



Cisco TelePresence Infrastructure Technical Handbook

Technical Support Guide

June 2012

Table of Contents

Document revision history	5
Introduction	6
Information on service request	7
Terminal software for TelePresence Infrastructure	8
There are multiple terminal emulation software available that may be used for retrieving logs from a system. They include the following:	8
Windows HyperTerminal (Serial, Telnet)	8
TeraTerm.....	8
Putty (Serial, Telnet, SSH)	8
How to use Windows Hyper Terminal	9
How to use TeraTerm.....	10
How to use Putty	11
File transfer software for TelePresence Infrastructure.....	12
There are multiple file transfer software applications available, that may be used for retrieving logs from Cisco Telepresence systems and/or uploading files to Cisco Telepresence system.	
Examples are:	12
Command Prompt	12
WinSCP	12
How to use Windows Command Prompt	13
How to use WinSCP	14
Packet Capture software for Cisco TelePresence Infrastructure and Systems	15
There are multiple packet capture software that may be used for analyzing communications traffic between Cisco Telepresence systems such as:	15
Wireshark (IP packet sniffer)	15
RS-232 Serial Connection	16
How to capture a log from TelePresence Video Communication Server (VCS).....	18
Logs – VCS	18
IP issues (H323/SIP)	19
Reboot Issue	19
Sniffer the packet on VCS	19
Default factory VCS	20
Reset Password on VCS.....	20
Revert back previous software version on VCS.....	20
How to upgrade TelePresence Video Communication Server software	21
How to capture a log from Gatekeeper (GK) and Border Controller (BC)	23
IP issues (H323)	23
Reboot Issue	23
Sniffer the packet on GK/BC	23
Default factory GK/BC	24
Reset Password on GK/BC	24

How to upgrade Gatekeeper (GK) and Border Controller (BC) software	25
How to capture a log from TelePresence MCU and IP/ISDN Gateway	26
Logs – MCU.....	26
Logs – IP Gateway	27
Logs – ISDN Gateway.....	28
IP issues (H323/SIP)	29
Event log and Event Capture Filter	29
Reboot Issue	29
Sniffer the packet on TelePresence MCU or IP/ISDN Gateway	30
Reset Password on TelePresence MCU or IP/ISDN Gateway	31
How to upgrade TelePresence MCU and IP/ISDN Gateway	32
Upgrade software by using FTP software	32
Upgrade software by using Compact Flash Card	33
How to capture a log from MPS series.....	34
IP issue (H323/SIP)	34
ISDN issue.....	34
Reboot Issue	34
Default factory MPS	35
How to upgrade MPS series	37
How to capture a log from Classic MCU/ISDN Gateway	38
IP issue (H323).....	38
ISDN issue.....	38
Reboot Issue	39
Default factory Classic MCU/ISDN Gateway	39
How to upgrade Classic MCU/ISDN Gateway	40
How to capture a log from Telepresence Server	41
Logging H.323 or SIP messages	41
Working with Call Detail Records.....	42
Call Detail Record log controls	42
Call Detail Record log.....	42
Logs – Telepresence Server	43
How to capture a log from MSE8000.....	44
Event log.....	44
Logs – MSE8000	45
How to capture a log from TelePresence Management Suite	46
This chapter explains how to capture the complete log files available for TelePresence Management Suite, Provisioning Directory, and Windows server. Also provide additional faultfinding information.	46
All retrieved logs should be attached to the service request including a description. When possible compress multiple attachments into one file.	46

Log from TelePresence Management Suite.....	46
Log from Windows server.....	46
Log from TelePresence Management Suite components and faultfinding	47
Phonebook (Corporate Directory) Common Errors.....	49
Upgrading from a previous TelePresence Management Suite version	49
Security patch for TelePresence Management Suite Server Appliance	49
Compatibility with existing Integration Portfolios	49
Uninstall TelePresence Management Suite	50
Useful TelePresence Management Suite Related Document References	50
Logs – Telepresence Management Suite	51
How to capture logs from Conductor	52
Logs – Conductor	54
How to capture logs from Advanced Media Gateway	55
Logs – Advanced Media Gateway	56

Document revision history

Date	Description
February 2011	- Migrated TANDBERG Management Suite Handbook Rev 1.2 version into TelePresence Infrastructure Handbook.
March 2011	- Corrected Baud Rate for TelePresence Server/TelePresence MCU/TelePresence ISDN Gateway/TelePresence IP Gateway/IPVCR
March 2012	- Updated how to extract logs from following systems: Conductor
May 2012	- Added Log framework diagrams - Added Advanced Media Gateway, Telepresence Server, MSE8000

Introduction

Each system will be provided with its own User Guide, Quick Reference Guide and if needed, an installation manual. This document is a quick reference handbook for basic troubleshooting to assist with providing an understanding of basic troubleshooting method on Cisco TelePresence Infrastructure Products.

Logs framework diagram symbols

Capture the following log files for the different scenarios:



= Standard (*always attach these logs to the service request*)

= If interworked call (*attach only if the call is interworked*)

= Advanced (*TAC normally request these log*)

Log = Logs from Admin (SSH/Telnet) or the Web Interface

Log = Logs from Root Shell (*these logs can only be captured from root (SSH)*)

Information on service request

To assist the Cisco TelePresence TAC with providing quick resolution, the Cisco TelePresence TAC requires a minimum amount of information for each service request.

When creating a technical service request, please include the following information:

- Describe in detail the problem/issue
- Describe how often the problem occurs
- Describe the latest operation before problem occurs, if any
- Describe in detail, the procedure to recreate the problem, if any
- Describe in detail, which steps have already been taken in investigating the problem
- Describe the equipment used and the system serial number (from all sites involved)
- Provide the software version of system (from all sites involved)
- Logs from system including configuration and system status

Terminal software for TelePresence Infrastructure

Important: Please start the log capture from all systems involved in the call before calls/conferences are started so we capture all the call setup process and ensures that all output is logged to a file so none is lost.

There are multiple terminal emulation software available that may be used for retrieving logs from a system. They include the following:

Windows HyperTerminal (Serial, Telnet)

Can be found under: Start Menu – All Programs – Accessories – Communications – HyperTerminal.

The Windows Hyper Terminal supports the Telnet protocol only. Please remember to enable the Capture Text option (menu “Transfer” – “Capture Text”).

TeraTerm

Down load the TeraTerm installation file from <http://sourceforge.jp/projects/ttssh2/releases/>

Supports multiple Protocols, including Telnet and SSH which are the two relevant protocols for the TelePresence Endpoint portfolio. It will automatic detect serial port if you are using USB to serial converter and option for save log with time stamp.

Putty (Serial, Telnet, SSH)

Download the Putty installation file from

<http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html>

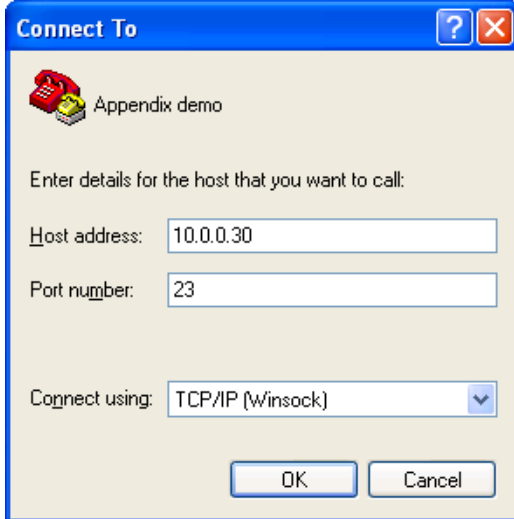
Supports multiple Protocols, including Telnet and SSH which are the two relevant protocols for the TelePresence Endpoint portfolio.

How to use Windows Hyper Terminal

This following page explains how to use Windows Hyper Terminal.

Please note, Windows Vista and Windows 7 may not have Hyper Terminal installed on default setting.

1. Start Hyper Terminal: Start Menu – All Programs – Accessories – Communications – HyperTerminal Supports the Telnet protocol only.
2. Under “Connect using” select “TCP/IP (Winsock)” and enter the System IP address.

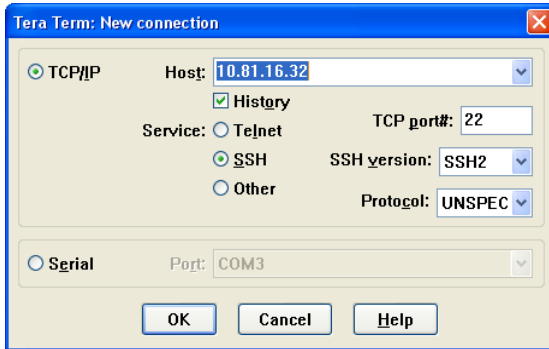


3. Default password is cisco, TANDBERG or blank unless changed. Some Infrastructure products have “admin” or “root” as login name.
4. To save retrieve logs: Enable the Capture Text option (menu “Transfer” – “Capture Text”), and save it as a *.log file.
5. Type in the respective commands described in Appendix.

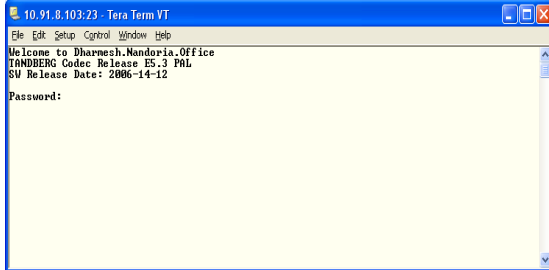
How to use TeraTerm

This following page explains how to use TeraTerm.

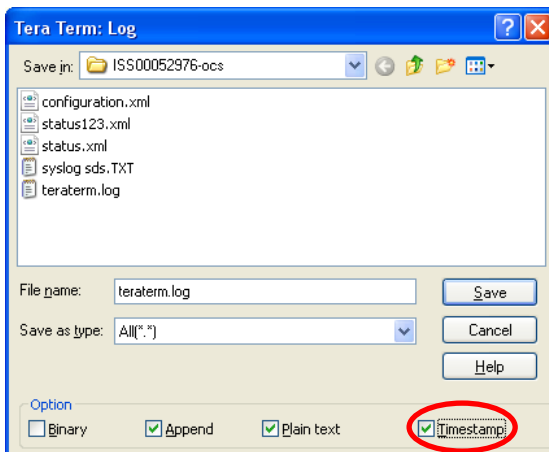
1. Start TeraTerm: Start Menu – All Programs – TeraTerm Pro with TTSSH2 – TeraTerm Pro (if install software as default setting).
2. Select “Telnet” and enter the System IP address in “Host”.
(Or select “SSH” and enter the System IP address in “Host” in order to establish SSH connection between systems.)



3. Default password is cisco, TANDBERG or blank unless changed. Some Infrastructure products have “admin” or “root” as login name.



4. To save retrieve logs: Select “Log” from File menu and select location of saving file and file name. You may check “Timestamp” option which will add timestamp on log base on PC’s clock information.
(Example of timestamp format on log: [Wed Feb 25 15:10:30 2009]).

