



TelePresence

Troubleshooting Guide for TelePresence Management Suite (TMS) for Video Conferencing

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

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

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

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

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

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

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

Troubleshooting Guide for TelePresence Management Suite (TMS) for Video Conferencing
August 2012 Edition
© 2012 Cisco Systems, Inc. All rights reserved.

Table of Contents

1	INTRODUCTION	5
1.1	Release Notes	5
2	TMS SCHEDULING	5
2.1	Scheduled meeting not launching as planned	5
2.2	User can't find scheduled meeting	5
3	TMS WEBHELP	6
4	THE SQL DATABASE	6
4.1	SQL error	6
4.2	How to fix	7
5	JAVA APPLET	7
5.1	What it does	7
5.2	Java error	7
5.2.1	How to fix	7
	Authentication	7
	Java installation	7
	Proxy issues	8
	Slow or incomplete loading	8
6	PHONE BOOK	9
6.1	Global Directory	9
6.2	Corporate Directory	9
6.2.1	Phone book errors	9
7	TMS LOGS	10
7.1	When to get logs	10
8	TMS SERVICES	10
8.1	TMSAgentService	10
8.2	TMSDatabaseScannerService	11
8.3	TMSLiveService	12
8.4	TMSSchedulerService	12
8.5	TMSServerDiagnosticsService	12
8.5.2	How to fix	13
8.6	TMSSnmpService	13
8.6.2	How to fix	13
9	THE WEB SERVER (IIS)	14
9.1	IIS errors	14
9.2	How to fix	15
10	TMS PORTS	15
11	COMMON ISSUES	15
11.1	CDR's not reporting back to TMS	15
11.2	Cannot access the TMS webpage	15
11.3	Control Conference Center (CCC) Java Error	16
11.4	TMS is slow	16
11.5	No HTTP response	16
	Related documents	16

List of Tables

Table 1 - Release Notes	5
--------------------------------------	----------

List of Figures

Figure 1 List Conferences in TMS	5
Figure 1 Accessing TMS WebHelp	6

1 Introduction

The Cisco TelePresence Management Suite (Cisco TMS) is a portal for managing and monitoring your video conferencing systems from a single structured overview. Cisco TMS provides centralized control for on-site and remote video systems, and a deployment and scheduling system for your entire video network. This document provides a troubleshooting guide on Cisco TMS components.

1.1 Release Notes

Table 1 - Release Notes

Technical Change	Title(s) of Affected Section(s)	Changes Made By	Date
Initial release		Senait Mebrahtu	7/11/2012
2nd release		Senait Mebrahtu	7/30/2012

2 TMS Scheduling

2.1 Scheduled meeting not launching as planned

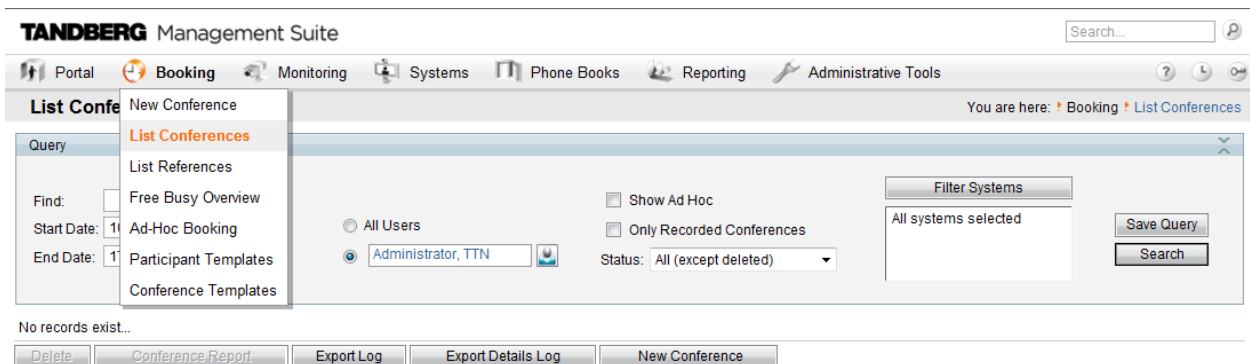
First check the status of the endpoints booked in the conference. It could be that the endpoint is off-line or an end-user is not answering the call.

2.2 User can't find scheduled meeting

To search for the specific **Conference** affected, use one or multiple search possibilities in **List Conferences** as specified in figure 1.

