TANDBERG

TANDBERG is now a part of Cisco

TANDBERG EX90 Administrator Guide

Thank you for choosing TANDBERG!

Your TANDBERG EX90 has been designed to give you many years of safe, reliable operation.

This part of the TANDBERG EX90 documentation is aimed at administrators working with the setup of the EX90.

Our main objective with this Administrator Guide is to address your goals and needs. Please let us know how well we succeeded!

May we recommend that you visit the TANDBERG web site regularly for updated versions of this guide.

The user documentation can be found on our web site. Go to: http://www.tandberg.com/docs.

TANDBERG is now a part of Cisco.

Introduction 3
Intellectual property rights 4
Trademark 4
Disclaimer 4
Patent information 4
Copyright notice 4
User documentation 4
System overview 5

Using the web interface 6
The web interface 7
Connect to the EX90 7
Password protection 7
The system information page 8
Software upgrade 9
Software versions 9
Software release notes and upgrade files 9
Release key 9
Option key 9
Advanced configuration 10
Custom wallpaper 11
File format and picture size 11
Upload the custom wallpaper file 11
Activate the new wallpaper 11
Making calls from the web interface 12
Uploading certificates 13
Viewing XML files 14
Log files 15

The Advanced Configuration 16
Description of the advanced configuration settings 17
The Audio settings 17
The Camera settings 17
The Conference settings 19
The H323 Profile settings 21
The Network settings 23
The NetworkServices settings 26
The Phonebook settings 28
The Provisioning settings 29
The SerialPort settings 30
The SIP Profile settings 30
The Standby settings 31
The SystemUnit settings 32
The Time settings 33
The Video settings 34
The Experimental menu 39

Appendices 40
Password protection 41
Setting the codec administrator password 41
Password protection of the web interface 41
Optimal Definition Profiles 42
CE Declaration for TANDBERG EX90 43
China RoHS table 44
Supported RFCs in SIP 45
Current RFCs and drafts supported in SIP 45
Media capabilities supported in SIP 45
Technical specifications 46

CHAPTER 1

INTRODUCTION

Intellectual property rights

This Administrator Guide and the Products to which it relates contain information that is proprietary to TANDBERG and its licensors.

Information regarding the Products is found on the page entitled License Agreements and Patent Information.

This Administrator Guide may be reproduced in its entirety, including all copyright and intellectual property notices, in limited quantities in connection with the use of the Products. Except for the limited exception set forth in the previous sentence, no part of this Administrator Guide may be reproduced, stored in a retrieval system, or transmitted, in any form, or by any means, electronically, mechanically, by photocopying, or otherwise, without the prior written permission of TANDBERG. Requests for such permission should be addressed to tandberg@tandberg.com.

Trademark

Trademarks used in this document are the property of their respective holders.

TANDBERG – is now a part of Cisco
Philip Pedersens vei 20
1366 Lysaker, Norway
Tel: +47 67 125 125 Fax: +47 67 125 234
E-mail: tandberg@tandberg.com

Disclaimer

The specifications for the Products and the information in this document are subject to change at any time, without notice by TANDBERG.

Every effort has been made to supply complete and accurate information in this Administrator Guide, however, TANDBERG assumes no responsibility or liability for any errors or inaccuracies that may appear in this document.

Patent information

The products described in this manual is covered by the following patents:

US7,499,416, US6,584,077, US5,838,664, US5,600,646, US5,003,532, US5,768,263, US5,991,277, US7,034,860, US7,295,613, US7,283,588, US7,512,708, EP1338127, EP1305927, US7,525,914

An updated list of the patents applying can be found on our web site.
Go to: ▶ www.tandberg.com/tandberg_pm.jsp .

Copyright notice

The product covered by this Administrator Guide is protected under copyright, patent, and other intellectual property rights of various jurisdictions. This prodt is Copyright © 2010, TANDBERG. All rights reserved. This product includes copyrighted software licensed from others.

For a complete oveview of the third party copyright and licenses, see the Legal and Safety Information document on the web. Go to: ▶ http://www.tandberg.com/docs

IMPORTANT: USE OF THIS PRODUCT IS SUBJECT IN ALL CASES TO THE COPYRIGHT RIGHTS AND THE TERMS AND CONDITIONS OF USE REFERRED TO ABOVE. USE OF THIS PRODUCT CONSTITUTES AGREEMENT TO SUCH TERMS AND CONDITIONS.

User documentation

We recommend you visit the TANDBERG web site regularly for updated versions of the user documentation. Go to: ▶ www.tandberg.com/docs

System overview

The system is delivered with:

- TANDBERG EX90 unit
- TANDBERG inTouch controller with cable
- Handset with cable
- Cables (VGA to DVI adapter, DVI-I cable, Stereo audio cable 3.5mm, Ethernet cable)
- AC Adapter and power cable

The camera can be tilted and used as a document camera.

TANDBERG EX90

TANDBERG inTouch controller unit

TANDBERG EX90, rear view

Detach the rear side cover when connecting cables.

When finished, snap on the rear cover.

A handset can be mounted to the inTouch EC unit.

The TANDBERG EX90 can be configured using the inTouch controller and from the web interface.

For full access to the configurable parameters, the web interface must be used—the inTouch controller provides access to a limited set of parameters only.

The web interface

The web interface allows for remote administration of the system.

Connect to the EX90

Open a web browser and enter the ***IP address*** of the codec.

How to find the IP address:

- To find the IP address, open the System Information page on the inTouch unit. Tap the icon in the lower left corner and select ***Settings*** > ***System Information***.