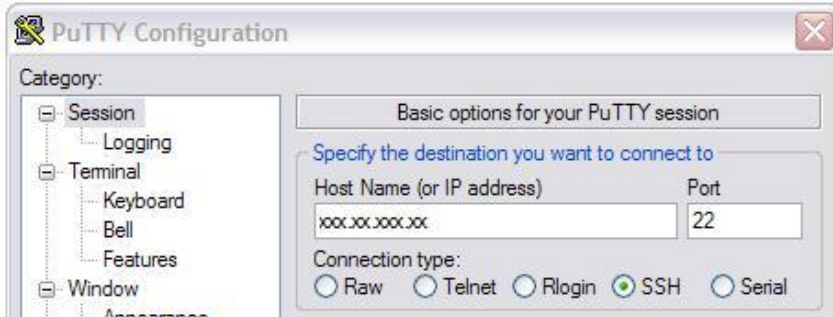


5. Type in the respective commands described in Appendix.

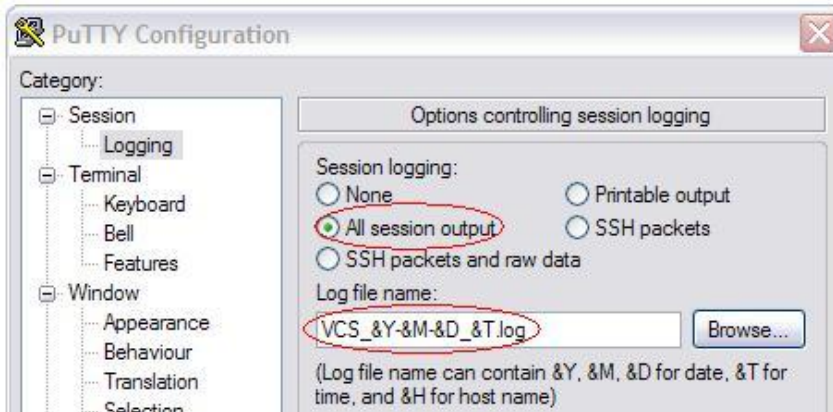
How to use PuTTY

This following page explains how to use PuTTY.

1. Start PuTTY
2. Select "Telnet" and enter the System IP address in "Host Name".
(Or select "SSH" and enter the System IP address in "Host Name" in order to establish SSH connection between systems.)



3. Default password is cisco, TANDBERG or blank unless changed. Some Infrastructure products have "admin" or "root" as login name.
4. To save retrieve logs: Select "Logging" and choose "All session output" and select location of saving file and file name at "Log file name".



5. Type in the respective commands described in Appendix.

File transfer software for TelePresence Infrastructure

There are multiple file transfer software applications available, that may be used for retrieving logs from Cisco Telepresence systems and/or uploading files to Cisco Telepresence system. Examples are:

Command Prompt

Can be found under: Start Menu – All Programs – Accessories – Command Prompt. Command Prompt support ftp base file transfer between local PC and TelePresence Infrastructure.

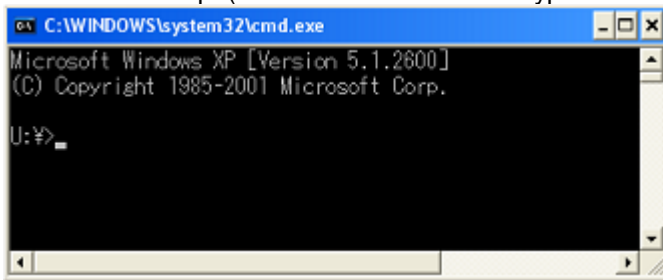
WinSCP

Download the WinSCP installation file from <http://winscp.net/eng/index.php>
Support SCP protocol with GUI for Windows base PC which use for safely copying of file between local PC and TelePresence Infrastructure.

How to use Windows Command Prompt

This following page explains how to use Command Prompt for ftp.

1. Start Command Prompt Hyper Terminal: Start Menu – All Programs – Accessories – Command Prompt (or Start Menu – Run... - type “cmd” and click “ok”)



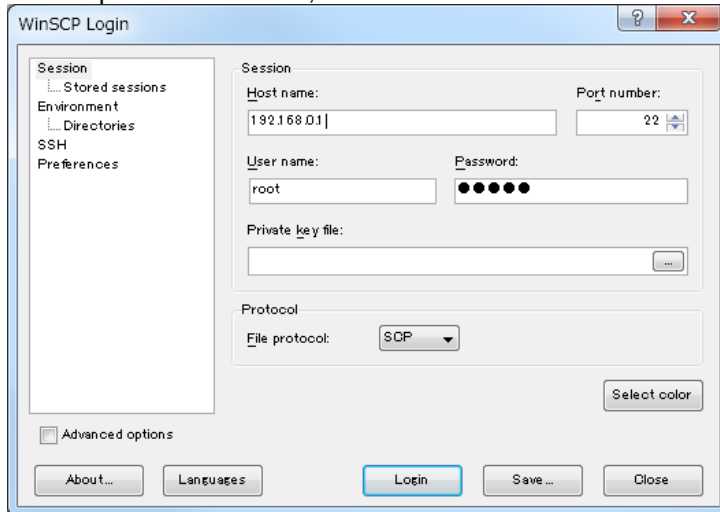
2. Navigate location for saving download file or file folder which to upload to system by using “cd” command.
For example, save the download log to log folder under C drive on PC, “cd C:\log”.
3. Establish ftp connection by using “ftp <ip address>” command.
4. Default password is cisco, TANDBERG or blank unless changed. Some Infrastructure products have “admin” or “root” as login name.
5. Basic command which will use on ftp session
 - o ls – list the file directory
 - o cd <foldername> - navigate to specified directory/folder
 - o hash - Toggle printing “#” for each buffer transferred
 - o bin – set to binary transfer mode
 - o get <filename> – download specified file from codec to PC
 - o put <filename> – upload specified file to codec from PC
6. Type “bye” to terminate ftp session between codec and PC

How to use WinSCP

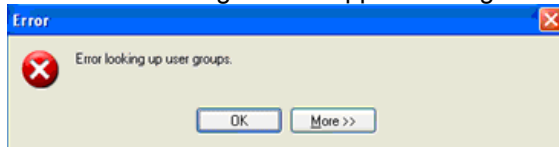
This following page explains how to use WinSCP

1. Start WinSCP: Start Menu – All Programs – WinSCP – WinSCP (if install software as default setting).
2. Select “SCP” as Protocol, enter the System IP address in “Host name”, “root” in “User name” and system password in “Password”.

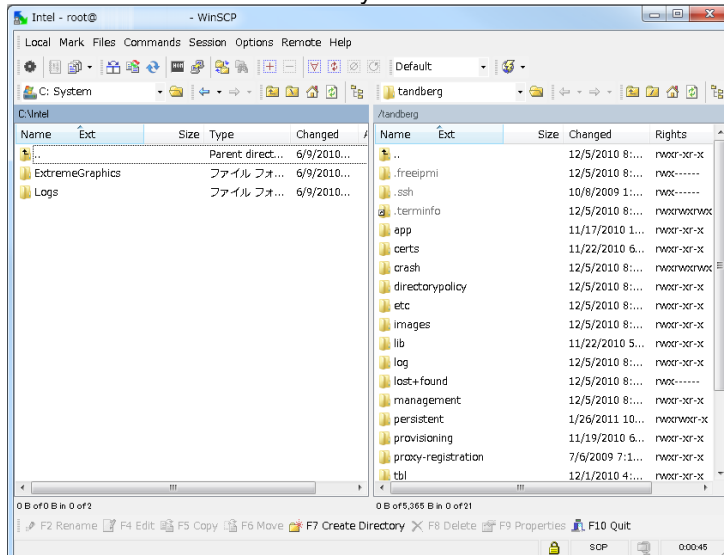
Default password is cisco, TANDBERG or blank unless changed.



3. After verifying the information click on “Login”.
If the error message below appear during the connection process, just click “OK” and proceed.



4. Find the log file that would like to retrieve from right side of GUI windows and drag it to left side of GUI windows which is your local PC



Packet Capture software for Cisco TelePresence Infrastructure and Systems

Important: Please start the log capture from all systems involved in the call before calls/conferences are started so we capture all the call setup process and ensures that all output is logged to a file so none is lost.

There are multiple packet capture software that may be used for analyzing communications traffic between Cisco Telepresence systems such as:

Wireshark (IP packet sniffer)

Download the Wireshark installation file from <http://www.wireshark.org/download.html>

Wireshark is the network protocol analyzer, and is standard across industries.

RS-232 Serial Connection

Most of TelePresence Infrastructure has the D-Sub 9 pin data port on the back of the unit that may be used for configuration and administration. The data port may also use for initial configuration. Software upgrades may also be monitored via the serial ports.

Any RS-232 emulation can be used, such as Microsoft HyperTerminal, TeraTerm, etc. The default connectivity parameters are:

Model	Parameter	
Gatekeeper Border Controller	Baud Rate	115200 bps
	Data Bits	8
	Parity	None
	Stop Bits	1
	Flow Control	None
	Interface	D-Sub 9 pin interface on front of unit
	Note	Require reverse cable/adapter

Model	Parameter																		
Video Communication Server (VCS)	Baud Rate	115200 bps																	
	Data Bits	8																	
	Parity	None																	
	Stop Bits	1																	
	Flow Control	None																	
	Interface	RJ45 interface on front of unit																	
	Note	Require RJ45-D-Sub9pin cable for console connection.																	
	Pin Assignment	<table border="1"> <thead> <tr> <th>Male RJ45 pin</th> <th>Female DB9 pin</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>8</td> </tr> <tr> <td>2</td> <td>6</td> </tr> <tr> <td>3 TXD</td> <td>2</td> </tr> <tr> <td>4 GND</td> <td>5</td> </tr> <tr> <td>5 GND</td> <td>5</td> </tr> <tr> <td>6 RXD</td> <td>3</td> </tr> <tr> <td>7</td> <td>4</td> </tr> <tr> <td>8</td> <td>7</td> </tr> </tbody> </table>	Male RJ45 pin	Female DB9 pin	1	8	2	6	3 TXD	2	4 GND	5	5 GND	5	6 RXD	3	7	4	8
Male RJ45 pin	Female DB9 pin																		
1	8																		
2	6																		
3 TXD	2																		
4 GND	5																		
5 GND	5																		
6 RXD	3																		
7	4																		
8	7																		

Model	Parameter	
Classic MCU ISDN Gateway	Baud Rate	9600 bps
	Data Bits	8
	Parity	None
	Stop Bits	1
	Flow Control	None
	Interface	D-Sub 9 pin interface on back of unit
Model	Parameter	

Media Processing System (MPS)	Baud Rate	9600 bps																		
	Data Bits	8																		
	Parity	None																		
	Stop Bits	1																		
	Flow Control	None																		
	Interface	RJ45 interface (COM1) on front of System Control Blade																		
	Note	Require RJ45-D-Sub9pin cable for console connection																		
	Pin Assignment	<table border="1"> <thead> <tr> <th>Male RJ45 pin</th> <th>Female DB9 pin</th> </tr> </thead> <tbody> <tr> <td>1 DCD</td> <td></td> </tr> <tr> <td>2 RTS</td> <td></td> </tr> <tr> <td>3 GND</td> <td></td> </tr> <tr> <td>4 TXD</td> <td>2</td> </tr> <tr> <td>5 RXD</td> <td>3</td> </tr> <tr> <td>6 GND</td> <td>5</td> </tr> <tr> <td>7 CTS</td> <td></td> </tr> <tr> <td>8 DTR</td> <td></td> </tr> </tbody> </table>	Male RJ45 pin	Female DB9 pin	1 DCD		2 RTS		3 GND		4 TXD	2	5 RXD	3	6 GND	5	7 CTS		8 DTR	
Male RJ45 pin	Female DB9 pin																			
1 DCD																				
2 RTS																				
3 GND																				
4 TXD	2																			
5 RXD	3																			
6 GND	5																			
7 CTS																				
8 DTR																				

Model	Parameter																			
TelePresence Server	Baud Rate	38400 bps																		
	Data Bits	8																		
	Parity	None																		
	Stop Bits	1																		
TelePresence MCU	Flow Control	None																		
TelePresence ISDN Gateway	Interface	RJ45 interface on front of unit																		
	Note	Require RJ45-D-Sub9pin cable for console connection																		
TelePresence IP Gateway	Pin Assignment	<table border="1"> <thead> <tr> <th>Male RJ45 pin</th> <th>Female DB9 pin</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>8</td> </tr> <tr> <td>2</td> <td>6</td> </tr> <tr> <td>3 TXD</td> <td>2</td> </tr> <tr> <td>4 GND</td> <td>5</td> </tr> <tr> <td>5 GND</td> <td>5</td> </tr> <tr> <td>6 RXD</td> <td>3</td> </tr> <tr> <td>7</td> <td>4</td> </tr> <tr> <td>8</td> <td>7</td> </tr> </tbody> </table>	Male RJ45 pin	Female DB9 pin	1	8	2	6	3 TXD	2	4 GND	5	5 GND	5	6 RXD	3	7	4	8	7
Male RJ45 pin		Female DB9 pin																		
1		8																		
2		6																		
3 TXD		2																		
4 GND		5																		
5 GND		5																		
6 RXD		3																		
7	4																			
8	7																			
IPVCR																				

How to capture a log from TelePresence Video Communication Server (VCS)

Important: Please start the log capture from all systems involved in the call before calls/conferences are started so we capture all the call setup process and ensure that all output is logged to a file so none is lost.

