Cisco TelePresence Management Suite

Installation and Upgrade Guide

Last Updated: June 2020

Software version 15.8

Contents

Introduction 7

Prerequisites 8

- Estimating Your Deployment Size 8
- Hardware Requirements 9
  - Regular Deployment and Cisco Business Edition 6000 9
  - Large Deployment 10
  - Recommended Hardware and Virtualization for Regular Deployments 11
  - Recommended Hardware and Virtualization for Large Deployments 12
- Server Software and Configuration Requirements 12
  - Operating System and Software 13
  - Access Requirements During Installation 13
  - Date and Time Configuration 13
- SQL Server Software and Permission Requirements 14
  - Software 14
  - Network 14
  - Configuration and Permissions 14
- Client Software Requirements 15
- Server Network Dependencies 16
  - Ports Used by Cisco TMS 16
- Compatibility with Extensions 17
- Upgrade Requirements and Recommendations 18
  - Virtual Directories within IIS 18
  - Redundant Deployments 18
  - Instructions for Customers Upgrading from 14.4 or 14.4.1 Who Use Cisco TMSXE 18
  - Instructions for Customers Upgrading from 14.4 or 14.4.1 Who Use Cisco TMSXN 19
  - Versions Earlier than 14.2 20
  - Cisco TMS Agent Legacy Provisioning 20
  - Versions Earlier than 13.2 21

Deployment best practices 22

- Database Maintenance Planning 22
  - Recovery Model 22
  - Regular Maintenance Tasks 23
- Security 23
  - Web and API Communication 23
  - Communication with Systems 24
- Initial Cisco TMS Setup 24

User Management 24
Zones 24
Folder Hierarchy 24
Default Settings for Conferences 24
Installing or Upgrading Cisco TMS 26
Before You Start 26
Running the Installer 26
Creating or Upgrading the Database 31
Adding Release Keys and Pre-configuring the Network Settings 31
Pre-configuring Zones and Setting Install Folder Location 33
Adding a Certificate 34
Installing Cisco TMS Log Collection Utility 35
Enabling the Windows SNMP Service 39
Accessing Cisco TMS for the First Time 39
Setting up a Redundant Deployment 42
Preliminary Information 42
Supported Configurations 42
Licensing 42
Database Redundancy 42
Cisco TelePresence Management Suite Provisioning Extension 43
Limitations in a Redundant Deployment Using a Load Balancer 43
Deploying with a Load Balancer 43
Recommended Hardware 43
Active Directory and User Authentication Requirements 43
Overview 43
Architectural Overview and Network Diagram 45
Installing and Configuring 46
Testing that Failover Works 47
Upgrading Cisco TMS 47
Recovery in Case of a Failing Node 48
Troubleshooting with Managed Systems in a Redundant Deployment 48
Deploying a Hot Standby 48
Setting up the Primary Cisco TMS Server 49
Setting up the Secondary Cisco TMS Server 49
Synchronizing Local Files 50
Optional: Enable TLS Client Certificates 50
Upgrading Cisco TMS 50
Recovery if the Primary Server Fails 51
Upgrading a Redundant Deployment from Version 14.4 or Later 52
Before You Upgrade the Servers 52
Upgrade the Primary Node 52
Upgrade the Secondary Node 52

Upgrading a Redundant Deployment from a Cisco TMS Version Earlier than 14.4 52
Before You Upgrade the Servers 52
Upgrade and Configuration for the Primary Server 52
Updating the NLB Configuration and Verification on the Primary Server 53
Upgrade and Configuration for the Secondary Server 53
Example ACE Configuration 53
Example F5 BIG-IP Configuration 54
Local Files for Synchronization 57
Moving or Uninstalling Cisco TMS 60
Moving Cisco TMS to a New Server 60
Before You Start 60
Moving the Application and Database 60
After Moving the Application 62
Moving Cisco TMSXE 62
Moving Cisco TMSPE 62
Moving Database to external SQL server 64
Moving Cisco TMSAE 65
Uninstalling Cisco TMS 65
Removing All Cisco TMS Information from a Server 65
Moving Cisco TMS Database to External SQL Server 66
Uninstall TMS Log Collector 67
Troubleshooting 68
Installation Times Out 68
Upgrading Windows OS software from 2008R2 to 2012R2, stops 'TMSSchedulerService' 68
Troubleshooting steps 68
Solution 68
Cisco TMS Installation or Upgrade terminated due to SQL Server connection issue 69
Troubleshooting steps 69
Solution 69
Cisco TMS Installation or Upgrade on Windows Server 2016/2012R2 terminates, if TLSv1.0 is disabled 70
Troubleshooting steps 71
Solution 71
Appendixes 72
Appendix 1: Restricting IIS Modules to Minimal Required 72
Appendix 2: Configuring IIS Request Flood Protection 73
IIS 8 and 8.5 73
IIS 7 76
Cisco TMS Bundle 77
Running the installer 77
Notices 86

Accessibility notice 86
Obtaining Documentation and Submitting a Service Request 86
Cisco Legal Information 87
Cisco Trademark 87

Introduction

Cisco TelePresence Management Suite (Cisco TMS) is a portal for managing and monitoring your videoconferencing network from a single, structured interface. Cisco TMS provides centralized control for on-site and remote video systems, and a deployment and scheduling system for your entire video network.

Cisco TMS automates system configuration for a basic telepresence network, operating right out of the box. You can tune Cisco TMS behavior to suit your organization's needs, set up user permissions, and configure your network model so that all of Cisco TMS call handling functionalities are available.

This document provides information for new installations and for upgrading and uninstalling an existing version, as well as moving Cisco TMS to a new server.

Note: When using Cisco TMS, do not use any other telepresence management system, including Cisco TelePresence Manager, on your telepresence network.

Related documents

The following table lists documents and websites referenced in this document, and other supporting documentation. All documentation for the latest version of Cisco TelePresence Management Suite can be found at: http://www.cisco.com/c/en/us/support/conferencing/telepresence-management-suite-tms/tsd-products-support-series-home.html

Documentation for Cisco TMS extensions can be found at: http://www.cisco.com/c/en/us/support/conferencing/telepresence-management-suite-extensions/tsd-products-support-series-home.html

Table 1 Related documents

Title	Link
Cisco TelePresence Management Suite Release Notes	http://cisco.com
Installing licenses; release and options keys for the Cisco TelePresence Management Suite	http://cisco.com
Cisco TelePresence Management Suite Administrator Guide	http://cisco.com
Cisco TelePresence Management Suite Provisioning Extension Deployment Guides	http://cisco.com
Cisco TelePresence Video Communication Server Cluster Creation and Maintenance Deployment Guide	http://cisco.com

Tip: Click the question mark icon (**?**) in the top-right corner of any Cisco TMS page to access the web help.

Training

Training is available online and at our training locations. For more information on all the training we provide and where our training offices are located, visit www.cisco.com/go/telepresencetraining

Glossary

A glossary of TelePresence terms is available at: tp-tools-web01.cisco.com/start/glossary/

Prerequisites

This chapter covers hardware and software requirements, and other considerations and dependencies that must be reviewed before installing or upgrading Cisco TelePresence Management Suite.

Estimating Your Deployment Size 8
Hardware Requirements 9
Server Software and Configuration Requirements 12
SQL Server Software and Permission Requirements 14
Client Software Requirements 15
Server Network Dependencies 16
Compatibility with Extensions 17
Upgrade Requirements and Recommendations 18

Estimating Your Deployment Size

The requirements for Cisco TMS depend on and grow with the size and complexity of the deployment. The complexity of an installation is driven primarily by the volume of activity and number of endpoints controlled by and bookable in Cisco TMS.

Use the following chart to identify the relative size of your deployment. If your intended deployment matches multiple level criteria, apply the highest level.

	Regular and Cisco BE6000	Large
Cisco TMS	▪ < 200 controlled systems ▪ < 100 concurrent participants ▪ < 50 concurrent ongoing scheduled conferences	▪ < 5000 systems that use system licenses, that is, controlled systems, systems registered to Unified CM that are added to Cisco TMS, and Unmanaged Rooms. Adding more than 5000 such systems is not supported. ▪ < 1800 concurrent participants ▪ < 250 concurrent ongoing scheduled conferences

Cisco TMSXE	< 50 endpoints bookable in Microsoft Exchange	< 1800 endpoints bookable in on-premises Microsoft Exchange or < 1000 endpoints bookable in Office 365 or a combination of on-premises Exchange and Office 365 Note that with Office 365, latency towards Exchange is likely to be greater than for an on-premises deployment. This may lead to Cisco TMSXE occasionally saving a booking before all related events have been processed. Users will then receive multiple email notifications for the same booking.
Cisco TMSPE	■ < 1000 Collaboration Meeting Rooms ■ < 2000 Cisco VCS-provisioned users (Note: Cisco VCS provisioning not supported on BE6000)	■ < 48,000 Collaboration Meeting Rooms ■ < 100,000 Cisco VCS-provisioned users
Co-residency	All three applications and Microsoft SQL Server may be co-resident.	■ Cisco TMSXE must be on a dedicated server. ■ Cisco TMS and Cisco TMSPE must use an external SQL Server.

Other factors that influence Cisco TMS performance and scale include:

- The number of users accessing the Cisco TMS web interface.
- Concurrency of scheduled or monitored conferences.
- The use of ad hoc conference monitoring.
- Simultaneous usage of Cisco TMSBA by multiple extensions or custom clients. Booking throughput is shared by all scheduling interfaces including the Cisco TMS **New Conference** page.

Actual booking speed will vary based on the meeting size, features, and schedule complexity around the meeting.

Hardware Requirements

Find the appropriate hardware requirements below based on your estimated deployment size.

All applications including SQL Server may also be installed on virtual machines with specifications corresponding to these hardware requirements

Regular Deployment and Cisco Business Edition 6000

In a regular deployment, Cisco TMS and extensions can be co-located on the same server.

	Requirement	Cisco BE6000
CPU	2 cores (Xeon 2.4 GHz or larger), dedicated	1 vCPU
Memory	8 GB, dedicated	4 GB vRAM, dedicated

	Requirement	Cisco BE6000
Disk space provided on server	60 GB	60 GB

Note that Cisco TMSPE on Cisco Business Edition 6000 does not include Cisco VCS-based user provisioning for endpoints or FindMe.

Large Deployment

In a large deployment, Cisco TMSXE and SQL Server must be external, while Cisco TMS and Cisco TMSPE are always co-resident.

Cisco TMS and Cisco TMSPE Server

	Requirement
CPU	2 cores (Xeon 2.2 GHz or larger), dedicated
Memory	8 GB, dedicated
Disk space provided on server	80 GB Note: For successful running of Cisco TMS / Cisco TMSPE, 20% of disk space must be free.

Microsoft SQL Server

This server must be in the same time zone as the Cisco TMS server.

	Requirement
CPU	4 cores (Xeon 2.2 GHz or larger), dedicated
Memory	16 GB, dedicated
Disk space provided on server	60 GB

When planning for a large deployment, also keep in mind that:

- The disk space needed for a large **tmsng** database is typically 20-30 GB.
- The size of the three Cisco TMSPE databases will not exceed 6 GB in most deployments.
- The prime performance limiters in SQL Server are RAM and disk I/O. For optimum performance, increase these values as much as possible.

Cisco TMSXE Server

The requirements for this server correspond to the recommended hardware requirements for the supported operating systems.

Recommended Cisco TMS Configuration Changes

To decrease the load on SQL Server and Cisco TMS services in a large deployment, we strongly recommend the following settings :

- **Administrative Tools > Configuration > Conference Settings**: Set **Default Reservation Type for Scheduled Calls** to *One Button To Push*

- **Administrative Tools > Configuration > General Settings**: Set **Route Phone Book Entries** to *No*
- **Administrative Tools > Configuration > Network Settings**: Set **Enable Ad Hoc Conference Discovery** to *Only for MCUs* or *No*.

Recommended Hardware and Virtualization for Regular Deployments

Cisco has tested and recommends the following specifications for regular deployments up to the supported maximum. Using the specifications described below, the entire Cisco TMS deployment can be hosted on a single rack-mounted server.

Hardware

Server	Cisco UCS C220 M3S Rack Server
CPU	2 x Intel Xeon Processor E5-2430 v2 (2.50 GHz)
Disk	8 x 146GB 6G SAS 15K RPM SFF HDD/hot plug/drive sled mounted, in a RAID-6 configuration. Part number: A03-D146GC2.
Disk controller	LSI MegaRAID 9265-8i 6Gb/s
Memory	4 x 8 GB/1600 MHz
Hypervisor software	VMware ESXi 6.5 and 6.0 host the three virtual machines with the specifications described below.

Cisco TMS and Cisco TMSPE Virtual Machine

CPU	2 x vCPU
Memory	8 GB
Disk	120 GB

Microsoft SQL Server Virtual Machine

CPU	2 x vCPU
Memory	8 GB
Disk	120 GB

Cisco TMSXE Virtual Machine

CPU	2 x vCPU
Memory	8 GB
Disk	100 GB

Recommended Hardware and Virtualization for Large Deployments

Cisco has tested and recommends the following specifications for large deployments up to the supported maximum. Using the specifications described below, the entire Cisco TMS deployment can be hosted on a single rack-mounted server.

Hardware

Server	Cisco UCS C220 M3S Rack Server
CPU	2 x Intel Xeon Processor E5-2430 v2 (2.50 GHz)
Disk	8 x 146GB 6G SAS 15K RPM SFF HDD/hot plug/drive sled mounted, in a RAID-6 configuration. Part number: A03-D146GC2.
Disk controller	LSI MegaRAID 9265-8i 6Gb/s
Memory	4 x 8 GB/1600 MHz
Hypervisor software	VMware ESXi 6.5 and 6.0 host the three virtual machines with the specifications described below. Note: Cisco TMS has been qualified with VMware File system 5.

Cisco TMS and Cisco TMSPE Virtual Machine

CPU	4 x vCPU
Memory	8 GB
Disk	200 GB

Microsoft SQL Server Virtual Machine

CPU	4 x vCPU
Memory	16 GB
Disk	250 GB

Cisco TMSXE Virtual Machine

CPU	4 x vCPU
Memory	8 GB
Disk	100 GB

Server Software and Configuration Requirements

The software requirements are independent of the size of your deployment. For size-appropriate hardware requirements, see Estimating Your Deployment Size, page 8 and Hardware Requirements, page 9.

Operating System and Software

Product	Version	Additional notes
Windows Server	▪ Windows Server 2016 64 bit ▪ Windows Server 2012 R2 64 bit ▪ Windows Server 2012 64 bit	▪ The server operating system must be English, Japanese, or Chinese. ▪ Standard/DataCenter editions all supported for Windows Server 2012 and 2016. ▪ We recommend that new installations use Windows Server 2016. ▪ Using the latest service pack is recommended for all versions. ▪ Note: Windows Server 2016 has a known issue with HTTP2 for Windows authentication. You must disable HTTP2 on Windows Server 2016 using following registry entry and continue using HTTP, until the issue is fixed by Microsoft. – `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\HTTP\Parameters` · `EnableHttp2Tls REG_DWORD 0` · `EnableHttp2Cleartext REG_DWORD 0` Restart the Windows Server after making registry changes. Installation on Active Directory Domain Controller is not supported. ▪ **Note**: Before upgrading to Cisco TMS 15.8, ensure that the Windows Updates are up to date.
.NET Framework	▪ 4.7 .NET Framework ▪ 4.7.1 .NET Framework	Must be installed prior to running the Cisco TMS installer. Note: .NET Framework 4.7 may get automatically installed from Windows Update Service.

Windows Updates

Enable and apply Windows Updates according to the network policy of your organization.

Windows Server FIPS

The enabling of FIPS mode on a Windows Server hosting Cisco TMS could cause adverse effects on the ability of Cisco TMS to manage its devices. For instructions, see Microsoft support article *System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing*.

Access Requirements During Installation

The administrator performing the installation must have administrator access to the Windows server.

Date and Time Configuration

NTP Server Recommended

The time setting on the Windows server must be correct for Cisco TMS to function correctly, and the date and time on the Cisco TMS and SQL Server must be identical, if the servers are separate.

We therefore strongly recommend keeping both servers in the same Active Directory domain and setting them up to use the same NTP (Network Time Protocol) server. For instructions, see the Microsoft support article *How to configure an authoritative time server in Windows Server*.

Time Zone

Changing time zone of the Windows Server hosting Cisco TMS is not supported once Cisco TMS is initially installed with a fresh database.

SQL Server Software and Permission Requirements

Cisco TMS stores all its customer data in its SQL database named **tmsng**. This self-contained storage allows for convenient backup and recovery of customer information.

For new installations, the installer creates **tmsng** using the SQL server defaults. Upgrades will reuse an existing Cisco TMS database.

See also:

- Database Maintenance Planning, page 22 for maintenance best practices
- Estimating Your Deployment Size, page 8 and Hardware Requirements, page 9 for size-appropriate hardware requirements

Software

This has been tested on the following. One of the following is required:

Product	Version	Service pack	Additional notes
Microsoft SQL Server 2017	All versions, 64 bit only		Deployments with databases that can be expected to grow larger than 10 GB must therefore use the full edition. We recommend using Microsoft SQL Server 2014/2016/2017 for new installations. Note: The Microsoft SQL Server 2014/2016/2017 Express have a 10 GB database size limit.
Microsoft SQL Server 2016	All versions, 64 bit only	Service pack 1	
Microsoft SQL Server 2014	All versions, 64 bit only	Service pack 2	
SQL Server Browser			Must be running when using a named instance on a separate server for the database.
SQL Native Client 11	13.0.1601.5 or later version		If Cisco TMS and SQL Server are hosted on different servers, SQL Native Client 11 must be installed on Cisco TMS Server before installation or upgrade of Cisco TMS. Ensure that Native Client 13.0.1601.5 or later version is installed. For more information, refer to the section Cisco TMS Installation or Upgrade terminated due to SQL Server connection issue, page 69.

Network

The latency between the Cisco TMS server and the SQL server must not exceed 20 ms.

Configuration and Permissions

The default SQL language must be set to English.

Authentication Modes

For installation and upgrading, *SQL Server and Windows Authentication mode* (mixed mode) must be enabled on the database server.

After installation is completed, mixed mode can be disabled and *Windows Authentication* enabled until the subsequent upgrade.

For instructions on changing authentication modes, see the TMS Tools chapter of *Cisco TelePresence Management Suite Administrator Guide* or the web help.

User and Database Creation

When installing or upgrading Cisco TMS and using an existing SQL Server, the installer prompts for a SQL database user and password. The default is to enter the server sa (system administrator) username and password.

Note: Usage of semicolon (;) in sa password is not supported by Cisco TMS.

If the sa account is not available, use one of the following:

- Use automatic setup, but with security limited role.
  a. Ask your SQL server administrator to create an SQL user and login that has the *dbcreator* and *securityadmin* server roles.
  This account will be the service account for Cisco TMS.
  b. When prompted for SQL Server credentials during installation, enter the username and password for that account.
  Cisco TMS will create the **tmsng** database automatically using the server defaults, assign itself as the owner and continue to use the supplied account to access the database after installation.
- Ask your SQL server administrator to manually create the database with a maximum security limited user role:
  - A database named **tmsng** with database collation Latin1_General_CI_AI (case insensitive and accent insensitive).
  - An SQL user and login to use for the Cisco TMS Service account and grant the user the *dbowner* role for the tmsng database. This permission must be kept after installation for Cisco TMS to function. The SQL user must use *dbo* as a default schema.

Snapshot Isolation

The following snapshot isolation settings are configured automatically for **tmsng** by the installer, and must remain set as follows:

- ALLOW_SNAPSHOT_ISOLATION must be set to ON
- READ_COMMITTED_SNAPSHOT must be set to ON

Required Database Settings

Note: Modification of settings applied during installation to the **tmsng** database is not supported.

Client Software Requirements

All users including administrators access Cisco TMS using the web interface.

A Windows username and password to the Cisco TMS server is required to sign in. Use either a domain account, if the server is joined to a domain, or a local machine account.

Web browser	Cisco TMS is tested with: ■ Microsoft Internet Explorer version 11 ■ Firefox version 77 ■ Google Chrome version 83 Other browsers may work, but are not actively tested and supported.
Java Runtime Environment (JRE)	Version 8 is recommended. JRE is required for using the **Monitoring** pages in Cisco TMS. If it is not installed, most browsers will prompt you to download and install the browser plug-in automatically. If this is not possible due to security restrictions, install it manually on the client computer from the JRE installation file which can be downloaded from http://www.java.com.

Server Network Dependencies

The following network dependencies must be considered before installing Cisco TMS:

- Domain membership preferred: Each user logging into Cisco TMS needs a Windows User Login to authenticate to the web site. Users must have either a local account on the Cisco TMS Windows Server or a Domain account that the server trusts through Active Directory. By making the server a member of the domain, all trusted domain users can automatically use their existing Windows credentials to log into Cisco TMS. You can still limit what users can do after they have logged into Cisco TMS using Cisco TMS permissions. Active Directory membership is the recommended deployment for most installations because it avoids creating local Windows accounts for each user.
- Cisco TMS website accessible by IP and Hostname: not all devices support DNS hostnames or Port Numbers, the Cisco TMS web site must therefore be accessible by an IP Address on port 80. Some functionality requires Cisco TMS to be reachable by hostname; therefore Cisco TMS should also be accessible by a fully qualified domain name.
- Mail server access: Cisco TMS requires access to an SMTP server to be able to send email. Your company's existing mail servers can be used for this. Note that Cisco TMS supports SMTP AUTH login for authentication if required.
- Network access to managed devices:Cisco TMS needs specific protocols and access to manage devices. Any network firewalls or NAT routers must allow traffic to flow to and from Cisco TMS.
- Microsoft IIS components ASP.NET and ASP must be enabled.
- Windows Firewall is enabled by default and controls both inbound and outbound ports. For information on which ports must be opened when Windows Firewall is enabled, see Ports Used by Cisco TMS, page 16.
- Make sure anti-virus programs or other security measures are not blocking applications from sending mail directly using the SMTP port.

Ports Used by Cisco TMS

The following ports are used by Cisco TMS and must be enabled in the Windows firewall. Not all services will be used in all installations, depending on the configuration and the devices used.

Service or system	Transport protocol	Port	Direction (relative to Cisco TMS)	
			In	Out
FTP	TCP	20, 21		X
HTTP	TCP	80	X	X

Service or system	Transport protocol	Port	Direction (relative to Cisco TMS)	
			In	Out
HTTP for Cisco TelePresence System (CTS)	TCP	8081		X
HTTPS	TCP	443	X	X
HTTPS for Cisco TelePresence System (CTS)	TCP	9501		X
HTTPS for Unified CM	TCP	8443		X
LDAP	TCP	389		X
LDAPS	TCP	636		X
Polycom GAB	TCP	3601	X	
SMTP	TCP	25		X
SNMP	UDP	161		X
SNMP Traps	UDP	162	X	X
SSH	TCP	22		X
Telnet	TCP	23		X
Telnet Challenge	TCP	57		X
Telnet Polycom	TCP	24		X

For SQL connections, the TCP port used by a default SQL server instance is configurable, and the port used by a named SQL server instance is dynamic, changing whenever the service restarts. For instructions on making your SQL server listen to a particular port, see the TechNet article Configure a Server to Listen on a Specific TCP Port (SQL Server Configuration Manager).

Multiple IP Addresses Not Supported

Cisco TMS cannot use multiple IP addresses and will only bind to the first available network interface. Multiple network cards or IP aliases on the same card are therefore not supported. Multiple IPv4 addresses and multiple IPv6 addresses are not supported, but single IPv4 address and single IPv6 address is supported.

