Cisco TelePresence Infrastructure Technical Handbook

Technical Support Guide

D14485.10

March 2011

Contents

Document revision history

Revision	Date	Description
D14485.09	February 2011	- Reformat from TP Solution Support – APAC TP Infrastructure Handbook Rev 1.8 version. - Migrated TANDBERG Management Suite Handbook Rev 1.2 version into TelePresence Infrastructure Handbook.
D14485.10	March 2011	- Corrected Baud Rate for TelePresence Server/TelePresence MCU/TelePresence ISDN Gateway/TelePresence IP Gateway/IPVCR

Introduction

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

Information on service request

To ensure Cisco TelePresence TAC to assist technical service request and provide quick resolution, TelePresence TAC require a minimum amount of information for each service request.

When reporting the technical service request, please ensure:

- Describe in detail about problem/issue
- Describe how often the problem occurs
- Describe the latest operation before problem occurs, if any
- Describe in detail, 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)
- Describe 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 is multiple terminal software that may use for retrieving the log from system:

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)

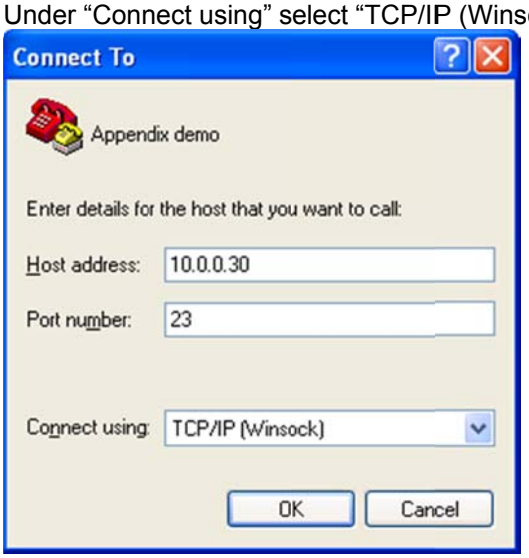
Download the Putty installation file from
http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

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.

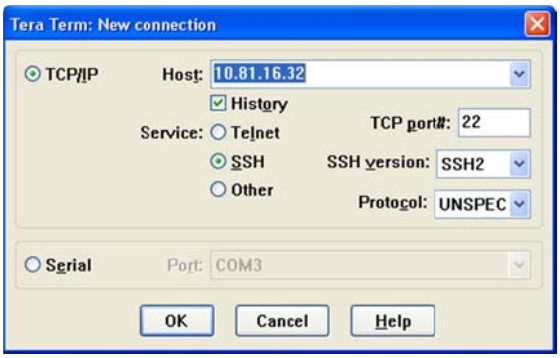


3. Default password is cisco, TANDBERG or blank unless changed. Some Infrastructure products have “admin” or “root” as login name.
4. To save retrieve logs: Enable the Capture Text option (menu “Transfer” – “Capture Text”), and save it as a *.log file.
5. Type in the respective commands described in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

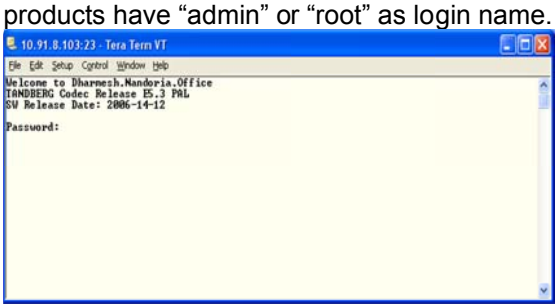
How to use TeraTerm

This following page explains how to use TeraTerm.

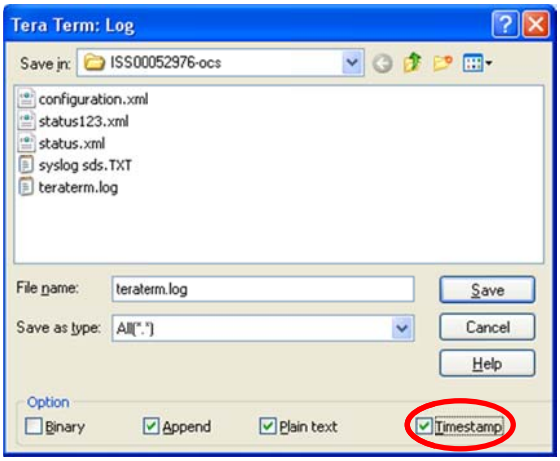
1. Start TeraTerm: Start Menu – All Programs – TeraTerm Pro with TTSSH2 – TeraTerm Pro (if install software as default setting).
2. Select “Telnet” and enter the System IP address in “Host”.
   (Or select “SSH” and enter the System IP address in “Host” in order to establish SSH connection between systems.)



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]).