This chapter explains how to capture the complete log file available for TelePresence Video Communication Server (VCS). The table below lists the commands needed for the Cisco TelePresence VCS. Please type all commands in the same Telnet/SSH session.

All retrieved logs should attach to ticket including a description and compress multiple attachments into one file.

Logs – VCS

The logs in the diagram below should be included on initial support requests for each scenario.

Logs \ Scenario	Calls disconnect after X mins	Not able to call X	Cluster issues	Reboot issues	OCS/Lync issues	Registration issues	Presence issues	Network issues
Xstatus								
Xconfiguration								
Diagnostics Network (DEBUG)								
Diagnostics Interworking (DEBUG)								
Diagnostics Interworking (INFO)								
Diagnostics B2BUA (DEBUG)								
Diagnostics B2BUA (INFO)								
Event log								
Configuration log								
Network log								
Call media statistics (traversal calls only)								
TCPDUMP								
System Snapshot (Full)								
Tools								
Nslookup								
Ping								
Trace route								
Other devices								
Endpoint(s) Xstatus								
Endpoint(s) Xconfiguration								
Endpoint(s) "syslog/idx" log								
Endpoint(s) TCPDUMP								
OCS SIP log (all SIP flags)								
Other useful information								
Network diagram								

* For more information, please see the introduction section “Logs framework diagram symbols”

IP issues (H323/SIP)

Commands in bold

- Open the console/telnet/ssh session with VCS
- **xstatus**
- **xconfig**
- Go to the Web interface (<https://vcsip/ loggingsnapshot>) and start a **diagnostics log** with DEBUG level
(Prior X7.0 use “**netlog 2**”, X3.x or prior software version, please use “**syslog 3**”)
- **Note:** If any interworking or B2BUA is involved in the call, please set these levels to DEBUG as well
- Make a call and keep running until you have recreated the problem
(Add markers if necessary)
- Hang up call
- **Stop** the diagnostics log
(X7.0 and prior; “**netlog 0**” (X3.x or prior software version, please use “**syslog 0**”)
Don't worry that the screen is scrolling, just type in and press return to stop the netlog output
- Attach file to the ticket – Remember to name these or include a description and compress multiple attachments into one file

Reboot Issue

Commands in bold

- Open Web interface session with the VCS
- Go to the System snapshot page on the VCS (**Maintenance > System Snapshot**)
- Click **Create system snapshot**
- **Note:** The system snapshot may take several minutes to be created, and will be large file. Once the snapshot has been created a pop up box will appear request location to save the file to.
- Go to Incident reporting page on VCS (**Maintenance > Incident reporting > View**)
- **Note:** Restart an incident report should be generate and will be available for download from this page
- Attach file to the ticket – Remember to name these or include a description and compress multiple attachments into one file

Sniffer the packet on VCS

Note: This method should only use when request by TelePresence TAC.

Important: This works on both H.323 and SIP call, however it must disable encryption. For SIP, make sure not to use TLS for signaling.

Commands in bold

- Open the console/ssh session with VCS and login as “root” user
- **cd /**
- **cd mnt/harddisk**
- **mkdir temp**
- **cd temp**
- **tcpdump -w tcpdump1.pcap -s 0 -C10 -l ip and not port 22**
- Make a call and keep running until you have recreated the problem
- **Ctrl + C**
- Open WinSCP and retrieve the sniffer log under /mnt/harddisk/temp directory.
- **Important:** Tracing log MUST delete as temp folder has limited desk space and not design to capture log.
- Attach file to the ticket after zip compress it – Remember to name these or include a description and compress multiple attachments into one file

Note: if for short sniffer, following step will also works.

- Open the console/ssh session with codec and login as “root” user
- **tcpdump -w /tmp/tcpdump.pcap -s 0 ip and not port 22**
- Make a call and keep running until you have recreated the problem
- **Ctrl + C**
- Open WinSCP and retrieve the sniffer log under /tmp directory.

Important: Tracing log MUST delete as tmp folder has limited desk space and not design to capture log.

- Attach file to the ticket after zip compress it – Remember to name these or include a description and compress multiple attachments into one file

Default factory VCS

Commands in bold

- Open the console/telnet/ssh session with VCS
- Take backup of system configuration and option keys
- **xCommand DefaultValuesSet Level:3**

Note: DefaultValuesSet will not add the default links with which the system ships from the factory. The DefaultLinksAdd command will configure back default link between default zone/subzone.

Note: The certificates and policy files are not removed.

- Open the console/telnet/ssh session with VCS
- **xCommand DefaultLinksAdd**

Default factory VCS (X7<)

- Take backup of system configuration and option keys
- Open the console/ssh session to the VCS
- Login as root
- **factory-reset**
- Follow the procedure
- Reboot

Reset Password on VCS

Commands in bold

- Connect serial/console connection
- Restart the GK/BC
- Login with the user name **PWREC**. No password is required.
- You will be prompted for a new password.

```

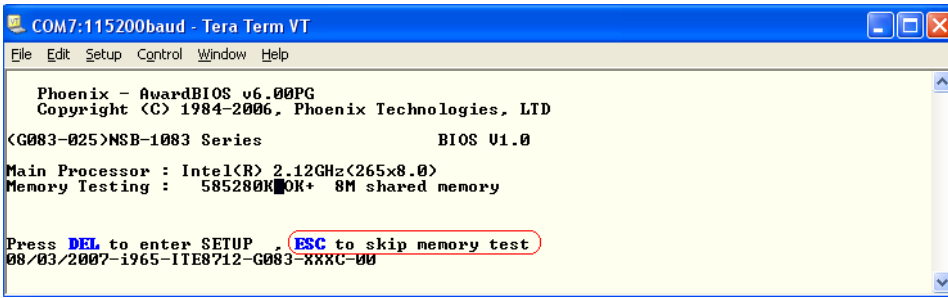
COM8:115200baud - Tera Term VT
File Edit Setup Control Window Help
TANDBERG BC login: PWREC
ACCESS GRANTED. YOU WILL BE PROMPTED FOR A PASSWORD TWICE
PASSWORD:
PLEASE RETYPE PASSWORD:
WELCOME TO
TANDBERG BORDER CONTROLLER RELEASE Q5.2
SW RELEASE DATE: 2007-06-22
OK
WRITING PASSWORDS THROUGH TANDBERG APPLICATION FAILED.
RESTORING PASSWORDS TO PASSWORD FILE DIRECTLY, TO ALLOW
MANUAL RECOVERY PROCESS.
TANDBERG BC login:
    
```

Note: The PWREC account is only active for one minute following a restart. Beyond that time you will have to restart the system again to change the password. Because access to the serial port allows the password to be reset, it is recommended that you install the GK/BC in a physically secure environment.

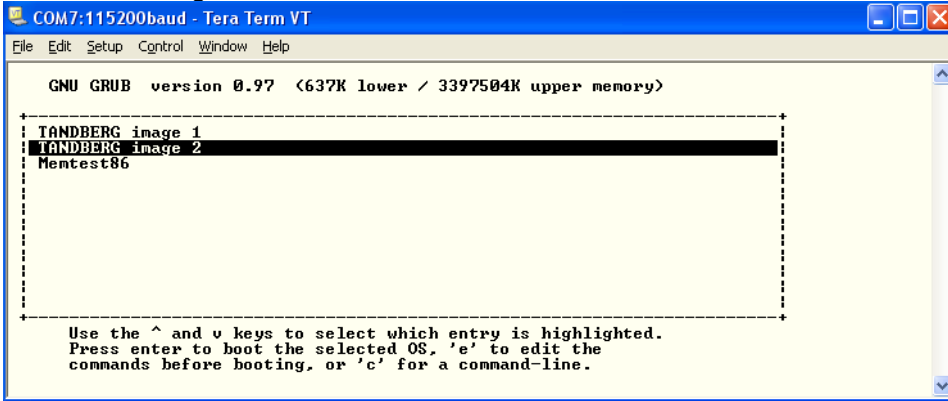
Revert back previous software version on VCS

Commands in bold

- Connect serial/console connection
- Restart the VCS
- Press **ESC** to skip memory test



- Wait for following screen.



- Select non-highlight “TANDBERG image x” by using arrow **up** / **down** key and then press **enter** key. VCS will start up with previous install software version.
Note: This software select menu will be available for 3 seconds only.

How to upgrade TelePresence Video Communication Server software

This chapter explains how to upgrade TelePresence VCS by using SCP software for in case of problem with upgrading software from WebGUI or TMS.

Commands in bold

- Upload the release key file using SCP/PSCP to the /tmp folder on the system.
 Example:
scp release-key root@<BC/GK IP address>:/tmp/release-key
or
pscp release-key root@<BC/GK IP address>:/tmp/release-key
- Enter password when prompted
 Type password in “Password:”. Default password is cisco or TANDBERG unless changed.
- Copy the software image using SCP/PSCP.

Note: SW file name should rename to “tandbergimage.tar.gz” before upload it to /tmp.

Example:

scp s4200n51.tar.gz root@<BC/GK IP addr.>:/tmp/tandberg-image.tar.gz

or

pscp s42100n51.tar.gz root@<BC/GK IP addr.>:/tmp/tandbergimage.tar.gz

- Enter password when prompted
 Type password in “Password:”. Default password is cisco or TANDBERG unless changed.
- Wait until the software has installed completely
- Reboot the BC/GK manually from Web GUI, from telnet session, etc.

Note: You may upgrade SW similar way by using WinSCP application as well.

How to capture logs from VCS X7.x

The “netlog” is now called “Diagnostics log”. To capture the diagnostics log, you will have to do this through the WebUI.

1. Go to the **Diagnostic logging** page (**Maintenance > Diagnostics > Diagnostic logging**).
2. Optional. Set the logging levels:
 - a. **Network log level:** the log level for call signaling messages.
 - b. **Interworking log level:** the log level for SIP/H.323 interworked call diagnostics.
 - c. **B2BUA calls log level:** the log level for calls passing through the **B2BUA**.
 - You should only change these log levels on the advice of Cisco customer support.
 - For normal network issues, select **DEBUG** level for network (leave Interworking as **INFO**)
 - For interworking issues, select **DEBUG** level for both network and interworking
 - These settings affect the amount of logging information that is included in the diagnostic log.
3. Click **Start new log**.
4. Optional. Enter some **Marker** text and click **Add marker**.
 - The marker facility can be used to add comment text to the log file before certain activities are performed. This helps to subsequently identify the relevant sections in the downloaded diagnostic log file.
 - You can add as many markers as required, at any time while the diagnostic logging is in progress. You can also supply marker text when starting or stopping the log file.
 - Marker text is added to the log with a "**DEBUG_MARKER**" tag.
5. Reproduce the system issue you want to trace in the diagnostic log.
6. Click **Stop logging**.
7. Click **Download log** to save the diagnostic log to your local file system. You are prompted to save the file (the exact wording depends on your browser).
8. Send the downloaded diagnostic log file to your Cisco support representative, if you have been requested to do so.