- Find by conference name
- By **Start Date** and **End Date**
- **All Users** or specify a user
- **Show Ad Hoc Conferences**
- **Only Recorded Conferences** (No recording possibilities yet so no Conferences show)
- **Status of the conference**
- Filter on specific systems

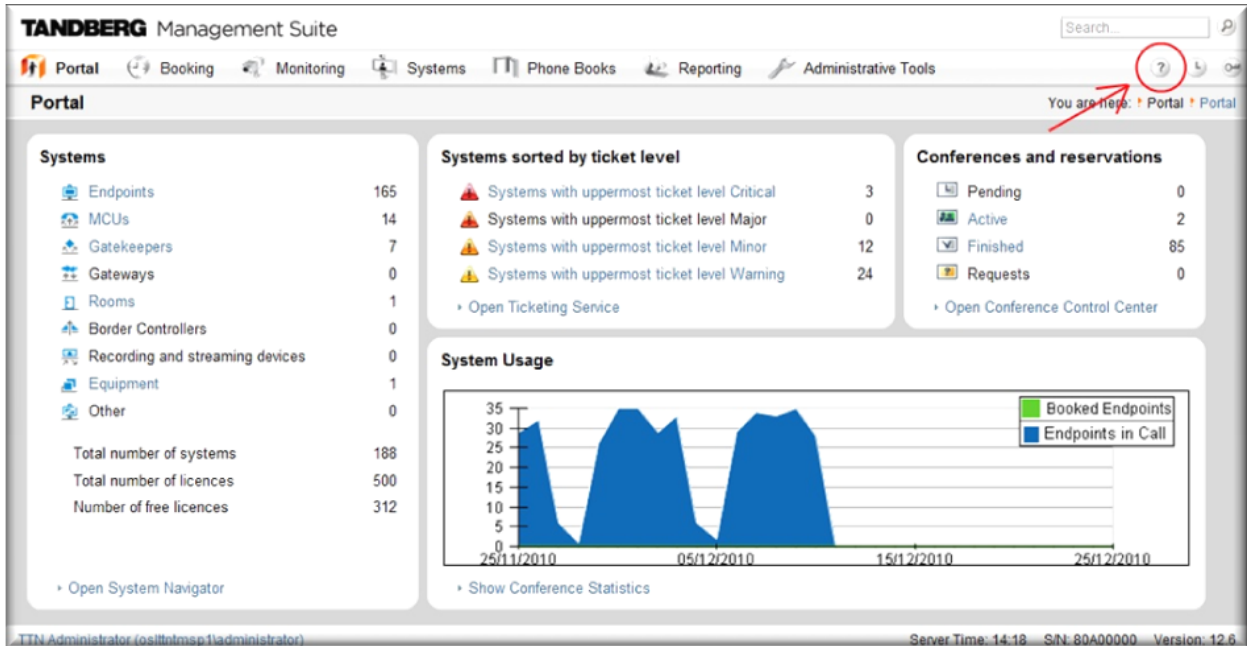
Figure 1 List Conferences in TMS



3 TMS WebHelp

TMS WebHelp is a reference guide that helps you to understand the usage of each tab in the TMS web interface.

Figure 1 Accessing TMS WebHelp



4 The SQL database

The SQL database is where all information in use by TMS is stored except software files for system upgrade and the services' log files.

The database is called **TMSNG** and can run on SQL 2005 or 2008 server. During the installation of TMS the **sa** account on the SQL server is automatically chosen to create and access the database.

To choose a different account you can select **Custom installation**.

The account used to run and upgrade TMS must have **dbowner** permissions to the **tmsng** database, while a user that also has access to master.mdf is required for creating the **tmsng** database the first time.

4.1 SQL error

TMS does not load or you get a stack trace declaring that the SQL server is unavailable: SQL Server does not exist or access denied is displayed.

4.2 How to fix

Make sure that the SQL server is running by checking the SQL agent of the server or by going into services and making sure that the MSSQLSERVER service is running.

- Check if you can access the database using MS SQL studio express.
- Run an **osql** script towards the database and see if it returns any data. This script returns the number of systems in the TMS database. Depending on the SQL configuration, run one of the following commands from the TMS server itself:

```
osql -E -d tmsng -Q "select count(*) from objsystem"
```

```
osql -E -S .\SQLTMS -d tmsng -Q "select count(*) from objsystem"
```

- Make sure that the information TMS uses to connect to the database is correct. This information was historically only stored in the registry, but is now also encrypted and stored in the web.config file. Therefore using the TMS Tools application, found under **Cisco TMS** in the **Start** menu of the TMS server, is recommended to change and make sure this information is correct.