Password protection

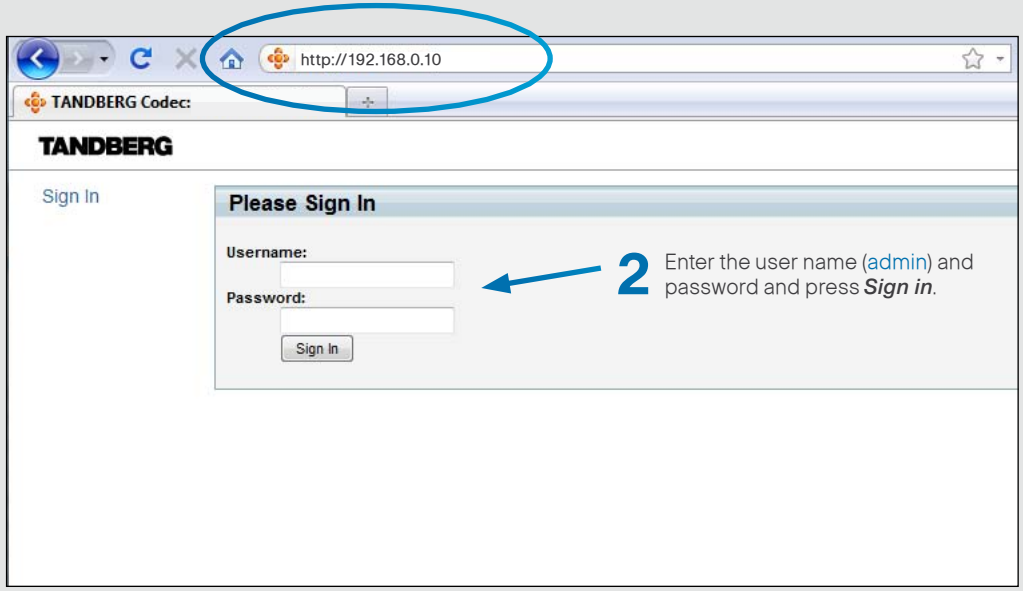
The web interface can be password protected. It uses the same user name and password as defined for the codec that is integrated in the EX90.

NOTE! If a codec password has been defined, be aware that after having defined or changed the administrator password, a reboot of the codec is required to activate the codec password on the web interface.

Read more about password protection in the Password Protection section in this guide.

If the web interface is password protected

1 Enter the IP address of the EX90.



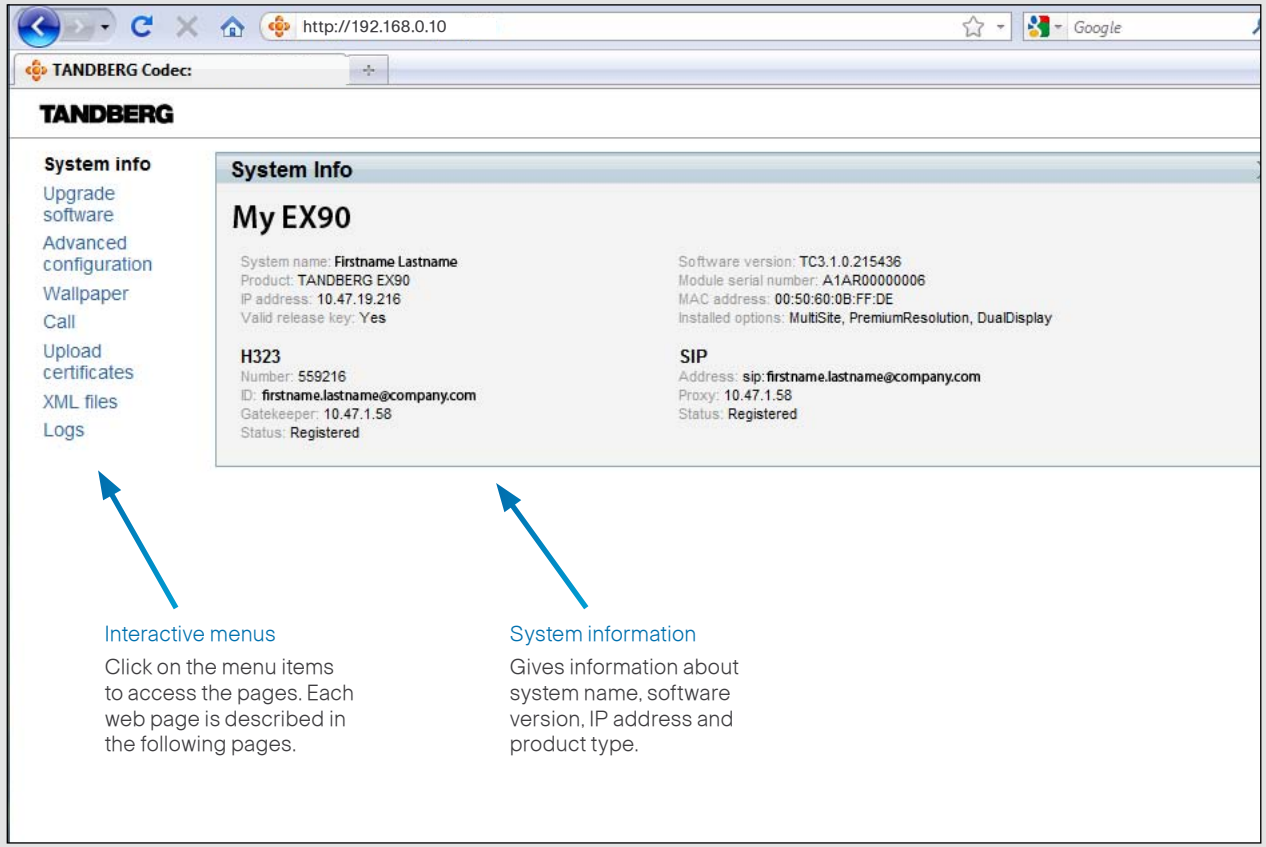
2 Enter the user name (admin) and password and press ***Sign in***.

The system information page

From the web interface you have the following menu options:

- System info
- Upgrade software
- Advanced configuration
- Wallpaper
- Call
- Upload certificates
- XML files
- Logs

System information



Interactive menus

Click on the menu items to access the pages. Each web page is described in the following pages.

System information

Gives information about system name, software version, IP address and product type.

Software upgrade

From this page you can do software upgrades and adding release key and option keys.

Software versions

The EX90 is using the TC software version TC3.1 or higher.

NOTE: Contact your system administrator if you have questions about the software version.