Cisco TMS can manage both a public and a private network as long as the two networks are interconnected via routing in the network. Both networks cannot be directly connected to Cisco TMS using multiple network interface cards.

Compatibility with Extensions

Product	Version
Cisco TelePresence Management Suite Extension for Microsoft Exchange	5.8
Cisco TelePresence Management Suite Provisioning Extension	1.14

Note: The most recent version is always required for all features and fixes to be available.

Upgrade Requirements and Recommendations

Review all sections below that apply to the version of Cisco TMS you are currently running before starting your Cisco TMS upgrade.

Virtual Directories within IIS

When upgrading from any version of Cisco TMS, all virtual directories are deleted and recreated when installing a new version. Beware that this also removes any custom settings on virtual directories.

Redundant Deployments

See Upgrading a Redundant Deployment from a Cisco TMS Version Earlier than 14.4, page 52.

Instructions for Customers Upgrading from 14.4 or 14.4.1 Who Use Cisco TMSXE

For further background information on the requirement for this upgrade procedure see Cisco TelePresence Management Suite Software Release Notes (14.4.2).

Upgrading Cisco TMSXE and Cisco TMS

Customers who use Cisco TMSXE and are upgrading from 14.4 or 14.4.1 must follow these upgrade instructions in the order given:

1. Upgrade Cisco TMSXE to version 4.1.
2. Upgrade to this version of Cisco TMS.
3. Wait for 15 minutes, then check the Cisco TMSXE log: **TMSXE-log-file.txt** for a line saying: `INFO ReplicationEngine - No changes on TMS.`
   This confirms that all problematic bookings Cisco TMS could resolve automatically have been replicated correctly from Cisco TMS to Microsoft Exchange.

   If you do not see this line, contact your Cisco support representative.

Resolving Duplicate Conferences in Cisco TMS

You must follow this second procedure as soon as possible after upgrade, but it does not need to be done immediately, nor does it require a maintenance window.

1. Go to Cisco TMS and check for a critical TMS ticket stating: 'Conference series with duplicate external primary keys found'.
   - If you do not see this ticket, no further action is required.
   - If you do see the ticket, continue to steps 2 and 3.
2. In Cisco TMS Tools, run the **Resolve Duplicate Keys** tool to select the correct conferences from the list of duplicates.
   If it is not clear which conference is the correct one, review the Exchange resource calendars for the systems involved in the conference. If most or all of the resource calendars are in agreement with one of the duplicate conferences, that is probably the correct one to select.

   If it is still not possible to identify the correct conference, contact the conference owner.
3. Wait for 15 minutes, then check the Cisco TMSXE log: **TMSXE-log-file.txt** for a line saying: `INFO ReplicationEngine - No changes on TMS`. This confirms that all remaining problematic bookings have been replicated correctly from Cisco TMS to Microsoft Exchange. If you do not see this line, contact your Cisco support representative.

Manually Resolving Any Remaining Duplicate Appointments in Exchange Resource Calendars

In some deployments, there may be a small number of duplicate Exchange appointments in the resource calendars that are not identified or cleaned up automatically during the upgrade to Cisco TMS this version of Cisco TMS.

It is most likely that the duplicates occurred if conferences were created either from Conference Templates, or by copying existing conferences in versions of Cisco TMS earlier than 14.4, and these conferences were subsequently edited (either in Cisco TMS or in Microsoft Exchange) in 14.4 or 14.4.1.

Use the following procedure to identify and resolve these duplicate Exchange appointments:

1. Log on to the Cisco TMSXE server and run the Meeting Analyzer with a search window from now to the end of your scheduling horizon.
   For large deployments we recommend doing this outside business hours, or that you run the Meeting Analyzer with a smaller search window, as this will reduce the load on the Exchange server.
2. In the Meeting Analyzer report, look for appointments that are flagged as “No matching conferences found in Cisco TMS”.
   If there are no appointments with this flag, no further action is required.

   If you do see flagged appointments, continue to step 3.
3. Logged in as a user with full access to the Exchange resource calendars:
   a. Open Microsoft Outlook.
   b. Find one of the duplicate appointments identified in step 2.
4. If the duplicate appointment has a different start time, end time, or subject than its counterpart in Cisco TMS, delete it from all Exchange resource calendars.
   If there are no differences between the appointments, follow the procedure in 'Forcing a change to identify the correct appointment', below.
5. Go to step 3 and process another problematic appointment.

Forcing a Change to Identify the Correct Appointment

If there are two or more appointments in the resource calendar with the same start time, end time, and subject, you will be unable to differentiate between the duplicate and any appointments that you have to delete. To force a change that will enable you to see a difference and therefore identify the correct appointment:

1. In Cisco TMS, go to **Booking > List Conferences**, and locate the conference.
2. Edit the conference, reduce its duration by 5 minutes and click **Save Conference**.
   This duration is important as Cisco TMSXE will ignore changes of 3 minutes or less.
3. Wait for the Cisco TMSXE replicator to process the change and update the Exchange resource calendars with the new end time—this could take a few minutes.
4. The appointment in Exchange that has a new end time is the one that is correctly linked to Cisco TMS: now delete the one or more duplicate appointments that did not get a new end time.
5. In Cisco TMS, reinstate the original end time of the conference.

Instructions for Customers Upgrading from 14.4 or 14.4.1 Who Use Cisco TMSXN

For further background information on the requirement for this upgrade procedure see Cisco TelePresence Management Suite Software Release Notes (14.4.2).

Upgrading Cisco TMS and Resolving Duplicate Conferences

Customers who use Cisco TMSXN and are upgrading from 14.4 or 14.4.1 must first upgrade to this version of Cisco TMS, and then follow this procedure as soon as possible after upgrading, but it does not need to be done immediately, nor does it require a maintenance window:

1. Wait 15 minutes for the Cisco TMSXN Synchronizer to process data from Cisco TMS.
2. In Cisco TMS, check for a critical TMS ticket stating: 'Conference series with duplicate external primary keys found'.
   If you do not see this ticket, no further action is required.

   If you do see the ticket, continue to step 4.
3. In **TMS Tools**, run the **Resolve Duplicate Keys** tool to select the correct conferences from the list of duplicates.
   If it is not clear which conference is the correct one, review the Domino calendars for the systems involved in the conference. If most or all of the resource calendars are in agreement with one of the duplicate conferences, that is probably the correct one to select.

   If it is still not possible to identify the correct conference, contact the conference owner.

Restarting the Cisco TMSXN Synchronizer

This process will initiate a re-replication from Cisco TMS to Domino, so that all future bookings that exist in Cisco TMS will be written to Domino if they do not already exist:

1. From Domino Administrator, open **Files > Video Conference Resources**.
2. Go to **Reservations > By Date**, and select any reservation.
3. Select **Actions > Restart Synchronizer**.
4. Monitor the Domino log file, and wait for a statement that says: `Agent printing: Synchronizer from zero finished`. Once you see this statement, all bookings from Cisco TMS have been re-replicated to Domino.

Versions Earlier than 14.2

Cisco TMS time zone support was improved in 14.2, and a time zone update tool was provided to mitigate discrepancies in time zone data after upgrading from previous versions. The last version that supported this tool was 14.3.2.

You must upgrade to 14.3.2 and run the time zone tool before upgrading to the current version if:

- You have users scheduling conferences from both the United States and Europe, or both the northern and the southern hemispheres.
- You are in a country where DST rules vary between states or regions, for example Australia.

Caution: Upgrading directly in either of the above scenarios will lead to data inaccuracies.

You do *not* need to upgrade by way of 14.3.2 if Cisco TMS and all organizers booking meetings on your telepresence network are in the same time zone or in time zones with the same DST rules, such as the United States excluding Arizona and Hawaii.

For details and instructions on the time zone update, see *Cisco TMS Installation and Upgrade Guide* for 14.3.2.

After sorting out any time zone inconsistencies, you can upgrade to 15.8.

Cisco TMS Agent Legacy Provisioning

If upgrading from 13.2.x or any earlier version using the legacy provisoning feature, you must migrate to Cisco TelePresence Management Suite Provisioning Extension *before* upgrading to Cisco TMS 15.8.

Note that this migration requires Cisco TMS version 13.2; if currently using an older version, you must:

1. Upgrade Cisco TMS to 13.2.x.
   If upgrading from a version earlier than 13, you will need to obtain a Cisco TMS 13 release key from Cisco to perform this upgrade.
2. Install Cisco TMSPE, migrating your provisioning database following the instructions in *Cisco TelePresence Management Suite Provisioning Extension Deployment Guide* for Cisco TMS 13.2.

3. Consider whether your deployment may need to upgrade via 14.3.2 due to the time zone changes, see Versions Earlier than 14.2, page 20.
4. Any time zone issues resolved, upgrade to Cisco TMS 15.8.

Versions Earlier than 13.2

The default booking confirmation email templates and phrase files were updated in 13.2. If you are upgrading from any version prior to 13.2 where these templates have been customized templates, the new additions are not automatically added to your customized files, but are still available for use.

To see the default usage of these new values and have them in your templates, customers with customized Booking Confirm templates or phrases must:

1. Go to **Administrative Tools > Configuration > Edit Email Templates**.
2. Open the **Booking Confirm** template.
3. Click **Revert to Default**.

Once set to default, you can re-add the customizations back into the templates or phrase files.

Versions Earlier than 13.0

Upgrades back to and including version 13.0 are tested and supported for Cisco TMS 15.8. For earlier versions, perform a new installation rather than an upgrade, as changes to the server requirements, database and backend have been substantial.

Deployment best practices

This chapter covers best practices for installation and initial configuration of Cisco TMS.

Database Maintenance Planning 22
Security 23
Initial Cisco TMS Setup 24

Database Maintenance Planning

Cisco TMS and Cisco TMSPE both create databases according to the default settings of the SQL server. The databases are:

- **tmsng** (Cisco TMS)
- **tmspe** (Cisco TMSPE main)
- **tmspe_vmr** (Cisco TMSPE Collaboration Meeting Rooms)
- **tms_userportal** (Cisco TMSPE self-service portal)

Below are the best practices for setting up and keeping a maintenance plan for your database or databases. Database management must be handled through an external tool such as Microsoft SQL Server Management Studio Express.

Recovery Model

Depending on the desired behavior, the databases may be set up to use the simple or the full recovery model. For detailed descriptions on the features of each recovery model, see the MSDN article Recovery Models (SQL Server).

Simple Recovery

For typical Cisco TMS deployments, we recommend using the simple recovery model, which only supports recovery between backups.

With this model, you will back up the database at regular intervals, but omit the transaction log. The database will reclaim log space to limit file sizes, the database transaction log size is modest, and it does not continue to grow in between database backups.

Full Recovery

Experienced SQL Server administrators with larger Cisco TMS deployments may prefer the additional capabilities and integrity tools offered by the full recovery model, which supports recovery to any point in time using database transaction logs.

With this recovery model, the database transaction log file will grow continuously between backups, and can cause the database run out of space and halt if left unmaintained.

Regular database and transaction log backups are mandatory with this recovery model.

Identifying or Changing the Recovery Model

To identify or change the recovery model of your database, see the Microsoft instructions for your version of SQL Server:

- View or Change the Recovery Model of a Database (SQL Server 2016)

Regular Maintenance Tasks

As a best practice, set up regular maintenance tasks for backups and index maintenance. Beware that database maintenance impacts Cisco TMS performance. Perform these tasks during your organization's scheduled maintenance windows.

Backup

Set up tasks to back up the server in accordance with your organization's recovery policies, and once per week as a minimum:

- Back Up and Restore of SQL Server Databases (SQL Server 2016)

Index Maintenance

Perform maintenance on the database indexes at regular intervals to avoid excessive fragmentation. We suggest rebuilding the indexes monthly, or when fragmentation goes past 30%.

- Reorganize and Rebuild Indexes (SQL Server 2016)

SQL Server Maintenance Plan

If using the full version of SQL Server (not Express), built-in maintenance plan features and a wizard are available for tasks like the above. For guidance, see the following Microsoft articles:

- Create a Maintenance Plan (SQL Server 2016)

Database Size Management

We strongly recommend *against* having a regular maintenance task for shrinking the database. Over time, the database size will normally stabilize, and can be specified as a fixed size with an added 30% buffer.

On some occasions, the database size may grow significantly during an upgrade. In these cases, we recommend a one-time operation to shrink the database.

Security

This section presents recommended and suggested measures to make your Cisco TMS deployment more secure.

Web and API Communication

By default, the Cisco TMS installer will set up HTTPS for web communication, offering to create a self-signed certificate if the administrator does not provide one. For improved security, we strongly recommend using valid certificates signed by a certificate authority.

For detailed information on security settings, see **Advanced Security Settings** > **Communication Security** section in Cisco TMS Administrator Guide.

Configuring IIS for Improved Security

In IIS Manager:

1. Disable the Polycom phonebook component if not using Polycom systems:
   a. Expand the tree view for your Default Web Site.
   b. Right-click the **/pwx** component and select **Remove**.
2. Disable HTTP for web and API transactions:
   a. Click on the **/tms** component to select it.
   b. In the **IIS** section, double-click on **SSL Settings**.
   c. Check **Require SSL** and, in the **Actions** panel, click **Apply**.
   d. Expand the **/tms** component and click on **/public** to select it.
   e. In the **IIS** section, double-click on **SSL Settings**.
   f. Uncheck **Require SSL** and, in the **Actions** panel, click **Apply**.
3. Set up request flood protection, see Appendix 2: Configuring IIS Request Flood Protection, page 73 for instructions.

Communication with Systems

Cisco TMS will as a default use HTTP to communicate with systems, or SNMP for some legacy systems.

If using legacy systems, you can enable SNMP by enabling the **Windows SNMP Service** on the server.

Note: SNMP traps must be send through F5 Load Balancer to Cisco TMS servers in redundant setup for legacy endpoints like MXP and Polycom.

Initial Cisco TMS Setup

The Cisco TMS configuration can generally be modified at any point after deployment and during operation. However, for ease of maintenance and operation, we recommend that you configure user account policies, zones, and basic conference defaults immediately after installation and before allowing users into the system.

Instructions can be found in the built-in Cisco TMS help or *Cisco TMS Administrator Guide*.

User Management

We strongly recommend using Microsoft Active Directory to manage all Cisco TMS users.

Zones

You can configure an initial zone setup during installation. To view or modify the configuration after installation, go to **Administrative Tools > Locations > ISDN Zones** or **> IP Zones**.

Folder Hierarchy

Before beginning to add systems to Cisco TMS, we strongly recommend planning a well-structured and scalable folder hierarchy for endpoints and infrastructure systems in **Systems > Navigator**.

Default Settings for Conferences

Before users start booking conferences, we recommend that you review and adjust the default settings for connection type, bandwidth, and so on. Go to **Administrative Tools > Configuration > Conference Settings**.

Installing or Upgrading Cisco TMS

This chapter covers the procedures to perform a new installation or upgrade of Cisco TMS.

Before You Start 26
Running the Installer 26
Accessing Cisco TMS for the First Time 39

Before You Start

Make sure that you have:

- considered all relevant Prerequisites, page 8 for an installation in your environment
- the desired Cisco TMS software bundle downloaded from Cisco.com
- a Cisco TMS release key and option keys for systems and features that you plan to add immediately

If you are upgrading, also make sure to review the Upgrade Requirements and Recommendations, page 18 for any particular procedures or requirements that apply when upgrading from your current version of Cisco TMS.

It is strongly recommended to backup a copy of Cisco TMS database (tmsng) prior to updating since restoring the backup database is only method of reverting it to the prior version.

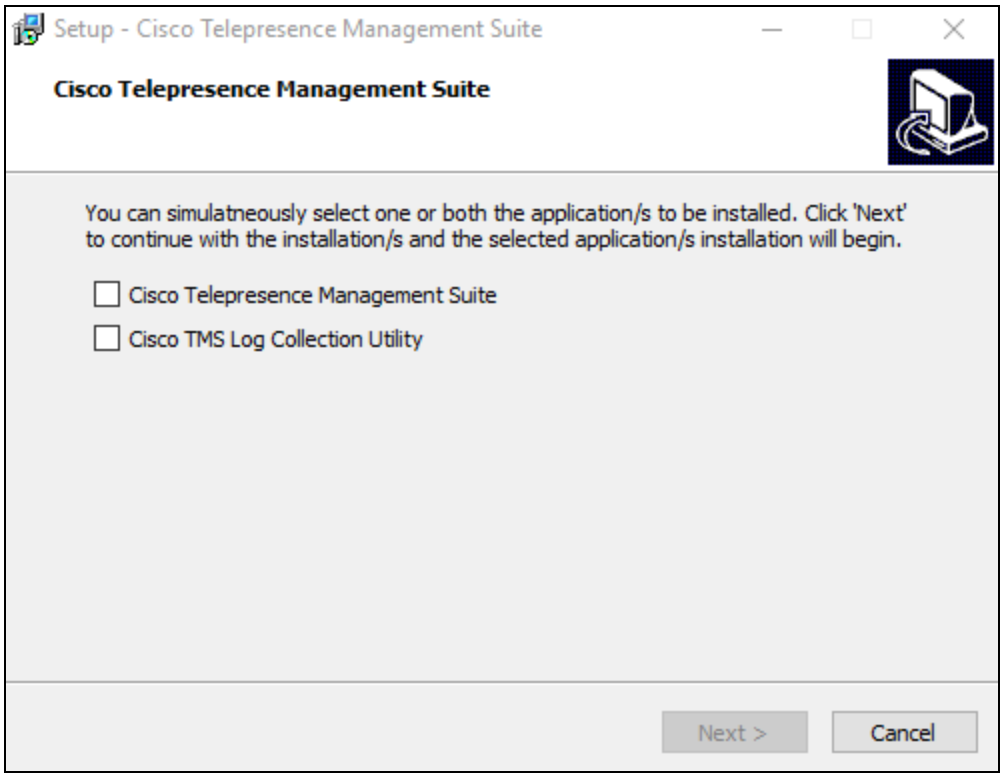
You may be prompted to reboot the server more than once during installation. The installer automatically resumes after the server reboots.

Running the Installer

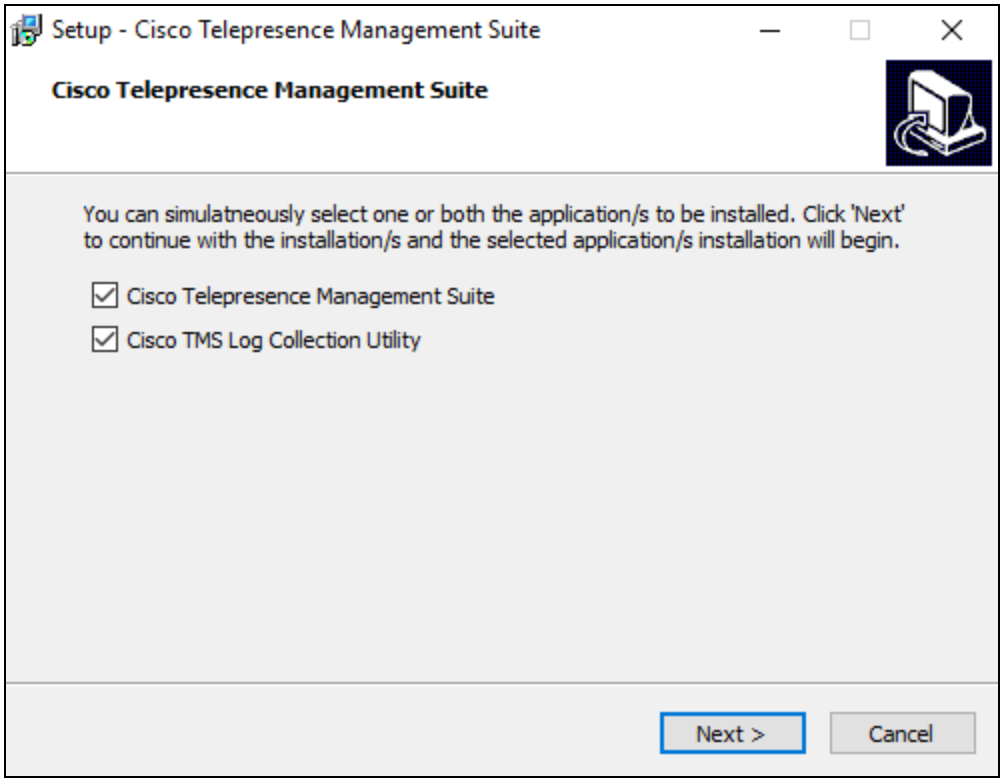
Note that depending on Windows components needing to be added, you may be prompted to reboot the server more than once during installation. The installer automatically resumes after the server reboots.

1. Close all open applications and disable virus-scanning software and other software that may prevent an installation from getting completed.
2. Extract the **Cisco TMS.zip** archive to a folder.
3. Run the **Cisco TMS** executable as administrator.

