway DID Mapping** under **Extended Settings** for the MCU in **System Navigator** is enabled, dial in ISDN call routes for the MCU will use those ISDN numbers rather than the gateway's DID number. Which ISDN numbers to use should be based on your network's dial plan and translations. Handling of routing or translation of those ISDN numbers to the actual conference aliases must be provisioned in your network's dial plan and is not configured by enabling this setting.

Multiple Network Interfaces

The MCU supports multiple network interfaces, and more than one network interface may be enabled when used with Cisco TMS. However, all management and awareness of the device will only interact with one port. The second port will not be visible in Cisco TMS views.

Network Requirements

To be managed by Cisco TMS in the traditional 'Managed by Cisco TMS' mode, a system requires full bi-directional communication over the IP network to Cisco TMS with the following ports and protocols.

Service	Protocol	Port Number	Allows Connections (relative to system)
HTTP Or HTTPS	TCP TCP	80 443	Inbound
HTTP Or HTTPS*	TCP TCP	80 443	Outbound
SNMP (optional)	UDP	161	Inbound

***** Only used when Secure-Only Management is enabled, otherwise provisioning/feedback/phonebooks must use HTTP for connections to Cisco TMS and HTTP *must not be blocked on the network*.

Note: Network systems that rewrite source addresses will interfere with communications to Cisco TMS and proxies that require authentication may also hinder communications from systems to Cisco TMS.

Cisco TMS Behind Firewall mode

Supported	No
Changes to Requirements	This system type is not supported by Behind Firewall mode, so its configuration and network requirements do not change.

Cisco TMS Secure-Only mode

Supported	Yes
Changes to Requirements	The network requirements change in that HTTP and SNMP will not be used and no longer are required. All connectivity to the system will be via HTTPS (TCP Port 443) inbound and outbound with the system. When enabled, the management URL setting in the managed system will be changed to HTTPS instead of HTTP.

Device Notes/Limitations

- When using scheduling features of Cisco TMS with the MCU, conferences should only be started from Cisco TMS. Creating conferences outside of TMS, such as via the auto-attendant or permanent conferences on the MCU may cause aliasing or capacity conflicts which may lead to failure of scheduled conferences
- Cisco TMS must be able to read the gatekeeper and/or SIP registrar from the MCU to allow scheduling of the MCU. So MCUs reachable only via SIP Trunk and not registration will not be schedulable in Cisco TMS.
- Nodes defined as a slave in a cluster can be added to Cisco TMS, but their functionality will be reduced to only monitoring Connection Status. Clustered MCUs should have their master node added into Cisco TMS to schedule and manage the MCU functions of the cluster.
- Use of the SNMP service in the MCU is optional. If not enabled, automatic discovery of the MCU is not available, and the MCU must be added as with the ‘Non-SNMP’ option enabled when adding it into Cisco TMS.

Cisco TelePresence Server

At a glance

TMS version tested	13.2.1
Product status	Active

Product software versions - tested	2.2(1.54)
	2.3(1.50)

Product software versions - target	2.2, 2.3

Cisco TelePresence Server in this section refers to the TelePresence Server 7010 and MSE 8710 series of MCUs and their model variants.

Configuration Requirements

The following configuration requirements must be met for the device to be managed by Cisco TMS in the traditional 'Managed by Cisco TMS' mode:

- Cisco TMS must be provided a username and password of an account on the MCU that has administrator privileges.
- HTTPS and/or HTTP service must be enabled on their default ports

The following settings are required, but can be configured automatically by Cisco TMS after the device is added to Cisco TMS if **Enforce Management Settings** is enabled (recommended)

- feedback receiver URL - must be set to point to the Cisco TMS server. This setting is not accessible via the device's web interface but will be configured automatically when the device is added to Cisco TMS

Conference Aliasing

Note: It is important that aliases are configured prior to opening the MCU for scheduling by users. If you change the aliases used by Cisco TMS for the MCU, existing scheduled meetings that use that MCU will need to be rebooked by editing the existing conference to update the conference to the new aliases.