Note that:

- Only one diagnostic log can be produced at a time; creating a new diagnostic log will replace any previously produced log.
- The VCS continually logs all system activity to a unified log file. The diagnostic logging facility works by extracting a portion of this unified log. On busy systems the unified log file may become full over time and will discard historic log data so that it can continue logging current activity. This means that all or part of your diagnostic log could be overwritten. The system will warn you if you attempt to download a partial diagnostic log file.
- The diagnostic log will continue logging all system activity until it is stopped, including over multiple login sessions and system restarts.
- The various **log level** settings cannot be changed while a diagnostic log is in progress. The log levels are reset to their original values when you stop the diagnostic log.
- Diagnostic logging can only be controlled through the web interface; there is no CLI option as in previous versions.

How to capture a log from Gatekeeper (GK) and Border Controller (BC)

Important: Please start the log capture from all systems involved in the call before calls/conferences are started so we capture all the call setup process and ensure that all output is logged to a file so none is lost.

This chapter explains how to capture the complete log file available for Gatekeeper (GK) and Border Controller (BC). The table below lists the commands needed for the GK and BC. Please type all commands in the same Telnet/SSH session.

All retrieved logs should attach to ticket including a description and compress multiple attachments into one file.

IP issues (H323)

Commands in bold

- Open the console/telnet/ssh session with GK/BC
- **xstatus**
- **xconfig**
- **syslog 3**
- Make a call and keep running until you have recreated the problem
- Hang up call
- **syslog 0**
Don't worry that the screen is scrolling, just type in and press return to retrieve system status log
- Attach file to the ticket – Remember to name these or include a description and compress multiple attachments into one file.

Reboot Issue

Commands in bold

- After GK/BC restart open the console/telnet/ssh session with GK/BC
- **eventlog all**
- Attach file to the ticket – Remember to name these or include a description and compress multiple attachments into one file

Sniffer the packet on GK/BC

Note: This method should only use when request by TelePresence TAC.

Important: This works on H.323 call, however it must disable encryption.

Commands in bold

- Open the console/ssh session with codec and login as "root" user
 - **tcpdump -n -s 1500 -w /tmp/tcpdump.pcap ip and not port 22**
 - Make a call and keep running until you have recreated the problem
 - **Ctrl + C**
 - Open WinSCP and retrieve the sniffer log under /tmp directory.
- Important:** Tracing log MUST delete as tmp folder has limited desk space and not design to capture log.
- Attach file to the ticket – Remember to name these or include a description and compress multiple attachments into one file

Default factory GK/BC

Commands in bold

- Open the console/telnet/ssh session with GK/BC
- Take backup of system configuration and option keys
- **xCommand DefaultValuesSet Level:3**

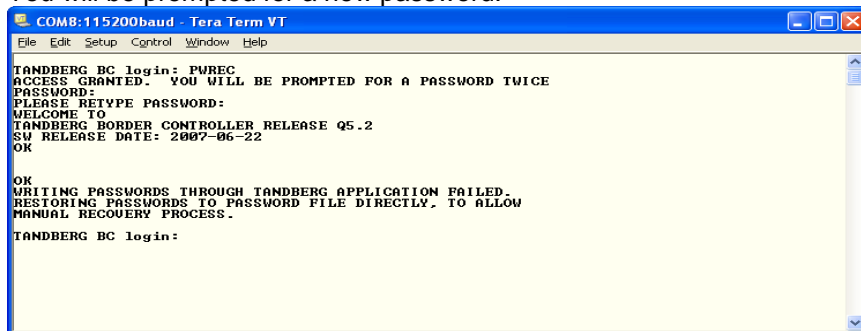
Note: DefaultValuesSet will not add the default links with which the system ships from the factory. The DefaultLinksAdd command will configure back default link between default zone/subzone. The certificates and policy files are not removed.

- Open the console/telnet/ssh session with GK/BC
- **xCommand DefaultLinksAdd**

Reset Password on GK/BC

Commands in bold

- Connect serial/console connection
- Restart the GK/BC
- Login with the user name **PWREC**. No password is required.
- You will be prompted for a new password.



```

COMB:115200baud - Tera Term VT
File Edit Setup Control Window Help
TANDBERG BC login: PWREC
ACCESS GRANTED. YOU WILL BE PROMPTED FOR A PASSWORD TWICE
PASSWORD:
PLEASE RETYPE PASSWORD:
WELCOME TO
TANDBERG BORDER CONTROLLER RELEASE Q5.2
SW RELEASE DATE: 2007-06-22
OK
WRITING PASSWORDS THROUGH TANDBERG APPLICATION FAILED.
RESTORING PASSWORDS TO PASSWORD FILE DIRECTLY, TO ALLOW
MANUAL RECOVERY PROCESS.
TANDBERG BC login:

```

Note: The PWREC account is only active for one minute following a restart. Beyond that time you will have to restart the system again to change the password. Because access to the serial port allows the password to be reset, it is recommended that you install the GK/BC in a physically secure environment.

How to upgrade Gatekeeper (GK) and Border Controller (BC) software

This chapter explains how to upgrade GK/BC by using SCP software for in case of problem with upgrading software from WebGUI or TMS.

Commands in bold

- Upload the release key file using SCP/PSCP to the /tmp folder on the system.

Example:

```
scp release-key root@<BC/GK IP address>:/tmp/release-key
```

or

```
pscp release-key root@<BC/GK IP address>:/tmp/release-key
```

- Enter password when prompted
Type password in "Password:". Default password is cisco or TANDBERG unless changed.
- Copy the software image using SCP/PSCP.

Note: SW file name should rename to "tandbergimage.tar.gz" before upload it to /tmp.

Example:

```
scp s42000n51.tar.gz root@<BC/GK IP addr.>:/tmp/tandberg-image.tar.gz
```

or

```
pscp s42100n51.tar.gz root@<BC/GK IP addr.>:/tmp/tandbergimage.tar.gz
```

- Enter password when prompted
Type password in "Password:". Default password is cisco or TANDBERG unless changed.
- Wait until the software has installed completely
- Reboot the BC/GK manually from Web GUI, from telnet session, etc.

Note: You may upgrade SW similar way by using WinSCP application as well.

How to capture a log from TelePresence MCU and IP/ISDN Gateway

Important: Please start the log capture from all systems involved in the call before calls/conferences are started so we capture all the call setup process and ensure that all output is logged to a file so none is lost.

This chapter explains how to capture the complete log file available for TelePresence MCU and IP/ISDN Gateway Components.

All retrieved logs should attach to ticket including a description and compress multiple attachments into one file.

Logs – MCU

The logs in the diagram below should be included on initial support requests for each scenario.

Logs \ Scenario	Reboot issue	Call setup (simple)	Call setup (complex)	Audio/Video issues	Network problems	H.323/SIP/Conference registrations	Clustering	Hardware failure
Configuration.xml								
Event log								
H323/SIP Log								
Serial Log								
Screenshot								
Conferencing_diagnostics.txt (from Status > General page)								
TCPDUMP								
Other devices								
VCS(s) Xstatus								
VCS(s) Xconfiguration								
VCS(s) diagnostics log (DEBUG)								
VCS(s) diagnostics interworking log (DEBUG)								
VCS(s) TCPDUMP								
Other useful information								
Network diagram								
If MCU is unresponsive (serial works, but no WebUI), login with serial and type following commands: h323debug, mutexes, threads								

* For more information, please see the introduction section “Logs framework diagram symbols”

Logs – IP Gateway

The logs in the diagram below should be included on initial support requests for each scenario.

Logs \ Scenario	<i>Reboot issue</i>	<i>Call setup (simple)</i>	<i>Call setup (complex)</i>	<i>Audio/Video</i>	<i>Network problems</i>
<i>Configuration.xml</i>					
<i>Event log</i>					
<i>H323/SIP Log</i>					
<i>Disgnostics file</i>					
<i>Serial Log</i>					
<i>Screenshot</i>					
<i>TCPDUMP</i>					
Other devices					
<i>VCS(s) Xstatus</i>					
<i>VCS(s) Xconfiguration</i>					
<i>VCS(s) diagnostics log (DEBUG)</i>					
<i>VCS(s) diagnostics interworking log (DEBUG)</i>					
<i>VCS(s) TCPDUMP</i>					
Other useful information					
<i>Network diagram</i>					

* For more information, please see the introduction section “Logs framework diagram symbols”

Logs – ISDN Gateway

The logs in the diagram below should be included on initial support requests for each scenario.

Logs \ Scenario	<i>ISDN Layer 1 issues</i>	<i>Call drops</i>	<i>Calls not completing</i>	<i>Reboot issue</i>	<i>Hardware Failure</i>
<i>Configuration.xml</i>					
<i>H323/SIP log</i>					
<i>Event log (standard level)</i>					
<i>"event log" with following detailed filters : ISDN - errors,warning,information and trace NAT or ISDN Q.921 - detailed</i>					
<i>"event log" with the following detailed filters: Connection, dialplan, dspapi, H.320 and ISDN set to "Errors, warnings, information and trace" logging level</i>					
<i>"event log" with the following detailed filters: BAS set to "detailed trace" logging level Connection, dialplan, dspapi, H.320 and ISDN set to "Errors, warnings, information and trace" logging level</i>					
<i>CDR log</i>					
<i>Diagnostic file</i>					
<i>Serial Log</i>					
<i>TCPDUMP</i>					
Tools					
<i>Ping</i>					
Other devices					
<i>Endpoint(s) Xstatus</i>					
<i>Endpoint(s) Xconfiguration</i>					
<i>Endpoint(s) "syslog"</i>					
<i>Endpoint(s) TCPDUMP</i>					
<i>Switch/PBX configuration and verify that data services (video capabilities) are enabled on the PRI lines</i>					
Other useful information					
<i>Network diagram</i>					

* For more information, please see the introduction section "Logs framework diagram symbols"

IP issues (H323/SIP)

Commands in bold

- Open the Web GUI, go to **Events > H.323 / SIP log** and then click **Enable logging**.
Important: For all logging, always delete old logs first by click **Clear Log** before making any testing call.
- Reproduce the exact issue that you would like the support team to troubleshoot for example, by dialing from the endpoint to the TelePresence MCU or IP/ISDN Gateway.
Important: It is essential for any H.323 or SIP log to show the initial connection being established between the endpoint and the TelePresence MCU or IP/ISDN Gateway, because the negotiation which happens at this stage explains the behavior of the two devices later on in the call. An H.323 or SIP log started part-way through an established call is not useful for troubleshooting.
- After the issue has been reproduced, click **Disable logging** on the H.323 log page.
- On the H.323 log page, click **Download as XML**.
Save the resulting XML file then attach file to the ticket – Remember to name these or include a description and compress multiple attachments into one file.

Event log and Event Capture Filter

- If calls are not completing or dropping straight away, obtain an event log with following “Capture Filter” settings:
 - **Connection, dialplan, dspapi, H.320** and **ISDN** set to “**Errors, warnings, information and trace**” logging level
 - The rest of the options should be “**Errors, warnings and information**” left as logging level
- If calls are connecting but not completing/ issues with codec negotiations etc.:
 - **BAS** set to “**detailed trace**” logging level
 - **Connection, dialplan, dspapi, H.320** and **ISDN** set to “**Errors, warnings, information and trace**” logging level
 - The rest of the options should be “**Errors, warnings and information**” left as logging level
- If ISDN Layers are not coming up:
 - For ISDN GW 3200:
 - **ISDN** set to “**Errors, warnings and trace**” logging level
 - **NAT** set to “**Detailed trace**” logging level
 - The rest of the options should be “**Errors, warnings and information**” left as logging level
 - For ISDN GW 3201:
 - **ISDN** set to “**Errors, warnings and trace**” logging level
 - **ISDN-Q921** set to “**Detailed trace**” logging level
 - The rest of the options should be “**Errors, warnings and information**” left as logging level

Important: always place single call when retrieving the log and delete any previous logs.

Important: revert back to default logging level after the test.