5 Java Applet

5.1 What it does

The Sun Java applet version is used for displaying dynamic information in the Conference Control Center, Graphical Monitor, and Map Monitor. The Java applet adds functionality related to graphics, clicking, right-clicking, and drag-and-drop actions.

5.2 Java error

- When entering the Conference Control Center, Graphical Monitor, or Map Monitor, you are prompted for a username and password.
- The applet does not load, and there is no Java (coffee cup) icon in the notification area.
- The applet does not load, but Java is installed.
- The applet loads very slowly.
- Conference snapshots are not displayed on some clients.

5.2.1 How to fix

A proxy server might be preventing the Java applet from retrieving the necessary data from the TMS server. To open the Java console, right-click the Java icon in the notification area and select Open Console. Error messages stating *Unknown source* are displayed. To solve this problem, try one or more of the following methods:

Authentication

The Java Applet requires the users to authenticate themselves if the TMS server is not part of the domain (or a trusted domain) the user is logged into. The solution is to make the TMS server part of the domain, or insert the username and password when prompted for each session.

Java installation

The Java virtual machine is not installed on the machine, and the client PC does not have direct access to the Internet to download it automatically. To retrieve go to <http://www.java.com/> to download and install Java.

Proxy issues

- If using the TMS server's IP address when accessing TMS, try with the TMS server's host name.
- Configure the Java client through the Java Control Panel to use Direct Connection rather than using the browser's proxy settings.
- The proxy server may have to be configured to allow this kind of traffic from the TMS server to the clients.

Slow or incomplete loading

The applet normally finishes loading within five (5) seconds after the **Monitoring** link is pressed. If you experience a significantly higher loading time, complete the following steps:

- Turn off caching in Java and delete the existing temporary files:
 1. Open the **Java Control Panel**.
 2. Click the **General** tab.
 3. Click **Settings**, click **View Applets**.
 4. De-select **Enable Caching** in the lower left corner.
 5. Click **OK**.
 6. Click **Delete Files**.
 7. **Select all** check boxes.
 8. Click **OK**.
 9. Click **OK**.
 10. Click **OK**.
- Remove old or duplicate Java clients from Internet Explorer:
 1. In the Internet Explorer menu, click **Tools**.
 2. Click the **Programs** tab.
 3. Click **Manage Add-ons**.
 4. Disable all old or duplicate Java plug-ins.
- Remove **Google Desktop**. We have seen issues where Google Desktop is conflicting with the Java plug-in and significantly increasing the loading time of Java applets. Other desktop search engines **like MSN Search** does not show the same symptoms.
- If using Java build 1.6.0_31, you need to de-select **Enable** the next generation Java plug-in under **Advanced** on the Java Control Panel to make the **Graphic and Map Monitor** work as expected.

6 Phone book

6.1 Global Directory

The **Global Directory** is a file stored on the codec where the entries cannot be changed via the remote control. The file is transmitted by HTTP to all endpoints that are subscribing to one or more phone books in Cisco TMS. Multiple phone books are merged into one phone book. If containing more than 400 entries, only the first 400 are shown on the endpoint. The file is transmitted to the endpoint on the intervals set in the **Administrative Tools > Configuration > General Settings > Phone Books Update Frequency** field.

NOTE: This only works on endpoints (Tandberg MXP and Classic) that support the globdir.prm file.

6.2 Corporate Directory

The **Corporate Directory** is an XML service on the Cisco TMS server that allows the endpoint to retrieve the phone books directly from the server every time the phone book button on the endpoint is pressed. It allows for a hierarchy of phonebooks and multiple phone numbers on every entry. The **Corporate Directory** is also searchable.

6.2.1 Phone book errors

The following errors will be displayed on the endpoint if the corporate directory is not working properly:

Message	Explanation or suggested solution
Request timed out, no response	The TMS server is busy, try again.
Warning: directory data not retrieved: 404	The endpoint is configured with the IP address of a different web server than the TMS server. The corporate directory path on the endpoint is wrong.
Warning: directory data not retrieved: 401	The "Public" virtual directory on the TMS server is not configured to allow Anonymous Access. The most common problem here is that anonymous access is set, but the account used has been overwritten by a group policy. The default IUSR user is a part of the guest account, and typically group policies disable this account.
TMS: No phonebook(s) set on this system	No phonebook(s) set on this system in TMS. Configure the endpoint to subscribe to phonebooks in TMS. Using NAT on the endpoint can lead to TMS not recognizing the system and not allowing it to retrieve any phone books.
Request timed out, no response	The endpoint is configured with the IP address of a non existing web server.
No contact with server	The IIS is restarting or in a state where corrupted messages are received.