Software release notes and upgrade files

TANDBERG recommends reading the software release notes before upgrading the software. The software release notes and upgrade files are available from the TANDBERG ftp site.

Go to: ▶ http://ftp.tandberg.com/pub/software/endpoints/tc/

Release key

The release key is required to be able to use any of the released software.

Contact your TANDBERG representative to obtain the release key.

Option key

An option is required to activate any optional functionality, and you may have several option keys in your system. The options available are:

- Natural presenter
- Premium resolution
- Multisite
- Dual display

Contact your TANDBERG representative to obtain the option key(s).

Upgrade software

How to upgrade the software on the codec

1. Before you can start the upgrade you must download the software upgrade file. The file format: "s52000tc3_0_0.pkg" (each software version has a unique file name)
2. Click ***Browse..*** and select the .PKG file
3. Click the ***Upgrade*** button to start the installation.
4. Leave the system for a few minutes to allow the installation process to complete. You can follow the progress on this page. When the upgrade is successfully completed a message will appear.

How to add the release and option keys

Contact your TANDBERG representative to obtain the required key(s). If you will add both a release key and one or more option keys, the valid procedure will be:

1. Enter the ***release key*** and press ***Add***.
   The key format: "1TC001-1-0C22E348" (NOTE! This example is for illustration purpose only. Each system will have a unique key)
2. Enter the ***option key*** and press ***Add***.
   The key format: "1N000-1-AA7A4A09" (NOTE! This example is for illustration purpose only. Each system will have a unique key)
3. If you have more than one option key, add the remaining keys.
4. ***Reboot*** the codec.

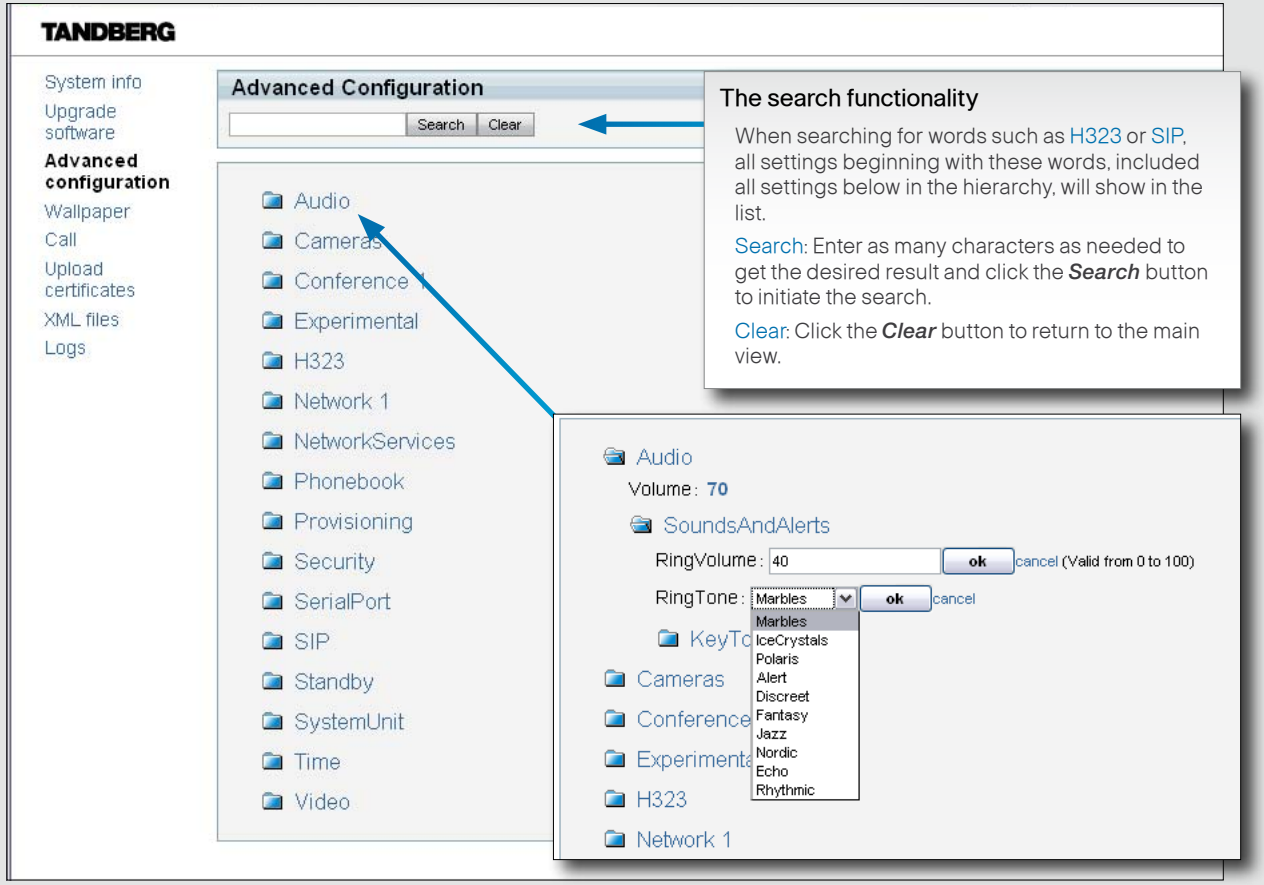
Advanced configuration

The web interface allows for remote administration of the system.

The Advanced configuration defines the system settings and are structured in a hierarchy, making up a database of system settings.

The system settings are explained in the Advanced configuration section in this guide.

Advanced Configuration



Edit: To change a value, click on the value to see the expanded view as shown above.

Value space: The value space is specified, either as a drop down list or as text, when you edit a value.

OK: Press the ***ok*** button to save the new value.

Cancel: Select ***Cancel*** to leave without saving.

Custom wallpaper

If you want the company logo or a custom picture to be displayed on screen, you may very well use a custom wallpaper.