Aliases used for conferences created by Cisco TMS on the MCU are based on the Meeting ID settings defined for the MCU in **System Navigator**. One alias is computed for each possible conference the MCU could host, up to the total number of ports in the MCU.

Meeting IDs are defined per MCU in **System Navigator** under **Extended Settings** for the system. The **First Meeting ID** value is used for the first alias, and each additional alias is created by incrementing the alias by the **Meeting ID step** value. The computed Meeting IDs are used as the H.323 alias to register for conferences by Cisco TMS scheduling.

SIP aliases are created using the same Meeting ID settings in Cisco TMS, but the SIP Outbound domain is suffixed to the Meeting ID to create the aliases. The MCU's SIP Outbound domain setting is found in **Configuration** > **System Settings** of the MCU's web interface.

The resulting computed aliases to be used by Cisco TMS are listed in the **View Settings** page for the MCU in **System Navigator**.

For dial-in for conferences to function, **the Register With Gatekeeper** and **Conference SIP Registration** settings under **MCU Settings** must be enabled on scheduled conferences. These are enabled by default in Cisco TMS, and their default value for new conferences is managed in the **Extended Settings** page for the device in **System Navigator**.

Multiple Network Interfaces

The MCU supports multiple network interfaces, and more than one network interface may be enabled when used with Cisco TMS. However, all management and awareness of the device will only interact with one port. The second port will not be visible in Cisco TMS views.

Network Requirements

To be managed by Cisco TMS in the traditional 'Managed by Cisco TMS' mode, a system requires full bi-directional communication over the IP network to Cisco TMS with the following ports and protocols.

Service	Protocol	Port Number	Allows Connections (relative to system)
HTTP Or HTTPS	TCP TCP	80 443	Inbound
HTTP	TCP	80	Outbound

Note: Network systems that rewrite source addresses will interfere with communications to Cisco TMS and proxies that require authentication may also hinder communications from systems to Cisco TMS.

Cisco TMS Behind Firewall mode

Supported	No
Changes to Requirements	This system type is not supported by Behind Firewall mode, so its configuration and network requirements do not change.

Cisco TMS Secure-Only mode

Supported	No
Changes to Requirements	This system type is not supported by secure-only mode, so its configuration and network requirements do not change.

Device Notes/Limitations

- When using scheduling features of Cisco TMS with the MCU, conferences should only be started from Cisco TMS. Creating conferences outside of TMS, such as via the auto-attendant or permanent conferences on the MCU may cause aliasing or capacity conflicts which may lead to failure of scheduled conferences
- Cisco TMS must be able to read the gatekeeper and/or SIP registrar from the MCU to allow scheduling of the MCU. So MCUs reachable only via SIP Trunk and not registration will not be schedulable in Cisco TMS.
- TelePresence Servers defined to have their conferences managed by an external server (slave blade) can be added to Cisco TMS, but their functionality will be reduced to only monitoring Connection Status. Clustered MCUs should have their master node added into Cisco TMS to schedule and manage the MCU functions of the cluster.
- Due to lack of SNMP support, when adding this type of system into Cisco TMS, you must use the **Discovery Non-SNMP Systems** option when adding the system.

Cisco TelePresence Conductor

At a glance

TMS version tested	13.2.1
Product status	Active
Product software versions - tested	
Product software versions - target	

This section is incomplete in this revision of the documentation and will be completed in an upcoming revision of this document.

TANDBERG MPS

At a glance

TMS version tested	13.2.1
Product status	Maintain
Product software versions - tested	
Product software versions - target	J4.7

TANDBERG MPS represents the MPS 800 and MPS 200 modular MCU systems. It does not include MPS systems used exclusively as gateway systems.