Reboot Issue

- Open the Web GUI, and login as “admin” user
- Download Diagnostic information log.
 - Prior to MCU 4.0 and ISDN Gateway 2.0 Software release: go to Home and then click **Diagnostic information**

Administrator options

- [System status](#)
- [System settings](#)
- [View and configure conferences](#)
- [Configure user accounts](#)
- [Update user profile](#)
- [Configure conference endpoints](#)
- [Configure gateways](#)
- [View event log](#)

- [Configure network](#)
- [Update system software](#)

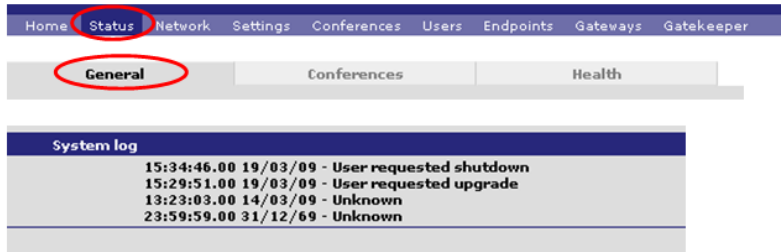
- [Streaming-only interface](#)
- [Diagnostic information](#)

Click Download as text and decide on a folder for the file.

- MCU 4.0 and ISDN Gateway 2.0 or newer software release:
The diagnostic file can be download with the download button locates at Status->General page.
go to Status > General then click **Download diagnostic information**



- Take snapshot of system status information page [Status > General](#)



- Attach file to the ticket – Remember to name these or include a description and compress multiple attachments into one file.

Sniffer the packet on TelePresence MCU or IP/ISDN Gateway

Note: This method should only use when request by TelePresence TAC.

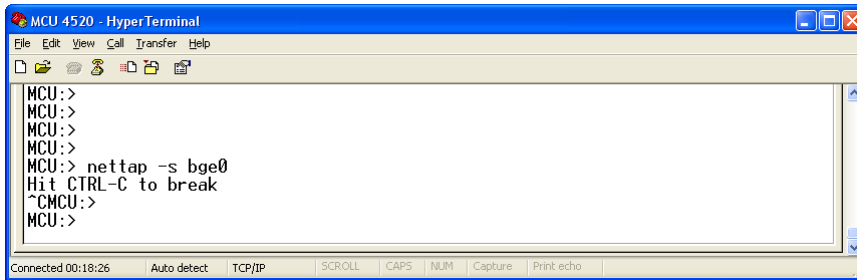
Note: Require 2.4 or newer released software on MCU.

Important: This works on both H.323 and SIP call, however it must disable encryption. For SIP, make sure not to use TLS for signaling.

Important: Make sure to have compact flash card in the TelePresence MCU or ISDN/IP Gateway Products external slot.

Commands in bold

- Open the console session
- **nettap -s bge0** for Port A sniffer (**nettap vfx0** for 8510 MCU Blade)
or
- **nettap -s bge1** for Port B sniffer



- Make a call and keep running until you have recreated the problem
- **Ctrl + C** to stop
- Download Sniffer log
 - Prior to MCU 4.0 and ISDN Gateway 2.0 Software release: User must download the network capture file with FTP Go to the web interface and then new link called **Download network capture file** is now available in top home page.

Administrator options

- [System status](#)
- [System settings](#)
- [View and configure conferences](#)
- [Configure user accounts](#)
- [Update user profile](#)
- [Configure conference endpoints](#)
- [Configure gateways](#)
- [View event log](#)

- [Configure network](#)
- [Update system software](#)

- [Streaming-only interface](#)
- [Diagnostic information](#)
- [Download network capture file](#)

- MCU 4.0 and ISDN Gateway 2.0 or newer software release: User must download the network capture file with FTP directly from Hardware.
 - Click this link to download the file.
 - Attach file to the ticket – Remember to name these or include a description and compress multiple attachments into one file.
- Note:** You may download capture file by using FTP application as well

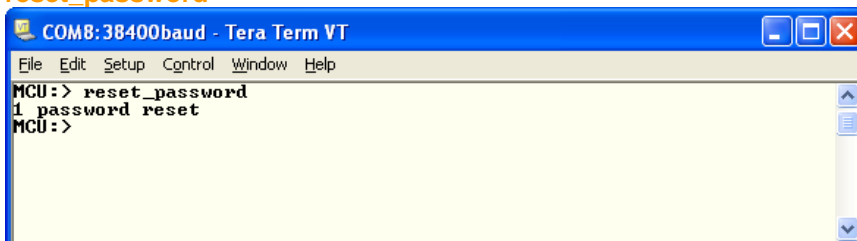
Reset Password on TelePresence MCU or IP/ISDN Gateway

Note: This method work for

- MCU with 2.1(1) or newer released version (till prior to 4.0 release)
- IPVCR with 2.1(1) or newer released version
- ISDN Gateway with 1.3(1.1) or newer released version (till prior to 2.0 release)

Commands in bold

- Open the console session
- **reset_password**



- After executing this command Administrator account comes to default. User name: admin, and no password.

How to capture a log from MPS series

Important: Please start the log capture from all systems involved in the call before calls/conferences are started so we capture all the call setup process and ensure that all output is logged to a file so none is lost.

This chapter explains how to capture the complete log file available for MPS series. The table below lists the commands needed for the MPS series. Please type all commands in the same Telnet session.

All retrieved logs should attach to ticket including a description and compress multiple attachments into one file.

IP issue (H323/SIP)

Commands in bold

- Open the console/telnet/ssh session with MPS
- **xstatus**
- **xconfig**
- **syslog 3**
- Make a call and keep running until you have recreated the problem
- **xstatus**, if issue related to video/audio channel status etc.
Don't worry that the screen is scrolling, just type in and press return to retrieve system status log
- Hang up call
- **syslog off**
Don't worry that the screen is scrolling, just type in and press return to turn off logging
- Attach file to the ticket – Remember to name these or include a description and compress multiple attachments into one file

ISDN issue

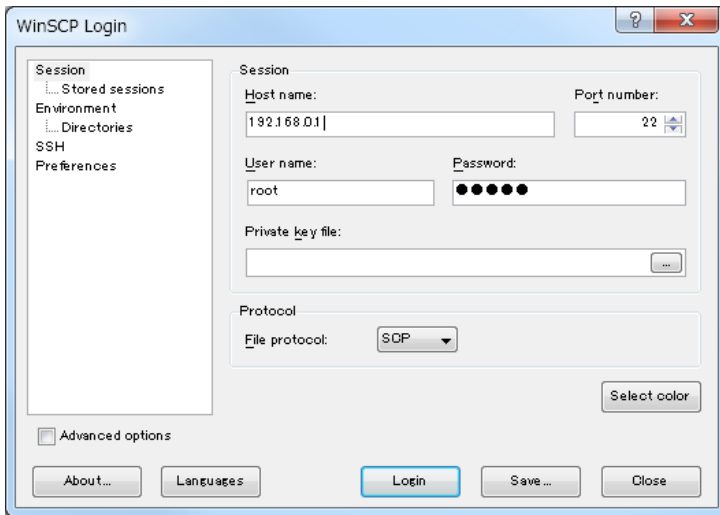
Commands in bold

- Open the console/telnet/ssh session with MPS
- **xstatus**
- **xconfig**
- **syslog 3**
- **isdn on**
- Make a call and keep running until you have recreated the problem
- **xstatus**, if issue related to video/audio channel status etc.
Don't worry that the screen is scrolling, just type in and press return to retrieve system status log
- Hang up call
- **syslog off**
Don't worry that the screen is scrolling, just type in and press return to turn off logging
- **isdn off**
- **dumph221**
- **isdn off**
- **dumph221**
- Attach file to the ticket – Remember to name these or include a description and compress multiple attachments into one file

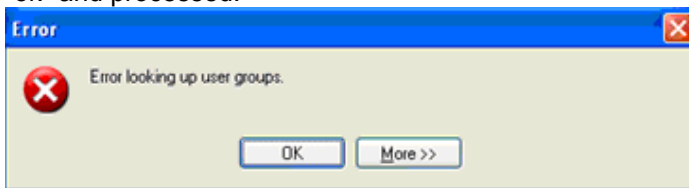
Reboot Issue

Commands in bold

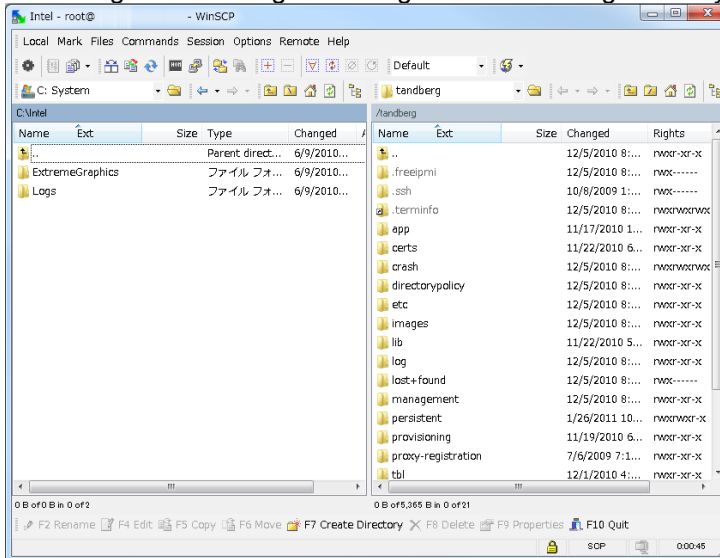
- Open the WinSCP session with MPS
- Login as "root" user



- Following error message below may appear during the connection process, but please click “ok” and processed.



- Retrieving the entire log folder “log” under /tandberg directory.

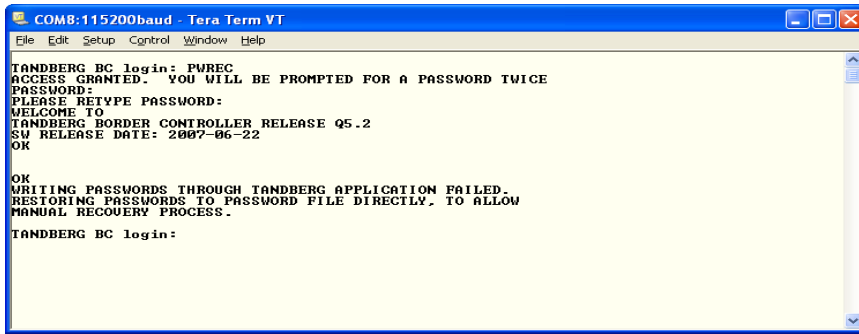


- Please do not open this folder. Simply drag it to your desktop, zip it and attached file to the ticket – Remember to name these or include a description.

Default factory MPS

Commands in bold

- Open the console/telnet/ssh session with MPS
- Take backup of system configuration and option keys
- **xCommand DefaultValuesSet Level:3**
- Reset Password on MPS Connect serial/console connection
- Restart the MPS
- Login with the user name **PWREC**. No password is required.
- You will be prompted for a new password.



```
COM8:115200baud - Tera Term VT
File Edit Setup Control Window Help

TANDBERG BC login: PWREC
ACCESS GRANTED. YOU WILL BE PROMPTED FOR A PASSWORD TWICE
PASSWORD:
PLEASE RETYPE PASSWORD:
WELCOME TO
TANDBERG BORDER CONTROLLER RELEASE Q5.2
SW RELEASE DATE: 2007-06-22
OK

WRITING PASSWORDS THROUGH TANDBERG APPLICATION FAILED.
RESTORING PASSWORDS TO PASSWORD FILE DIRECTLY. TO ALLOW
MANUAL RECOVERY PROCESS.
TANDBERG BC login:
```

Note: The PWREC account is only active for one minute following a restart. Beyond that time you will have to restart the system again to change the password. Because access to the serial port allows the password to be reset, it is recommended that you install the MPS in a physically secure environment.

How to upgrade MPS series

This chapter explains how to upgrade MPS series by using scp software for in case of problem with upgrading software from WebGUI or TMS.