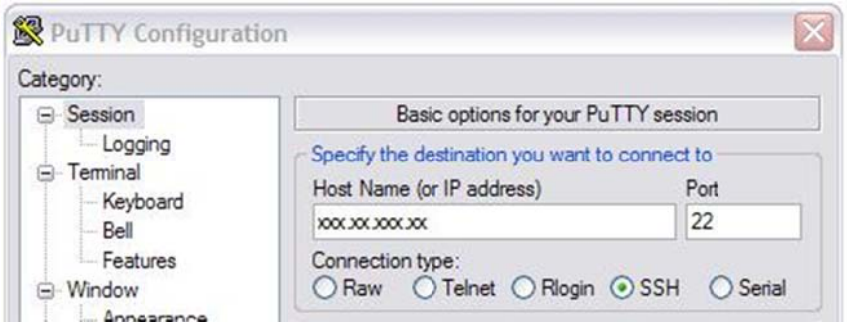


5. Type in the respective commands described in Appendix.

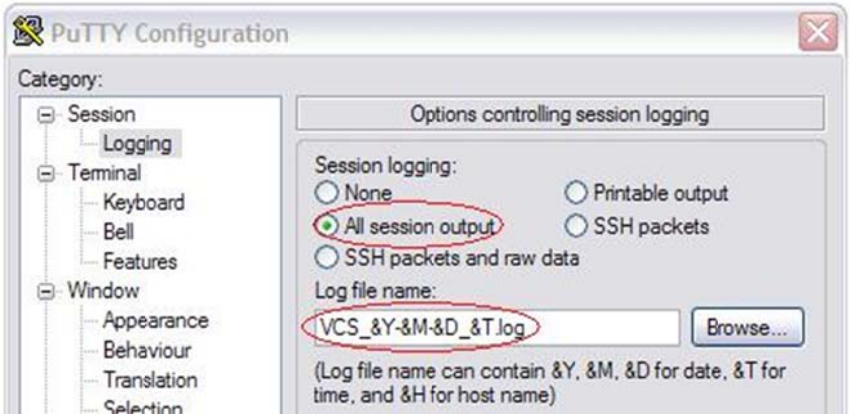
How to use Putty

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 is multiple file transfer software that may use for retrieving the log from system or/and uploading file to system:

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

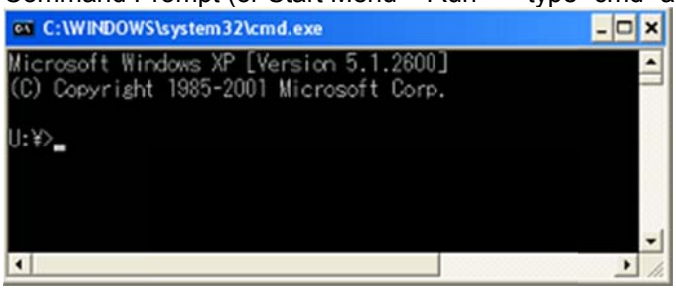
Download the WinSCP installation file from http://winscp.net/eng/index.php

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”)

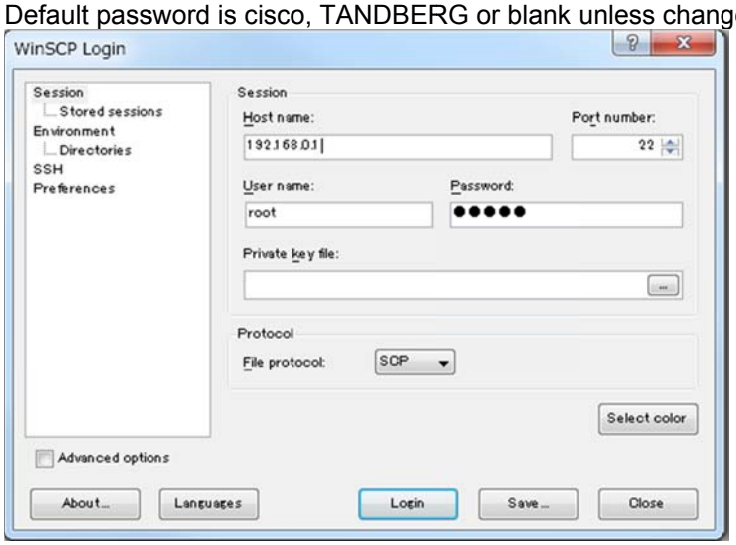


2. Navigate location for saving download file or file folder which to upload to system by using “cd” command.
   For example, save the download log to log folder under C drive on PC, “cd C\log”.
3. Establish ftp connection by using “ftp <ip address>” command.
4. Default password is cisco, TANDBERG or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

How to use WinSCP

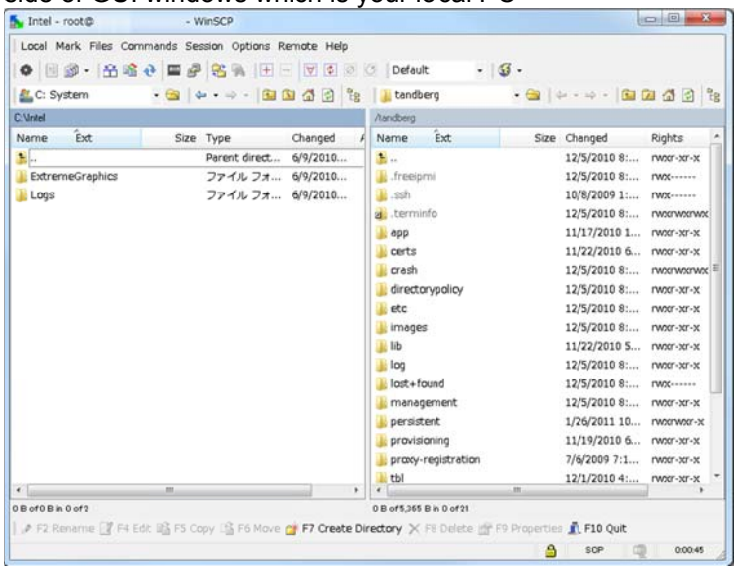
This following page explains how to use WinSCP

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



Sniffer 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 is multiple sniffer software that may use for retrieving the log from system:

Wireshark (IP packet sniffer)

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

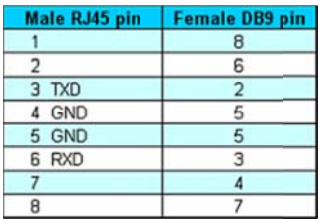
Wireshark is the network protocol analyzer, and is standard across industries.