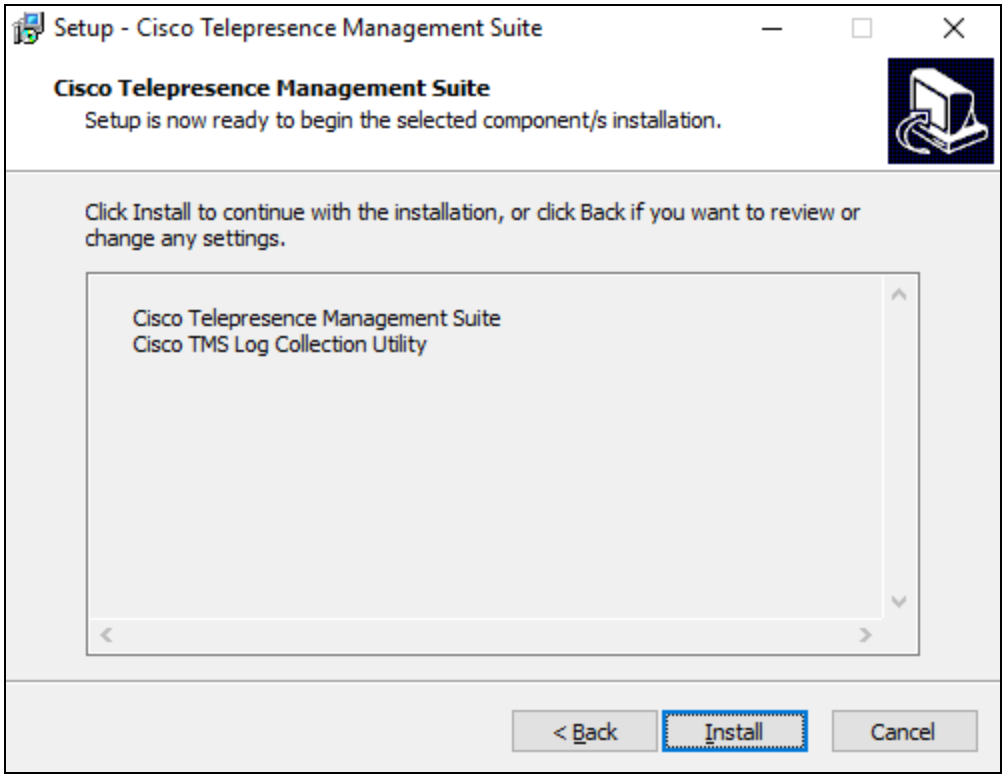
4. When the installer package is executed, a dialog box will appear which displays the following options:
   a. Cisco Telepresence Management Suite
   b. Cisco TMS Log Collection Utility



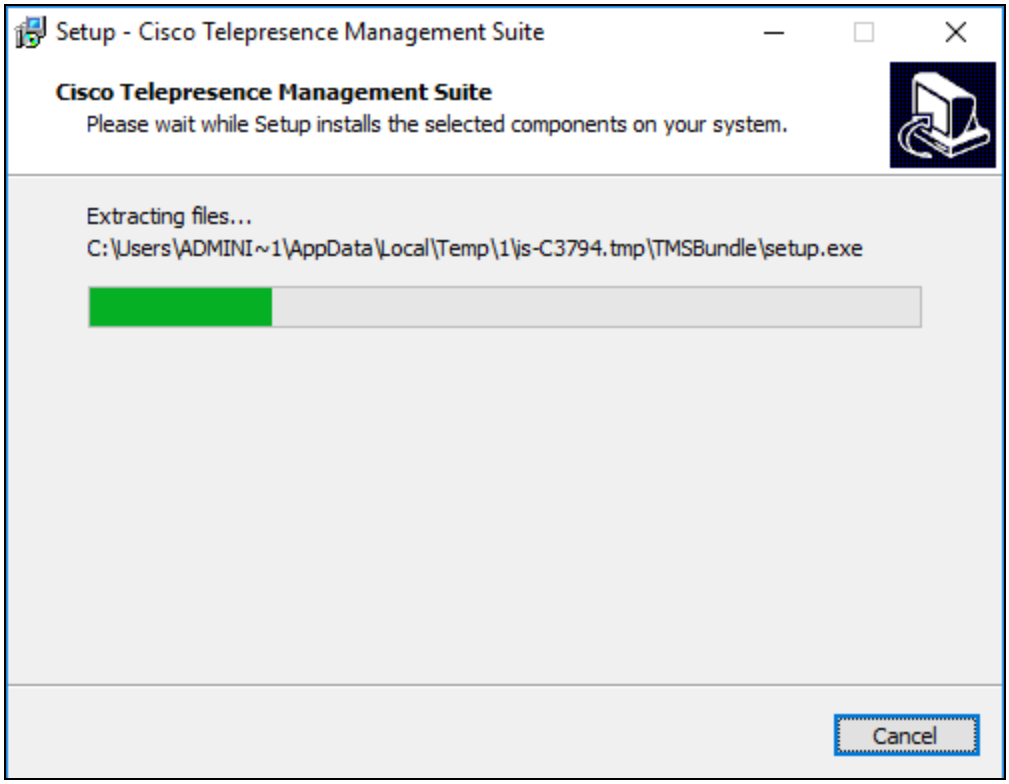
5. Select the application that you want to install and click '**Next**'.



6. Click **'Install'** to install the selected applications.



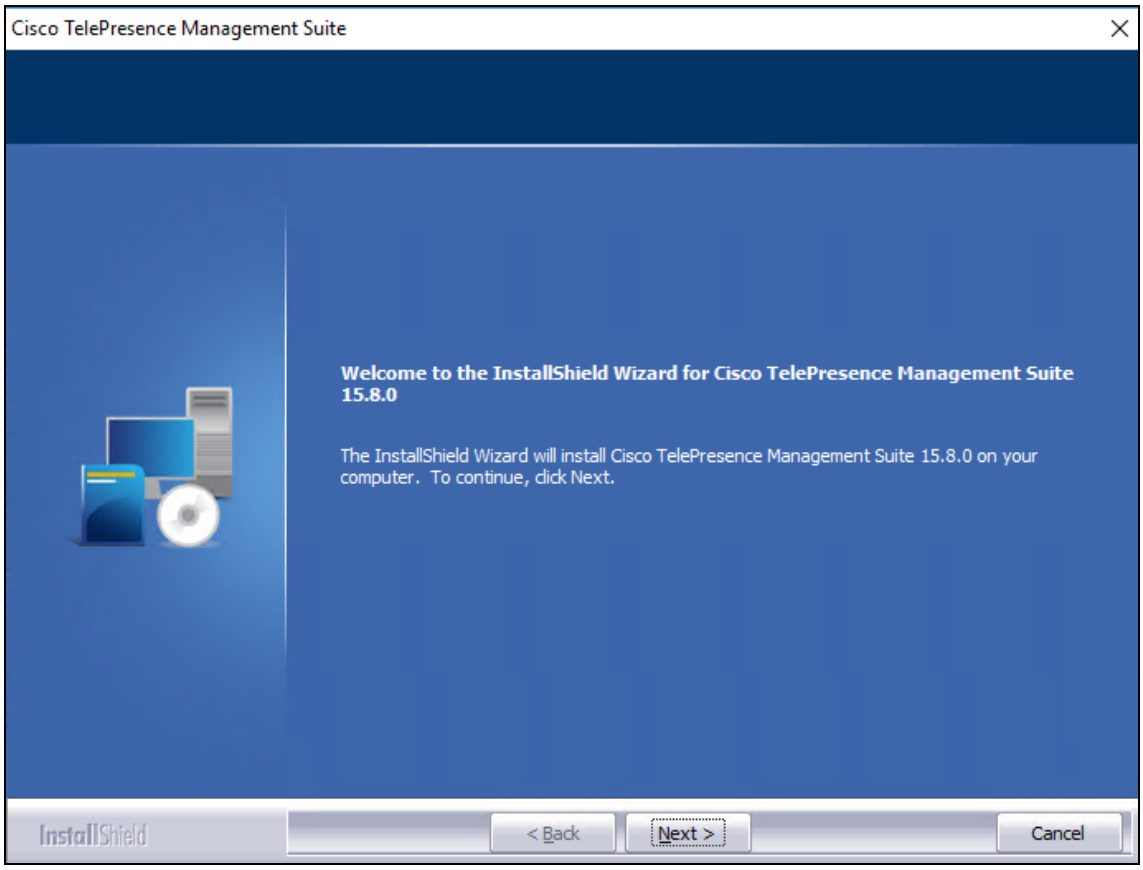
7. The installation will begin.



Note: If both options are selected, Cisco TMS will be installed followed by Cisco TMS Log Collection Utility installation.

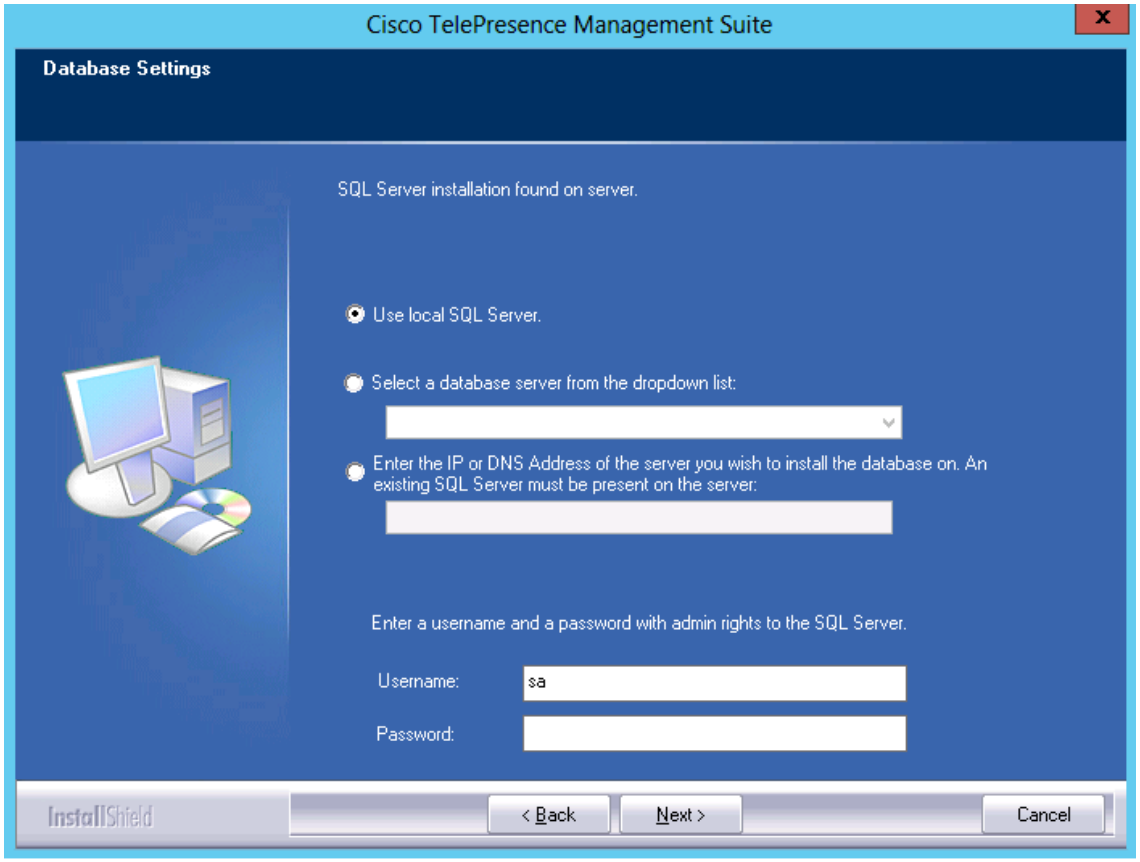
8. The installer checks the hardware and software configuration of the server. A warning or error message may be displayed depending on your server's configuration. Follow the instructions given in the prompts and install any missing components.
9. If an earlier version of Cisco TMS is currently installed, you are prompted to upgrade.
   - Click **Yes** to continue. Upgrading removes the old version and upgrades the existing Cisco TMS database.
   - Click **No** to abort the installation and leave the current installation untouched.

10. When the **Welcome** screen is displayed, click **Next** to continue.



11. Click **Yes** to accept the license agreement.
The installer now searches for an existing SQL Server and Cisco TMS database.

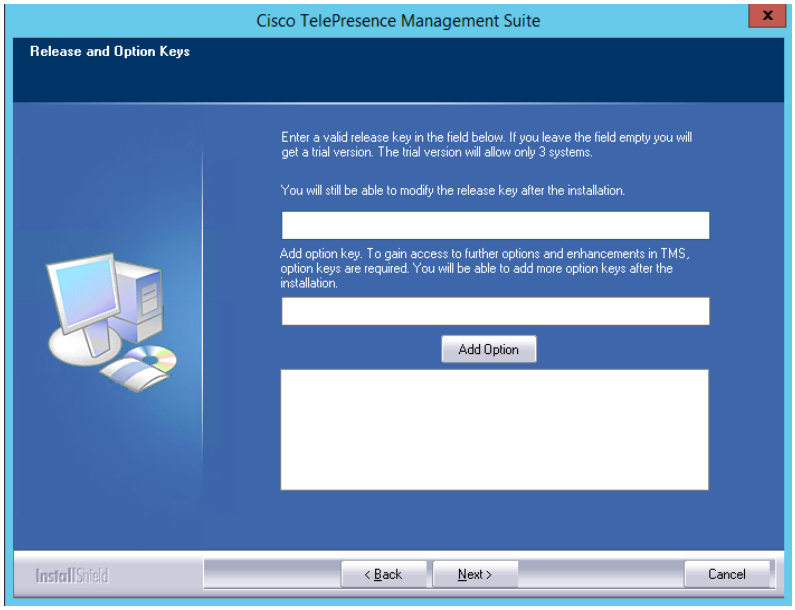
Creating or Upgrading the Database



- If the installer does not find an existing Cisco TMS database, but locates a local installation of SQL Server, enter the username and password to allow the installer to create a new database. Click **Next**.
- If using an external SQL Server, which is required for large deployments, enter all connection details. Click **Next**.
- If the installer finds an existing Cisco TMS database, the dialog will be pre-populated with the previously specified SQL Server. When prompted, enter the username and password and click **Next**.
  - Click **Yes** to upgrade the existing database to the current version and retain the existing information. We recommend that you back up the database before it is upgraded using the appropriate tools. See also Database Maintenance Planning, page 22.
  - If clicking **No**, you must proceed to stop the installer and manually remove the database if you wish to use the same SQL Server, before you can install a new Cisco TMS database.

Adding Release Keys and Pre-configuring the Network Settings

The **Release and Option Keys** dialog is now displayed, and any existing keys are shown if upgrading.



A new release key is required if performing a new installation or upgrading to a new major release. If no release key is entered, an evaluation version of Cisco TMS will be installed. This includes support for three systems.

Option keys enable additional systems, extensions, or features. They may also be added post installation by going to **Administrative Tools > Configuration > General Settings**.

For questions regarding release or option keys, contact your Cisco Reseller or Cisco Support.

1. Enter the release key if necessary.
   The release key *must* be entered before adding option keys.
2. Enter each option key, then click **Add Option**.
   Option keys are validated as they are added.
3. When done adding keys, click **Next**.
   The **Network Settings** screen is displayed.

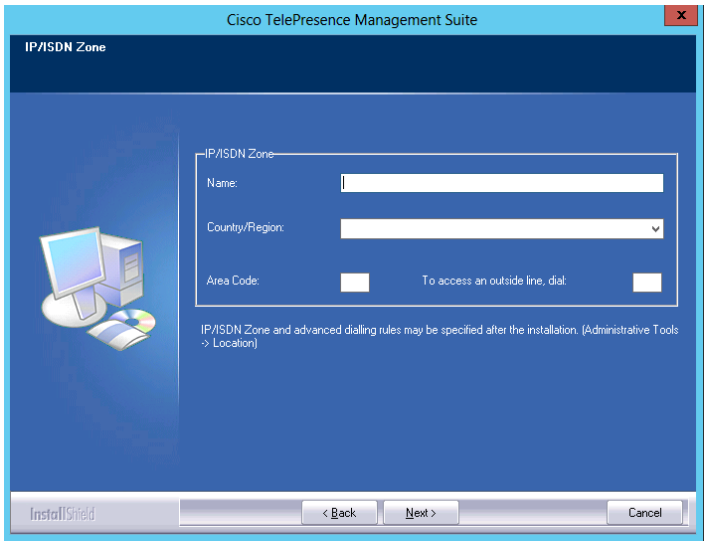
4. You can now pre-configure default settings to allow Cisco TMS to immediately start working with a basic network configuration. The settings can be changed after installation.
If upgrading, values from the existing database are displayed.

Field label	Description
TMS Server IPv4 Address	The IPv4 address of the local server.
TMS Server IPv6 Address	The IPv6 address of the local server. If IPv6 is not enabled on the Windows Server, this field can be left blank.
IP Broadcast/Multicast Addresses [...]	The broadcast address(es) for the networks that Cisco TMS is to automatically search for devices. (Systems that Cisco TMS discovers can be automatically added to Cisco TMS with their management settings added.) Multiple broadcast addresses can be entered separated by commas. Cisco TMS will search networks by sending a SNMP Discovery packet to the supplied addresses. The default value will be the broadcast address of the Cisco TMS server's network. Note that the Windows SNMP Service is disabled by default for new installations.
Enable automatic registration of systems in TMS	If enabled, systems Cisco TMS discovered on the network will automatically be added into a folder in Cisco TMS and have their management settings configured. This setting is disabled by default.
Sender E-mail Address	The email address you wish to appear in the **From** field of messages sent by Cisco TMS. Example: `videomanagement@example.com`.
SMTP Server Address	The network address of the SMTP server Cisco TMS will use to send email. Additional authentication configuration settings can be set up post installation as needed.

5. Click **Next** when done modifying the settings.
Cisco TMS then contacts the supplied SMTP server to verify the settings and warns you if it was not able to contact the server.

   If this is a new installation, the **IP/ISDN Zone** screen will then be displayed.

Pre-configuring Zones and Setting Install Folder Location



Zones are a configuration concept used by Cisco TMS to route phone numbers and aliases when scheduling calls and using phone books.

The information entered during installation creates the first IP and ISDN zones in Cisco TMS, which will be set as the initial default to allow a basic IP and ISDN network to operate after installation. Additional zones and configurations must be added post installation for networks with multiple locations or more complex elements.

1. Fill in zone information as detailed below:

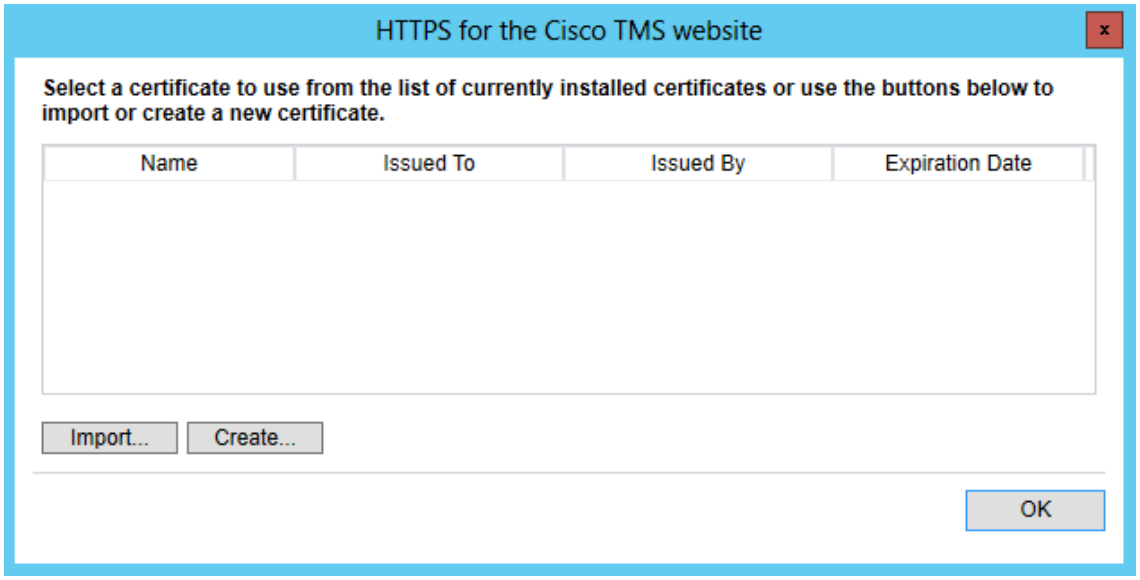
Field label	Description
Name	A descriptive name for the zone, normally referencing the city or building.
Country/Region	The country this zone is located in. This is used for ISDN dialing information.
Area Code	The area code for the location, if applicable. This is used for ISDN dialing information
To access an outside line, dial	The prefix to reach an outside line on your ISDN circuits, if applicable.

2. When you have finished modifying the settings, click **Next**.
   The **Folder Settings** screen will be displayed.
3. Specify the Cisco TMS installation path, then click **Next**.
   The **Encryption Key** screen will be displayed.
4. Click **Generate** to create a new key to encrypt system username and password data in the Cisco TMS database, or add an existing key from a previous installation of Cisco TMS if applicable, then click **Next**.
   The **Start Copying Files** screen will be displayed.
5. Verify all the settings in the displayed summary, then click **Next**.

   The installation process will start.

Adding a Certificate

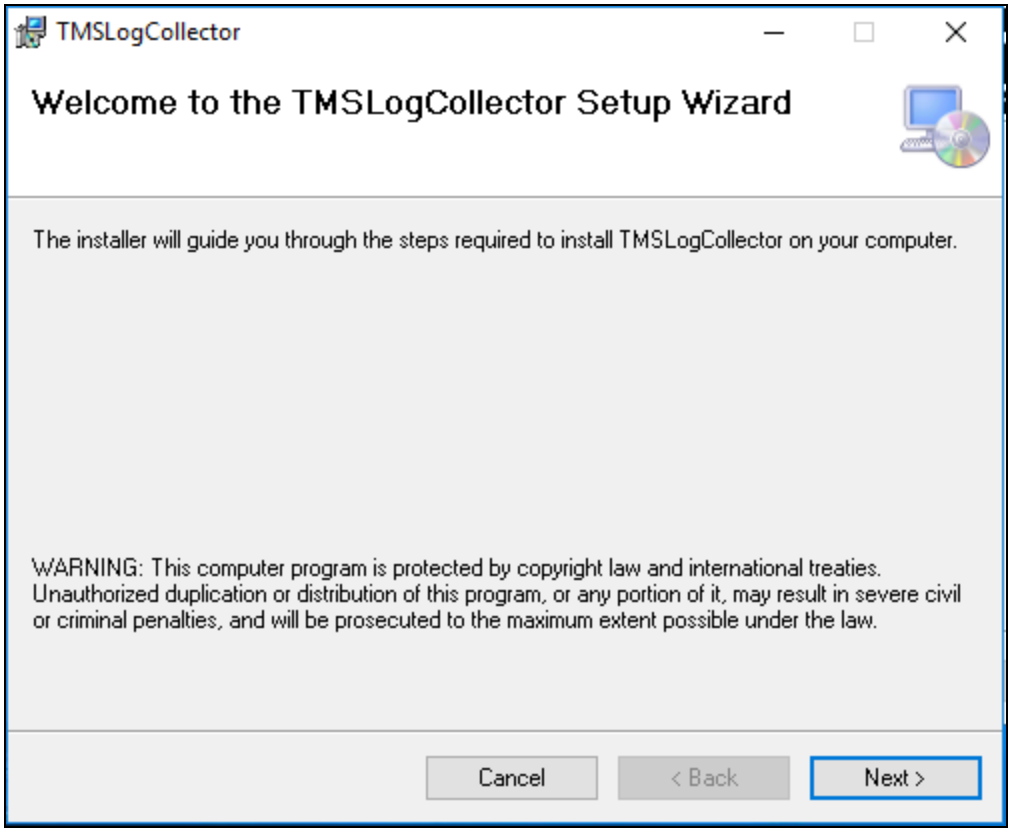
Once the installation is finished, import or create a TLS certificate that enables HTTPS access to the Cisco TMS website. We strongly recommend using a green certificate from a trusted CA unless installing in a test environment.



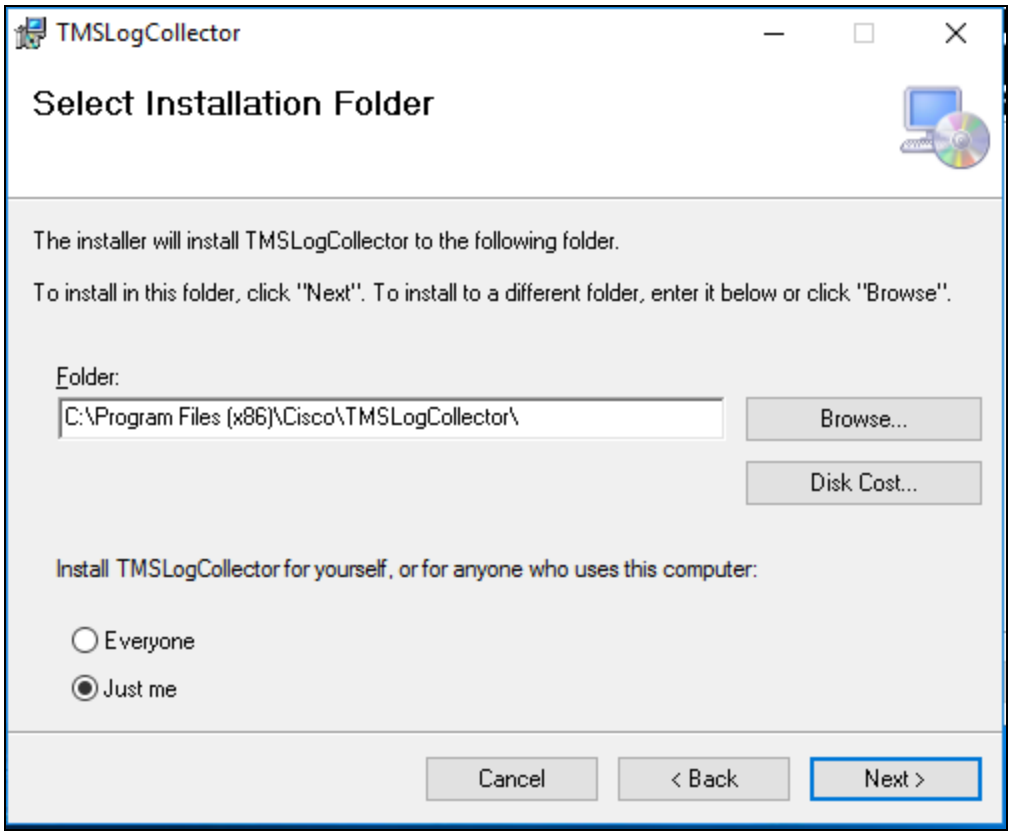
1. Click **Import** to add an existing certificate in .pfx format, or click **Create** for a self-signed certificate.
2. When the import is completed, click **OK**.
3. The setup wizard will now complete. Click **Finish**.
4. If necessary, you will be prompted to reboot the server.