This section is incomplete in this revision of the documentation and will be completed in an upcoming revision of this document.

TANDBERG MCU

At a glance

TMS version tested	13.2.1
Product status	Deprecated
Product software versions - tested	
Product software versions - target	D3.10

TANDBERG MCU represents the TANDBERG 8+8 and 16+16 MCU products.

This section is incomplete in this revision of the documentation and will be completed in an upcoming revision of this document.

Polycom MGC MCU Series

At a glance

TMS version tested	13.2.1
Product status	Deprecated
Product software versions - tested	
Product software versions - target	8.0.2

Polycom MGC MCU series represents the MGC-100, MGC-50, and MGC-25 MCU products from Polycom.

This section is incomplete in this revision of the documentation and will be completed in an upcoming revision of this document.

Radvision/Cisco viaIP MCUs

At a glance

TMS version tested	13.2.1
Product status	Deprecated
Product software versions - tested	
Product software versions - target	4.2.10

The Radvision/Cisco viaIP MCUs represents the MCUs based on the Radvision viaIP platform including MCU-30, MCU-60, MCU-100, Cisco 3540, Cisco 3511.

This section is incomplete in this revision of the documentation and will be completed in an upcoming revision of this document.

Infrastructure Products

Cisco Unified Communications Manager

At a glance

TMS version tested	13.2.1
Product status	Active
Product software versions - tested	8.6.2
Product software versions - target	8.x, 9.x

Cisco Unified Communications Manager refers to all instances of Cisco Unified Communications Manager (Unified CM) independent of the specific platform hosting Cisco Unified CM. This does not apply to other editions such as Express or Business Editions.

Configuration Requirements

The following configuration requirements must be met for the device to be managed by Cisco TMS in the traditional 'Managed by Cisco TMS' mode:

For Cisco TMS to communicate with the Cisco UCM, the following services must be active in Cisco UCM:

- Cisco AXL Web Service on the Cisco Unified CM node to be added to Cisco TMS
- Cisco RIS Data Collector on the Cisco Unified CM Publisher node
- Cisco CTIManager on at least one of the nodes in the Cisco Unified CM Cluster

See the Cisco UCM Configuration Guide for the Cisco TelePresence System for details on service activation

An application user and user group with sufficient permissions must exist in Cisco Unified CM for Cisco TMS to communicate with the UCM node. All Cisco TelePresence endpoints and rooms should be assigned to the application user's profile. The application user must be assigned to a user group with at least the following roles enabled:

- Standard AXL API Access
- Standard CTI Enabled
- Standard SERVICEABILITY
- Standard CCM Admin Users
- Standard RealtimeAndTraceCollection

For more detailed instructions on creating an application user and user group, please see the Cisco TMS Administrator Guide. CTS Endpoints that are managed by the Cisco Unified CM that will be added to Cisco TMS require the following settings:

- **Allow Control of Device from CTI** be enabled
- **Room Name** defined
- **SSH AdminLife** set to 0

For more information, please see the Cisco TMS Administrator Guide.

Network Requirements when Cisco TMS managed

To be managed by Cisco TMS, a system requires full bi-directional communication over the IP network to Cisco TMS with the following ports and protocols.

8443 https

Service	Protocol	Port Number	Allows Connections (relative to system)
HTTPS	TCP	443	Inbound
CUCM Services	TCP	8443	Inbound

Cisco TMS Behind Firewall mode

Supported	No
Changes to Requirements	This system type is not supported by Behind Firewall mode, so its configuration and network requirements do not change.

Cisco TMS Secure-Only mode

Supported	No
Changes to Requirements	This system type is not supported by secure-only mode, so its configuration and network requirements do not change.

Device Notes/Limitations

- Use of Cisco Unified CM version 8.6.x or later is necessary for Native Interop modes and is strongly suggested for its later SIP functionalities in TelePresence
- A **Managed System** tab is added to System Navigator for the system to show the details of telepresence systems known to the Unified CM
- Due to lack of SNMP usage, when adding this type of system into Cisco TMS, you must use the **Discovery Non-SNMP Systems** option when adding the system.