Note: The corporate directory path can be checked on the endpoints through web or command line interface.

For MXP under endpoints **configuration > general configuration > external phone book settings**
For C-series and EX under **configuration > advance configuration > phonebook**

7 TMS logs

The log is in **C:\Program Files\TANDBERG\TMS\wwwTMS\Data\Logs\tmsdebug**

7.1 When to get logs

- In CCC the call status shows still InCall, Idle or Disconnected
 - **TMSDatabaseScannerService**
- The call doesn't launch and CCC event log is pretty much empty.
 - **TMSLiveService.**
- When pressing the phonebook button the Polycom remote nothing shows up.
 - **TMSPLCMDirectoryService.**
- Meeting booked in TMS but it didn't launch.
 - **TMSSchedulerService.**
- No CDRs, and TMS is not adding new systems automatically.
 - **TMSSnmpService.**
- When logging into TMS and CCC, I'm receiving SQL errors.
 - **Log-Web and Log-WebPublic.**
 - This is responsible for access to the TMS web interface and communications to the database.
 - Symptoms include receiving SQL exception errors, TMS web application errors, and XML issues.

8 TMS services

The following are services TMS requires to run, symptoms when the services are not functioning properly, and how to fix problems.

8.1 TMSAgentService

This service starts the local **TMS Agent**. The TMS Agent is needed for provisioning **Cisco Video** jabber(Movi) clients and **E20** endpoint.

8.1.1 Symptoms

You are unable to create or edit groups or users within TMS on page **Systems > Provisioning > Directory**

8.1.2 How to fix

1. Check the logs for symptoms or error messages at **c:\Program Files\Tandberg\TMS\wwwTMS\Data\Logs\tmsdebug\log-provisioningservice.txt** on the server.
2. Restarting the service or the TMS server normally fixes any problem with this service.

8.2 TMSDatabaseScannerService

The TMSDatabaseScannerService checks the status and configuration of existing systems. The scanner checks:

- The connection status
- The call status
- The system configuration

If a system is unavailable, the service receives that status until the next scan, or until the endpoint sends a trap to TMS.

Note: The scanner pauses for 15 min after the scan has finished.

The scanner process is a moderately CPU-intensive process for the server and should be tuned according to the need for updated system information in TMS. To scan one system takes from two seconds up to approximately 20 seconds (worst case). Scanning 100 systems might take from three minutes up to 30 minutes.

The scanner reads the system connection status and call status on every scan, but only reads the full system configuration in intervals defined in the field System Force Refresh Interval (in hours). The scanner updates 20 connection statuses in parallel and reads five full system configurations in parallel.

To improve response time, Cisco TMS runs an extra connection status check every 30 seconds for systems in these categories:

- Cisco TelePresence MCU
- gateways
- gatekeepers
- border controllers
- recording devices
- supervisors
- Cisco TelePresence Server (TS 7010)
- Cisco TelePresence System (CTS)

8.2.1 Symptoms

The symptoms are that the system information and system status in TMS is outdated. Systems not responding still have the status InCall or Idle.

8.2.2 How to fix

1. Check the logs for symptoms or error messages at **c:\Program Files\Tandberg\TMS\wwwTMS\Data\Logs\tmsdebugVog-TMSDatabaseScanner.txt** on the server.
2. Restarting the service or the TMS server normally fixes any problem with this service.

8.3 TMSLiveService

This service allocates conferences on the MCUs, issues a dial commands to the endpoints and the MCUs and monitors the activity of the participants during a conference.

8.3.1 Symptoms

- The call does not start, and the log in the **Conference Control Center** is almost empty.
- You could have only one line that says "**Created**" in the log. You might have more lines there if the conference has been changed – but none of them is related to launching the conference.

8.3.2 How to fix

1. Check the logs for symptoms or error messages at **c:\Program Files\Tandberg\TMS\wwwTMS\Data\Logs\tmsdebug\log-liveservice.txt** on the server.
2. Restarting the service or the TMS server normally fixes any problem with this service.

8.4 TMSSchedulerService

This service is responsible for launching events at set times. Examples of events are:

- System Restore.
- System Upgrade.
- Update Phonebooks.

This service also reminds the TMSLiveService to start a conference if needed.

Note: TMSLiveService keeps track of all booked conferences, but loses this information if it is restarted.