Commands in bold

- Open the console/telnet/ssh session with MPS
- Login MPS as “root” user
- Set new release key by to /tmp folder
- **cd /tmp**
- **echo xxxxxxxxxxxxxxxxx > release-key** (xxxxxxxxxxxxxxxxxx is new release key)
- **exit**
- copy (upload) new software to MPS under /tmp folder by using SCP/PSCP application.
scp release-key root@<MPS IP address>:/tmp/tabasco-image.tar.gz

or

pscp release-key root@<MPS IP address>:/tmp/tabasco-image.tar.gz

Note: SW file name should rename to “tabasco-image.tar.gz” before upload it to /tmp.

Note: Upgrade will automatically start once SW file upload completely. However if the upgrade did not start immediately, by executing following command will start sw upgrade immediately.

/sbin/installimage /tmp/tabasco-image.tar.gz /tmp/release-key

- Wait until the software has installed completely
- Reboot the MPS manually from Web GUI, from telnet session, etc.
- **Note:** You may use WinSCP application for entire this process including setting up release-key file as well.

How to capture a log from Classic MCU/ISDN Gateway

Important: Please start the log capture from all systems involved in the call before calls/conferences are started so we capture all the call setup process and ensure that all output is logged to a file so none is lost.

This chapter explains how to capture the complete log file available for Classic MCU and Classic ISDN Gateway. The table below lists the commands needed for the Classic MCU and Classic ISDN Gateway. Please type all commands in the same Telnet session.

All retrieved logs should attach to ticket including a description and compress multiple attachments into one file.

IP issue (H323)

Commands in bold

- Open the console/telnet session with MCU/GW
- **ati1i4i5i6i7i9**
- **dispparam**
- **xconfig**
- **ipstat**
- **netstat**
- **syslog on**
- Make a call and keep running until you have recreated the problem
- **statin**, if issue related to video/audio channel status etc.
Don't worry that the screen is scrolling, just type in and press return to retrieve system status log
- **statout**, if issue related to video/audio channel status etc.
Don't worry that the screen is scrolling, just type in and press return to retrieve system status log
- Hang up call
- **syslog off**
Don't worry that the screen is scrolling, just type in and press return to turn off logging
- Attach file to the ticket – Remember to name these or include a description and compress multiple attachments into one file

ISDN issue

Commands in bold

- Open the console/telnet session with MCU/GW
- **ati1i4i5i6i7i9**
- **dispparam**
- **xconfig**
- **ipstat**
- **netstat**
- **syslog on**
- **isdn on**
- Make a call and keep running until you have recreated the problem
- **statin**, if issue related to video/audio channel status etc.
Don't worry that the screen is scrolling, just type in and press return to retrieve system status log
- **statout**, if issue related to video/audio channel status etc.
Don't worry that the screen is scrolling, just type in and press return to retrieve system status log
- Hang up call
- **syslog off**
Don't worry that the screen is scrolling, just type in and press return to turn off logging
- **isdn off**
- **dumph221**

- Attach file to the ticket – Remember to name these or include a description and compress multiple attachments into one file

Reboot Issue

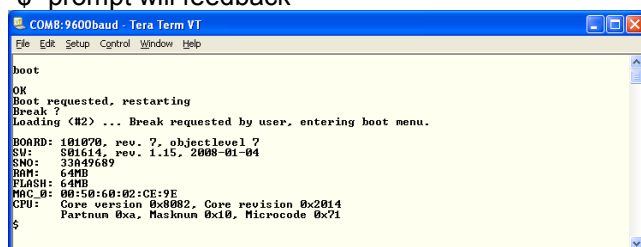
Commands in bold

- After codec restart open the console/telnet/ssh session with MCU/GW
- **eventlog**
or
- Download event. log file from root directory of MCU/GW
- Open Command prompt (and change home directory, if necessary)
- **ftp <ipaddress>**
- Default password is TANDBERG unless changed. Please enter any user name (e.g. admin) as login name.
- **hash**
- **bin**
- **get event.log**
- **bye**
- The event. log file transfer to directory of Command Prompt specified.
- Attach file to the ticket – Remember to name these or include a description and compress multiple attachments into one file

Default factory Classic MCU/ISDN Gateway

Commands in bold

- Open the console/telnet/ssh session with MCU/ISDN GW
- Take backup of system configuration and option keys
- **defvalues set factory**
or
- Open the console session with codec by using RS232 cable
- Take backup of system configuration and option keys
- Restart codec and break the boot sequence
- **Ctrl + Break** (for hyper terminal), or **Alt + B** (for TeraTerm/Putty)
- “\$” prompt will feedback



```

boot
OK
Boot requested, restarting
Break ?
Loading (#2) ... Break requested by user, entering boot menu.
BOARD: 181970, rev. 7, objectlevel 7
SW: S01614, rev. 1.15, 2008-01-04
SNO: 33049689
RAM: 64MB
FLASH: 64MB
MAC_0: 00:50:60:02:CE:9E
CPU: Core version 0x0002, Core revision 0x2014
Partnum 0xa, Masknum 0x10, Microcode 0x71
$

```

- **eee**
- **q**
- MCU/GW will automatically restart

How to capture a log from Telepresence Server

Event log

The TelePresence Server stores the 2000 most recently captured messages generated by its sub-systems. It displays these on the [Event log](#) page ([Logs > Event log](#)). In general these messages are provided for information, and occasionally *Warnings* or *Errors* may be shown in the Event log.

Customer support can interpret logged messages and their significance for you if you are experiencing a specific problem with the operation or performance of your TelePresence Server.

You can:

- Click the column headers to sort the events
- Click the page numbers to jump through the displayed log in steps of 100 events
- Download the log as text: go to [Logs > Event log](#) and click **Download as text**
- Change the parameters of the display to limit the information to your area of interest ([Logs > Event display filter](#))
- Change the level of detail collected in the traces by editing the [Event capture filter](#) page

Note: You should not modify the event capture filter unless instructed to do so by customer support. Modifying these settings can impair the performance of your TelePresence Server

Logging H.323 or SIP messages

The [H.323/SIP log](#) page records every H.323 and SIP message received by or transmitted from the TelePresence Server.

The H.323/SIP log is disabled by default because the volume of messages affects performance, but the support team may ask you to enable it to assist in troubleshooting.

Click **Enable H323/SIP logging** to start recording these protocol messages. You can also **Download as XML** for further processing or to send to support.

When you're satisfied that the issue is resolved, you should **Disable H323/SIP logging** and then **Clear log** to avoid impacting the performance of the unit in future.

Working with Call Detail Records

The TelePresence Server can display up to 2000 Call Detail Records. However, the TelePresence Server is not intended to provide long-term storage of Call Detail Records. If you wish to retain CDR logs, you must download them and store them elsewhere.

When the CDR log is full, the oldest logs are overwritten.

To view and control the CDR log, go to **Logs > CDR log**. Refer to the tables below for details of the options available and a description of the information displayed.

- Call Detail Record log controls
- Call Detail Record log

Call Detail Record log controls

The CDR log can contain a lot of information. The controls in this section help you to select the information for display that you find most useful. When you have finished making changes, click **Update display** to make those changes take effect. Refer to the table below for a description of the options:

CDR log controls		
Field	Field description	Usage tips
Messages logged	The current number of CDRs in the log.	-
Filter records	The list of CDR record types that the TelePresence Server logs.	Leave the boxes blank to display all records, or check the boxes of the record types you're interested in.
Filter string	Use this field to limit the scope of the displayed Call Detail Records. The filter string is not case-sensitive.	The filter string applies to the Message field in the log display. If a particular record has expanded details, the filter string will apply to these as well.
Expand details	By default, the CDR log shows only brief details of each event. When available, select from the options listed to display more details.	Selecting <i>All</i> will show the greatest amount of detail for all messages, regardless of which other options are selected.

Call Detail Record log

The Call Detail Record log displays as a long table which may span multiple pages and includes up to 2000 rows. In addition to the filtering described above, you can navigate the log in the following ways:

- To sort ascending or descending by any of the columns, click the column header
- To filter the log for all records related to a particular conference or participant GUID, click the GUID (click **Show all** to reverse this filter)
- To jump to a particular page in the displayed list of records, click the page number

Click **Download as XML** if you wish to process the log in your text editor, or archive it for future reference. This button *downloads all the records* currently stored on the box; it ignores any display filters you have set on the web page.

Note: Avoid downloading CDR logs when the unit is under heavy load; performance may be impaired.

Click **Clear all records** if you want to empty the log memory.

Caution: Clear all records permanently removes all records from the TelePresence Server. You cannot retrieve cleared records.

Logs – Telepresence Server

The logs in the diagram below should be included on initial support requests for each scenario.

Logs \ Scenario	<i>Reboot issue</i>	<i>Call setup (simple)</i>	<i>Call setup (complex)</i>	<i>Audio/Video issues</i>	<i>Network problems</i>	<i>H.323/SIP/Conference registrations</i>	<i>Clustering</i>
<i>Configuration.xml</i>							
<i>Event log</i>							
<i>H323/SIP Log</i>							
<i>Serial Log</i>							
<i>System log (from Status page)</i>							
<i>Screenshot</i>							
<i>Conferencing_diagnostics.txt (from Status page)</i>							
<i>TCPDUMP</i>							
Other devices							
<i>VCS(s) Xstatus</i>							
<i>VCS(s) Xconfiguration</i>							
<i>VCS(s) diagnostics log (DEBUG)</i>							
<i>VCS(s) diagnostics interworking log (DEBUG)</i>							
<i>VCS(s) TCPDUMP</i>							
Other useful information							
<i>Network diagram</i>							

* For more information, please see the introduction section “Logs framework diagram symbols”

How to capture a log from MSE8000

Event log

The last 2000 status messages generated by the Supervisor are displayed in the **Event log** page (**Logs > Event log**). In general these messages are provided for information, and occasionally *Warnings* or *Errors* may be shown in the Event log. The presence of such messages is not cause for concern necessarily; if you are experiencing a specific problem with the operation or performance of the Supervisor, TANDBERG customer support can interpret logged messages and their significance for you.

You can:

- Change the level of detail collected in the traces by editing the **Capture filter** page. You should not modify these settings unless instructed to do so by TANDBERG customer support.
- Display the log as text: go to **Logs > Event log** and click **Download as text**.
- Change which of the stored Event log entries are displayed by editing the **Display filter** page
- Send the event log to one or more syslog servers on the network for storage or analysis. The servers are defined in the **Syslog** page. For more information, refer to Logging using syslog logs (in the help contents on the MSE)
- Empty the log by clicking **Clear log**.

Event capture filter

The Event capture filter allows you to change the level of detail to collect in the Event log traces.

Note: You should not modify these settings unless instructed to do so by TANDBERG customer support. Modifying these settings can impair the performance of your Supervisor.

Normally, the capture filter should be set to the default of Errors, warnings and information for all logging sources. There is no advantage in changing the setting of any source without advice from TANDBERG customer support. There is a limited amount of space available to store logged messages and enabling anything other than Errors, warnings and information could cause the log to become full quickly.

Event display filter

The Event display filter allows you to view or highlight stored Event log entries. Normally, you should not need to view or modify any of the settings on this page.

Audit log

The audit log records any user action on the Supervisor which might compromise the security of the unit, of its functions, or of the network. For more information, refer to Working with the audit logs (in the help contents on the MSE).

Logs – MSE8000

The logs in the diagram below should be included on initial support requests for each scenario.