Installing Cisco TMS Log Collection Utility

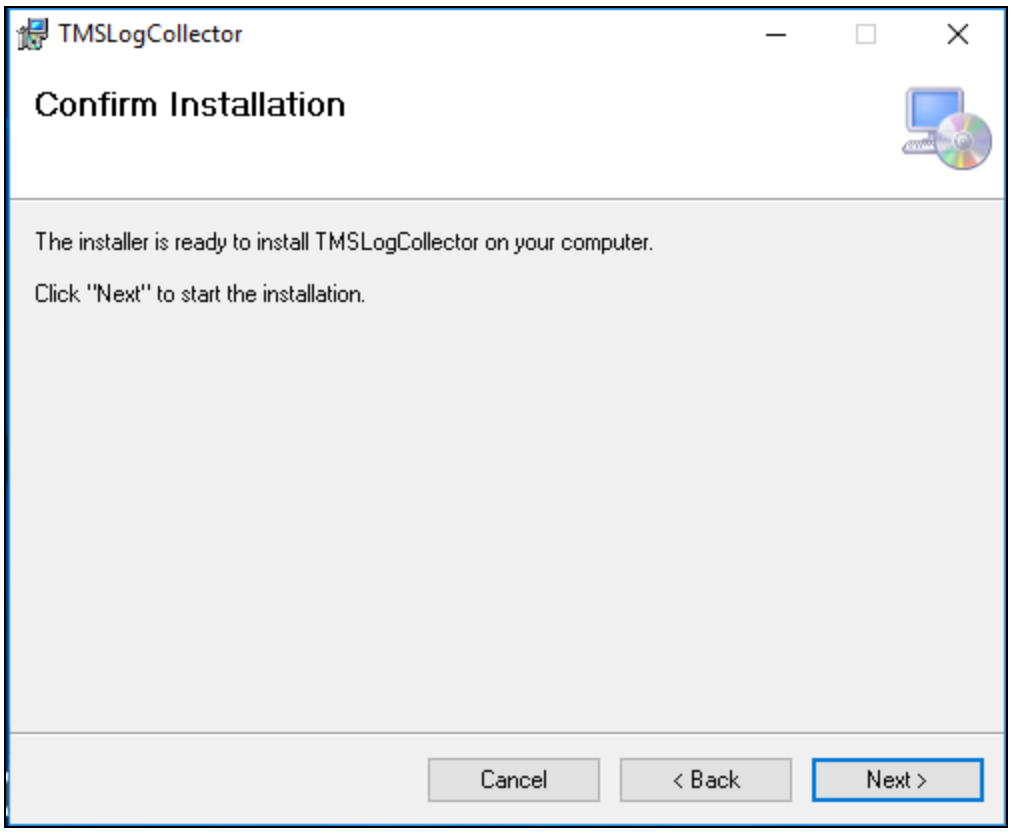
1. After Cisco TMS installation is completed, then Cisco TMS Log Collection Utility installation dialog box will be displayed. For more information on how to begin Cisco TMS Log Collection Utility installation, refer to **Step 4** in Running the Installer, page 26 section. Click **'Next'** to continue.



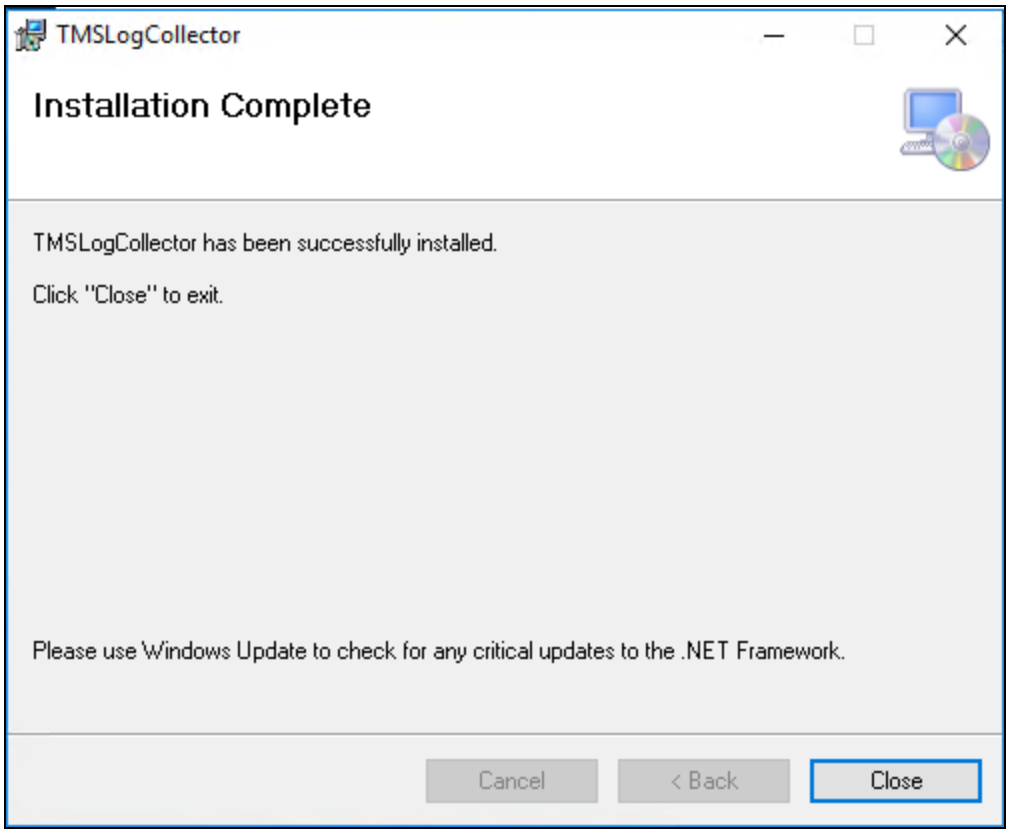
2. Browse to the directory/folder in which you want to install Cisco TMS Log Collection Utility. Select the option if you want to install Cisco TMS Log Collection Utility for self or for everyone. Click **'Next'** to continue

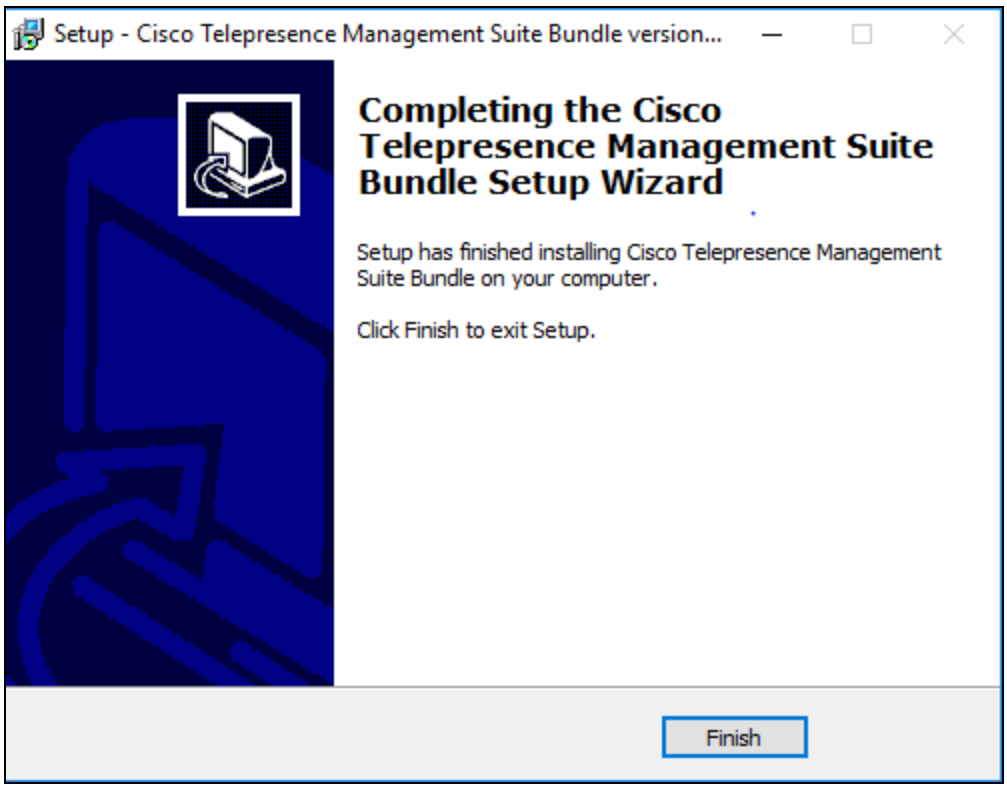


3. Click '**Next**' to start installation.

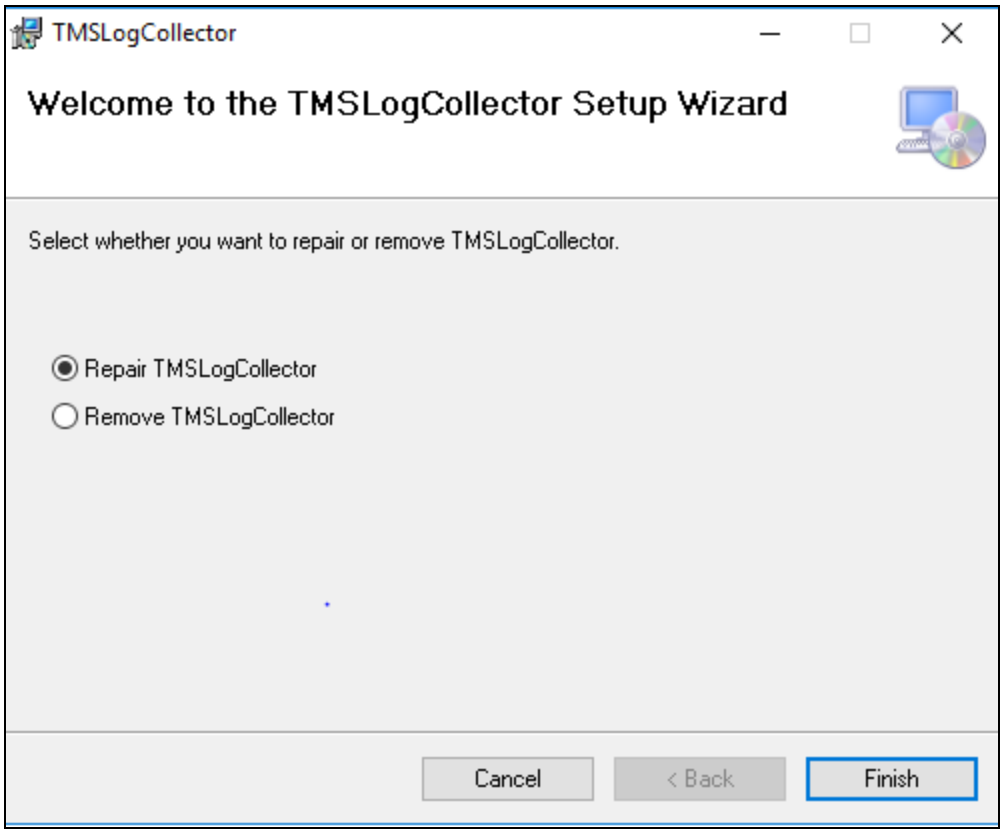


4. Once the installation is successfully completed, click **'Close'** to exit.


TMSLogCollector
Installation Complete
TMSLogCollector has been successfully installed.
Click "Close" to exit.
Please use Windows Update to check for any critical updates to the .NET Framework.
Cancel
< Back
Close


Setup - Cisco Telepresence Management Suite Bundle version...
Completing the Cisco Telepresence Management Suite Bundle Setup Wizard
Setup has finished installing Cisco Telepresence Management Suite Bundle on your computer.
Click Finish to exit Setup.
Finish

Note: When both the applications are already installed and user tries to run the installer package again, then Cisco TMS will work as per its original behavior. However for Cisco TMS Log Collection Utility, a dialog box will appear to Repair or to Remove Cisco TMS Log Collection Utility.



Enabling the Windows SNMP Service

Windows SNMP Service is disabled by default for new installations of Cisco TMS. Customers using legacy equipment that requires SNMP can enable this service after installation.

Accessing Cisco TMS for the First Time

Once Cisco TMS is installed, access the web interface using a browser:

1. Do one of the following:
   - Use the shortcut provided in the Cisco program group in the Windows **Start** menu.
   - Enter `https://<serveraddress>/tms` in your web browser's URL field, where <serveraddress> is the hostname (recommended) or IP address of your server. Using the hostname accommodates integrated authentication with Active Directory.

2. If accessing the web site from the server console, you will usually authenticate automatically with your currently logged in username and Cisco TMS will open. If not, you will be asked for authentication details. Most browsers will display two fields in the login window that appears—a username and password field. How you enter your username will depend on the type of Windows account you are using.

Field	Description	Example
Domain Users	Username should be entered as `domain\username`. The `username@<Domain DNS name>` format is also suitable, but less commonly used.	**`corp\firstname.lastname`**
Local Windows Accounts	Username should be entered as `machinename\username`	**`tms-2\administrator`**

3. A window called **Edit Personal Information** will pop up after you successfully authenticate. If this window does not appear, look for pop-up blocking alerts from your browser, and disable pop-up blocking for Cisco TMS.
4. Fill in your details and click **Update Your Personal Information**.

Setting up a Redundant Deployment

Cisco TMS supports deployment in a redundant configuration, increasing the availability of the application.

This chapter describes the requirements, configuration, and limitations of deploying Cisco TMS in the two supported redundant scenarios.

It is assumed that the reader has an understanding of Cisco TMS, Cisco TMS installation, and Windows Server operating systems, as well as an advanced level of understanding of computer networking and network protocols.

Preliminary Information 42
Deploying with a Load Balancer 43
Deploying a Hot Standby 48
Upgrading a Redundant Deployment from Version 14.4 or Later 52
Upgrading a Redundant Deployment from a Cisco TMS Version Earlier than 14.4 52
Example ACE Configuration 53
Example F5 BIG-IP Configuration 54
Local Files for Synchronization 57

Preliminary Information

Supported Configurations

For a fully redundant Cisco TMS deployment with an automatic failover process, you must set up two Cisco TMS servers with a network load balancer (NLB) in front. For new deployments, we recommend using an F5 BIG-IP load balancer for load-balancing IP traffic between the two Cisco TMS servers, therefore this document describes how to deploy Cisco TMS with an F5 BIG-IP appliance. We also support using a Cisco ACE 4710 Application Control Engine Appliance. Migrating from the previous redundancy model to this improved model if you are using an ACE load balancer is described in Upgrading a Redundant Deployment from a Cisco TMS Version Earlier than 14.4, page 52.

This chapter also describes how to deploy two Cisco TMS servers using a Hot Standby model.

Regardless of which of the two redundancy models you choose to deploy, no more than two Cisco TMS servers can be used. Deploying more than two Cisco TMS servers in a redundant setup is neither tested nor supported by Cisco.

Deploying two Cisco TMS servers will increase Cisco TMS availability, but will not in any way increase Cisco TMS scalability.

Other models of load balancer with alternative configurations may work with Cisco TMS, but have not been tested by Cisco.

Licensing

Only one live database can be used in a redundant Cisco TMS implementation, therefore both servers will use the same Cisco TMS serial number and the same set of release and option keys.

Database Redundancy

Cisco TMS relies heavily on its SQL database, so a fully resilient Cisco TMS solution will also utilize one of the high-availability technologies offered by SQL Server.

Cisco TelePresence Management Suite Provisioning Extension

Implementing Cisco TMSPE in a redundant environment is described in the Provisioning Extension Deployment Guides.

Limitations in a Redundant Deployment Using a Load Balancer

Note the following when implementing redundancy in your Cisco TMS environment:

- Automatic update of the System Connectivity setting for systems (**Administrative Tools > Configuration > Network Settings > Update System Connectivity for Systems**) is disabled in a redundant environment.
- Tasks such as phone book and Active Directory synchronization could fail if a failover takes place:
  - while the tasks are running.
  - immediately before the tasks are scheduled to run.
- Conferences will not be affected during a failover due to the frequency of retries for allocation and connection.
- If using your own or a 3rd party booking client you must use the client session mechanism introduced in version 13 of Cisco TMSBA.See Cisco TMS Booking API Programming Reference Guide for more details.

Deploying with a Load Balancer

Configuring two Cisco TMS servers (also referred to as "nodes" in this context) with a network load balancer (NLB) provides a truly redundant Cisco TMS setup with fully automatic fail-over.

Recommended Hardware

For new deployments, we recommend using an F5 BIG-IP load balancer. We also currently support using a Cisco ACE 4710 Application Control Engine Appliance, but support for this load balancer will be withdrawn in a future version of Cisco TMS.

Active Directory and User Authentication Requirements

- Both Cisco TMS servers must be members of the same Windows domain.
- All Cisco TMS users must be imported from and authenticated using Active Directory.
- Using local user accounts is not supported for this redundancy model.

Overview

Nodes

Cisco TMS is a cluster-aware application when deployed behind a Network Load Balancer (NLB). When two Cisco TMS servers are connected to the same tmsng database and redundancy is enabled in **Administrative Tools > Configuration > General Settings**, one of the servers immediately becomes the active node, while the other server becomes the passive node. Only one node can be active at any given time.

The active node behaves exactly like a stand-alone Cisco TMS server.

The passive node:

- Remains in a standby mode with its web pages and services locked down.
- Refuses all incoming traffic from users and managed systems.

While a node is passive, traffic to the tmsng database is kept to a minimum, so that the passive node does not significantly alter overall Cisco TMS performance.

Failover

The process of nodes switching between passive or active status is called a failover. A failover can occur either automatically, or can be manually initiated by an administrator.

Automatic failover will take place if one of the following occurs:

- The active node detects that its own services are unresponsive or disabled.
- The passive node detects that the active node's services are unresponsive or disabled.

When a failover is triggered, the formerly passive node is immediately elevated to being active, at the same time as the formerly active node retires its services and web interface into standby mode. It can take up to 1 minute for the change to be detected by the NLB, during which time Cisco TMS will be partially unavailable. Manual failovers should therefore only be initiated outside of normal business hours.

Cisco TMS uses a simple counting mechanism to decide whether it should initiate an automatic failover. The process is as follows:

1. Each Cisco TMS service (including IIS) on both the active and passive node continuously writes a keep-alive notification to the tmsng database showing when it was last functional.
2. The active node monitors this list of services and timestamps, categorizing services that have sent notifications within the last minute as operational. If it sees that the passive node has more operational services than the active node has itself, it retires and passes control over to the other node, which then becomes active.
3. As a fallback mechanism, the passive node also monitors the timestamps and forces a failover if the active node stops writing keep-alive notifications.

The Network Load Balancer

The NLB monitors the status of both nodes, and directs all incoming traffic only to the active node. No incoming traffic should ever be directed to the passive node, unless a failover has happened (see Overview, page 43).

To monitor the status of the nodes, the NLB must be set up to probe a specific URL (displayed in **Administrative Tools > TMS Server Maintenance**) on both nodes every five seconds. Probing this URL also serves another purpose, as both Cisco TMS nodes keep track of how often it is accessed. If a node stops receiving probe requests to the URL, it will assume that the network link between the NLB and itself is down, and mark its own IIS service as being inactive. If this happens on the active node, it will trigger a failover as described above.

Network Topology and Communication with Managed Systems

Incoming network traffic from users and managed systems is routed to the Cisco TMS servers through the NLB. A Virtual IP address (VIP) must be assigned to the NLB, and a DNS record must be created pointing to the NLB's VIP. The VIP (or associated DNS record) is then used as the management and feedback address for all managed systems.

The NLB's hostname and IP address(es) must be entered in Cisco TMS **> Administrative Tools > Configuration > Network Settings > Advanced Network Settings for Systems on Internal LAN** and **Advanced Network Settings for Systems on Public Internet/Behind Firewall**.

Once the IP address and hostname values in **Network Settings** have been changed, the Database Scanner service enforces these new network settings on the managed systems. The systems then start directing traffic to the NLB, which forwards the requests to the Cisco TMS servers.

Outgoing traffic from Cisco TMS's own services does not go through the NLB; the active Cisco TMS node will bypass the NLB when managing systems. For this reason, Cisco TMS's logic for automatically updating the system connectivity setting and parameters based on information in IP protocol headers is disabled when Cisco TMS redundancy is enabled. For further information on how Cisco TMS communicates with managed systems, refer to the chapter *System management overview* in the Cisco TMS Administrator Guide.

Organizations that make significant changes to their network after deploying a redundant Cisco TMS solution must manually verify that system connectivity between Cisco TMS and managed systems still works after the network

change. An example of a change that would require connectivity verification would be the introduction of a new proxy between the managed systems and Cisco TMS.

See Deploying with a Load Balancer, page 43 for instructions on implementing this configuration.

Architectural Overview and Network Diagram

Example Configuration

In the example below the following values are used:

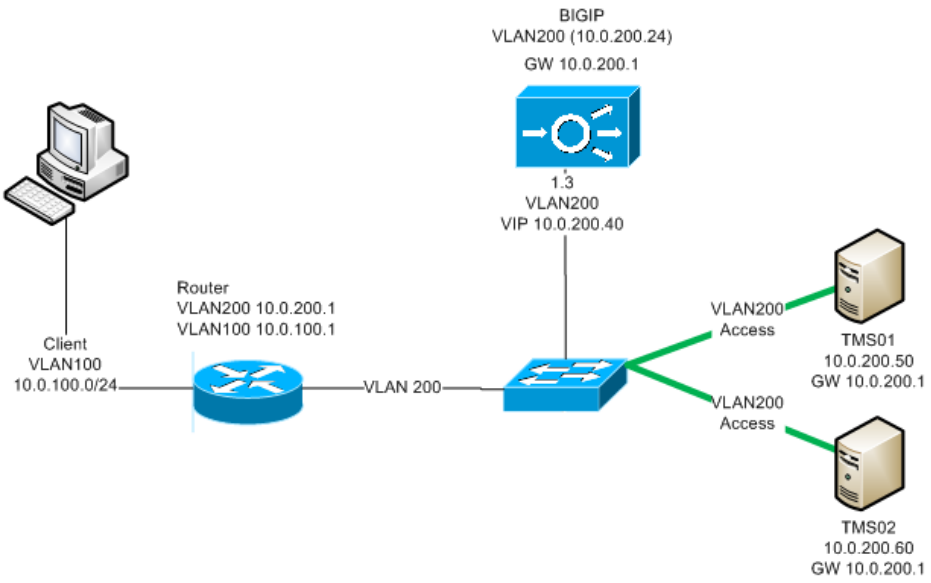
Table 2 VLAN200

Device	IP address	Hostname
F5 BIG-IP Virtual IP Address	10.0.200.40	tms.example.com
tms01	10.0.200.50	tms01.example.com
tms02	10.0.200.60	tms02.example.com

Table 3 VLAN100

Device	IP address	Hostname
Managed systems and users	10.0.100.0/24	

- There are two Virtual LANs, VLAN200 and VLAN100.
- The F5 BIG-IP is configured on VLAN200.
- The two Cisco TMS servers (tms01 at 10.0.200.50 and tms02 at 10.0.200.60) are configured on VLAN200.
- All clients (managed systems and users) are configured on VLAN100.
- All traffic to the virtual IP address of the F5 BIG-IP is forwarded to one of the two Cisco TMS servers.
- All managed systems and users use the F5 BIG-IP's virtual IP address when communicating with Cisco TMS.
- The two Cisco TMS servers share a common, external tmsng database.