File format and picture size

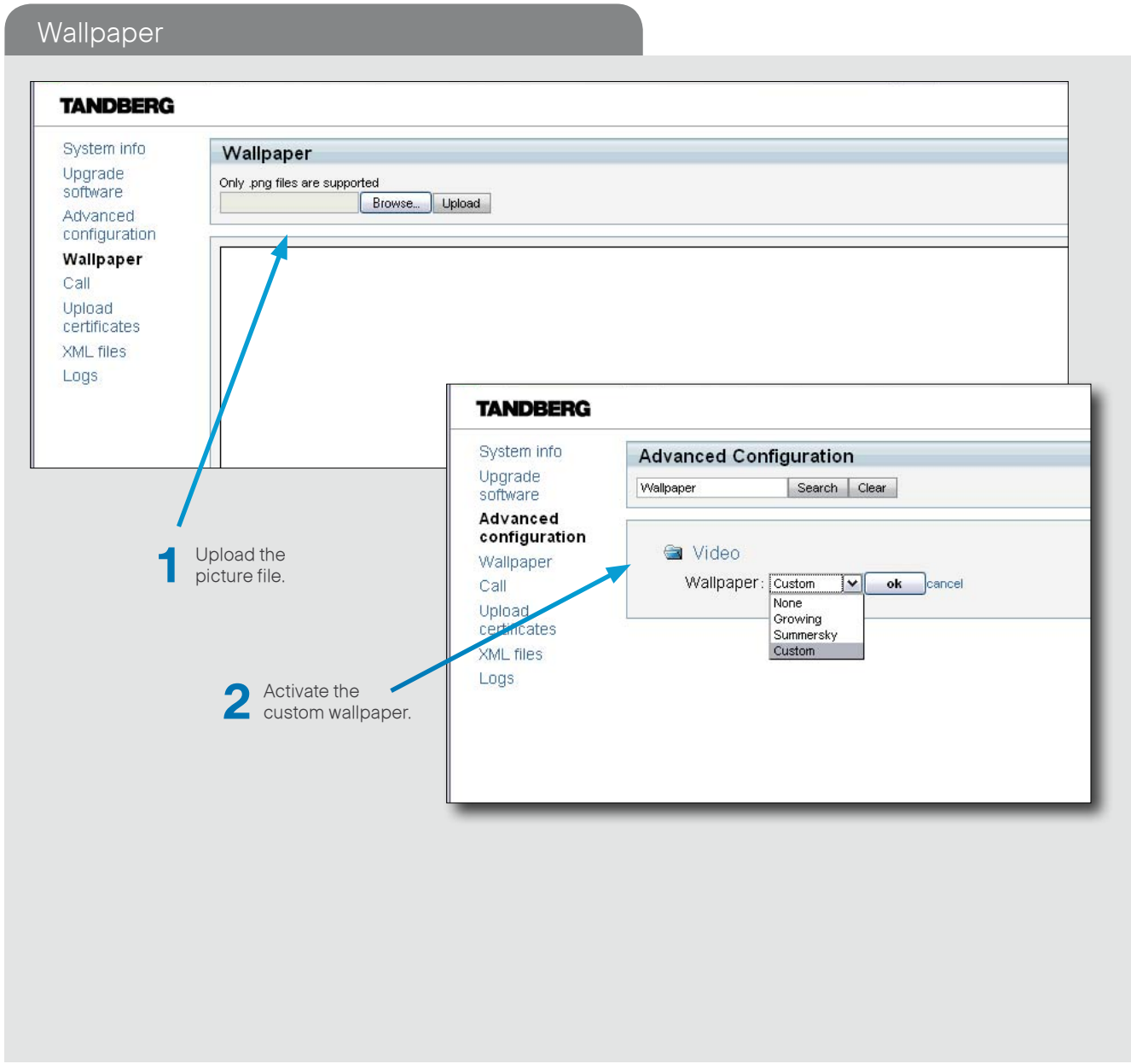
The picture file format for the custom wallpaper is PNG. The maximum size is 1920x1200pixels.

Upload the custom wallpaper file

1. Press ***Browse..*** and locate the wallpaper file (.PNG)
2. Press ***Upload*** to save the file to the codec.
3. Refresh the web page to see the wallpaper you just uploaded.

Activate the new wallpaper

1. Move to the ***Advanced configuration*** page and enter `wallpaper` in the search field. From the drop down list, select ***Custom***. The new wallpaper will be displayed on screen.
2. If the new wallpaper does not show on screen, you may have to toggle once between Wallpaper: ***None*** and ***Custom*** to make the change take effect.



Making calls from the web interface

After you have made all the configurations, from a remote location, is convenient to be able to make calls from the video system to ensure everything works as expected.

How to make a call

Input field: Enter one or more characters in the input field, until the name you want to call appears in the dynamic search list; or, enter the complete name or number.

Dial: Press ***Dial*** to initiate the call.

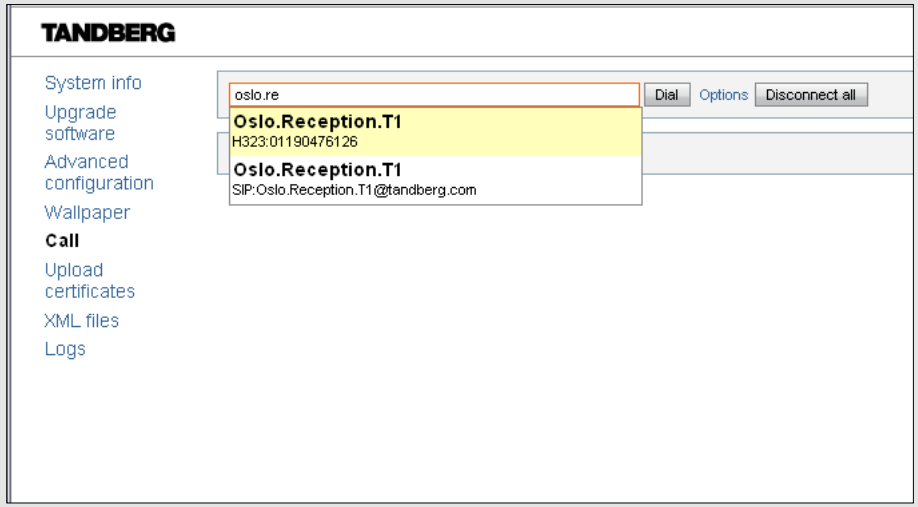
Disconnect all: Press ***Disconnect all*** to end all calls.