8.4.1 Symptoms

Scheduled events do not start.

8.4.2 How to fix

1. Check the logs for symptoms or error messages at **c:\Program Files\Tandberg\TMS\wwwTMS\Data\Logs\tmsdebug\log-schedulerservice.txt** on the server.
2. Restarting the service or the TMS server normally fixes any problem with this service.

8.5 TMSServerDiagnosticsService

This service is responsible for checking the server disk space, the database size and that the other services are running

8.5.1 Symptoms

A TMS ticket is opened if:

- a service is not running.
- free disk space is less than 10%.
- the database is 90% of max size.

8.5.2 How to fix

1. Check the logs for symptoms or error messages at **c:\Program Files\Tandberg\TMS\wwwTMS\Data\Logs\tmsdebug\log-TMSServerDiagnosticsService.txt** on the server.
2. Restarting the service or the TMS server normally fixes any problem with this service.
3. Disk space can be cleared by deleting temp files and old log from the windows server, if that does not help then increase disk space.
4. Check the SQL database size; you may need to clean up old transaction logs.

8.6 TMSsnmpService

This service should be turned off if you have TMS set to HTTPS only. For more information, see [Cisco TMS Implementing Secure Management](#).

The snmp service collects traps from the endpoints and adds them directly to the database and it is responsible for broadcasting SNMP messages to discover newly added systems.

To specify the sub-ranges for where TMSsnmpService searches for new endpoints, go to TMS web *Administrative Tools > Network Settings > SNMP Broadcast/Multicast Address(es)*.

To specify the SNMP Broadcast Interval, go to *Administrative Tools > Network Settings* and modify the setting *SNMP Broadcast Interval* (in minutes). Cisco recommends setting *SNMP Broadcast Interval* to broadcast 2 times a day depending on video network size. Define multiple scan ranges by comma separating the ranges. By setting the *Broadcast/Multicast Address* value to 127.0.0.1, TMS does not scan for new systems via SNMP broadcast.

To quickly find which systems are online, you can use the *TMSsnmpService* and send *SNMP OID* queries to systems that are known to TMS, support SNMP and do not have status "No Response", "No SNMP Response" or similar.

To enable this feature:

- Go to **Administrative Tools > Network Settings**.
- Turn on the function **Scan SNMP** capable systems to allow quick discovery of inaccessibility.

Furthermore, you can specify the interval, and the maximum number of missed SNMP responses before the system gets the status **No SNMP Response**. If there is no response to SNMP queries, TMS uses an HTTP connection to check the status of the system.

8.6.1 Symptoms

- The statistics are empty.
- TMS does not receive system events.
- New systems are not automatically discovered.

8.6.2 How to fix

1. Make sure no other SNMP tool is running on the server, like **HP OpenView** or other server or network monitoring tools using Microsoft Windows' SNMP Component.
2. Check the logs for symptoms or error messages at **c:\Program Files\Tandberg\TMS\wwwTMS\Data\Logs\tmsdebug\log-TMSsnmpService.txt** on the server.
3. Restarting the service or the TMS server normally fixes any problem with this service.

9 The Web server (IIS)

TMS uses Microsoft Internet Information Services to make TMS available as a webpage. Since version 9.0, TMS has been developed with the Microsoft .NET platform and some extra components are therefore required on the IIS for TMS to work properly. ASP.NET version 4.0 is currently in use. These components are installed by Windows during the TMS installation as they are required by TMS, but not Cisco specific.

All web-related files are stored on the server in the location you specified during the installation. The default location is c:\Program Files\Tandberg\TMS\.

In the Internet Information, Server Manager shows that the installation has created five virtual directories.

1. TMS

- The Application that handles the TMS web interface.
- The virtual directory for this component on the IIS is: <http://serverIP/tms>.
- This component should have the **Directory Security (authentication settings on Windows 2008 server)** set to **Windows Integrated Authentication** (default), **Basic Authentication** or both.

2. TMS/public

- Handles **Corporate Directory for cisco** endpoints.
- Handles http traps from c-series,EX, MXP and MCU systems.
- The virtual directory for this component on the IIS is: **<http://serverIP/tms/public>**.
- This component should have the Directory Security set to Anonymous Access.

3. pwx

- Handles HTTP traps from Polycom systems.
- Handles phonebooks for Polycom systems.
- The virtual directory for this component on the IIS is: <http://serverIP/pwx>.
- This component should have the Directory Security set to Anonymous Access.
- This component can be removed if this TMS installation is not used with Polycom endpoints.