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	

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

<table>
<tr><th>Model</th><th colspan="2">Parameter</th></tr>
<tr><td rowspan="8">Media Processing System (MPS)</td><td>Baud Rate</td><td>9600 bps</td></tr>
<tr><td>Data Bits</td><td>8</td></tr>
<tr><td>Parity</td><td>None</td></tr>
<tr><td>Stop Bits</td><td>1</td></tr>
<tr><td>Flow Control</td><td>None</td></tr>
<tr><td>Interface</td><td>RJ45 interface (COM1) on front of System Control Blade</td></tr>
<tr><td>Note</td><td>Require RJ45-D-Sub9pin cable for console connection</td></tr>
<tr><td>Pin Assignment</td><td>
<table>
<tr><th>Male RJ45 pin</th><th>Female DB9 pin</th></tr>
<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>
</table>
</td></tr>
</table>

<table>
<tr><th>Model</th><th colspan="2">Parameter</th></tr>
<tr><td rowspan="8">TelePresence Server

TelePresence MCU

TelePresence ISDN Gateway

TelePresence IP Gateway

IPVCR</td><td>Baud Rate</td><td>38400 bps</td></tr>
<tr><td>Data Bits</td><td>8</td></tr>
<tr><td>Parity</td><td>None</td></tr>
<tr><td>Stop Bits</td><td>1</td></tr>
<tr><td>Flow Control</td><td>None</td></tr>
<tr><td>Interface</td><td>RJ45 interface on front of unit</td></tr>
<tr><td>Note</td><td>Require RJ45-D-Sub9pin cable for console connection</td></tr>
<tr><td>Pin Assignment</td><td>
<table>
<tr><th>Male RJ45 pin</th><th>Female DB9 pin</th></tr>
<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>
</table>
</td></tr>
</table>

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.

IP issues (H323/SIP)

Commands in bold

- Open the console/telnet/ssh session with VCS
- **xstatus**
- **xconfig**
- **netlog 2** (X3.x or prior software version, please use "**syslog 3**")
- Make a call and keep running until you have recreated the problem
- Hang up call
- **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 (**Maintenace > 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 (**Maintenace > Incident reporting > View**)

Note: Restart an incident report should be generate and will be avaliable 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 -I 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: DefaltValuesSet 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.

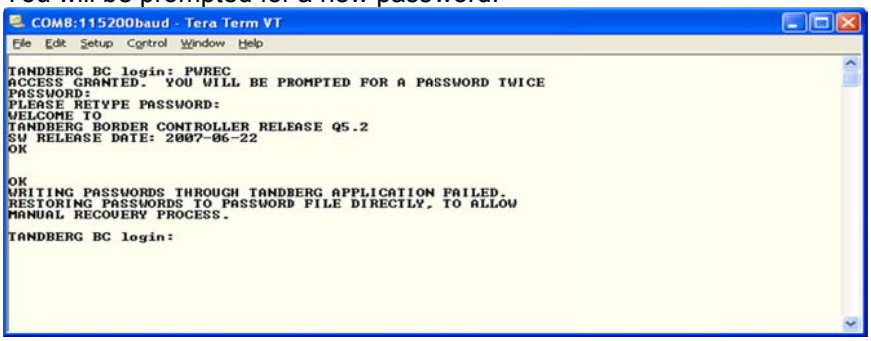
Note: The certificates and policy files are not removed.

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

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.



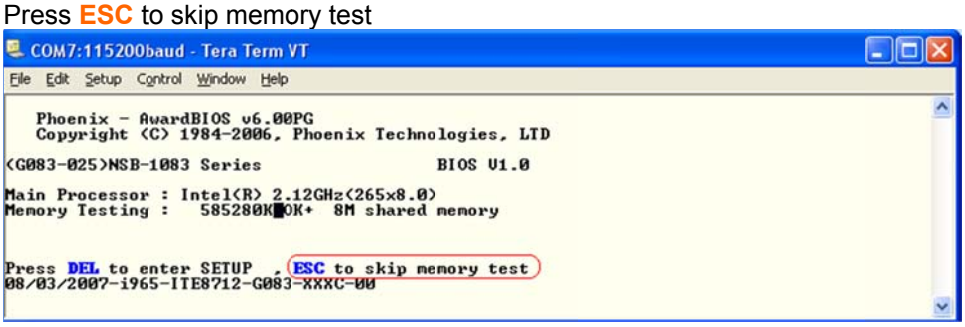
Note: The PWREC account is only active for one minute following a restart. Beyond that time you will have to restart the system again to change the password. Because access to the serial port allows the password to be reset, it is recommended that you install the GK/BC in a physically secure environment.