Cisco TelePresence Video Communication Server

At a glance

TMS version tested	13.2.1
Product status	Active
Product software versions - tested	X7.2 X6.1
Product software versions - target	X7.x, X6.x

Cisco TelePresence Video Communication Server (VCS) refers to both Control and Expressway variants of the product in both appliance and virtualized formats.

Configuration Requirements when Cisco TMS managed

The following configuration requirements must be met for the device to be managed by Cisco TMS in the traditional 'Managed by Cisco TMS' mode:

- Cisco TMS must use the *admin* user account on the device and must have the password for that account.
- **SNMP mode** should be enabled for full functionality and must be set to *v3 plus TMS Support* or *v2c*
- **SNMP Community Name -** set to a value listed in Cisco TMS's list of SNMP community names
- **Web Interface (over HTTPS)** setting must be enabled

The following settings are required, but can be configured automatically by Cisco TMS after the device is added to Cisco TMS if **Enforce Management Settings** is enabled (recommended)

- **ExternalManager Address** – set to the network address of the TMS server.
- **ExternalManager Path** – set to the management web service path in TMS.
- **ExternalManager Protocol** – set to *HTTP* (will be set to HTTPS if Secure-Only mode is enabled in Cisco TMS).

Multiple Network Interfaces

The VCS supports multiple network interfaces, and more than one network interface may be enabled when used with Cisco TMS. However, all management and awareness of the device will only interact with one port. The second port will not be visible in Cisco TMS views.

Network Requirements

If using the Cisco TMS Agent Legacy or Cisco TMS Provisioning Extension, additional configuration and network requirements that are not listed in this document are necessary. Please refer to the provisioning deployment documentation on Cisco.com

To be managed by Cisco TMS, a system requires full bi-directional communication over the IP network to Cisco TMS with the following ports and protocols.

Service	Protocol	Port Number	Allows Connections (relative to system)

Service	Protocol	Port Number	Allows Connections (relative to system)
HTTP Or HTTPS	TCP TCP	80 443	Inbound
HTTP Or HTTPS*	TCP TCP	80 443	Outbound
SNMP (optional)	UDP	161	Inbound

***** Only used when Secure-Only Management is enabled, otherwise provisioning/feedback/phonebooks must use HTTP for connections to Cisco TMS and HTTP *must not be blocked on the network*.

Note: Network systems that rewrite source addresses will interfere with communications to Cisco TMS and proxies that require authentication may also hinder communications from systems to Cisco TMS.

Cisco TMS Behind Firewall mode

Supported	No
Changes to Requirements	This system type is not supported by Behind Firewall mode, so its configuration and network requirements do not change.

Cisco TMS Secure-Only mode

Supported	Yes
Changes to Requirements	The network requirements change in that HTTP and SNMP will not be used and no longer are required. All connectivity to the system will be via HTTPS (TCP Port 443) inbound and outbound with the system. When enabled, the management URL setting in the managed system will be changed to HTTPS instead of HTTP.

Device Notes/Limitations

- Advanced Security Mode can not be used as it disables the ‘admin’ account which Cisco TMS must use to login to the device
- CDR Logging is not functioning for X7.2 See CDETS Case CSCub66229 for status updates
- Use of the SNMP service in the device is optional. If not enabled, automatic discovery of the device is not available, and the device must be added as with **Discovery Non-SNMP Systems** option enabled when adding it into Cisco TMS.

Cisco TelePresence Supervisor

At a glance

TMS version tested	13.2.1
Product status	Active

Product software versions - tested	2.2(1.17)
	2.1(1.18)

Product software versions - target	2.2, 2.1

Cisco TelePresence Supervisor in this section refers to the Cisco TelePresence Supervisor MSE 8050 blade for the MSE 8000 chassis.