Installing and Configuring

Installing Cisco TMS on tms01

1. Prior to installing Cisco TMS, set up an SQL Server instance on an external server.
2. Install Cisco TMS on the first node, using the instructions provided in Running the Installer, page 26
3. Point Cisco TMS to the external database server.
4. Make a note of the encryption key generated during the installation.
5. When enabling HTTPS during installation, use a certificate issued to tms.example.com.
6. Log in to the Cisco TMS web application to verify that it works correctly.
7. Go to **Administrative Tools > General Settings >Enable TMS Redundancy** and select *Yes*.

Note that once this setting is set to *Yes*, the setting **Administrative Tools > Configuration > Network Settings >Update System Connectivity for Systems** will be automatically disabled.

Installing Cisco TMS on tms02

1. Check that the operating system including service pack level on tms02 is exactly the same as on tms01.
2. Check that both servers are configured with the same time zone and verify that the clocks are synchronized.
3. Install Cisco TMS using the same external database server and installation directory as when setting up tms01. Install the same version of Cisco TMS.
4. Enter the encryption key generated during the installation on tms01. (If you did not make a note of it in step 4 above, this is found in **TMS Tools** on tms01 under **Security Settings**.)
5. Log into Cisco TMS – you should get an error stating that Cisco TMS is unavailable.

Testing Manual Failover

1. Go to the IP/hostname of tms01.
2. Go to: **Administrative tools > TMS Server Maintenance > TMS Redundancy**.
3. Make a note of which is the active node and click **Retire Active Node**.
4. Refresh the Cisco TMS web page.
5. You should get the '*Cisco TMS is unavailable*' error.
6. Go to the IP/hostname of tms02.
   You should see that the other node is now the active node and you can access Cisco TMS.

Setting up the Network Load Balancer

Once the second node is operational, set up the network load balancer:

1. Configure the NLB to forward HTTP and HTTPS connections as well as SNMP traps to the active node.
2. For Polycom phonebooks to work, configure the NLB to forward tcp port 3601 to the active node.
3. Configure the NLB to probe the Probe URL:
   a. Set the NLB to probe the URL displayed here in Cisco TMS: **Administrative Tools > TMS Server Maintenance > TMS Redundancy > Probe URL** on both nodes. This must be probed aggressively, preferably every 5 seconds.
   b. Push all traffic to the active node (the one replying with HTTP 200).

Note: Ensure that the Probe URL is not monitored by any other monitoring application.

See Example F5 BIG-IP Configuration, page 54 for a reference F5 BIG-IP configuration.

Configuring Cisco TMS

On the active node:

1. In the Cisco TMS application go to **Administrative Tools > Configuration > Network Settings**.
2. Change the following IP address(es) and hostnames to the NLB's virtual IP address(es) and hostname:
   - **Event Notification > SNMP Traphost IP Address**
   - **Advanced Network Settings for Systems on Internal LAN**: all fields
   - **Advanced Network Settings for Systems on Public Internet/Behind Firewall**

On both nodes:

Verify that the Cisco TMS servers can reach the managed systems and vice versa by going to the web interface of some of the managed systems using a browser on the Cisco TMS servers.

Synchronizing Local Files

Some customizable files used by Cisco TMS are stored in the Windows server's local file system rather than in the tmsng database. The folders these files are stored in must be kept synchronized between the two servers. See Local Files for Synchronization, page 57 for a full list of the folders that must be synchronized.

Cisco TMS does not maintain any file synchronization process. The use of a 3rd party tool will be required. Refer to the documentation for 3rd party tool about information on proper configuration of file/ folder synchronization.

Optional: Enabling use of TLS Client Certificates

If you choose to use TLS client certificates in your deployment you must ensure that:

- The same options are selected in Cisco TMS Tools on both servers.
- The TLS certificates imported to both servers are identical.
- Both servers use the same mechanism for certificate revokation.

For more information see the chapter Cisco TMS Tools in the Cisco TMS Administrator Guide.

Testing that Failover Works

1. Log in to Cisco TMS using the VIP of the NLB.
2. Force a manual failover.
3. Wait 1 minute, then refresh your browser.
4. Go to **Administrative Tools > TMS Server Maintenance > TMS Redundancy**, and verify that a failover actually happened by looking at the **Failover Activity Log**.

Upgrading Cisco TMS

Upgrading Cisco TMS to a later software version must be done during a maintenance window, as upgrading will make Cisco TMS unavailable to users for a short period of time.

As the two Cisco TMS nodes share a common database, they must run the same software version at all times. It is therefore not possible to upgrade one node at a time and keep the other node operational to serve systems and users.

1. Log in to both Cisco TMS Windows servers.
2. Disable file replication to temporarily stop synchronizing local files.
3. Stop all the TMS services, as well as the IIS service on both nodes.
4. Upgrade one of the nodes to the new software version. This will upgrade the tmsng database.
5. Log in to the Cisco TMS web application on this server to verify that it works correctly.

The probes on the NLB will now pick up that the upgraded server is the active node. Users and managed systems can now use Cisco TMS again.

1. Upgrade the second Cisco TMS node.
2. The installer will detect that the database has already been upgraded, and offer to continue using the updated database: select **Yes**. The installer will then update the binaries and leave the database alone.
3. Log in to the Cisco TMS web application on the active server, and force a manual failover. Verify that the second server becomes active within one minute.
4. Enable file replication.

Check that the network settings have not been changed during the install process:

1. In the Cisco TMS application go to **Administrative Tools > Configuration > Network Settings**.
2. Check that the following IP address(es) and hostnames are set to the NLB's virtual IP address(es) and hostname:
   - **Event Notification > SNMP Traphost IP Address**
   - **Advanced Network Settings for Systems on Internal LAN**: all fields
   - **Advanced Network Settings for Systems on Public Internet/Behind Firewall**

Recovery in Case of a Failing Node

No immediate action is required in the event of a server failure. If the passive node goes down, the active node continues its operations as normal. If the active node goes down, the passive node will become active automatically, and the NLB will detect the failure and direct all traffic to the new active node.

Expect a delay of approximately one minute while the failover takes place. During this time the 'Unable to connect to Cisco TMS' error will be shown on the web page.

Troubleshoot the failing node's software and hardware as you normally would, and bring it back online once it is operational.

Troubleshooting with Managed Systems in a Redundant Deployment

Capturing a Wireshark trace on the active Cisco TMS server will show all incoming traffic as coming from the NLB. You will therefore be unable to easily identify the communication between Cisco TMS and the managed systems you are interested in.

Before you begin troubleshooting, do the following:

1. For all the systems you are investigating, temporarily set the management address to the address of the active Cisco TMS server.
2. Take the Wireshark capture.
3. Once you have finished taking the trace, set the management address of all the systems back to the address of the NLB.

Logs

- Log files must be gathered from both Cisco TMS servers.
- If changing the log levels, ensure that this is done on both servers. The exception to this is if you are changing the log level for a very short time, for example if you increase the log level, reproduce the problem and then immediately decrease the log level again.

Deploying a Hot Standby

Keeping an additional Cisco TMS server as a warm spare in case of failure is known as the "Hot Standby" redundancy model.This requires manual intervention if there is a failure on the primary Cisco TMS server, and is therefore a

switchover solution rather than a failover solution.

One Cisco TMS server is active at any given time with this redundancy model. The hot standby server must be kept up to date with security patches and other upgrades so that it is ready for activation within a few minutes if the primary server fails.

Note that the hot standby redundancy model requires the tmsng database to be located on an external SQL server, and that the two Cisco TMS servers must be in the same Windows domain.

In this deployment, do not enable redundancy using **General Settings > Enable TMS Redundancy**.

In the instructions below the following examples are used:

Server	DNS Name	IP Address
Primary Cisco TMS Server (tms01)	tms01.example.com	10.0.0.10
Secondary Cisco TMS Server (tms02)	tms02.example.com	10.0.0.11

The examples assume that you use IPv4. If you also use IPv6, change the IPv6 addresses accordingly.

Setting up the Primary Cisco TMS Server

Prior to installing Cisco TMS:

1. Set up an SQL server instance on an external server.
2. Set up a DNS record: tms.example.com pointing to the IP address of the primary server tms01 (10.0.0.10).

Installing Cisco TMS:

1. Install Cisco TMS on tms01 using the instructions provided in the Cisco TMS Installation and Getting Started Guide, pointing Cisco TMS to the external database server you used in Step 1 above.
2. Make a note of the encryption key generated during the installation.
3. When enabling HTTPS during installation, use a certificate issued to tms.example.com.
4. Log in to the Cisco TMS web application to verify that it works correctly.

All users and managed systems must use tms.example.com when connecting to Cisco TMS. The server's own hostname (tms01.example.com) must not be used.

After verifying that the installation of Cisco TMS was successful:

1. In Cisco TMS go to **Administrative Tools > Configuration > Network Settings**.
2. Enter *tms.example.com* in the **TMS Server Fully Qualified Hostname** and **TMS Server Address (Fully Qualified Hostname or IPv4 Address)** fields.

Do not use local user accounts when logging in to Cisco TMS. All user accounts must be domain accounts, so that they are available if you have to swap to the secondary server, tms02.

Setting up the Secondary Cisco TMS Server

1. Check that the operating system including service pack level on tms02 is exactly the same as on tms01.
2. Check that the servers are both configured with the same time zone; failure to do this will mean that the start and end times of scheduled conferences are incorrect in the case of a switchover.

3. Run the Cisco TMS installer on tms02:
   a. Enter the IP address of the external SQL server when prompted.
   b. Install to the same directory as on tms01 and use the same log directory as on tms01. This is important because the log directory path is stored as an Environment Variable in Windows and not in the SQL database.
   c. Enter the encryption key generated during the installation on tms01.
   d. Use the same certificate used on tms01 when enabling HTTPS.
4. Log in to the Cisco TMS web application to verify that it works correctly.
5. On tms02 go to **Administrative Tools > Configuration > Network Settings > Advanced Network Settings for Systems on Internal LAN**. Make sure the IP address is tms01 (10.0.0.10) and the hostname is tms.example.com as the installer could have changed these values.
6. Open the Services Management Console on tms02:
   - Stop all the Cisco TMS services – they all have names starting with TMS.
   - Stop the Internet Information Services (IIS) service called World Wide Web Publishing Service.
   - Set the Startup Type of the IIS and TMS services to “Manual”.

Tms02 is now ready to act as a warm spare in the case of a failure on tms01.

Note that in **Administrative Tools > Server Maintenance > TMS Service Status** you will see the services for both servers. Click on **Clear List** to remove the stopped services on tms02 from the list.

Synchronizing Local Files

Some customizable files used by Cisco TMS are stored in the Windows server's local file system rather than in the tmsng database. The folders these files are stored in must be kept synchronized between the two servers. See Local Files for Synchronization, page 57 for a full list of the folders that must be synchronized.

Cisco TMS does not maintain any file synchronization process. The use of a 3rd party tool will be required. Refer to the documentation for 3rd party tool about information on proper configuration of file/ folder synchronization.

If you swap the two servers in the event of a failure on the primary server, change the synchronization mechanism you set up for keeping the folders on tms01 and tms02 in synch so that it now synchronizes from tms02 to tms01.

Optional: Enable TLS Client Certificates

If you choose to use TLS client certificates in your deployment you must ensure that:

- The same options are selected in Cisco TMS Tools on both servers.
- The TLS certificates imported to both servers are identical.
- Both servers use the same mechanism for certificate revokation.

For more information see the chapter Cisco TMS Tools in the Cisco TMS Administrator Guide.

Upgrading Cisco TMS

You must keep the Cisco TMS software versions on the primary and secondary servers consistent. After upgrading the primary server, you must upgrade the secondary server as soon as possible. If the primary server fails while the secondary server is on an older software version, you will not be able to swap the servers until you have upgraded the secondary server to the newer Cisco TMS software version.

1. Disable file replication to temporarily stop synchronizing local files.
2. Upgrade the primary server.
3. Upgrade the secondary server.
4. Log in to the Cisco TMS web application to verify that it works correctly.

5. In the Cisco TMS application go to **Administrative Tools > Configuration > Network Settings**.
6. Check that the following IP address(es) and hostnames are set to IP address: 10.0.0.10 and hostname: tms.example.com:
   - **Event Notification > SNMP Traphost IP Address**
   - **Advanced Network Settings for Systems on Internal LAN**: all fields
   - **Advanced Network Settings for Systems on Public Internet/Behind Firewall**
7. Stop the TMS services and set them to Manual again.
8. Enable file replication.

Recovery if the Primary Server Fails

If the primary server: tms01 fails and becomes unusable, changing the secondary server: tms02 into an operational state will take no more than a few minutes.

1. Unplug tms01 from the network.
2. Change the IP address of tms02 to the old IP address of tms01, for example 10.0.0.10.
3. Verify that tms02 is reachable on its new IP address.
4. Open the Cisco TMS Tools application and go to **Configuration > Change DB Connect Settings**.
5. Click **OK** to verify that tms02 still has the correct password, as the password to the database might have changed since you initially set up tms02.
6. In the Services Management Console:
   a. Change the Startup Type of all the TMS services and the World Wide Web Publishing Service to *Automatic*.
   b. Start the services.

Tms02 is now the active Cisco TMS server. As you have instructed managed systems to use tms.example.com when communicating with Cisco TMS, no reconfiguration is needed on the managed systems themselves.

To verify that tms02 operates correctly:

1. Schedule a short conference two minutes into the future.
2. See that it launches and is torn down as expected.
3. Check that you can monitor it using the **Conference Control Center**.
4. Check that Cisco TMS generates a call detail record (CDR) for the conference.

To verify that Cisco TMS is communicating with systems:

1. Wait approximately 20 minutes for the TMS Database Scanner Service to complete a full run.
2. Go to **Systems > System Overview** in Cisco TMS.
3. Select all the systems in the tree to the left, and select **Network Settings > TMS To System Connectivity** in the tree to the right.
4. Click **View** and then check that no systems have their **Status** set to *NoResponse*.

Note that in **Administrative Tools > Server Maintenance > TMS Service Status** you will see the services for both servers. Click on **Clear List** to remove the stopped services on tms01 from the list.

Before connecting tms01 to your network:

1. Change its IP address to tms02's old value, for example 10.0.0.11.
2. Disable all the TMS services and IIS.

Once the problem with tms01 has been fixed, it will become the warm spare in case tms02 ever goes down.

Note: Do not add tms01 back to the network before changing its IP address to a new value. This will lead to IP address conflicts that will cause unpredictable behavior in Cisco TMS.

Upgrading a Redundant Deployment from Version 14.4 or Later

Before You Upgrade the Servers

Do the following on both Cisco TMS servers:

1. Disable file replication to temporarily stop synchronizing local files.
2. Stop all the TMS services, as well as the IIS service.

Upgrade the Primary Node

1. Upgrade the primary Cisco TMS server in the normal way.
2. Go to **Administrative Tools > TMS Server Maintenance**, and verify that the server is listed as *Active* in the **TMS Redundancy** section. If it is listed as *Passive*, click **Refresh** repeatedly for up to a minute until the data is updated correctly.

Upgrade the Secondary Node

1. Upgrade the secondary Cisco TMS server in the normal way.
2. Through the Virtual IP of the NLB, go to **Administrative Tools > TMS Server Maintenance**, and verify that the second server appears as *Passive* in the **TMS Redundancy** section.
3. Verify that all TMS services (including TMSProbeURL) on the passive node appear as *Service On Standby* in the **TMS Services Status** section.
4. Test a manual failover by following the instructions in Testing Manual Failover, page 46.
5. Re-enable replication of local files between the two Cisco TMS nodes.

Upgrading a Redundant Deployment from a Cisco TMS Version Earlier than 14.4

Upgrading a redundant Cisco TMS deployment from a Cisco TMS version earlier than 14.4 requires making changes to the Network Load Balancer (NLB) configuration. Before upgrading, read Setting up a Redundant Deployment, page 42 to familiarize yourself with the new recommended NLB setup.

Before You Upgrade the Servers

Do the following on both Cisco TMS servers:

1. Disable file replication to temporarily stop synchronizing local files.
2. Stop all the TMS services, as well as the IIS service.
3. Change the Default Gateway so that the servers no longer use the NLB as their Default Gateway.
4. Verify that you still have network connectivity to managed systems, for example by browsing to a managed system's web interface.

Upgrade and Configuration for the Primary Server

1. Upgrade the primary Cisco TMS server in the normal way.
2. Once the upgrade has completed, log in to the Cisco TMS web interface. Go to **Administrative Tools > Configuration > General Settings**, and set **Enable TMS Redundancy** to *Yes*.

3. Go to **Administrative Tools > TMS Server Maintenance**, and verify that the server is listed as *Active* in the **TMS Redundancy** section. If it is listed as *Passive*, click **Refresh** for up to a minute until the data is updated correctly.
4. Make a note of the **Probe URL**.

Updating the NLB Configuration and Verification on the Primary Server

1. Migrate the NLB as described in **Example ACE configuration**. Use the probe URL from step 4 above.

   Note that the probing of the secondary server will fail at this stage as it has not been upgraded yet.
2. On the primary server, go to **Administrative Tools > TMS Server Maintenance**, and verify that *TMSProbeURL* now appears in the list in the **TMS Services Status** section.Go to **Administrative Tools > TMS Server Maintenance**, and verify that *TMSProbeURL* now appears in the list in the **TMS Services Status** section.
3. In a browser, enter the NLB's Virtual IP address (VIP), and verify that you are forwarded to Cisco TMS.

Upgrade and Configuration for the Secondary Server

1. Upgrade the secondary Cisco TMS server in the normal way.
2. Through the VIP of the NLB, go to **Administrative Tools > TMS Server Maintenance**, and verify that the second server appears as *Passive* in the **TMS Redundancy** section.
3. Verify that all TMS services (including TMSProbeURL) on the passive node appear as *Service On Standby* in the **TMS Services Status** section.
4. Test a manual failover by following the instructions in Testing that Failover Works, page 47.
5. Re-enable replication of local files between the two Cisco TMS nodes.

Example ACE Configuration

The following example provides details when ACE configuration is used by load balancer with Cisco TMS. Applying this configuration will ensure that it works correctly with the new redundancy model.

For example:

```
probe http PROBE-HTTP-TMS
port 80
interval 2
faildetect 1
passdetect interval 2
request method head url /tms/public/IsAlive.aspx?guid=<TMS REDUNDANCY GUID>
expect status 200 200
open 1
rserver host TMS01
ip address 10.0.200.50
inservicer
server host TMS02
ip address 10.0.200.60
inservice
serverfarm host SFARM-TMS
failaction purge
probe PROBE-HTTP-TMS
rserver TMS01
```

```
inservice
rserver TMS02
inservice
class-map match-any L4-CLASS-TMS
2 match virtual-address 10.0.200.40 tcp eq 443
3 match virtual-address 10.0.200.40 tcp eq 80
4 match virtual-address 10.0.200.40 udp eq 162
5 match virtual-address 10.0.200.40 tcp eq 3601
policy-map type loadbalance first-match L7-POLICY-TMS
class class-default serverfarm SFARM-TMS
policy-map multi-match L4-POLICY-TMS
class L4-CLASS-TMS
loadbalance vip inservice
loadbalance policy L7-POLICY-TMS
loadbalance vip icmp-reply
nat dynamic 1 vlan 200
interface vlan 200
no ipv6 normalization
no ipv6 icmp-guard
ip address 10.0.200.24 255.255.255.0
no normalization
no icmp-guard
access-group input ALL
access-group output ALL
nat-pool 1 10.0.200.30 10.0.200.30 netmask 255.255.255.255 pat
service-policy input L4-POLICY-TMS
no shutdown
```

Example F5 BIG-IP Configuration

For example:

```
ltm default-node-monitor {
rule /Common/icmp and /Common/snmp_dca
}
ltm node /Common/TMS01 {
address 10.0.200.50
description "TMS NODE 01"
monitor /Common/icmp
}
ltm node /Common/TMS02 {
address 10.0.200.60
description "TMS NODE 02"
monitor /Common/icmp
```

```
}
ltm pool /Common/pl-TMS {
members {
/Common/TMS01:0 {
address 10.0.200.50
}
/Common/TMS02:0 {
address 10.0.200.60
}
}
monitor /Common/mn-TMS-HTTPS
}
ltm virtual /Common/vs-TMS-HTTP {
description "TMS Virtual Server for HTTP"
destination /Common/10.0.200.40:80
ip-protocol tcp
mask 255.255.255.255
pool /Common/pl-TMS
profiles {
/Common/fastL4 { }
}
source 0.0.0.0/0
source-address-translation {
type automap
}
translate-address enabled
translate-port enabled
vlans {
/Common/VLAN200
}
vlans-enabled
}
ltm virtual /Common/vs-TMS-HTTPS {
description "TMS Virtual Server for HTTPS"
destination /Common/10.0.200.40:443
ip-protocol tcp
mask 255.255.255.255
pool /Common/pl-TMS
profiles {
/Common/fastL4 { }
}
source 0.0.0.0/0
```

```
source-address-translation {
type automap
}
translate-address enabled
translate-port enabled
vlans {
/Common/VLAN200
}
vlans-enabled
}
ltm virtual /Common/vs-TMS-PLCM {
description "TMS Virtual Server for Polycom"
destination /Common/10.0.200.40:3601
ip-protocol tcp
mask 255.255.255.255
pool /Common/pl-TMS
profiles {
/Common/fastL4 { }
}
source 0.0.0.0/0
source-address-translation {
type automap
}
translate-address enabled
translate-port enabled
vlans {
/Common/VLAN200
}
vlans-enabled
}
ltm virtual /Common/vs-TMS-SNMPTRAP {
description "TMS Virtual Server for SNMPTRAP"
destination /Common/10.0.200.40:162
ip-protocol udp
mask 255.255.255.255
pool /Common/pl-TMS
profiles {
/Common/fastL4 { }
}
source 0.0.0.0/0
source-address-translation {
type automap
```

```
}
translate-address enabled
translate-port enabled
vlans {
/Common/VLAN200
}
vlans-enabled
}
ltm virtual-address /Common/10.0.200.40 {
address 10.0.200.40
arp enabled
icmp-echo enabled
mask 255.255.255.255
traffic-group /Common/traffic-group-1
}
ltm monitor https /Common/mn-TMS-HTTPS {
adaptive disabled
cipherlist DEFAULT:+SHA:+3DES:+kEDH
compatibility enabled
defaults-from /Common/https
destination *:443
interval 5
ip-dscp 0
recv 200
recv-disable 503
send "HEAD /tms/public/IsAlive.aspx?guid=<TMS REDUNDANCY GUID> HTTP/1.0\r\n"
time-until-up 0
timeout 16
}
```

Notes:

1. If you do not have any Polycom devices then it not required to configure port **3601**.
2. If you have enabled a higher security mode that disables the use of SNMP then it is not required to configure **SNMPTRAP** ports.
3. If you allow only https then http could be removed.