Revert back previous software version on VCS

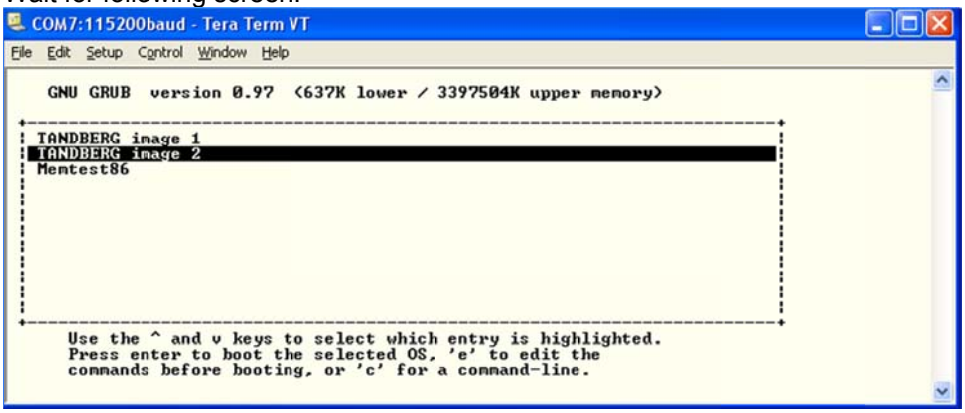
Commands in bold

- 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 (VCS) 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 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 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**

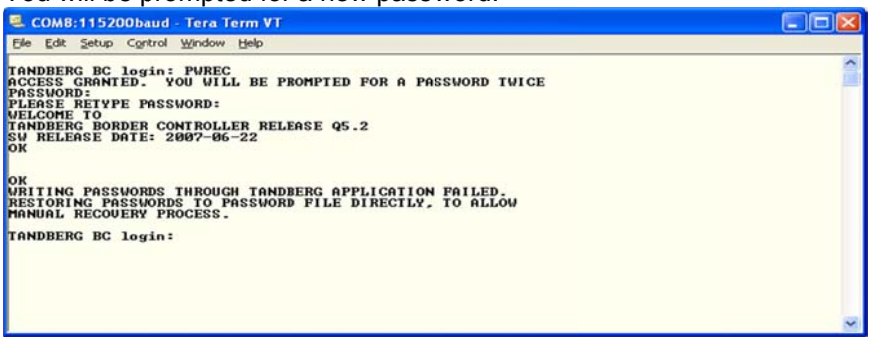
Note: DefaltValuesSet will not add the default links with which the system ships from the factory. The DefaultLinksAdd command will configure back default link between default zone/subzone. The certificates and policy files are not removed.

- 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.



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.

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.

Logs required for diagnostic/analysis

Below log should include on initial incident support request on each products and scenario.

Reported Problem		Required Logs						
		configuration.xml	Event Log	H.323 Log	Screen shot	diagnostic file	serial log	network capture (as request)
Codian MCU	Reboot	x				x	x	
	Call setup (simple case)	x	x	x				
	Call setup (complex case)	x	x	x				x
	Audio / Video	x	x	x	x			x
	Network problems	x	x		x			x
Codian ISDN GW	Reboot	x				x	x	
	Call setup (simple case)	x	x	x				
	Call setup (complex case)	x	x	x				x
	Audio / Video	x	x	x	x			x
	Network problems	x	x		x			x
Codian IPGW	Reboot	x				x	x	
	Call setup (simple case)	x	x	x				
	Call setup (complex case)	x	x	x				x
	Audio / Video	x	x	x	x			x
	Network problems	x	x		x			x

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**

    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.

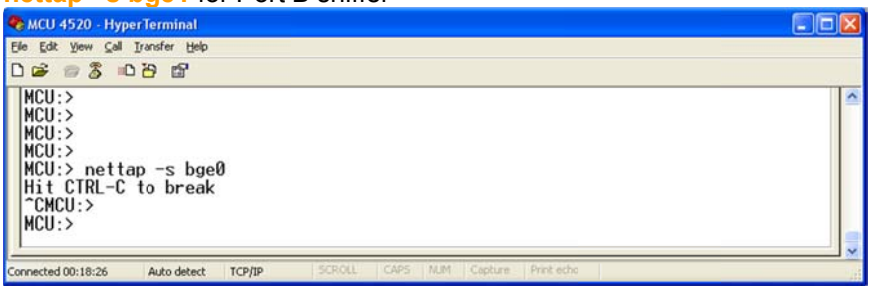
Note: Require 2.4 or newer released software on MCU.

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.

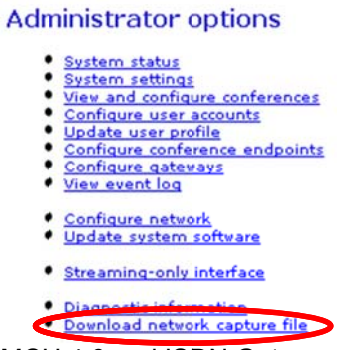
Important: Make sure to have compact flash card in the TelePresence MCU or ISDN/IP Gateway Products external slot.

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.



  - 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

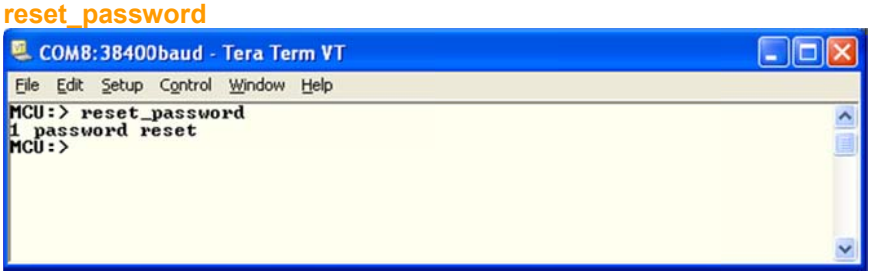
Reset Password on TelePresence MCU or IP/ISDN Gateway

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.