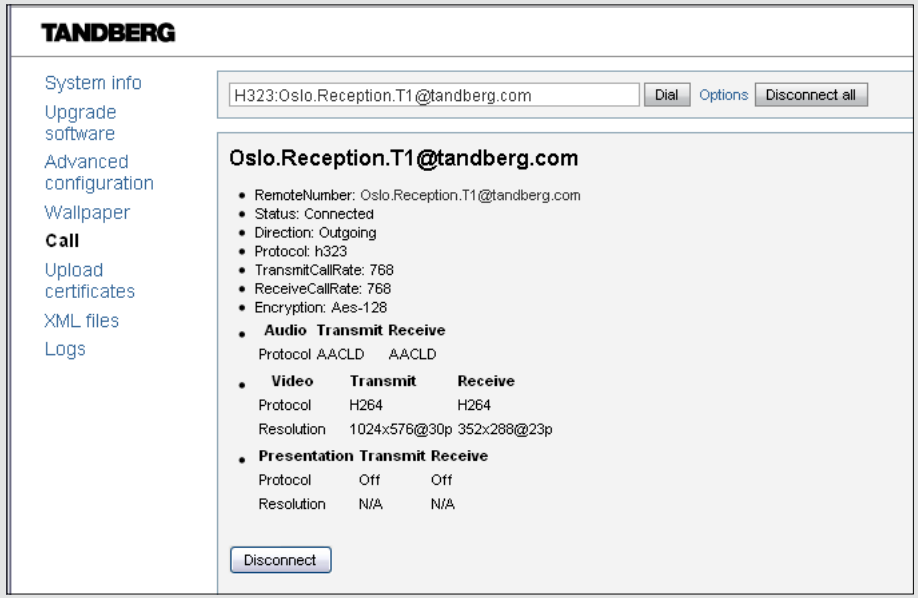
Options: Click ***Options*** to display the ***Call rate*** drop down list.

The call status page

- Remote number
- Status: Connected
- Direction: Incoming/Outgoing
- Protocol: H323/SIP
- Transmit and receive call rate
- Encryption
- Audio: transmit and receive protocol
- Video: transmit and receive protocol and resolution
- Presentation: transmit and receive protocol and resolution

Call and call status





Uploading certificates

A certificate is a text file which indicates a trusted third party (issuer or CA) verifying the authenticity of the unit.

Uploading the SSL certificate

To install the SSL certificate, you will need:

- HTTPS certificate (.PEM format)
- Private key (.PEM format)
- Passphrase (optional)

Contact your system administrator to obtain the required files.

- Click ***Browse...*** and locate the HTTPS certificate file (.PEM format)
- Click ***Browse...*** and locate the Private key file (.PEM format)
- Enter the ***Passphrase*** (optional).
- Click ***Upload*** to upload the certificates to the codec.

Uploading the Trusted CA certificate

To install the SSL certificate, you will need:

- Trusted CA list file (.PEM format)

Contact your system administrator to obtain the required file.

- Click ***Browse...*** and locate the file with the Trusted CA list (.PEM format)
- Click ***Upload*** to upload the certificate to the codec.

Upload certificates

Viewing XML files

The XML files are structured in a hierarchy building up a database of information about the codec.

- Select ***Configuration*** to see an overview of the system settings, which are controlled from the Advanced configuration menu, or from the API (Application Programmer Interface).
- The ***Status*** information is constantly updated by the system to reflect system and process changes. The status information is normally monitored from the API.
- Select ***Command*** to see an overview of the commands available to instruct the system to perform an action. The commands are issued from the API.
- The ***Directory*** file will be described later.
- Select ***Valuespace*** to see an overview of the value spaces.
- The ***Documentation*** file will be described later.

XML files

Log files

The log files are intended for support, and can be requested by TANDBERG when you are in contact with our support organization.

Current log files

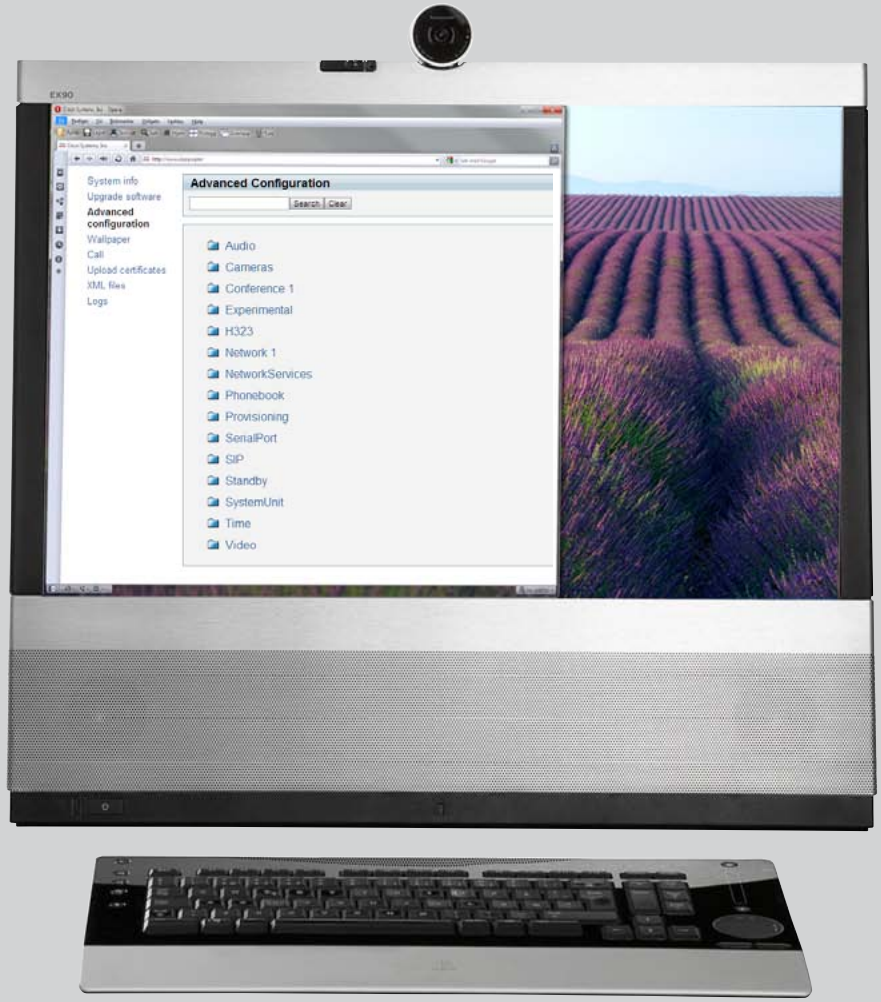
Time stamped event log files. Select ***Current log files*** and click on a text file to view the file or follow the instructions in the dialog box to save an application file.