4. XAPSite

- Handles communication between TMS and pre version 7 MGCs.
- The virtual directory for this component on the IIS is: <http://serverIP/XAPSite>.
- This component should have the Directory Security set to Anonymous Access.
- This component can be removed if this TMS installation is not used with a Polycom MGC with version 6.x or older.

5. TMSConferenceAPI

- This component warns the old Exchange API (TMS 7 and 8) that it must be upgraded.
- The virtual directory for this component on the IIS is: <http://serverIP/TMSConferenceAPI>.
- This component should have the Directory Security set to Anonymous Access.
- This component can be removed if this TMS installation does not have an older Exchange integration (TMS 8 or older).

9.1 IIS errors

- You cannot access the TMS page.
- The corporate directory not pushed to endpoints and statistics on endpoints are empty.

9.2 How to fix

1. Check that IIS is running.
2. Check that you can access the default webpage `http://TMSServerName`.
3. Check that the virtual directories exist on the TMS server.
4. Check that they are pointing to valid directories on the TMS server.
5. Check that the permission settings.
6. Check that the IIS allows for running .net extensions.
7. Logs are found on the TMS server under: ***c:\Program Files\Tandberg\TMS\wwwTMS\Data\Logs\tmsdebug\log-web.txt***

10 TMS Ports

Ports that needs to be opened in order for TMS to communicate and manage Telperesnce systems VTC systems

- HTTP TCP Port 80 inbound or HTTPS TCP Port 443 inbound.
- SNMP UDP Port 161 both directions.
- SNMP Traps UDP Port 162 outbound.
- Telnet – TCP Port 23 inbound (optional).

NOTE: When using Remote System/SOHO Support functionality is limited compared to an endpoint in which TMS has full access to. The endpoint must have outgoing HTTP or HTTPS access to the TMS server. These are system on public Internet or behind a firewall.

11 Common issues

11.1 CDR's not reporting back to TMS

Complete the following checklist:

- IP address of TMS is in the SNMP trap host field.
- External management service is on and pointed back to TMS.
- IIS has the default settings(as it is referenced on section 8).
- MXP, C-series, and EX endpoints reports CDR's through HTTP on anonymous side of the website to TMS.
- Classic endpoints reports CDR's through SNMP.

If the above points are correct, then there is a proxy or firewall not allowing feedback from endpoints to TMS.

11.2 Cannot access the TMS webpage

In IIS Web Service Extensions:

- Make sure ASP.Net V2.0 and later version is set to ***Allowed***.
- TMS uses ASP.Net to communicate to the SQL server and allows you to view TMS website.

11.3 Control Conference Center (CCC) Java Error

When accessing **CCC**, you see a red **X** in the top right corner.

1. Make sure you can view CCC from the TMS server.
2. If so, then check on other computers and see if they can view the CCC.
3. If you cannot see it on any of the Computers, then most likely the computers have a corporate policy restricting Java being launched from a 3rd party program.

To check java functionality go to www.java.com and make sure you can view the animation and upgrade to the latest Java version.

11.4 TMS is slow

TMS is responding very slow. TMS is just a program, so check the following on the Windows server:

- Disk space
- Make sure there are no rogue cookies and temp files
- RAM (Minimum of 1 GB)
- Anti Virus software (can be disable to check if it is contributing to slowness)
- 3rd party software installed (check task Manger on Windows server)
- Make sure there are NO modifications made to IIS
- Check if remote desktop access is having same issue
- Network traffic(if there is any proxy or Firewall setting)

11.5 No HTTP response

If a system cannot communicate with TMS using the HTTP or HTTPS protocols, then it generates a NO HTTP response warning. Check the following status:

- If status can be cleared by clicking *Force> refresh>* then returns, check whether a web proxy that requires authentication is present on the network, because this blocks traffic from the TMS services.
- If such a proxy is present, set up your network so that traffic between TMS and the endpoint is not routed through it or is trusted without requiring authentication.
- If status cannot be cleared by clicking *Force> refresh*, then try connecting to the system by using the web browser on the TMS server itself. If you are unable to connect to it over HTTP or HTTPS, log in to the system over SSH or telnet and make sure that it accepts HTTPS or HTTP connections.
- TMS has the system's correct IP address or hostname under *Systems > Navigator >Connection tab*.

Running packet trace from the TMS server, while trying to duplicate most of the above issues, also helps to better identify the cause of the problem.

Related documents

[Further information on Cisco TMS functionality is available online](#)

[Implementing Secure Management](#)

End of document