Configuration Requirements

The following configuration requirements must be met for the device to be managed by Cisco TMS in the traditional ‘Managed by Cisco TMS’ mode:

- Cisco TMS must be provided a username and password of an account on the device that has administrator privileges.
- HTTPS and/or HTTP service must be enabled on their default ports
- **SNMP Service** should be enabled on the default port for full functionality
- **SNMP RO Community Name** - set to a value listed in Cisco TMS’s list of SNMP community names

The following settings are required, but can be configured automatically by Cisco TMS after the device is added to Cisco TMS if **Enforce Management Settings** is enabled (recommended)

- feedback receiver URL - must be set to point to the Cisco TMS server. This setting is not accessible via the device’s web interface but will be configured automatically when the device is added to Cisco TMS

Multiple Network Interfaces

The Supervisor supports multiple network interfaces, and more than one network interface may be enabled when used with Cisco TMS. However, all management and awareness of the device will only interact with one port. The second port will not be visible in Cisco TMS views.

Network Requirements when Cisco TMS managed

To be managed by Cisco TMS in the traditional ‘Managed by Cisco TMS’ mode, a system requires full bi-directional communication over the IP network to Cisco TMS with the following ports and protocols.

Service	Protocol	Port Number	Allows Connections (relative to system)
HTTP Or HTTPS	TCP TCP	80 443	Inbound
HTTP	TCP	80	Outbound
SNMP (optional)	UDP	161	Inbound

Note: Network systems that rewrite source addresses will interfere with communications to Cisco TMS and proxies that require authentication may also hinder communications from systems to Cisco TMS.

Cisco TMS Behind Firewall mode

Supported	No
Changes to Requirements	This system type is not supported by Behind Firewall mode, so its configuration and network requirements do not change.

Cisco TMS Secure-Only mode

Supported	No
Changes to Requirements	This system type is not supported by secure-only mode, so its configuration and network requirements do not change.

Device Notes/Limitations

- Active alarms reported by the supervisor will be represented as tickets in Cisco TMS for the supervisor
- A **Supervisor** tab is added to System Navigator for the system to show the details of the blades inserted in the chassis
- Use of the SNMP service in the device is optional. If not enabled, automatic discovery of the device is not available, and the device must be added as with **Discovery Non-SNMP Systems** option enabled when adding it into Cisco TMS.

Cisco TelePresence ISDN GW

At a glance

TMS version tested	13.2.1
Product status	Active

Product software versions - tested	2.1(1.49)
	2.0(1.51)

Product software versions - target	2.1, 2.0

Cisco TelePresence ISDN GW in this section refers to the Cisco TelePresence ISDN Gateways models ISDN GW 3210/3220/3240/3241 and MSE 8310/8321 ISDN gateways. These products will be generically referred to as the ISDN GW in this section.

Configuration Requirements

The following configuration requirements must be met for the device to be managed by Cisco TMS in the traditional 'Managed by Cisco TMS' mode:

- Cisco TMS must be provided a username and password of an account on the device that has administrator privileges.
- HTTPS and/or HTTP service must be enabled on their default ports.
- **SNMP Service** should be enabled on the default port for full functionality.
- **SNMP RO Community Name** - set to a value listed in Cisco TMS's list of SNMP community names.

The following settings are required, but can be configured automatically by Cisco TMS after the device is added to Cisco TMS if **Enforce Management Settings** is enabled (recommended)

- feedback receiver URL - must be set to point to the Cisco TMS server. This setting is not accessible via the device's web interface but will be configured automatically when the device is added to Cisco TMS.

Multiple Network Interfaces

The gateway supports multiple network interfaces, and more than one network interface may be enabled when used with Cisco TMS. However, all management and awareness of the device will only interact with one port. The second port will not be visible in Cisco TMS views.