Historical log files

Time stamped historical log files. Select ***Historical log files*** and click on a file and follow the instructions in the dialog box to save the application file.

Log files

The TANDBERG EX90 can be configured via the inTouch controller or via its web interface. For full access to the configurable parameters, the web interface must be used—the inTouch controller provides access to a limited set of parameters only.



CHAPTER 3

THE ADVANCED CONFIGURATION

Description of the advanced configuration settings

In the following pages you will find a complete list of the system settings which are configured from the Advanced configuration menu on the web interface. The settings are presented in the same order as listed in the menus. The examples shows either the default value or an example of a value.

Open a web browser and enter the IP address of the EX90. To find the IP address, see the System Information page on the inTouch controller. Open the inTouch menu and tap the Setup > Settings > System information menu.

The Audio settings

Audio VolumeHandset

Set the volume on the handset.

Value space: <0..100>

Range: The value goes in steps of 5 from 0 to 100 (from -34.5dB to 15dB). Value 0 = Off.

`Example: Audio VolumeHandset: 70`

Audio VolumeHeadset

Set the volume on the headset.

Value space: <0..100>

Range: The value goes in steps of 5 from 0 to 100 (from -34.5dB to 15dB). Value 0 = Off.

`Example: Audio VolumeHeadset: 70`

Audio Volume

Set the volume on the loudspeaker.

Value space: <0..100>

Range: The value goes in steps of 5 from 0 to 100 (from -34.5dB to 15dB). Value 0 = Off.

`Example: Audio Volume: 70`

Audio SoundsAndAlerts RingVolume

Set the ring tone volume for an incoming call.

Value space: <0..100>

Range: The value goes in steps of 5 from 0 to 100 (from -34.5dB to 15dB). Value 0 = Off.

`Example: Audio SoundsAndAlerts RingVolume: 50`

The Audio settings, *cont...*

Audio SoundsAndAlerts RingTone

Select the ringtone for incoming calls.

Value space: <Marbles/IceCrystals/Polaris/Alert/Discrete/Fantasy/Jazz/Nordic/Echo/Rhythmic>

Range: Select a tone from the list of ringtones.

`Example: Audio SoundsAndAlerts RingTone: Jazz`

Audio SoundsAndAlerts KeyTones Mode

The system can produce a sound every time a key on the remote control is pressed.

Value space: <On/Off>

On: There will be a sound indicator when pressing keys on the remote control.

Off: The key tone on the remote control is switched off.

`Example: Audio SoundsAndAlerts KeyTones Mode: Off`

The Camera settings

Cameras PowerLine Frequency

Applies to cameras supporting PowerLine frequency anti-flickering, i.e PrecisionHD 1080p cameras.

Value space: <Auto/50Hz/60Hz>

Auto: Set to Auto to enable power frequency auto detection in the camera.

50Hz, 60Hz: Set to 50Hz or 60Hz.

`Example: Cameras PowerLine Frequency: Auto`

Cameras Camera [1] Backlight

The backlight functionality compensates for lights shining directly at the camera (usually the sun entering the window) to avoid a too dark image from the room.

Value space: <On/Off>

On: Turn on the camera backlight.

Off: Turn off the camera backlight.

`Example: Cameras Camera 1 Backlight: Off`

The Camera settings, *cont...*

Cameras Camera [1] IrSensor

The IR sensor LED is located in the front of the camera and flickers when the IR sensor is activated from the remote control. Both the TANDBERG camera and codec has an IR sensor. You would normally choose just one of them to be active at a time.

Value space: <On/Off>

On: Enable the IR sensor on the camera.

Off: Disable the IR sensor on the camera.

Example: `Cameras Camera 1 IrSensor: On`

Cameras Camera [1] FrameRate

Set the frame rate frequency.

Value space: <60Hz/30Hz>

60Hz: Set the frame rate to 60Hz.

30Hz: Set the frame rate to 30Hz.

Example: `Cameras Camera 1 FrameRate: 30Hz`

Cameras Camera [1] Brightness Mode

Set the camera brightness mode.

Value space: <Auto/Manual>

Auto: The camera brightness is automatically adjusted by the system.

Manual: Enable manual control of the camera brightness, e.g. the level of the brightness level setting will be used for the camera.

Example: `Cameras Camera 1 Brightness Mode: Auto`

Cameras Camera [1] Brightness Level

Set the brightness level. NOTE! Requires the Brightness Mode to be set to Manual.

Value space: <1..31>

Range: Select a value between 1 and 31.

Example: `Cameras Camera 1 Brightness Level: 1`

Cameras Camera [1] Whitebalance Mode

Set the camera whitebalance mode.

Value space: <Auto/Manual>

Auto: When set to Auto, the camera will continuously adjust the whitebalance depending on the camera view.

Manual: Set to Manual to enable manual control of the camera whitebalance, e.g. the level of the whitebalance level setting will be used for the camera.

Example: `Cameras Camera 1 Whitebalance Mode: auto`

The Camera settings, *cont...*

Cameras Camera [1] Whitebalance Level

Set the whitebalance level. NOTE! Requires the Whitebalance Mode to be set to manual.