Local Files for Synchronization

During installation of Cisco TMS, customizable files are added which must be synchronized between the two servers when using a redundant deployment.

The files include software and images which can be uploaded to Cisco TMS, and images created by Cisco TMS.

In a default installation the files are located here:

C:\Program Files (x86)\TANDBERG\TMS\Config\System

C:\Program Files (x86)\TANDBERG\TMS\wwwTMS\Public\Data\SystemSoftware

Note: Directories are created on first use, which means that the directory might not exist when setting up file replication between nodes.

Moving or Uninstalling Cisco TMS

This chapter covers the procedures for moving Cisco TMS to a new server and removing all components from an old server.

Moving Cisco TMS to a New Server 60
Uninstalling Cisco TMS 65
Moving Cisco TMS Database to External SQL Server 66
Uninstall TMS Log Collector 67

Moving Cisco TMS to a New Server

Whether a server is being decommissioned or you are expanding your deployment and need more hardware capabilities, follow the instructions below to move the Cisco TMS installation onto another server.

Before You Start

- We recommend keeping the network configuration the same on the new server, using the same DNS host name and IP address if possible. This will minimize the administrative tasks required after the move.
- Ensure that the same ports are open on the firewall for the new server as for the old server.
- If Cisco TMSPE is installed on the Cisco TMS server, it must be moved at the same time.

Cisco TelePresence Management Server (Appliance)

If you are moving from Cisco TelePresence Management Server (Appliance) to a new Windows server, contact your Cisco sales representative to purchase a new software-only copy of Cisco TMS. Then contact the Global Licensing Operations department via the Licensing Portal or the Licensing Support Request Form and ask them to re-host the option keys.

Moving the Application and Database

Copying Installation Data

Before following the procedure to move Cisco TMS with either a local or remote database:

1. Take a copy of the encryption key to enter on the new server during the installation process: On the Cisco TMS server, open TMS Tools and select **Security Settings > Encryption Key**. Copy to a notepad file.
2. If you are keeping the same IP address and use TLS Client Certificates from an external certificate authority, take a copy for use on the new server. If the new server's host name will change, you will need to generate new certificates.

SQL Database is Stored Locally on the Cisco TMS Server

The same version of Cisco TMS must be used on both servers, and they must both be in the same time zone.

1. Stop all TMS services and IIS on the original Cisco TMS server:
   a. Open the Services Management Console.
   b. Stop all the Cisco TMS services—they all have names starting with "TMS".
   c. Stop the Internet Information Services (IIS) service called World Wide Web Publishing Service.

2. Using SQL Server Management Studio Express, back up the SQL database, and copy the **tmsng.bak** file to the new Cisco TMSserver:
   a. Right-click on the **tmsng** database.
   b. Select **Tasks > Back Up... > Database...**
   c. Note the backup destination path and click **OK**.
   d. Copy the **tmsng.bak** file from its backup location to any location on the new server.
3. Install the same version of Cisco TMS on the new server:
   a. Select *Install the database on this server*.
   b. Do not enter any release or option keys.
   c. Enter the **IP Address** of the old server.
   d. Enter the **Encryption Key** from the old server.
4. Restore the SQL database using SQL Server Management Studio Express:
   a. Right click on the **tmsng** database.
   b. Select **Tasks > Restore > Database...**
   c. Under **Specify the source and location of backup sets to restore** select **From device** and browse to the location where you saved the **tmsng.bak** file.
   d. Click **OK** until you get back to the **Restore Database - tmsng** window.
   e. Under **Select the backup sets to restore**, check the box in the **Restore** column next to the appropriate backup file. Click **OK**.
5. Open the Cisco TMS web application and check that it works and that all your data is in place.
6. Copy the following customizable folders that were saved locally on the original server to the same locations on the new server if necessary—these folders are created on first use so you may have to manually create them. In a default installation the files are located here:
   - **C:\Program Files (x86)\TANDBERG\TMS\Config\System**
   - **C:\Program Files (x86)\TANDBERG\TMS\Data\GenericEndpoint**
   - **C:\Program Files (x86)\TANDBERG\TMS\Data\SystemTemplate**
   - **C:\Program Files (x86)\TANDBERG\TMS\wwwTMS\Data\CompanyLogo**
   - **C:\Program Files (x86)\TANDBERG\TMS\wwwTMS\Data\ExternalSourceFiles**
   - **C:\Program Files (x86)\TANDBERG\TMS\wwwTMS\Public\Data\SystemSoftware**

SQL Database is on a Remote Server

It is not necessary to use the same version of Cisco TMS in this case, as the database will be upgraded during the install procedure.

1. Stop all TMS services and IIS on the original Cisco TMS server:
   a. Open the Services Management Console.
   b. Stop all the Cisco TMS services—they all have names starting with "TMS".
   c. Stop the Internet Information Services (IIS) service called World Wide Web Publishing Service.
2. Install Cisco TMS on the new server, pointing to the existing external SQL database during installation.
3. Open the Cisco TMS web application and check that it works and that all your data is in place.

4. Copy the following customizable folders that were saved locally on the original server to the same locations on the new server if necessary—these folders are created on first use so you may have to manually create them. In a default installation the files are located here:
   - **C:\Program Files (x86)\TANDBERG\TMS\Config\System**
   - **C:\Program Files (x86)\TANDBERG\TMS\Data\GenericEndpoint**
   - **C:\Program Files (x86)\TANDBERG\TMS\Data\SystemTemplate**
   - **C:\Program Files (x86)\TANDBERG\TMS\wwwTMS\Data\CompanyLogo**
   - **C:\Program Files (x86)\TANDBERG\TMS\wwwTMS\Data\ExternalSourceFiles**
   - **C:\Program Files (x86)\TANDBERG\TMS\wwwTMS\Public\Data\SystemSoftware**

Moving with a New Network Configuration

In some cases it may be necessary to change the IP address and even the hostname of the Cisco TMS server as part of the move.

If so, once you have installed Cisco TMS on the new server and checked that it is connected to the database, and that all your data is present, do the following:

- Go to: **Administrative Tools > Configuration > Network Settings** and enter the new IP address and host name of the Cisco TMS server in **Advanced Network Settings for Systems on Internal LAN** and **Advanced Network Settings for Systems on Public Internet/Behind Firewall**.
- In **Administrative Tools > Configuration > Network Settings > Enforce Management Settings on Systems**, click **Enforce Now**.
- If the hostname of the server has changed, and you use local user accounts rather than Active Directory accounts, change the user domain using **TMS Tools > Utilities > Change User Domain**. Note that if using local user accounts, these will need to be manually recreated on the new server.
- For Polycom systems, change the SNMP **Console IP Address** manually to the new IP and/or host name of the Cisco TMS server and reboot each system.
- If using Cisco TMSXE, open the configuration tool and change the Cisco TMS connection details as required.
- If using Cisco TMSXN, open Domino Administrator to change the **Host name** on the resource reservation database created for Cisco TMS as required.
- For remote systems, change the **External Manager Address** on each system manually to the new IP address or host name.

After Moving the Application

Do not reactivate any services related to Cisco TMS on the original server after the move.

We strongly recommend removing Cisco TMS from the original server, see Removing All Cisco TMS Information from a Server, page 65 if not decommissioning the server itself.

Moving Cisco TMSXE

For instructions on moving Cisco TMSXE to a new server, see *Cisco TMSXE Deployment Guide*.

Except for very small deployments, Cisco TMSXE must not be installed on the same server as Cisco TMS. See the best practices section of the installation guide for details.

Moving Cisco TMSPE

Cisco TMSPE is always installed on the Cisco TMS server and must be moved as soon as Cisco TMS has been moved.

As with Cisco TMS, the Cisco TMSPE databases may be local or remote.

Local Database

To move Cisco TMSPE:

1. Stop the Provisioning Extension Windows service on the original server.
2. Follow the steps to copy and restore the tmspe databases described for Cisco TMS above, see SQL Database is Stored Locally on the Cisco TMS Server, page 60.
3. Install Cisco TMSPE on the new server, pointing the installer to the new tmspe database location.
4. If the network configuration for Cisco TMS has changed, go to **Administrative Tools > Configuration > Provisioning Extension Settings > Cisco TMS Settings**.
   If **Hostname** is not `localhost`, it must be updated to reflect the new Cisco TMS address.

Remote Database

To move Cisco TMSPE:

1. Stop the Provisioning Extension Windows service on the original server.
2. Install Cisco TMSPE on the new server, pointing the installer to the remote database location.

3. If the network configuration for Cisco TMS has changed, go to **Administrative Tools > Configuration > Provisioning Extension Settings > Cisco TMS Settings**.
If **Hostname** is not `localhost`, it must be updated to reflect the new address.

Moving Database to external SQL server

The following steps must be followed to move the database to an external SQL server:

1. Stop all TMS services and IIS on the Cisco TMS server:

a. Open Services Management Console.

b. Stop all Cisco TMS services as they all have names starting with **TMS**.

c. Stop Internet Information Services (IIS) service called World Wide Web Publishing Service.

2. Using SQL Server Management Studio, back up the SQL database, and copy **tmsng.bak** file to the External SQL Server

If Cisco TMSPE is installed, create a backup of Cisco TMSPE, tmspe_vmr and tms_userportal databases, if they listed in the databases.

a. Right click on **tmsng** database.

b. Select **Tasks > Back Up... > Database...**

c. Note the backup destination path and click **OK**.

d. Copy **tmsng.bak** file from its backup location to any location on the External Server.

e. Follow same steps for creating Cisco TMSPE database(s), if applicable.

3. Using SQL Server Management Studio to create a new database or databases with the same name **tmsng**

a. Right click on **Databases > New Database**

b. Enter **tmsng** for the database name and click **OK**.

c. Follow the same steps for creating Cisco TMSPE database(s) if applicable.

4. Restore SQL database using SQL Server Management Studio:

a. Right click on **tmsng** database.

b. Select **Tasks > Restore > Database...**

c. In **Specify the source and location of backup sets to restore** select **From device** and browse to the location where you have saved **tmsng.bak** file.

d. Click **OK** until you get back to **Restore Database - tmsng** window.

e. In **Select the backup sets to restore**, select the checkbox in **Restore** column next to the required backup file.

f. In **Select a page**, click **Options**, select the checkbox **Overwrite the Existing database (WITH REPLACE)** and click **OK**.

g. Follow the same steps for creating Cisco TMSPE database(s), if applicable.

5. Use TMS Tools to change Cisco TMS Database Connection settings

a. Launch **TMS** Tools application on **TMS** server.

b. Click **Configuration > Cisco TMS Database Connection**.

c. Enter the new External SQL server information for **Database Server/Instance > Enter Authentication information.** and click **Save**.

d. If Cisco TMSPE is installed, click Cisco TMSPE Database Connection and follow Step **C**.

6. Start all Cisco TMS services and IIS on Cisco TMS server:

a. Open Services Management Console.
b. Start all Cisco TMS services as they all have names starting with **TMS**.
c. Start Internet Information Services (IIS) service called World Wide Web Publishing Service.

Moving Cisco TMSAE

Cisco TMSAE is always installed on the Cisco TMS server, but all program data is stored externally on the data warehouse server.

To move the Cisco TMSAE installation after the Cisco TMS move:

1. Stop the TANDBERG Analytics Extension Windows service on the original server.
2. Install Cisco TMSAE on the new server, following the instructions in Cisco TMSAE Installation Guide. Make sure to:
   - Use the same virtual directory name as on the original server.
     If changing the virtual directory name, you will need to update the Cisco TMSAE path in Cisco TMS after installation.
   - Select the Use Preconfigured option so that you can point the installer to the existing Cisco TMSAE database on the warehouse server.
   - Provide the detail for the new Cisco TMS server when prompted, including the new hostname or IP address if this has changed.
3. Verify that the ETL job can run properly by going to **Administrative Tools > Analytics Extension** and clicking **Run ETL Job Now**.

Uninstalling Cisco TMS

This section tells you how to remove the Cisco TMS application. Note that under normal conditions, older versions of Cisco TMS are removed automatically by the Cisco TMS installer.

Uninstalling Cisco TMS removes the Cisco TMS application, web site, and services. It leaves customer data, logs, databases and database servers intact for use in future upgrades.

The uninstall wizard does not modify the SQL server in any way. See the next section if you want to completely remove all Cisco TMS information from the server, including the database servers.

To remove the Cisco TMS application:

1. Select '*Uninstall Cisco TMS*' from the Cisco program group in the **Start** menu or screen, or use **Add/Remove Programs** in the Windows Control Panel.
   A welcome window explains that the uninstallation script removes Cisco TMS, but the database and database server must be removed separately.
2. Click **Next**.
   The wizard removes the Cisco TMS services, website, and application data.

Removal of the Cisco TMS application is complete.

Removing All Cisco TMS Information from a Server

The uninstall wizard only removes the Cisco TMS application from the server so that Cisco TMS can easily be reinstalled or upgraded in the future.

Caution:

- These steps assume that the SQL server was installed by Cisco TMS, is not being used by any other applications, and is safe to remove. Do not remove the SQL server or its program folder if the SQL server is used by any other application.
- Following these steps will delete *all* Cisco TMS data. Do not proceed if you intend to save any information from your Cisco TMS installation.

To completely remove Cisco TMS and all of its data from your server, follow these instructions:

1. Run the Cisco TMS uninstall wizard using the instructions in the previous section.
2. If Cisco TMSPE is installed, uninstall according to the instructions in *Cisco TelePresence Management Suite Provisioning Extension Deployment Guide*.
3. Delete the program folder used by the Cisco TMS installation. The default location is **C:\Program Files (x86)\TANDBERG\TMS**.
4. Open the Windows registry editor: from the Start menu, select 'Run..' and enter 'regedit', then click **OK**.
5. Expand the tree on the left using the plus icons to find the Hive (folder) **HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Tandberg\TANDBERG Management Suite**.
6. Right-click on the **TANDBERG Management Suite** folder icon, and click **Delete**. Click **Yes** to confirm.
7. Close the Registry Editor.
8. Ask your Microsoft SQL Administrator to drop the database named **tmsng** from Microsoft SQL instance used by Cisco TMS.

The removal of Cisco TMS, the database, and all customer saved data, is now complete.

Moving Cisco TMS Database to External SQL Server

Follow the procedure to move the Cisco TMS database to an external SQL server:

1. Stop all TMS services and IIS on the original Cisco TMS server:
   a. Open the Services Management Console.
   b. Stop all the Cisco TMS services—they all have names starting with "TMS".
   c. Stop the Internet Information Services (IIS) service called World Wide Web Publishing Service.
2. Using SQL Server Management Studio Express, back up the SQL database, and copy the **tmsng.bak** file to the new SQL server:
   a. Right click on the **tmsng** database.
   b. Select **Tasks > Back Up... > Database...**
   c. Note the backup destination path and click **OK**.
   d. Copy the **tmsng.bak** file from its backup location to any location on the new server.
3. Restore the SQL database using SQL Server Management Studio Express:
   a. Right click on the **tmsng** database.
   b. Select **Tasks > Restore > Database...**
   c. Under **Specify the source and location of backup sets to restore** select **From device** and browse to the location where you saved the **tmsng.bak** file.
   d. Click **OK** until you get back to the **Restore Database - tmsng** window.
   e. Under **Select the backup sets to restore**, check the box in the **Restore** column next to the appropriate backup file. Click **OK**.
4. Go to Cisco TMS server and open TMS TOOLS.

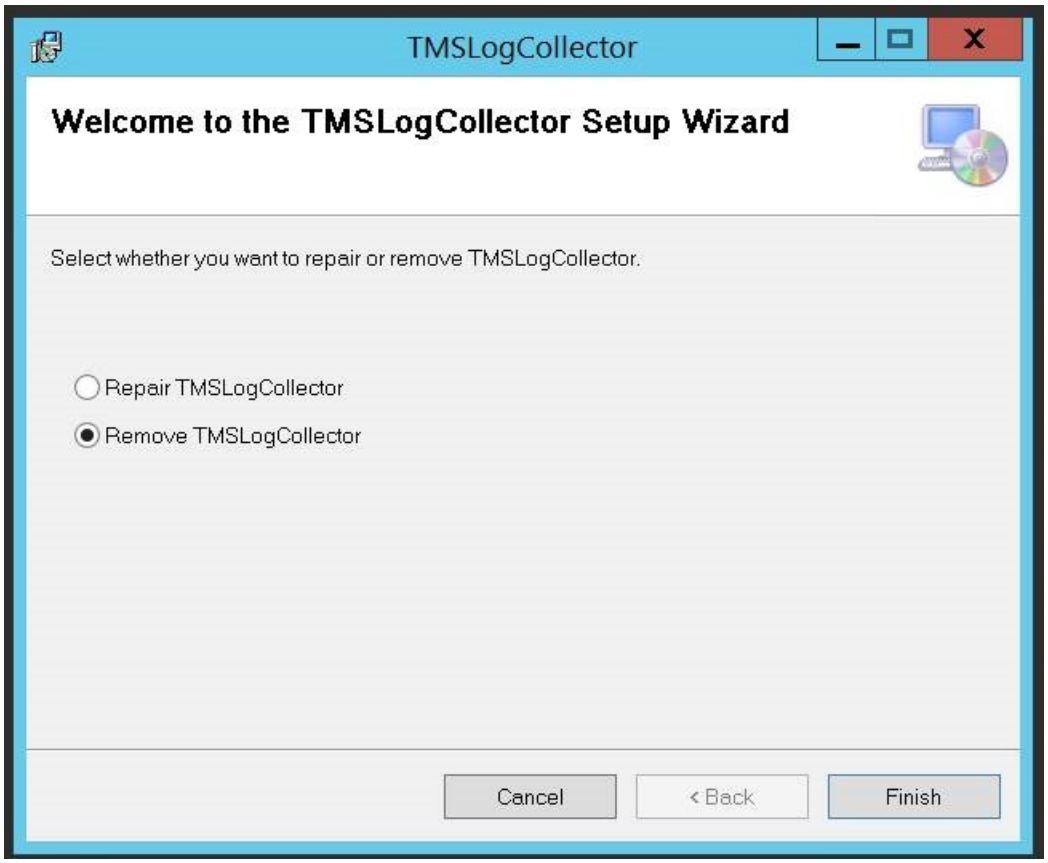
5. Go to **Configuration > Cisco TMS Database Connection** and provide **Database server and Instance in Database Server\Instance** text field. Click **Save**.
6. Start all the TMS servcies and IIS.
7. Open the Cisco TMS web application and check that it works and that all your data is in place.

Uninstall TMS Log Collector

1. Double click **TLCSetup**

   or

   Navigate to **Control panel>Uninstall Programs> TMS Log Collector >Unistall**.
2. Select **Remove TLC Logsetup**.



3. Click **Finish**.

Note: The uninstall procedure will not delete the log file of TMS Log Collector. You have to manually delete it.

Troubleshooting

Installation Times Out

The default database timeout value when upgrading Cisco TMS is 30 minutes. This value applies to each of the installer's internal database operations. For big deployments with years of call history and/or system data, some of the operations may need more than 30 minutes to complete.

This timeout value is configurable using a command line option. To use a timeout value of 60 minutes, run the installer from the command line as follows:

```
TMS15.8.exe /z"sqltimeout 60"
```

Substitute `60` with a higher value if needed.

We recommend using the default value of 30 minutes, and only increasing the timeout value if the initial upgrade attempt is failing.

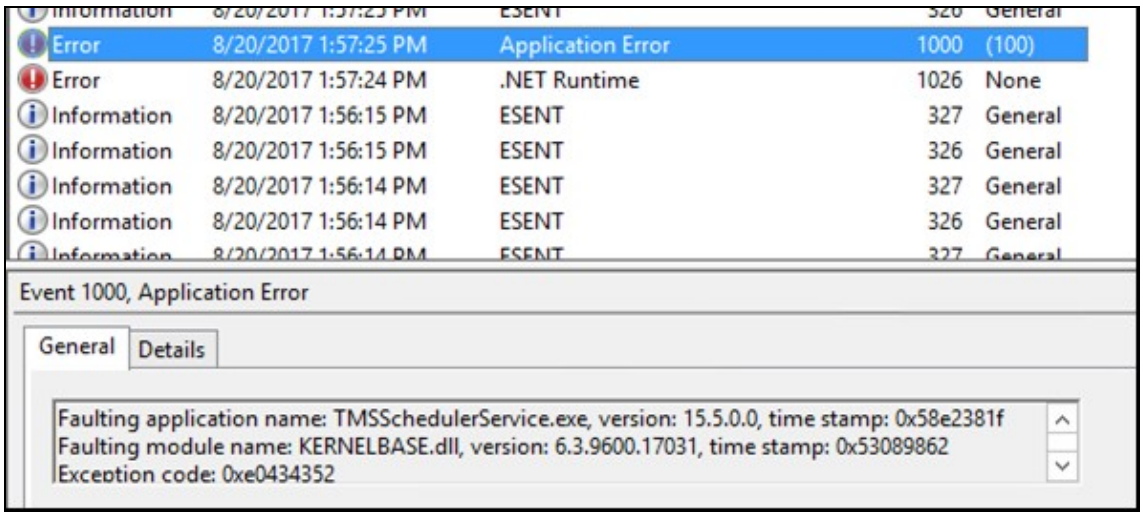
Upgrading Windows OS software from 2008R2 to 2012R2, stops 'TMSSchedulerService'

When Windows OS software is upgraded from 2008R2 that has Cisco TMS 15.5 version or below to 2012R2, sometimes it is noticed that **TMSSchedulerService** stops.

Troubleshooting steps

The following steps must be performed to troubleshoot this issue:

1. Check in Event Viewer (**Startmenu >> Event Viewer >> Windows Logs >> Application)** and the following error messages are displayed.



2. These messages confirm that .Net framework 4.5 has crashed after Windows upgrade and hence **TMSSchedulerService** has stopped.