Logs \ Scenario	<i>Reboot issues</i>	<i>Power Supplies / Fan Trays</i>	<i>Hardware</i>	<i>Network problems</i>	<i>Licensing</i>	<i>Clustering</i>
<i>Configuration.xml</i>						
<i>Alarm log</i>						
<i>Event log</i>						
<i>H323/SIP Log</i>						
<i>Disgnostics file</i>						
<i>Serial Log</i>						
<i>Screenshot</i>						
<i>TCPDUMP</i>						
Other useful information						
<i>Network diagram</i>						

* For more information, please see the introduction section “Logs framework diagram symbols”

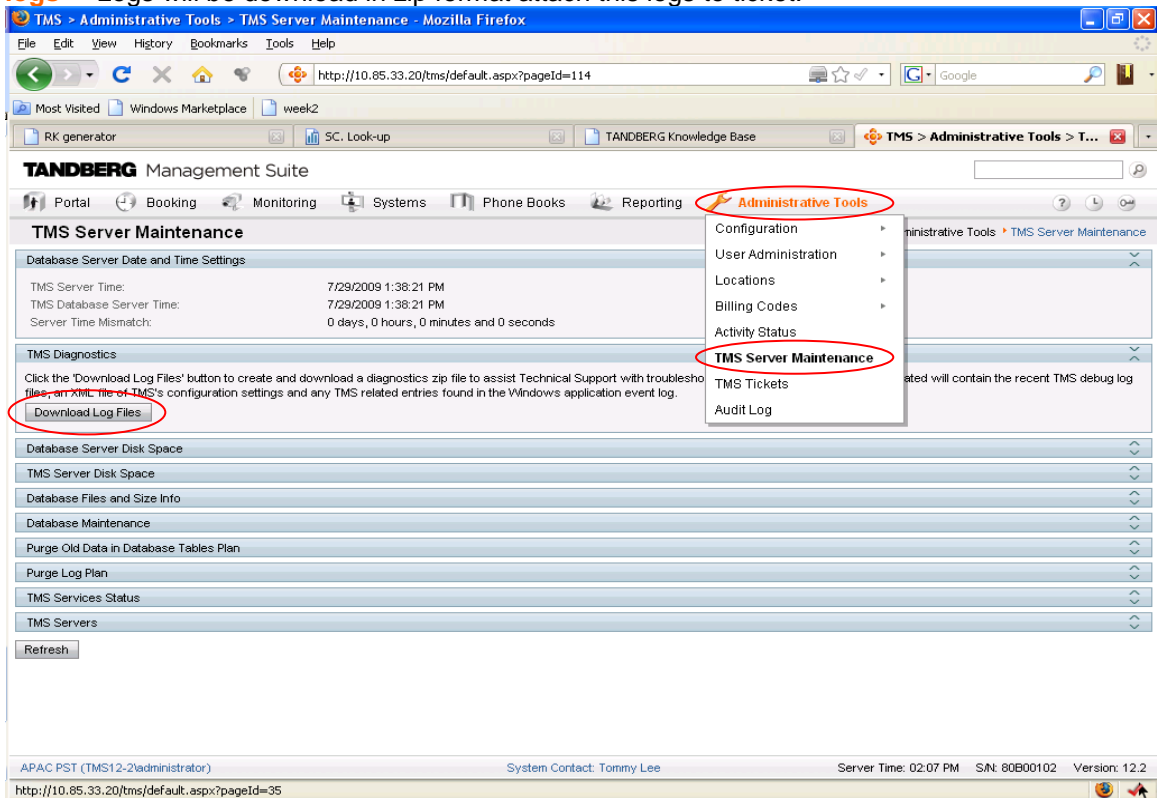
How to capture a log from TelePresence Management Suite

This chapter explains how to capture the complete log files available for TelePresence Management Suite, Provisioning Directory, and Windows server. Also provide additional faultfinding information.

All retrieved logs should be attached to the service request including a description. When possible compress multiple attachments into one file.

Log from TelePresence Management Suite

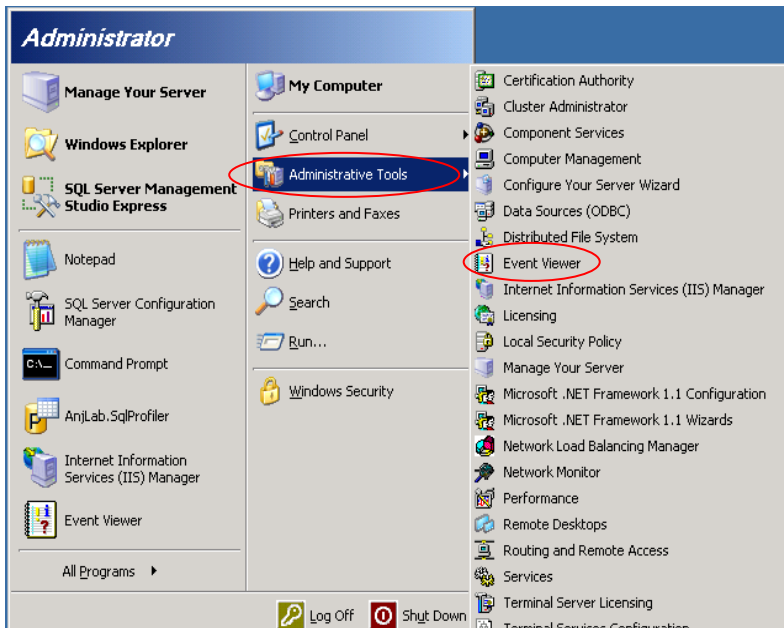
- For TMS 12.1 or older version, log files can be found on the TMS server at the following location: **C:\Program Files\TANDBERG\TMS\wwwTMS\Data\Logs\tmsdebug**
- For TMS 12.2 or newer version, log files can be found at (and download from) TMS Administrator Tools.
To take TMS logs : Go to **Administrative tools – TMS Server maintenance – Download logs** – Logs will be download in zip format attach this logs to ticket.



- The TMS Provisioning Directory Logs, logs TMS provides for Provisioning Directory can be found on the TMS server at the following location:
C:\Program Files\TANDBERG\TMS\wwwTMS\Data\Logs\tmsdebug
The name of the log files that you will want to look at with regards to the Provisioning Directory are as follows:
 - log-provisioning.txt
 - log-provisioningproxy.txt
 - log-provisioningservice.txt

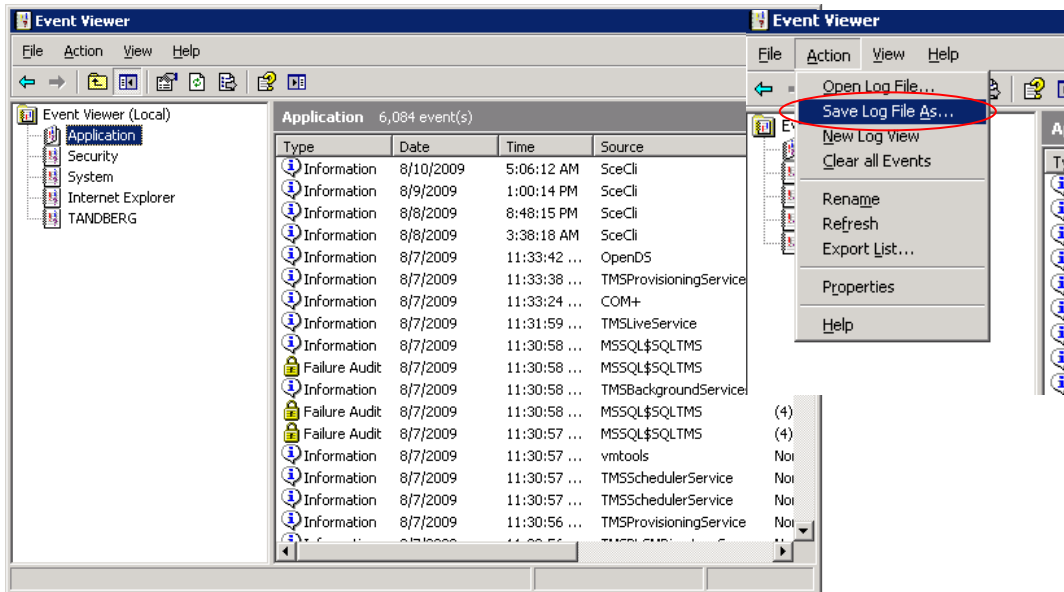
Log from Windows server

- The log files can be found on the server that TMS server is running by using Event Viewer function.
- To take Windows Server logs : Go to **Start → Administrator Tools → Event Viewer**



- The name of the log files that you will want to look at:
 - Application
 - System
 - TANDBERG

Important: Save the logs as .evt format only.



Log from TelePresence Management Suite components and faultfinding

Main TelePresence Management Suite components and faultfinding method:

a) TMSDatabaseScannerService

- What it does:
 - This service will check the connection status, the call status and the system configuration of existing systems on a user defined intervals.
- Symptoms:
 - The system information and system status in TMS is outdated.
- How to fix:
 - Restart the service, if that doesn't work restart the server.
 - Logs are found in \tmsdebug\log-TMSDatabaseScanner.txt

b) TMSLiveService

- What it does:

This service will set up launch and monitor a scheduled conference

- Symptoms:
The call does not start and the log in Conference Control Center is almost empty
 - How to fix:
 - Restart the service, if that doesn't work restart the server.
 - Logs are found in \tmsdebug\log-liveservice.txt
- c) TMSPLCMDirectoryService
- What it does:
This service is responsible for posting phonebooks to Polycom endpoints
 - Symptoms:
You don't get any phonebooks on you Polycom endpoint
 - How to fix:
 - Restart the service, if that doesn't work restart the server.
 - Logs are found in \tmsdebug\log-plcmdir.txt
- d) TMSSchedulerService
- What it does:
This service is responsible for launching events at set times. Events like system restore, system upgrade, call launch
 - Symptoms:
Scheduled events do not start
 - How to fix:
 - Restart the service, if that doesn't work restart the server.
 - Logs are found in c:\tmsdebug\log-schedulerservice.txt
- e) TMS Snmp Service
- What it does:
This service is collecting traps from the endpoints and is putting them directly into the database. It is also responsible for broadcasting SNMP messages to discover newly added systems.
 - Symptoms:
The statistics are empty
 - How to fix:
 - Restart the service, if that doesn't work restart the server.
 - Logs are found in \tmsdebug\log-watchdog.txt
- f) TMSProvisioningService
- What it does:
This service starts the local TMS-Agents and it is needed for provisioning
 - Symptoms:
Unable to create or edit groups or users within TMS on page Systems > Provisioning > Directory
 - How to fix:
 - Restart the service, if that doesn't work restart the server.
 - Logs are found in \tmsdebug\log-provisioningservice.txt

If you are using the Legacy TMS Agent, the OpenDS Log files can be located in the following path:

- Windows Server 32bit OS = *C:\Program Files\TANDBERG\TMS\Provisioning\OpenDS-2.0\logs*
- Windows Server 64bit OS = *C:\Program Files (x86)\TANDBERG\TMS\Provisioning\OpenDS-2.0\logs*

Phonebook (Corporate Directory) Common Errors

Common errors which may see with Phonebook service on TelePresence Management Suite. May see following errors on the endpoint if corporate directory is not working properly:

Message	Explanation or Suggested Solution
Request timed out, no response	<ul style="list-style-type: none"> The TMS server is busy, try again.
Warning: directory data not retrieved: 404	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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 will not allow it to retrieve any phone books.
Request timed out, no response	<ul style="list-style-type: none"> The endpoint is configured with the IP address of a non existing web server.
No contact with server	<ul style="list-style-type: none"> The IIS is restarting or in a state where corrupted messages are received.