Value space: <1..16>

Range: Select a value between 1 and 16.

Example: `Cameras Camera 1 Whitebalance Level: 1`

Cameras Camera [1] Focus Mode

Set the camera focus mode. When moving the camera, the system will use auto focus for a few seconds to set the right focus of the new camera position.

Value space: <Auto/Manual/ContinuesAuto>

Auto: The focus will be updated throughout the call. After a few seconds auto focus is turned off to prevent continuous focus adjustments of the camera.

Manual: Turn the autofocus off and adjust the camera focus manually.

ContinuesAuto: The focus is updated throughout the call, without being turned off.

Example: `Cameras Camera 1 Focus Mode: Auto`

Cameras Camera [1] Gamma Mode

Applies to cameras which supports Gamma mode. The Gamma Mode setting enables for gamma corrections. Gamma describes the nonlinear relationship between image pixels and monitor brightness. The TANDBERG PrecisionHD 720p camera supports Gamma Mode. Not supported on TANDBERG PrecisionHD 1080p camera.

Value space: <Auto/Manual>

Auto: Auto is the default and the recommended setting.

Manual: In severe light conditions, you may switch mode to manual and specify explicitly which gamma table to use by setting the Gamma Level.

Example: `Cameras Camera 1 Gamma Mode: Auto`

Cameras Camera [1] Gamma Level

By setting the Gamma Level you can select which gamma correction table to use. This setting may be useful in difficult lighting conditions, where changes to the brightness setting does not provide satisfactory results. NOTE! Requires the Gamma Mode to be set to Manual.

Value space: <0..7>

Range: Select a value between 0 and 7.

Example: `Cameras Camera 1 Gamma Level: 0`

The Conference settings

Conference [1] TelephonyPrefix

Enter the prefix to be used for telephony calls.

Value space: <S: 0, 80>

Format: String with a maximum of 80 characters.

Example: `Conference [1] TelephonyPrefix: "520"`

Conference [1] MaxTransmitCallRate

Specify the maximum transmit call rate to be used when placing or receiving calls.

Value space: <64..6000>

Range: Enter a value from 64 to 6000 kbps.

Example: `Conference 1 MaxTransmitCallRate: 6000`

Conference [1] MaxReceiveCallRate

Specify the maximum receive call rate to be used when placing or receiving calls.

Value space: <64..6000>

Range: Enter a value from 64 to 6000 kbps.

Example: `Conference 1 MaxReceiveCallRate: 6000`

Conference [1] IncomingMultisiteCall Mode

Set the incoming Multisite call mode. The TANDBERG MultiSite feature allows participants from more than two locations to join a meeting — by video and/or telephone.

Value space: <Allow/Deny>

Allow: Accept incoming calls to an already active call/conference. The incoming call will be added to the MCU conference.

Deny: The system will not accept incoming calls when you are in a call. The calling side will receive a busy signal.

Example: `Conference 1 IncomingMultisiteCall Mode: Allow`

Conference [1] AutoAnswer Mode

Set the AutoAnswer mode.

Value space: <On/Off>

On: Enable AutoAnswer to let the system automatically answer all incoming calls.

Off: The incoming calls must be answered manually by pressing the OK key or the green Call key on the remote control.

Example: `Conference 1 AutoAnswer Mode: Off`

The Conference settings, *cont...*

Conference [1] AutoAnswer Mute

The AutoAnswer Mute setting determines whether the microphone is muted when an incoming call is automatically answered. NOTE! Requires the AutoAnswer Mode to be enabled.

Value space: <On/Off>

On: The incoming call will be muted when automatically answered.

Off: The incoming call will not be muted.

Example: `Conference 1 AutoAnswer Mute: Off`

Conference [1] AutoAnswer Delay

Define how long (in seconds) an incoming call has to wait before it is answered automatically by the system. NOTE! Requires the AutoAnswer Mode to be enabled.

Value space: <0..50>

Range: Enter a value from 0 to 50 seconds.

Example: `Conference 1 AutoAnswer Delay: 0`

Conference [1] MicUnmuteOnDisconnect

The MicUnmuteOnDisconnect setting determines if the microphones should be automatically unmuted when all calls are disconnected. In a meeting room or other shared resource this could be done to prepare the system for the next user.

Value space: <On/Off>

On: Un-mute the microphones after the call is disconnected.

Off: If muted, let the microphones remain muted after the call is disconnected.

Example: `Conference 1 MicUnmuteOnDisconnect: On`

Conference [1] DoNotDisturb Mode

The Do Not Disturb setting determines whether or not there should be an alert on incoming calls.

Value space: <On/Off>

On: All incoming calls will be rejected, with no alert. The calling side will receive a busy signal when trying to call the codec. A message will display on screen, telling that Do not disturb is turned on, together with an option to turn off the Do not disturb. When turning off the Do not disturb mode you will see a list of the calls that have been rejected.

Off: The incoming calls will be alerted.

Example: `DoNotDisturb Mode: Off`

The Conference settings, *cont...*

Conference [1] FarEndControl Mode

Lets you decide if the remote side (far end) should be allowed to select your video sources and control your local camera (pan, tilt, zoom).

Value space: <On/Off>

On: Allows the far end to be able to select your video sources and control your local camera (pan, tilt, zoom). You will still be able to control your camera and select your video sources as normal.

Off: Do not allow the far end to select your video sources or to control your local camera (pan, tilt, zoom).

```
Example: Conference 1 FarEndControl Mode: On
```

Conference [1] FarEndControl SignalCapability

Set the far end control (H.224) signal capability mode.

Value space: <On/Off>

On: Enable the far end control signal capability.

Off: Disable the far end control signal capability.

```
Example: Conference 1 FarEndControl SignalCapability: On
```

Conference [1] Encryption Mode

Set the conference encryption mode. A padlock with the text "Encryption On" or "Encryption Off" displays on screen, for a few seconds, when the conference starts.

Value space: <BestEffort/On/Off>

BestEffort: The system will use encryption whenever possible.

> *In Point to point calls:* If the far end system supports encryption (AES-128), the call will be encrypted. If not, the call will proceed without encryption.