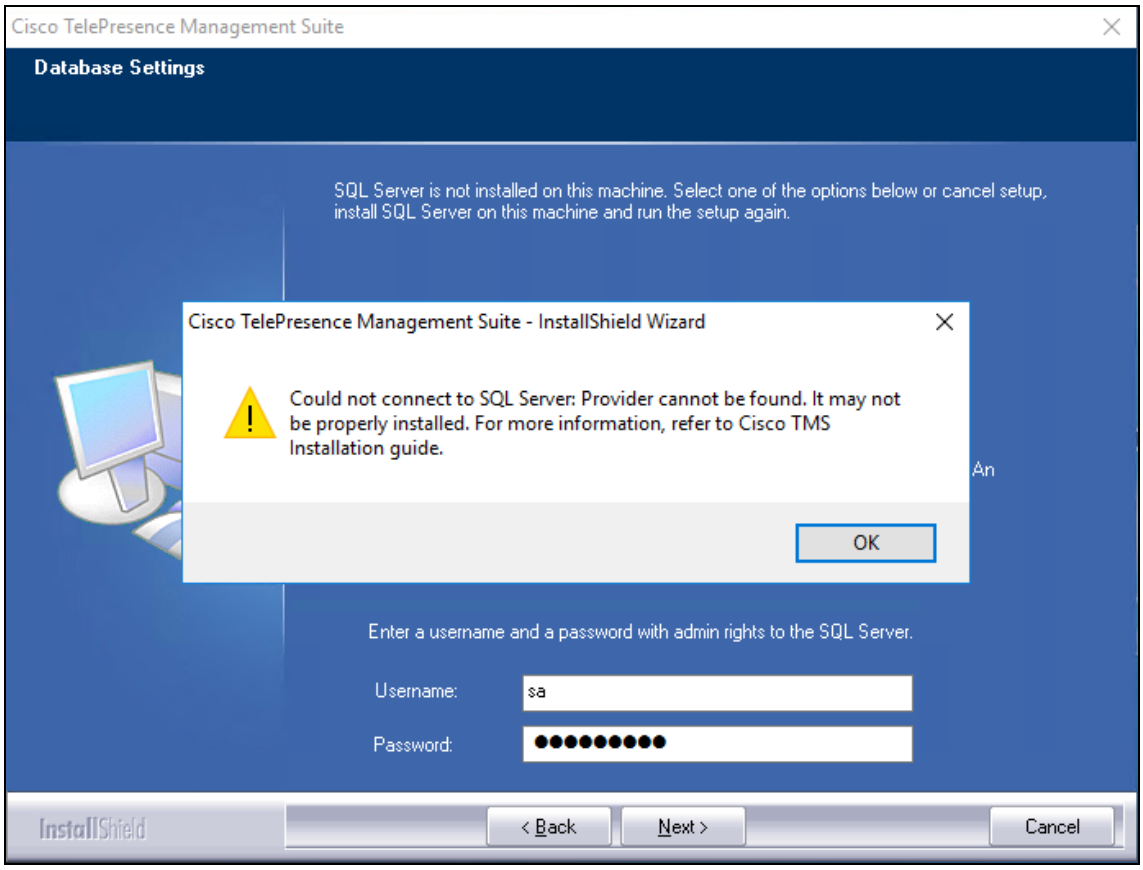
Solution

The following steps must be performed to resolve the issue:

1. Download and install **KB3186539** windows update patch from the following Microsoft link and reboot the server:
   https://www.catalog.update.microsoft.com/Search.aspx?q=KB3186539
2. After successful update, note that .Net Framework 4.7 is active and **TMSSchedulerService** is fully functional.

Cisco TMS Installation or Upgrade terminated due to SQL Server connection issue

Cisco TMS installation or upgradation is aborted due to SQL server connection issue when SQL Server Provider cannot be found. The following error message is displayed:



Troubleshooting steps

The following steps must be performed to troubleshoot this issue:

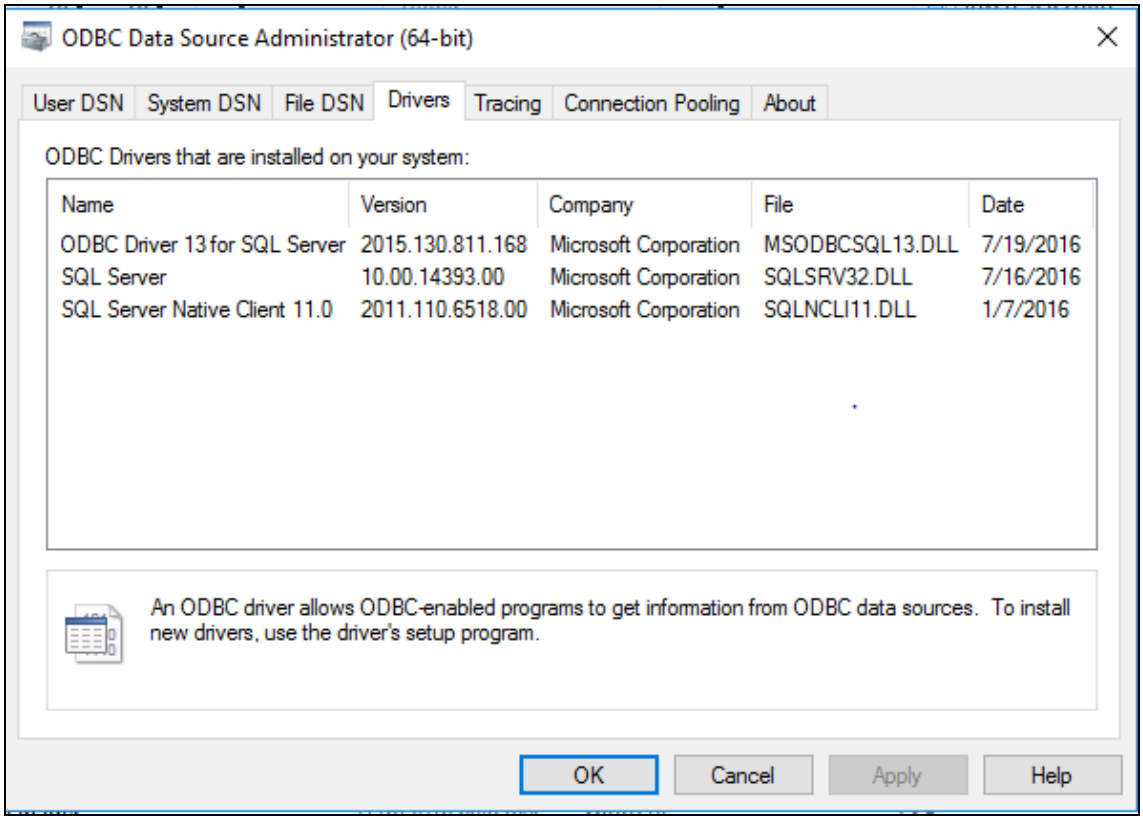
1. By default, Windows Server installation does not contain SQL Native Client.
2. In a deployment that has both SQL and Cisco TMS application on same Windows Server, Cisco TMS does not explicitly demand SQL Native Client installation, since SQL Server installation covers it.

Solution

The following steps must be performed to resolve the issue:

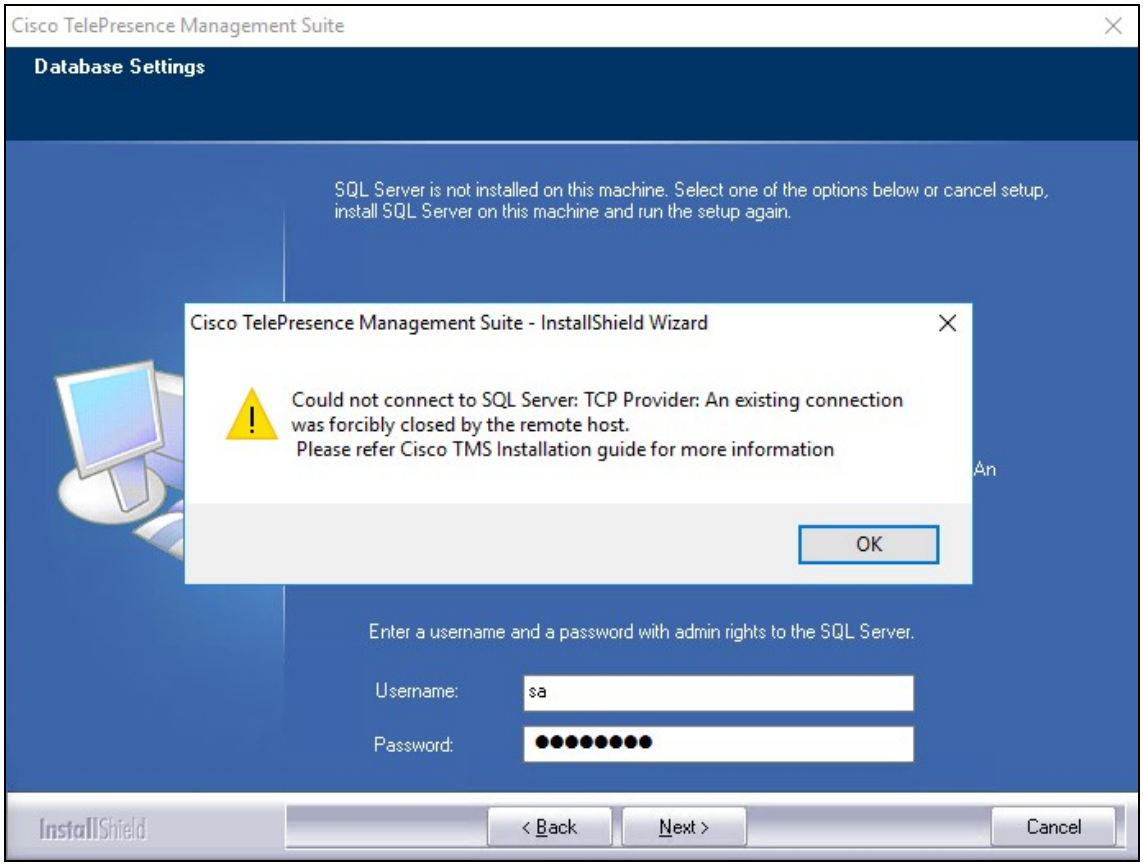
1. In a deployment where SQL and TMS application are on different Windows Server, administrator must install SQL Native Client 11 before installing TMS application.

- SQL Native client can be downloaded from the following link:
  - SQL Server 2016 (13.0.1601.5 and above) – https://www.microsoft.com/en-us/download/details.aspx?id=52676
    Note that Microsoft link feature pack version is **13.0.1601.5** and when SQL Server Native Client is installed on Windows Server, the installed version is **2011.110.6518.00**.



Cisco TMS Installation or Upgrade on Windows Server 2016/2012R2 terminates, if TLSv1.0 is disabled

When TLS version 1.0 is disabled, Cisco TMS installation or upgradation on Windows Server 2016/2012R2 is aborted. The following error message is displayed:



Troubleshooting steps

The following steps must be performed to troubleshoot this issue:

1. Check in Windows registry, if (HKey_Local_Machine\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols) TLSv1.0 is disabled.

Solution

The following step must be performed to resolve the issue:

1. Download and install the following SQL Server Native Client:

- SQL Server 2016 (13.0.1601.5 and above) – https://www.microsoft.com/en-us/download/details.aspx?id=52676

Appendixes

Appendix 1: Restricting IIS Modules to Minimal Required 72
Appendix 2: Configuring IIS Request Flood Protection 73
Cisco TMS Bundle 77

Appendix 1: Restricting IIS Modules to Minimal Required

IIS offers a modular system that allows an administrator to fine tune what components are installed and enabled on their server for the greatest security. To assist administrators who wish to further restrict their servers, the following list documents which modules are required for Cisco TMS. Modules may be controlled at either the site or server level (some are server level only) . The steps below assume that you are making changes at the server level.

Before removing modules, we recommend backing up your IIS configuration by using the command `%windir%\system32\inetsrv\appcmd.exe add backup "TMS"`.

To restore the backup later if needed, use the command `%windir%\system32\inetsrv\appcmd.exe restore backup "TMS"`

To modify which modules are enabled in IIS:

1. Open the **Internet Information Services (IIS) Manager**.
2. From the tree in the left section, click on your server's name.
3. In the center section, under **IIS**, double-click **Modules**.
   The list of installed Managed and Native Modules is displayed.
4. To remove a module, right-click the entry, or select the entry and go to the **Actions** panel, then select **Remove**.

The following modules are required for Cisco TMS and must *not* be removed:

- **AnonymousAuthenticationModule**
- **BasicAuthenticationModule**
- **DefaultDocumentModule**
- **DefaultAuthentication**
- **DigestAuthenticationModule**
- **HttpCacheModule**
- **HttpLoggingModule (recommended)**
- **HttprRedirectionModule**
- **IsapiFilterModule**
- **ProtocolSupportModule**
- **RequestFilteringModule**
- **Session**
- **StaticCompressionModule**
- **StaticFileModule**

- **WindowsAuthentication**
- **WindowsAuthenticationModule**

Appendix 2: Configuring IIS Request Flood Protection

To ensure Cisco TMS stability and protect against flooding in the event of very high numbers of concurrent incoming requests from systems, we recommend configuring IIS flood protection on your server.

A configuration procedure with recommended values is described below.

IIS 8 and 8.5

Follow the instructions below if your server is running IIS 8 and 8.5

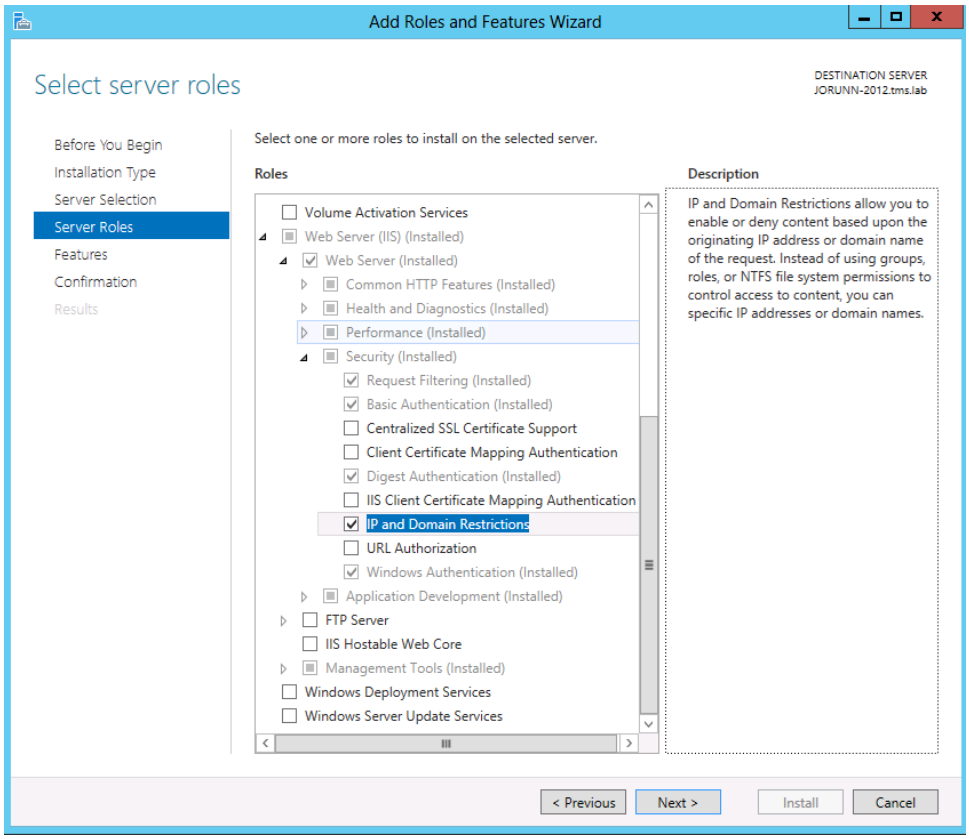
Enabling the IP and Domain Restrictions Role

1. Open the **Server Manager**.
2. In the start page, click **Add Roles and Features**. The **Add Roles and Features Wizard** is displayed with the **Before you begin** screen.
3. Verify that the server and password prerequisites mentioned are met, then click **Next**.
   The **Installation type** screen is displayed.
4. Select *Role-based or feature-based installation* and click **Next**.

   The **Server selection** screen is displayed.

5. Select the *Select a server from the server pool* option and ensure that the correct server is selected, then click **Next**.

   The **Select server roles** screen is displayed.



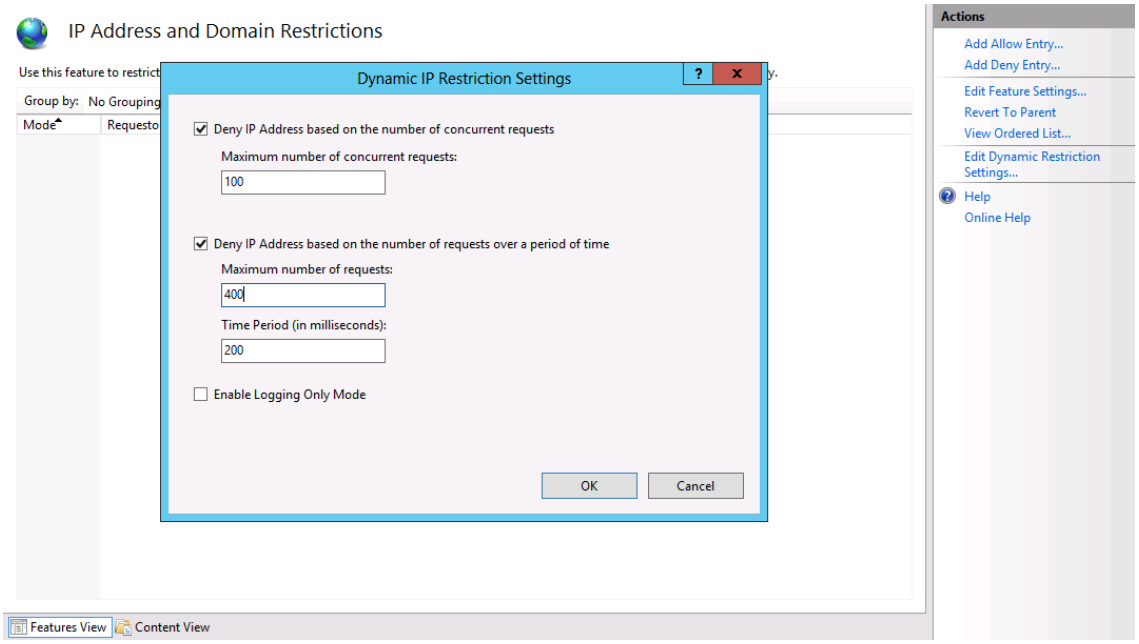
6. In the **Roles** pane, expand **Web Server (IIS) > Web Server > Security** and check **IP and Domain Restrictions**, then click **Next**.
   The **Features** screen is displayed.
7. Click **Next**.
   The **Confirmation** screen is displayed.
8. Click **Install**.
   Close the wizard when the installation is complete.

Configuring Dynamic IP Restrictions for the Default Site

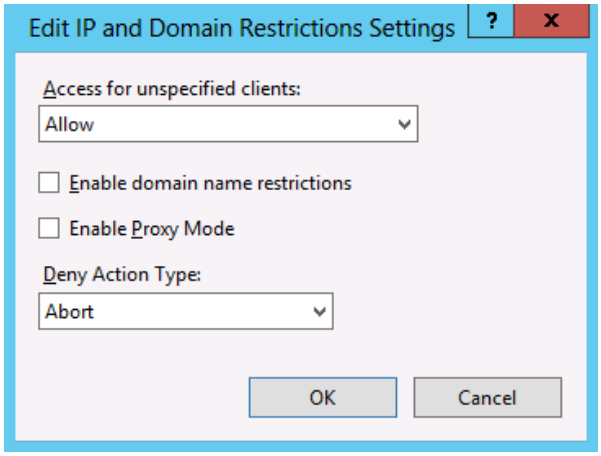
In IIS Manager:

1. Navigate to **Default Website** in the left-side panel, and click on the entry to display **Default Web Site Home**.
2. In the **IIS** section, double-click **IP Address and Domain Restrictions**.

3. In the **Actions** panel on the right, click **Edit Dynamic Restriction Settings**.
   The **Dynamic IP Restrictions** dialog opens.



4. In the dialog:
   a. Check **Deny IP Address based on the number of concurrent requests** and set the maximum number to `100`.
   b. Check **Deny IP Address based on the number of requests over a period of time**.
      Set the maximum number of requests to `400` and the time period in milliseconds to `200`, then click **OK**.
5. In the **Actions** panel on the right, click **Edit Feature Settings**.
   The **Edit IP and Domain Restriction Settings** dialog is displayed.



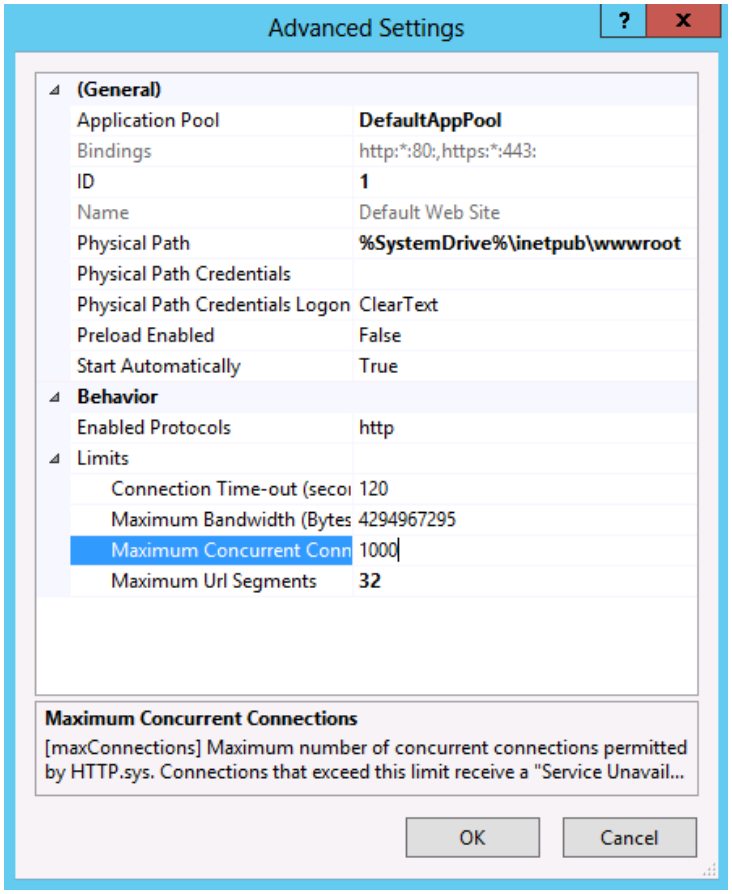
6. Set **Deny Action Type** to *Abort*.
7. Click **OK**.

Limiting the Total Number of Connections

In IIS Manager:

1. Navigate to **Default Website** in the left-side panel, and click on the entry to display **Default Web Site Home**.
2. Click on **Advanced Settings** in the right-side panel.

   The **Advanced Settings** dialog is displayed.



3. Under **Behavior > Limits**, set **Maximum Concurrent Connections** to `1000`.
4. Click **OK** to save.
5. Close IIS Manager.

IIS 7

Follow the instructions below if your server is running IIS version 7.

Installing the IIS Extension

Before you can configure flood protection, you must download and install the Dynamic IP Restrictions extension from IIS.NET on your server: http://www.iis.net/downloads/microsoft/dynamic-ip-restrictions

The download uses the Microsoft Web Platform Installer.

Configuring Dynamic IP Restrictions for the Default Site

In IIS Manager:

1. Navigate to **Default Website** in the left-side panel, and click on the entry to display **Default Web Site Home**.
2. Double-click **Dynamic IP Restrictions**.

3. Check **Deny IP addresses based on the number of concurrent requests** and set the maximum number to `100`.
4. Check **Deny IP addresses based on the number of requests over a period of time**.

   Set the maximum number of requests to `400` and the time period in milliseconds to `200`.
5. From the **Deny Action Type** dropdown, select *Abort Request (Close Connection)*.
6. Click **Apply** to save the changes.

Keeping IIS Manager open, you can now move on to limiting the total number of concurrent connections.

Limiting the Total Number of Connections

In IIS Manager:

1. Navigate to **Default Website** in the left-side panel, and click on the entry to display **Default Web Site Home**.
2. Click on **Advanced Settings...** in the right-side panel.
3. Under **Behavior > Connection Limits**, set **Maximum Concurrent Connections** to `1000`.
4. Click **OK** to save.
5. Close IIS Manager.