Network Requirements when Cisco TMS managed

To be managed by Cisco TMS in the traditional 'Managed by Cisco TMS' mode, a system requires full bi-directional communication over the IP network to Cisco TMS with the following ports and protocols.

Service	Protocol	Port Number	Allows Connections (relative to system)
HTTP Or HTTPS	TCP TCP	80 443	Inbound
HTTP	TCP	80	Outbound

Service	Protocol	Port Number	Allows Connections (relative to system)
SNMP (optional)	UDP	161	Inbound

Note: Network systems that rewrite source addresses will interfere with communications to Cisco TMS and proxies that require authentication may also hinder communications from systems to Cisco TMS.

Cisco TMS Behind Firewall mode

Supported	No
Changes to Requirements	This system type is not supported by Behind Firewall mode, so its configuration and network requirements do not change.

Cisco TMS Secure-Only mode

Supported	No
Changes to Requirements	This system type is not supported by secure-only mode, so its configuration and network requirements do not change.

Device Notes/Limitations

- Management URL configuration only applies in ISDN GW software 2.1 and later

Cisco TelePresence Content Server

At a glance

TMS version tested	13.2.1
Product status	Active
Product software versions - tested	
Product software versions - target	S5.0

Cisco TelePresence Content Server (TCS) refers to the media streaming and recording appliance product.

This section is incomplete in this revision of the documentation and will be completed in an upcoming revision of this document.

Cisco TelePresence IP VCR

At a glance

TMS version tested	13.2.1
Product status	Maintain
Product software versions - tested	
Product software versions - target	3.0

Cisco TelePresence IPVCR refers to the media recording and streaming products including the Cisco IP VCR 22xx series and MSE 8220 products.

This section is incomplete in this revision of the documentation and will be completed in an upcoming revision of this document.

Cisco TelePresence IP Gateway Series

At a glance

TMS version tested	13.2.1
Product status	Maintain
Product software versions - tested	
Product software versions - target	2.0

The Cisco TelePresence IP Gateway series refers to the Cisco IP GW 3500 series and IP GW MSE 8350 products.

This section is incomplete in this revision of the documentation and will be completed in an upcoming revision of this document.

TANDBERG ISDN Gateway

At a glance

TMS version tested	13.2.1
Product status	Deprecated
Product software versions - tested	
Product software versions - target	G3.2

TANDBERG ISDN Gateway refers to the H323<->H320 gateway appliance from TANDBERG. This does not include the MPS product being used as gateway.

This section is incomplete in this revision of the documentation and will be completed in an upcoming revision of this document.

TANDBERG 3G Gateway

At a glance

TMS version tested	13.2.1
Product status	Deprecated
Product software versions - tested	
Product software versions - target	R3.2

TANDBERG 3G Gateway refers to the H323<->H324 gateway appliance from TANDBERG.

This section is incomplete in this revision of the documentation and will be completed in an upcoming revision of this document.

TANDBERG EntryPoint

At a glance

TMS version tested	13.2.1
Product status	Deprecated

Product software versions - tested	
Product software versions - target	EP1.2

TANDBERG Entrypoint refers to the IVR network appliance from TANDBERG.

This section is incomplete in this revision of the documentation and will be completed in an upcoming revision of this document.

Radvision viaIP Gateway

At a glance

TMS version tested	13.2.1
Product status	Deprecated
Product software versions - tested	
Product software versions - target	5.1.0

Radvision viaIP Gateway refer to the PRI GW-P20 gateways of the viaIP family of products from Radvision.

This section is incomplete in this revision of the documentation and will be completed in an upcoming revision of this document.

TANDBERG Gatekeeper/Border Controller

At a glance

TMS version tested	13.2.1
Product status	Deprecated
Product software versions - tested	
Product software versions - target	N6.1/Q6.1

TANDBERG Gatekeeper refers to the appliance gatekeepers from TANDBERG including the Border Controller variant of the product.