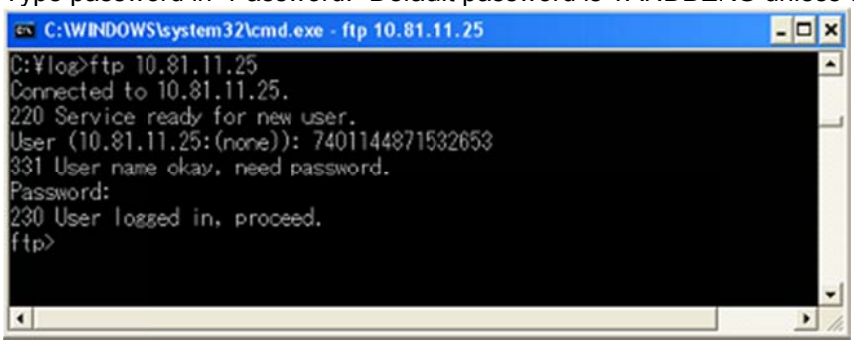
How to upgrade TelePresence MCU and IP/ISDN Gateway

This chapter explains how to upgrade TelePresence MCU and IP/ISDN Gateway by using ftp software or Compact Flash Card for in case of problem with upgrading software from WebGUI or TMS.

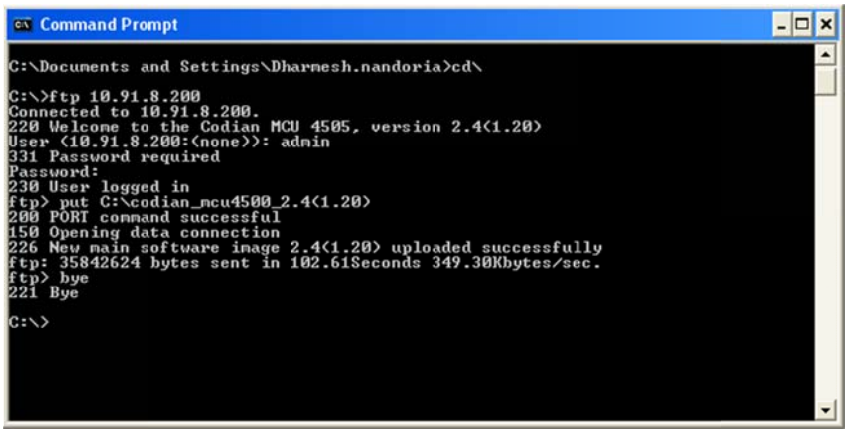
Upgrade software by using FTP software

Commands in bold

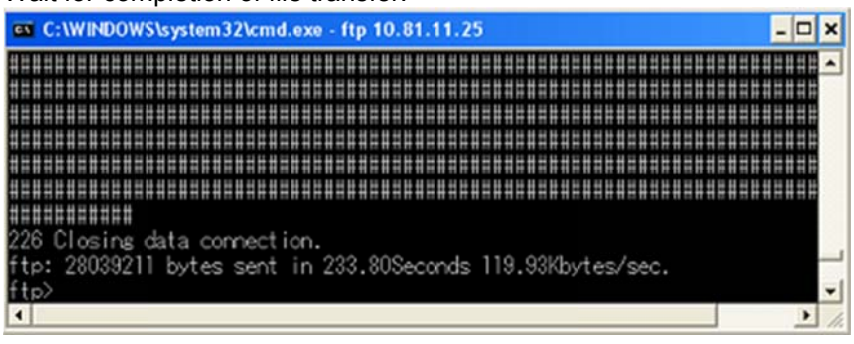
- Open Command prompt (may use any FTP client software)
- Change the directory, if necessary by using “cd” command
  For example, software folder locates under C drive on PC, then **cd C\software**
- **ftp <ipaddress>**
- Type **admin** in “User:”
- Type password in “Password:” Default password is TANDBERG unless changed.



- **hash**
- **bin**
- **put <softwarefile >** (or **put <location-of-software\software>**)
  For example, **put codian_mcu4500_2.4(1.20)**

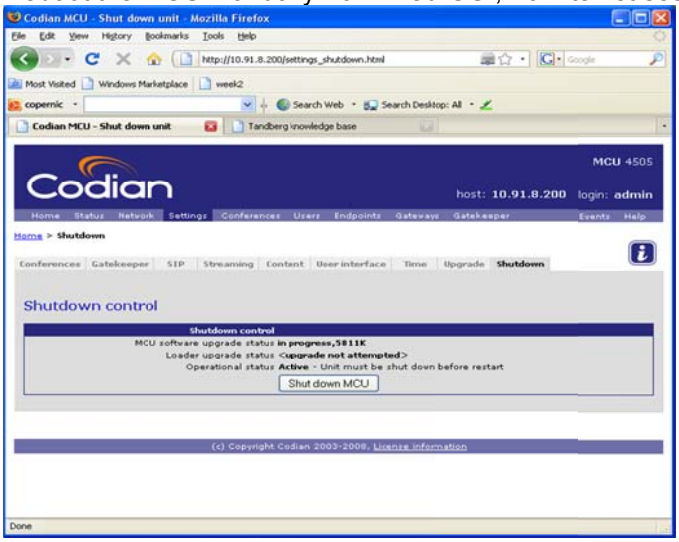


- Wait for completion of file transfer.