For further information, see the IIS.NET article *Using Dynamic IP Restrictions*.

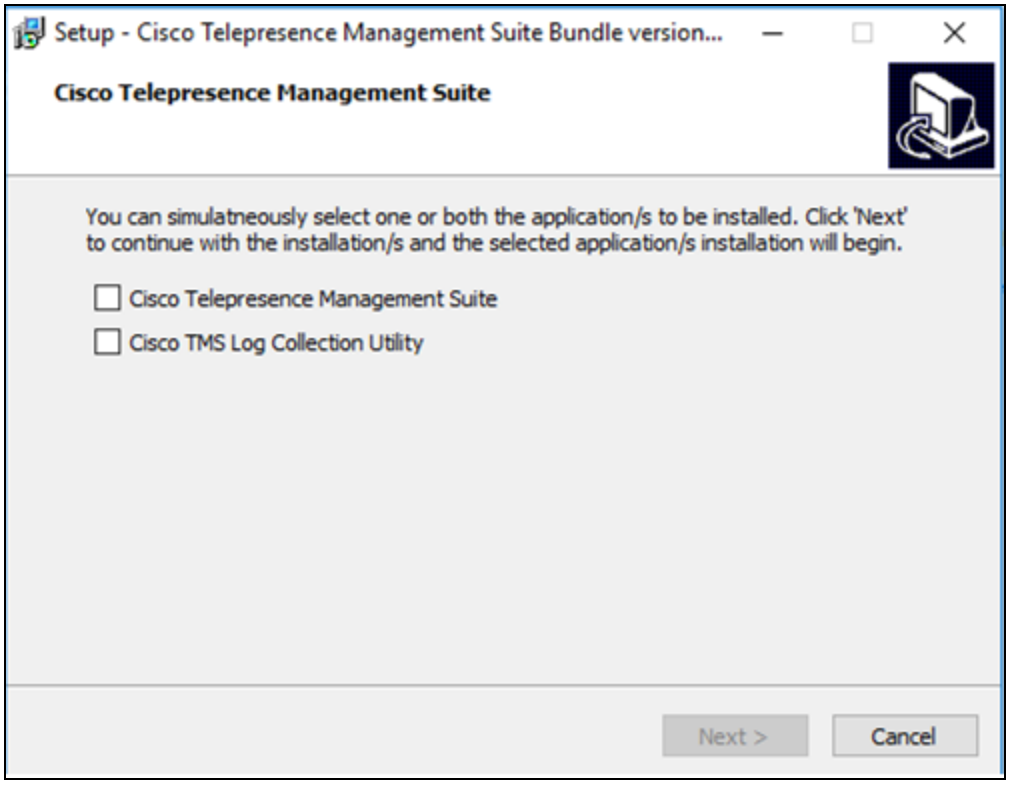
Cisco TMS Bundle

Cisco TMS provides a bundled installer with Cisco TMS Log Collection Utility Tool.

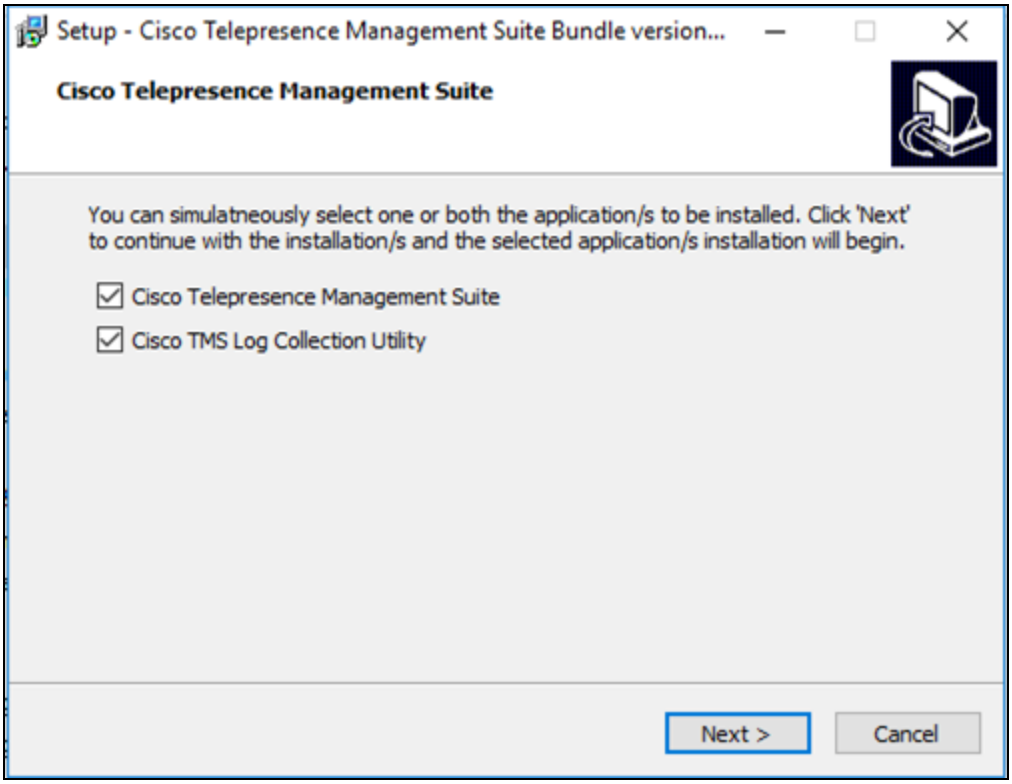
Running the installer

1. Close all the applications, disable virus-scanning software and other software that may prevent a complete installation.
2. Extract**Cisco TMS.zip** archive to a folder.
3. Run the **Cisco TMS** executable as administrator.
4. The installer will check hardware and software configuration of the server. A warning or error message may be displayed depending on your server's configuration. Follow the instructions given in the prompts and install any missing components.
5. When the installer package is executed, a dialog box will appear with the following two options:
   a. Cisco Telepresence Management Suite.
   b. Cisco TMS Collection Utility.

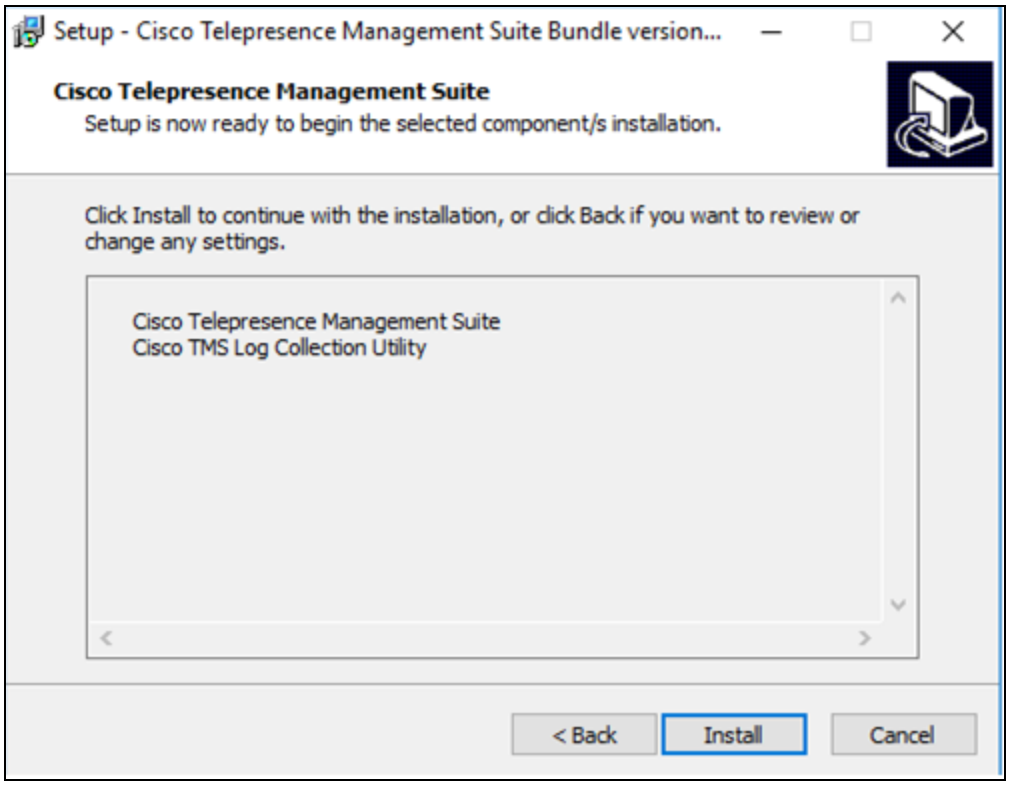
   Note: In case of selection of any one application, only that particular application will be installed.



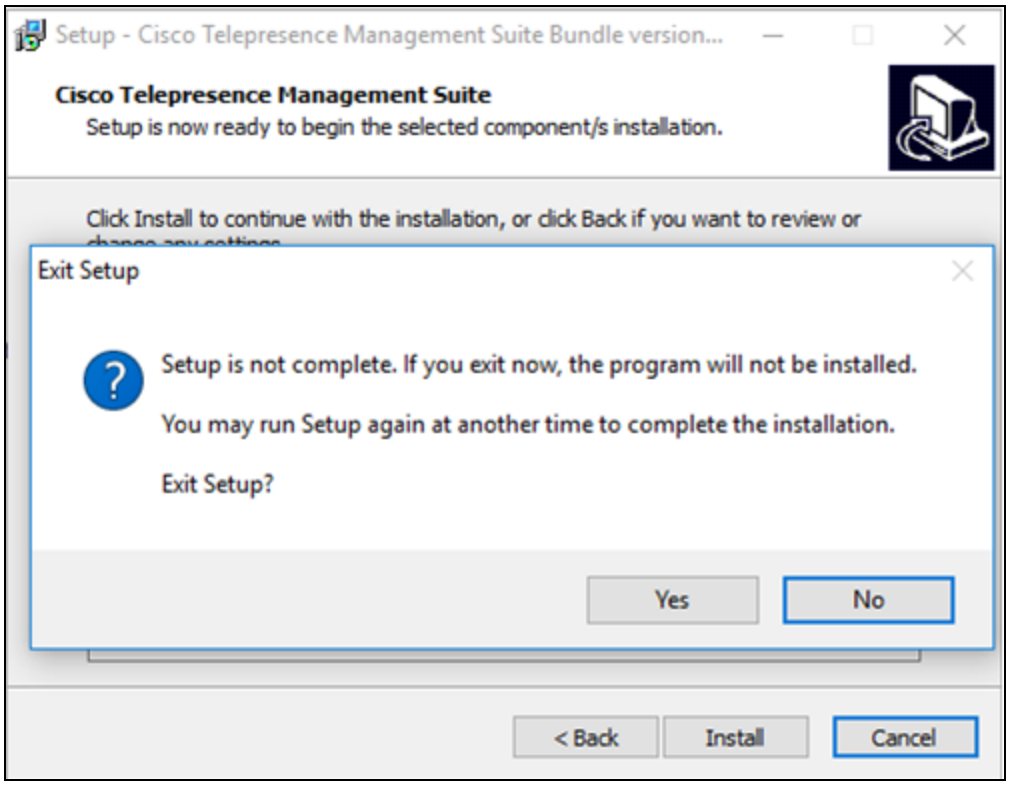
6. Based upon your choice, you can choose either both or any one of the application.



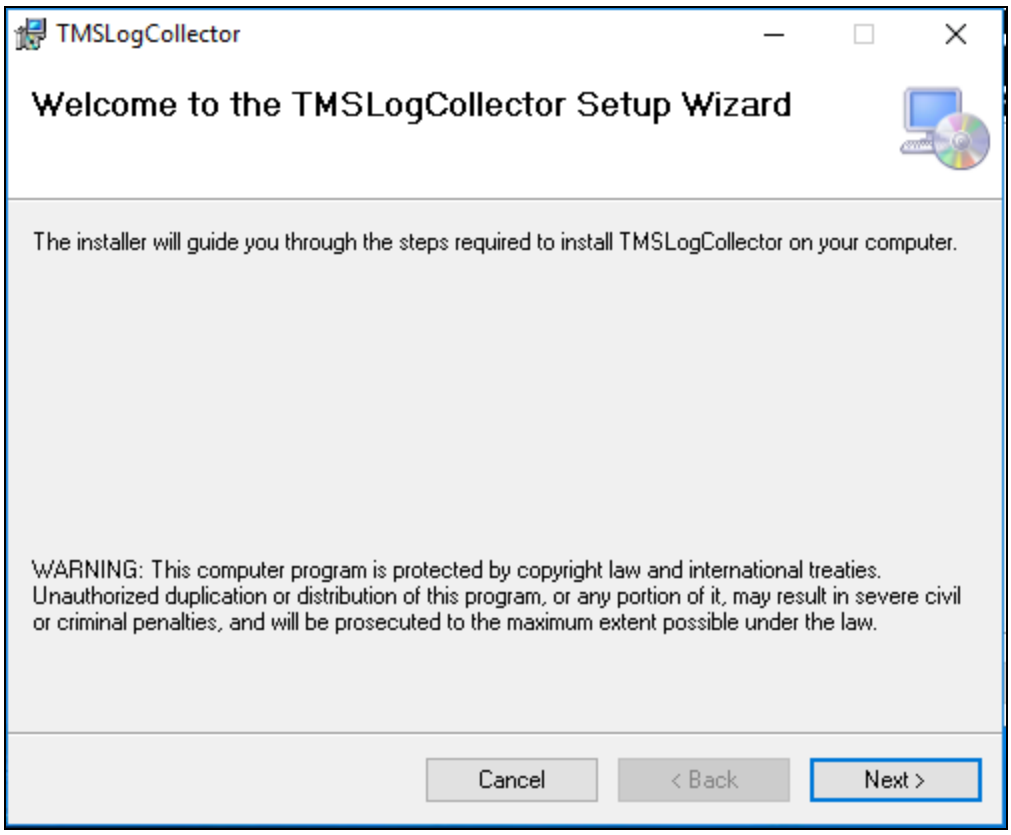
7. Click **'Next'** to continue the installation.
8. Click **'Install'** to install the selected applications.



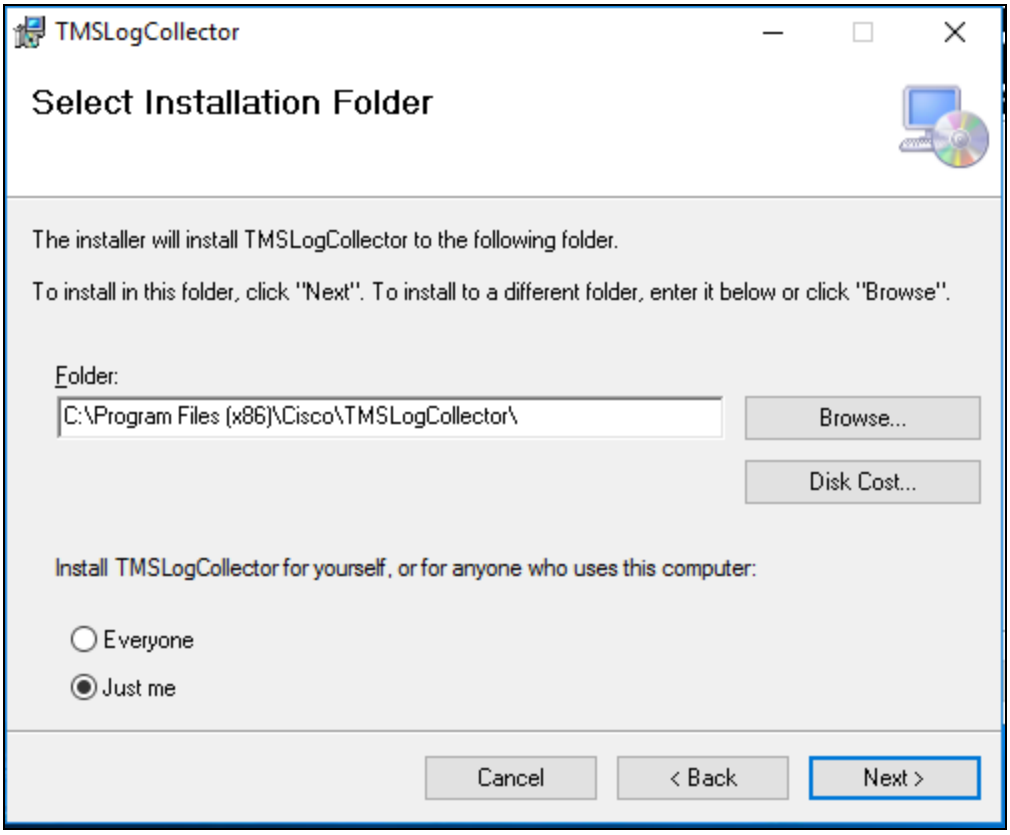
Note: When you click **'Cancel'**, in order to abort the installation process, a dialog box will prompt you to confirm to exit from installation.



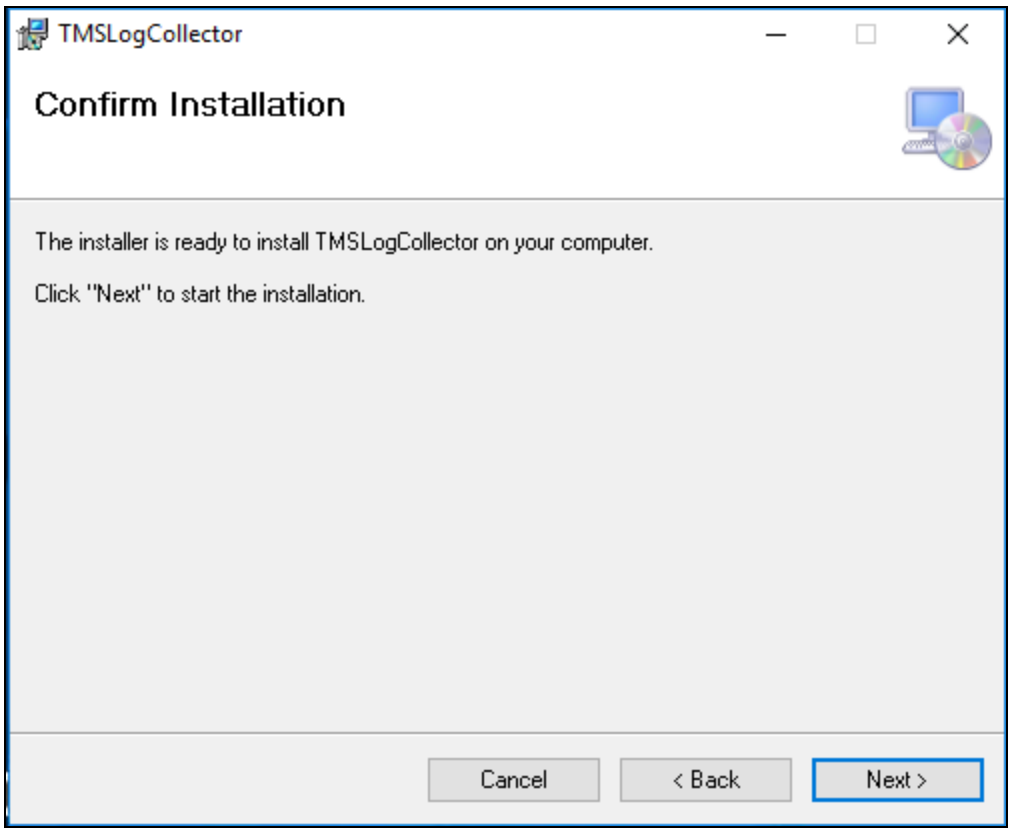
9. Follow the steps given in Step 5 of **Running the Installer** section of Cisco TMS Installation guide for installation of Cisco TMS.
10. Once the Cisco TMS installation is completed, then TLCU installation will continue to proceed. Click **'Next'** to continue.



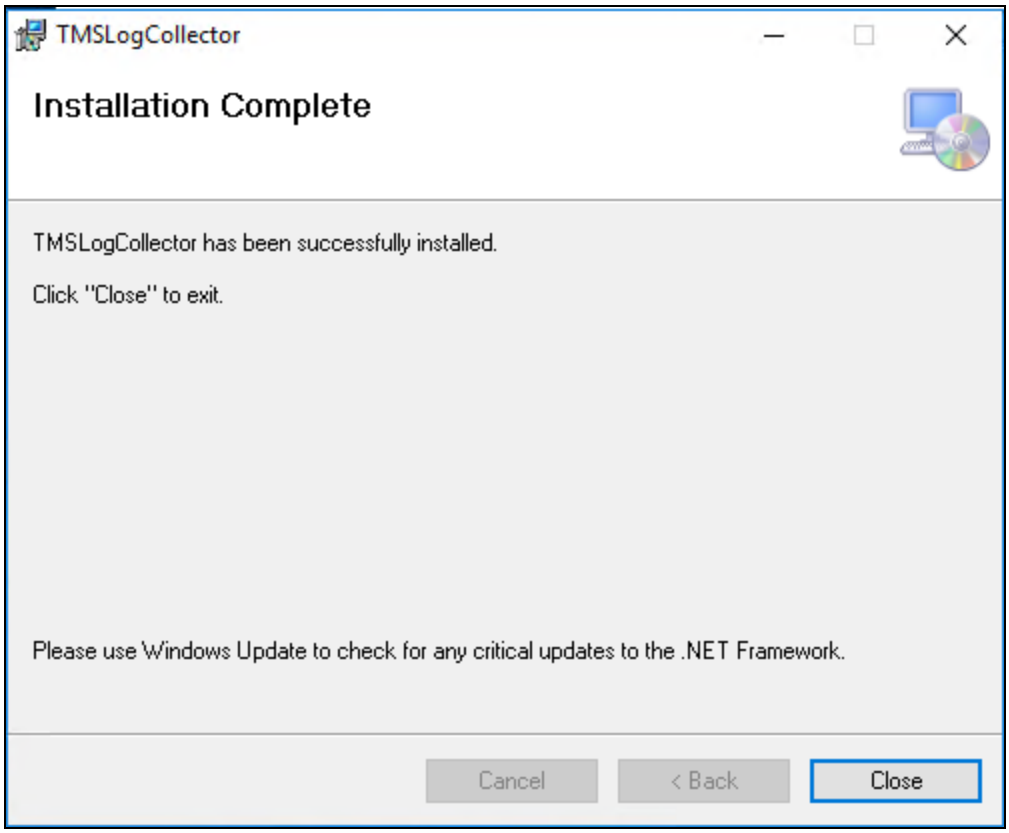
11. Select the option if you want to install TLCU for self or for everyone. Click **'Next'** to continue.



12. Click **'Next'** to start installation.



13. Once the installation is successfully completed, click **'Close'** to exit.



14. When both the applications are already installed and user tries to run the installer package again, then TMS will work as per its original behavior i.e. it will uninstall first then you have to again install the package. And, for TLCU a dialog box will appear to Repair or to Remove TLCU.

Notices

Accessibility notice

Cisco is committed to designing and delivering accessible products and technologies.

The Voluntary Product Accessibility Template (VPAT) for Cisco TelePresence Management Suite is available here:

http://www.cisco.com/web/about/responsibility/accessibility/legal_regulatory/vpats.html#telepresence

You can find more information about accessibility here:

www.cisco.com/web/about/responsibility/accessibility/index.html

Obtaining Documentation and Submitting a Service Request

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

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

Cisco Legal Information

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

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

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

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

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

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

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

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

© 2018 Cisco Systems, Inc. All rights reserved.

Cisco Trademark

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