This section is incomplete in this revision of the documentation and will be completed in an upcoming revision of this document.

Radvision ECS Gatekeeper

At a glance

TMS version tested	13.2.1
Product status	Deprecated
Product software versions - tested	
Product software versions - target	5.5.0

Ravision ECS Gatekeeper refers to the software gatekeeper from Radvision that could be run on a chassis blade or stand-alone PC.

This section is incomplete in this revision of the documentation and will be completed in an upcoming revision of this document.

Cisco MCM Gatekeeper

At a glance

TMS version tested	13.2.1
Product status	Deprecated
Product software versions - tested	
Product software versions - target	IOS 12.3(10)

Cisco MCM refers to the H.323 Gatekeeper feature set available in some Cisco routers.

This section is incomplete in this revision of the documentation and will be completed in an upcoming revision of this document.

Appendix A – Management Models

There are several modes available for how Cisco TMS may interact with devices. The management mode which impacts the way Cisco TMS communicates with devices and the functionality provided. Not all management modes are available for all device types. A description of each of the modes is provided below:

Cisco TMS Managed

System is managed by Cisco TMS exclusively. Cisco TMS expects bi-directional network connectivity with the system and the system communicates with Cisco TMS directly.

Cisco TMS Managed with Behind Firewall Connectivity

This is a special connectivity option available on a per system basis for systems being managed by Cisco TMS. In this mode, there is no connectivity from Cisco TMS to the system, only outbound connections from the system to Cisco TMS. This reduces some features within Cisco TMS, but enables a system to be managed when there is no direct access to the system from Cisco TMS because the managed device is behind a firewall or NAT router. When in this mode, the network requirements for a system change to requiring only HTTP or HTTPS (if enabled on Cisco TMS) outbound from the system.

Cisco TMS Managed with Secure-Only Connectivity

This is a special connectivity mode in Cisco TMS for system being managed by Cisco TMS where Cisco TMS will only use encrypted, secure protocols like HTTPS to communicate between the device and Cisco TMS. Additionally, the option of strict adherence to certificate security is available. This mode requires specific system support and will not apply to all system types.

When in this mode, only HTTPS inbound and outbound from a system is required for network connectivity. This mode can also be combined with Behind Firewall Connectivity. This mode requires specific configuration on the Cisco TMS server and managed systems. Please see the Implementing Secure Management Reference Guide for more information.

Cisco TMSPE Provisioned

Cisco TMSPE provisioning is an alternative deployment model that allows for a user-centric management, significantly higher number of systems managed and greater scaled performance compared to the traditional Cisco TMS managed model. In this model, all communication between the management platform and the system is over SIP and the system communicates with the Cisco TelePresence Video Communication Server (VCS) instead of with Cisco TMS. This allows a device to be deployed and only require SIP connectivity to the VCS. In this model, systems register with the Cisco TMSPE instead of being added to the Cisco TMS System Navigator. The Cisco TMS feature scope for Cisco TMSPE Provisioned systems differs from that of Cisco TMS Managed devices. Please see the Cisco TMS Provisioning Deployment Guide for more information.

Cisco Unified Communications Manager Provisioned

In this model, systems register to and are provisioned directly by the Cisco Unified Communications Manager and not Cisco TMS. Systems provisioned by Cisco Unified CM are not added to Cisco TMS for management under the traditional ‘Cisco TMS Managed’ mode and attempting to do so may cause erratic behavior and system failures. Specific systems support the Cisco Unified CM Provisioned mode in Cisco TMS where they can be added to Cisco TMS for scheduling and monitoring. Systems that register to Cisco Unified CM as a SIP registar but are not provisioned by Cisco Unified CM, may be managed by Cisco TMS as Cisco TMS managed devices without concern. For more information on features and configuration requirements for Cisco Unified CM provisioning, please see the Configuring Cisco Unified Communications Manager for the Cisco TelePresence System documentation.

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.