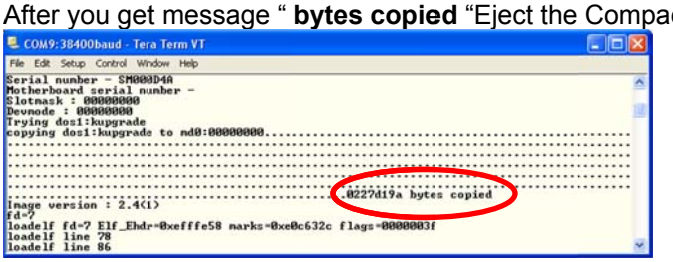
- **bye**

- Reboot the MCU manually from Web GUI, from telnet session, etc.



Upgrade software by using Compact Flash Card

- Extract the image from the .zip file to your hard drive and rename the extracted image to kupgrade.
- Obtain a Compact Flash card of between 32 and 256 Mb capacity, and some means of writing to it. USB compact flash card reader/writers are readily available.
- Copy kupgrade on to the Compact Flash card.
- Connect a serial terminal to the Console port of your unit using the connection settings on the unit's back label.
- Insert the Compact Flash card in to the slot on the unit's front panel and shutdown/restart the unit from the web interface.
- Watch the output on the serial terminal.
  After a few seconds, you will see several rows of '.....' appear, followed by a message telling you the number of bytes copied. This represents the copying of the kupgrade image from the external Compact Flash card to the unit's internal memory.
- After you get message " **bytes copied** "Eject the Compact Flash card from the external slot.



- The unit will complete the upgrade process and reboot of its own accord.

Important: If flash card is not removed then after reboot it will start upgrade process again.

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

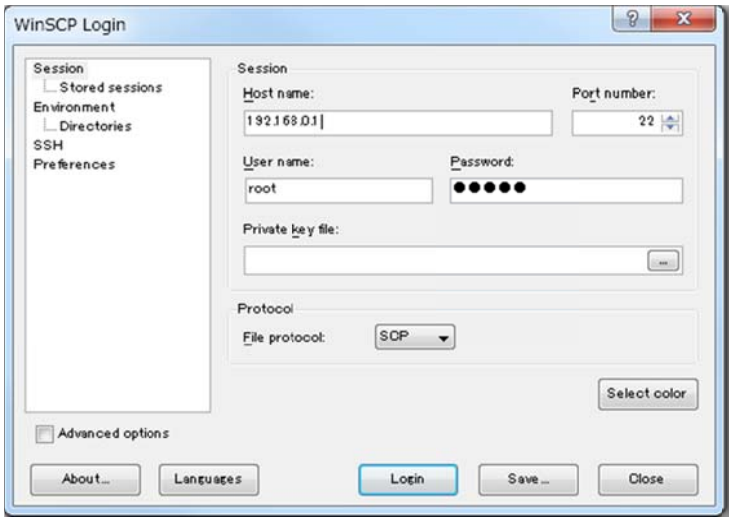
Commands in bold

- 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

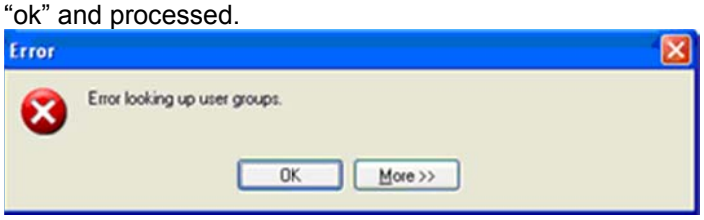
Reboot Issue

Commands in bold

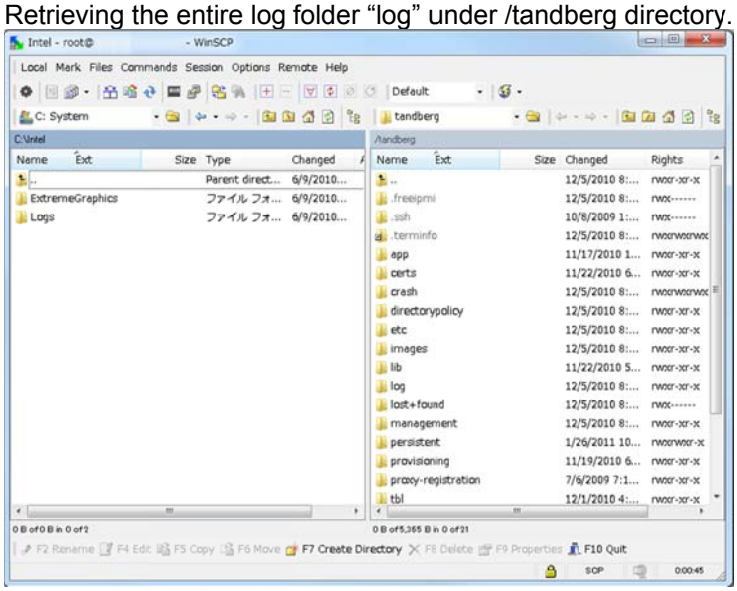
- Open the WinSCP session with MPS
- Login as “root” user



- 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.