Upgrading from a previous TelePresence Management Suite version

- Upgrading of the TelePresence Management Suite software itself is handled automatically by the TelePresence Management Suite installer. Some additional steps may be required to complete the upgrade depending on the previous version used.
- Important:** For detail please refer to the installation guide or the version specific Upgrade Notes

Security patch for TelePresence Management Suite Server Appliance

- Cisco will release a patch specifically for the Server Appliance within one calendar week of Microsoft's patch release. This file will only include relevant patches that need to be applied to the Server Appliance to patch the components the system uses to achieve the Cisco specific functionality. All patches released from Cisco are tested to ensure there are not effects on functionality from the Server Appliance.
- Please visit the following link for more detail information:
<http://www.tandberg.com/support/video-conferencing-security.jsp>

Compatibility with existing Integration Portfolios

- TelePresence Management Suite Integration Compatibility matrix for TMS12.6.x and TMS13.0:

Product	Compatible Version
TANDBERG See&Share	Version 3.3
TelePresence Management Suite Microsoft Exchange Integration	All Version
TelePresence Management Suite Microsoft LCS Integration	All Version
TelePresence Management Suite Conferencing Extensions	All Version
TelePresence Management Suite – IBM Lotus Notes Integration	All Version
TelePresence Management Suite – IBM Louts Sametime Integration	All Version

TelePresence Management Suite Movi for IBM Louts Sametime	All Version
TelePresence Management Suite 3 rd Party Booking API	All Version

Uninstall TelePresence Management Suite

- Uninstalling TMS will remove the TMS application, website, and services. It will leave any customer data, logs, databases and database servers intact for use in future upgrades. If you wish to completely remove all TMS information from the server, please refer to installation guide for more details.
- Uninstalling the TMS Application:
Start the uninstall wizard by selecting 'Uninstall TMS' from the TANDBERG Program Group in the Start Menu or by using Add/Remove Programs under the Windows Control Panel.

Useful TelePresence Management Suite Related Document References

Most of the documents below can be found in the TelePresence Management Suite Software package

- Software Release Note
- Installation and Getting Started
- Administrator Guide
- Product Support Document
- Redundancy Configuration and Overview (Fail-over or redundancy setup)
- Secure Server for TMS (Hardening Win 2003 server)
- TANDBERG Secure Management (Secure communication on TANDBERG products)
- 3rd Party Booking API (For programmer references)

Logs – Telepresence Management Suite

The logs in the diagram below should be included on initial support requests for each scenario.

Logs \ Scenario	Install issue	SQL issues	IIS issues	Provisioning Extensions	OpenDS issues	TMS services issues	Polycm integration issues	SNMP issues	Add system issues	Phonebook issues	Analytics Extension	Conference problems
Folders (Please compress all files in the folders to a .ZIP etc.)												
%TMSINSTALL%\wwwTMS\Data\Log												
%TMSINSTALL%\Provisioning\OpenDS-2.0\logs												
%TMS%\Analytics_Extension\AdminWeb\App_Data\Log												
%TMS%\TMSProvisioningExtension\app\logs												
From TMS Web User Interface												
"TMS Agent Diagnostics"												
Screenshots of the error												
Endpoint/MCU Call Log												
Scheduled Conference Cache												
Scheduler Events												
Scheduled Calls												
Call Details Records (CDR)												
Conference Event log												
Other devices												
TMS TCPDUMP												
Endpoint(s) Xstatus												
Endpoint(s) Xconfiguration												
Endpoint(s) "syslog"												
Endpoint(s) TCPDUMP												
SQL Log												
Other useful information												
Network diagram												
Windows Event Viewer logs (Everything, except security)												
Screenshot of the problem												
Ping												
ASP .NET/IIS logs												
%SystemDrive%\inetpub\logs\LogFiles												

* For more information, please see the introduction section "Logs framework diagram symbols"

How to capture logs from Conductor

Event Log

The Conductor provides an event logging facility for troubleshooting and auditing purposes. This Event Log is a list of all the events that have occurred on your system since the last upgrade and records information about such things as conference creation and deletion, requests to join a conference, alarms raised, and MCU status changes. It may also contain system-level information.

The Event Log holds 2GB of data; when this size is reached, the oldest entries are overwritten. However only the first 50MB of event log data can be displayed through the web interface.

The **Event Log** page (**Status > Event Log > All**) lets you view and search the Event Log. The other sub-menus under the **Status > Event Log** menu provide you with a filtered view of the Event

Log as follows:

- **Conference creation events** shows only those events relating to the creation of new conferences
- **Conference join events** shows only those events relating to users joining a conference
- **Conference destruction events** shows only those events relating to a conference being destroyed

Diagnostics logging

The **Diagnostic logging** tool (**Maintenance > Tools > Diagnostic logging**) can be used to assist in troubleshooting system issues. It allows you to generate a diagnostic log of system activity over a period of time, and then to download the log so that it can be sent to your Cisco customer support representative.

To use this tool:

1. Go to the **Diagnostic logging** page.
2. Click **Start new log**.
3. (Optional) Enter some **Marker** text and click **Add marker**.
 - The marker facility can be used to add comment text to the log file before certain activities are performed. This helps to subsequently identify the relevant sections in the downloaded diagnostic log file.
 - You can add as many markers as required, at any time while the diagnostic logging is in progress.
 - Marker text is added to the log with a "**DEBUG_MARKER**" tag.
4. Reproduce the system issue you want to trace in the diagnostic log.
5. Click **Stop logging**.
6. Click **Download log** to save the diagnostic log to your local file system. You are prompted to save the file (the exact wording depends on your browser).
7. Send the downloaded diagnostic log file to your Cisco support representative, if you have been requested to do so.

Note that:

- Only one diagnostic log can be produced at a time; creating a new diagnostic log will replace any previously produced log.
- The Conductor continually logs all system activity to a unified log file. The diagnostic logging facility works by extracting a portion of this unified log. On busy systems the unified log file may become full over time and will discard historic log data so that it can continue logging current activity. This means that all or part of your diagnostic log could be overwritten. The system will warn you if you attempt to download a partial diagnostic log file.
- The diagnostic log will continue logging all system activity until it is stopped, including over multiple login sessions and system restarts.

Clustered systems

Diagnostic logging can also be used if your Conductor is a part of a cluster, however some activities only apply to the "current" peer (the peer to which you are currently logged in to as an administrator):

- Each cluster peer maintains its own unified log, and logs activity that occurs only on that peer.
- The start and stop logging operations are applied to every peer in the cluster, regardless of the current peer.
- Marker text is only applied to log of the current peer.
- You can only download the diagnostic log from the current peer.
- To add markers to other peers' logs, or to download diagnostic logs from other peers, you must log in as an administrator to that other peer.

Enabling and disabling access over SSH

By default, the root account can be accessed over either a serial connection or SSH.

To enable and disable access to the root account using SSH:

1. Log in to the Conductor as **root**.
2. Type one of the following commands:
 - **rootaccess -s on** to enable access using SSH
 - **rootaccess -s off** to disable access using SSH
3. Type **exit** to log out of the root account.

If you have disabled SSH access while logged in using SSH, your current session will remain active until you log out, but all future SSH access will be denied. The only way you can then re-enable SSH access is to log in using a serial connection and run the **rootaccess -s on** command.

Resetting forgotten passwords

Note: the username and password for the administrator account is replicated across peers in a cluster. Therefore if you change the username or password on one peer, it will be changed on all other peers. The root account password is not replicated across peers.

If you have forgotten the password for either the **administrator** or the **root** account, you can reset it using the following procedure:

1. Connect a PC to the Conductor using the serial cable as per the “[Configuration using a serial cable](#)” below.
2. Restart the Conductor.
3. Log in from the PC with the username **pwrec**. No password is required.
4. When prompted, select the account (*root* or *admin*) whose password you want to change.
5. You will be prompted for a new password.

The **pwrec** account is only active for one minute following a restart. After that time you will have to restart the system again to change the password.

Configuration using a serial cable

To set the initial configuration using a PC connected to the Cisco TelePresence Conductor **DATA** port via a serial cable:

1. Connect the Ethernet LAN cable from the **LAN1** port on the front of the unit to your network.
2. Connect the supplied serial cable from the **DATA** port on the front of the unit to the serial port on a PC.
3. Start a terminal emulator program on the PC and configure it to use the PC's serial port as follows:
 - baud rate: 115200 bits per second
 - data bits: 8
 - parity: none
 - stop bits: 1
 - flow control (hardware and software): none



Do not leave a terminal emulator session open after it is no longer in use. An open session may cause issues during a system restart.

4. Turn on the power switch on the back right of the unit (adjacent to the power cable). The system will power up. If the unit does not start after 3 seconds, press the soft power button on the back left of the unit.

5. Wait until:

- the green PWR LED on the front of the unit is a steady green color (it may flash briefly during power up)
- the red ALM LED on the front of the unit has gone out
- the default IP address (192.168.0.100) is showing in the display panel on the front of the unit

6. Login

Logs – Conductor

The logs in the diagram below should be included on initial support requests for each scenario.

Logs \ Scenario	<i>Reboot issues</i>	<i>Conference setup</i>	<i>Network problems</i>
<i>Diagnostics log</i>			
<i>Event log</i>			
<i>TCPDUMP</i>			
<i>Screenshot</i>			
System Snapshot			
<i>Status</i>			
<i>Logs</i>			
<i>Full</i>			
Tools			
<i>Nslookup</i>			
<i>Ping</i>			
<i>Trace route</i>			
Other devices			
<i>VCS(s) Xstatus</i>			
<i>VCS(s) Xconfiguration</i>			
<i>VCS(s) diagnostics log (DEBUG)</i>			
<i>VCS(s) diagnostics interworking log (DEBUG)</i>			
<i>VCS(s) TCPDUMP</i>			
<i>MCU logs</i>			
Other useful information			
<i>Network diagram</i>			

* For more information, please see the introduction section “Logs framework diagram symbols”

How to capture logs from Advanced Media Gateway

Event Log

The last 2000 status messages generated by the AM gateway are displayed in the Event log page ([Logs > Event log](#)). Usually these are information messages, although occasionally Warnings or Errors may appear in the Event log. The presence of such messages is not cause for concern necessarily; if you are experiencing a specific problem with the operation or performance of the AM gateway, Cisco customer support can interpret logged messages and their significance for you.

You can:

- Change the level of detail collected in the traces by editing the Capture filter page. You should not modify these settings unless instructed to do so by Cisco customer support
- Display the log as text: go to [Logs > Event log](#) and click Download as text
- Change which of the stored Event log entries are displayed by editing the [Display filter page](#)
- Send the event log to one or more syslog servers on the network for storage or analysis. The servers are defined in the Syslog page
- Empty the log by clicking [Clear log](#)

Syslog

You can configure the AM gateway to send event messages to up to four syslog servers. To add or remove a syslog server, go to [Logs > Syslog](#) and make the changes you require (see Logging using syslog).

SIP log

The SIP log page records every SIP message received or transmitted from the AM gateway. The log can be exported in an .xml file.

By default the SIP log is disabled because it affects performance, but Cisco customer support may ask you to enable it if there is a problem with an AM gateway in your network.

CDR log

The CDR log includes all stored Call Detail Records, and all available details, regardless of the current filtering and display settings. You can download all or part of the CDR log in XML format using the web interface. When you start logging, the download button shows the range of record numbers but the delete button is grayed out until the log holds a certain number of logs.

To download the CDR log, click Download as XML to download all the log or Download X to Y as XML to download a range of events. (Note that if there are a large number of logged Call Detail Records, it may take several seconds to download and display them all.)

Logs – Advanced Media Gateway

The logs in the diagram below should be included on initial support requests for each scenario.

Logs \ Scenario	<i>Reboot issues</i>	<i>Call setup (simple)</i>	<i>Call setup (complex)</i>	<i>Network problems</i>	<i>OCSr2/Lync</i>
<i>Configuration.xml</i>					
<i>Event log</i>					
<i>SIP log</i>					
<i>Serial Log</i>					
<i>CDR log</i>					
<i>TCPDUMP</i>					
<i>Screenshot (Media stats)</i>					
<i>Diagnostics file</i>					
Other devices					
<i>VCS(s) Xstatus</i>					
<i>VCS(s) Xconfiguration</i>					
<i>VCS(s) diagnostics log (DEBUG)</i>					
<i>VCS(s) diagnostics interworking log (DEBUG)</i>					
<i>VCS(s) TCPDUMP</i>					
<i>OCS SIP Log</i>					
Other useful information					
<i>Network diagram</i>					

* For more information, please see the introduction section “Logs framework diagram symbols”

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

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

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

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

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

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

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

© 2012 Cisco Systems, Inc. All rights reserved.