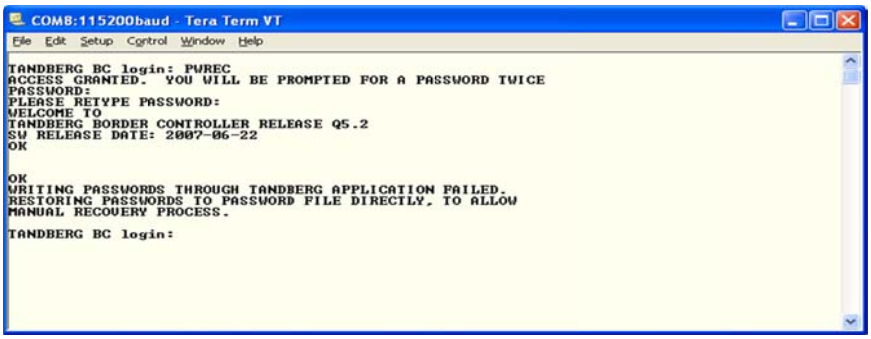


- Please do not open this folder. Simply drag it to your desktop, zip it and attached file to the ticket – Remember to name these or include a description.

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.



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 xxxxxxxxxxxxxxx > release-key** (xxxxxxxxxxxxxxx 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*>:/tm*p/tabasco-image.tar.gz*

  or

  pscp release-key root@<*MPS IP address*>:/tm*p/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**

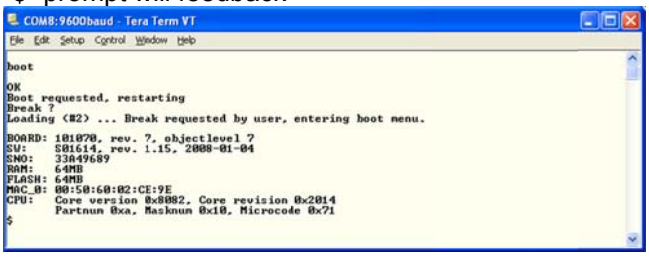
  or
- Download event. log file from root directory of MCU/GW
- Open Command prompt (and change home directory, if necessary)
- **ftp <ipaddress>**
- Default password is TANDBERG unless changed. Please enter any user name (e.g. admin) as login name.
- **hash**
- **bin**
- **get event.log**
- **bye**
- 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



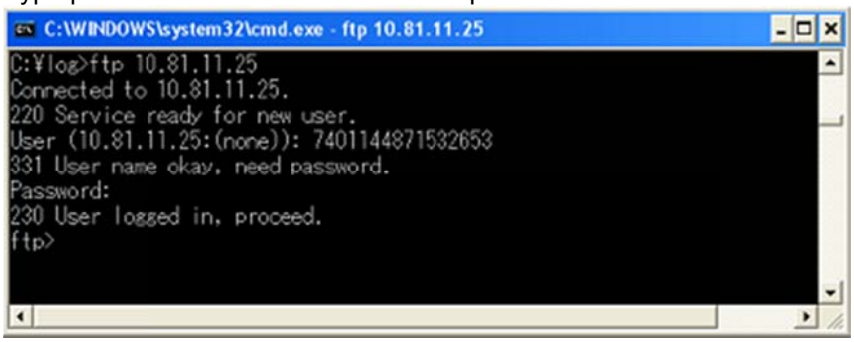
- **eee**
- **q**
- MCU/GW will automatically restart

How to upgrade Classic MCU/ISDN Gateway

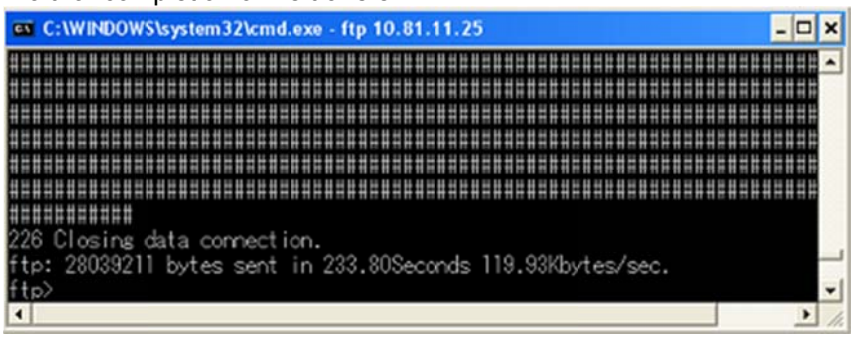
This chapter explains how to upgrade Classic MCU/ISDN Gateway by using ftp software for in case of problem with upgrading software from WebGUI or TMS.

Commands in bold

- Open Command prompt
- Change the directory, if necessary by using “cd” command
  For example, software folder locates under C drive on PC, then **cd C\software**
- **ftp <ipaddress>**
- Type software Release Key in “User:”
- Type password in “Password:”. Default password is TANDBERG unless changed.



- **hash**
- **bin**
- **put <softwarefile >** (or **put <location-of-software\software>**)
  For example, **put s40000d311.pkg**
- Wait for completion of file transfer.



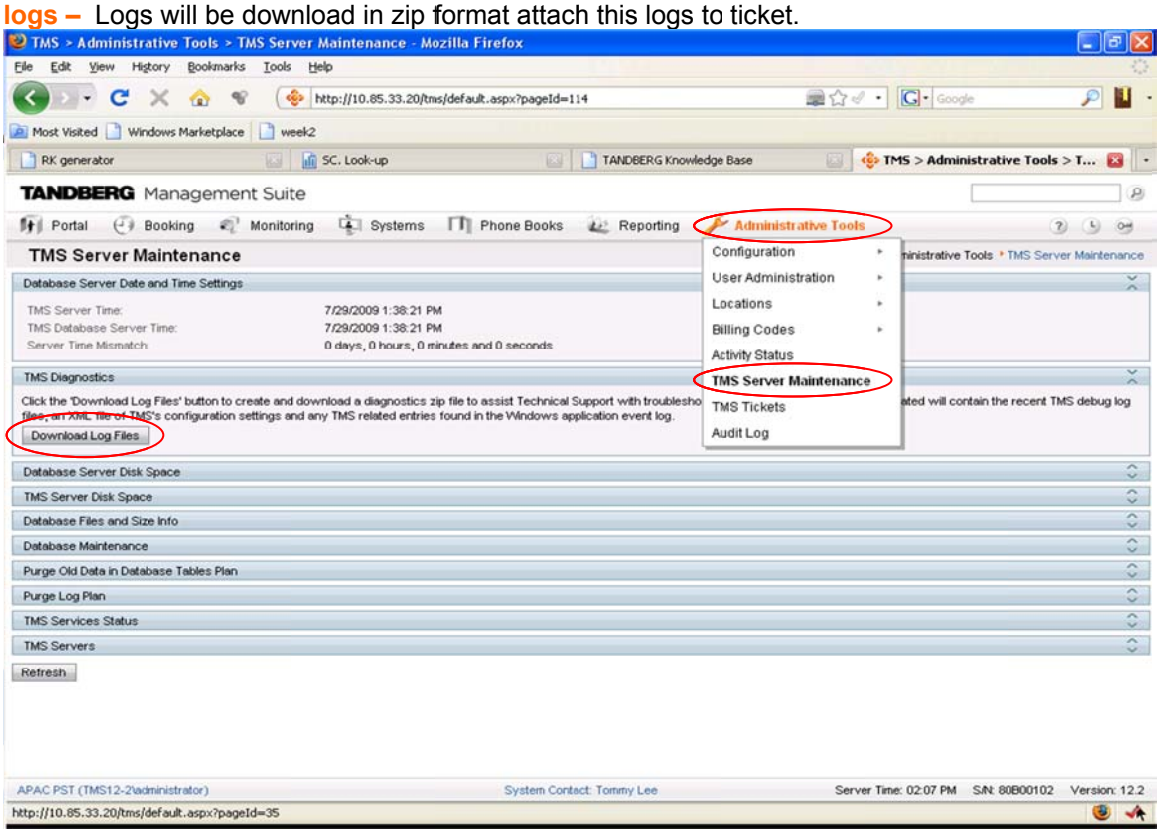
- **bye**
- Reboot the MCU manually from Web GUI, from telnet session, etc.

How to capture a log from TelePresence Management Suite

This chapter explains how to capture the complete log file available for TelePresence Management Suite logs, Provisioning Directory logs files, and Windows server logs. Also provide additional faultfinding information
All retrieved logs should attach to ticket including a description and 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.



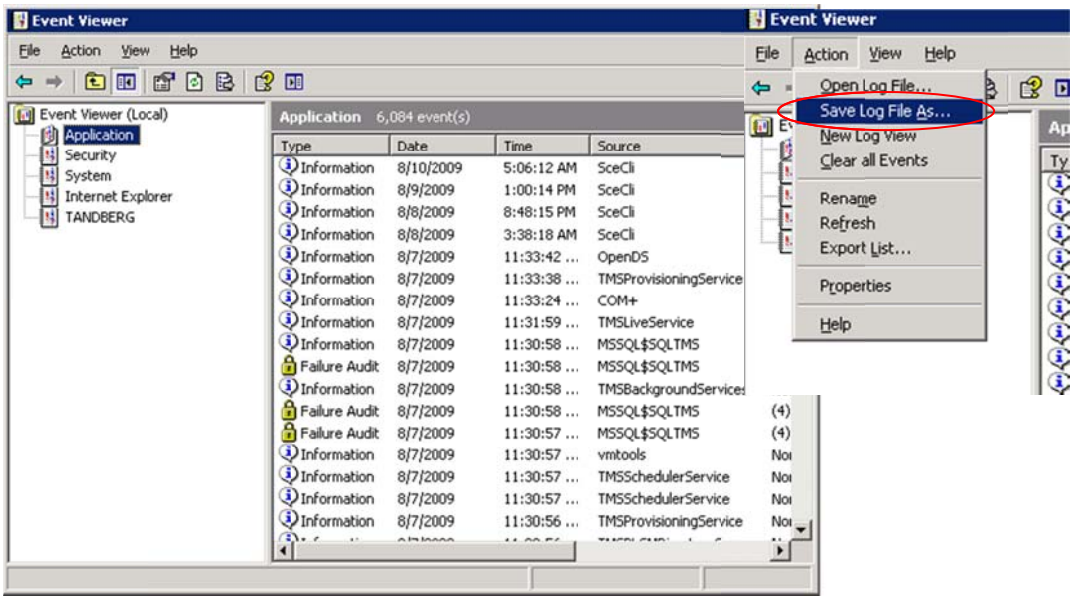
- The TMS Provisioning Directory Logs, logs TMS provides for Provisioning Directory can be found on the TMS server at the following location:
  C:\Program Files\TANDBERG\TMS\wwwTMS\Data\Logs\tmsdebug
  The name of the log files that you will want to look at with regards to the Provisioning Directory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

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	• 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 will not allow 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.

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 3rd 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)