> *In MultiSite calls:* In order to have encrypted MultiSite conferences, all sites must support encryption. If not, the conference will be unencrypted.

On: The system will only allow calls that are encrypted.

Off: The system will not use encryption.

```
Example: Conference 1 Encryption Mode: BestEffort
```

Conference [1] DefaultCall Protocol

Set the Default Call Protocol to be used when placing calls from the system.

Value space: <H323/SIP>

H.323: Select H.323 to ensure that calls are set up as H.323 calls.

SIP: Select SIP to ensure that calls are set up as SIP calls.

```
Example: Conference 1 DefaultCall Protocol: H323
```

The Conference settings, *cont...*

Conference [1] DefaultCall Rate

Set the Default Call Rate to be used when placing calls from the system.

Value space: <64..6000>

Range: Enter a value from 64 to 6000 kbps.

```
Example: Conference 1 DefaultCall Rate: 768
```

Conference [1] VideoBandwidth Mode

Set the conference video bandwidth mode.

Value space: <Dynamic/Static>

Dynamic: The available transmit bandwidth for the video channels are distributed among the currently active channels. If there is no presentation, the main video channels will use the bandwidth of the presentation channel.

Static: The available transmit bandwidth is assigned to each video channel, even if it is not active.

```
Example: Conference 1 VideoBandwidth Mode: Dynamic
```

Conference [1] VideoBandwidth MainChannel Weight

The available transmit video bandwidth is distributed on the main channel and presentation channel according to "MainChannel Weight" and "PresentationChannel Weight". If the main channel weight is 2 and the presentation channel weight is 1, then the main channel will use twice as much bandwidth as the presentation channel.

Value space: <1..10>

Select a value between 1 and 10.

```
Example: Conference 1 VideoBandwidth MainChannel Weight: 5
```

Conference [1] VideoBandwidth PresentationChannel Weight

The available transmit video bandwidth is distributed on the main channel and presentation channel according to "MainChannel Weight" and "PresentationChannel Weight". If the main channel weight is 2 and the presentation channel weight is 1, then the main channel will use twice as much bandwidth as the presentation channel.

Value space: <1..10>

Select a value between 1 and 10.

```
Example: Conference 1 VideoBandwidth PresentationChannel Weight: 5
```

The H323 Profile settings

H323 NAT Mode

The TANDBERG firewall traversal technology creates a secure path through the firewall barrier, and enables proper exchange of audio/video data when connected to an external video conferencing system (when the IP traffic goes through a NAT router). NOTE! NAT does not work in conjunction with gatekeepers.

Value space: <Auto/On/Off>

Auto: The system will try to determine if the "NAT Address" or the real IP-address should be used within signalling. This is done to make it possible to place calls to endpoints on the LAN as well as endpoints on the WAN.

On: The system will signal the configured "NAT Address" in place of its own IP-address within Q.931 and H.245. The NAT Server Address will be shown in the startup-menu as: "My IP Address: 10.0.2.1".

Off: The system will signal the real IP Address.

Example: `H323 NAT Mode: Off`

H323 NAT Address

Enter the external/global IP-address to the router with NAT support. Packets sent to the router will then be routed to the system.

In the router, the following ports must be routed to the system's IP-address:

* Port 1720
* Port 5555-5574
* Port 2326-2485

Value space: <S: 0, 64>

Format: String with a maximum of 64 characters.

Example: `H323 NAT Address: ""`

H323 Profile [1] PortAllocation

The H.323 Port Allocation setting affects the H.245 port numbers used for H.323 call signalling.

Value space: <Dynamic/Static>

Dynamic: The system will allocate which ports to use when opening a TCP connection. The reason for doing this is to avoid using the same ports for subsequent calls, as some firewalls consider this as a sign of attack. When Dynamic is selected, the H.323 ports used are from 11000 to 20999. Once 20999 is reached they restart again at 11000. For RTP and RTCP media data, the system is using UDP ports in the range 2326 to 2487. Each media channel is using two adjacent ports, ie 2330 and 2331 for RTP and RTCP respectively. The ports are automatically selected by the system within the given range. Firewall administrators should not try to deduce which ports are used when, as the allocation schema within the mentioned range may change without any further notice.

Static: When set to Static the ports are given within a static predefined range [5555–6555].

Example: `H323 Profile 1 PortAllocation: Dynamic`

The H323 Profile settings, *cont...*

H323 Profile [1] H323Alias ID

Lets you specify the H.323 Alias ID which is used to address the system on a H.323 Gatekeeper and will be displayed in the call lists. Example: "firstname.surname@company.com", "My H.323 Alias ID".

Value space: <S: 0, 49>

Format: String with a maximum of 49 characters

Example: `H323 Profile 1 H323Alias ID: "firstname.surname@company.com"`

H323 Profile [1] H323Alias E164

The H.323 Alias E.164 defines the address of the system, according to the numbering plan implemented in the H.323 Gatekeeper. The E.164 alias is equivalent to a telephone number, sometimes combined with access codes.

Value space: <S: 0, 30>

Format: Compact string with a maximum of 30 characters. Valid characters are 0–9, * and #.

Example: `H323 Profile 1 H323Alias E164: "90550092"`

H323 Profile [1] CallSetup Mode

The H.323 Call Setup Mode defines whether to use a Gatekeeper or Direct calling when establishing H323 calls.

NOTE! Direct H.323 calls can be made even though the H.323 Call Setup Mode is set to Gatekeeper.

Value space: <Direct/Gatekeeper>

Direct: An IP-address must be used when dialling in order to make the H323 call.

Gatekeeper: The system will use a Gatekeeper to make a H.323 call. When selecting this option the H323 Profile Gatekeeper Address and H323 Profile Gatekeeper Discovery settings must also be configured.

Example: `H323 Profile 1 CallSetup Mode: Gatekeeper`

H323 Profile [1] Gatekeeper Address

Enter the IP address of the Gatekeeper. NOTE! Requires the H.323 Call Setup Mode to be set to Gatekeeper and the Gatekeeper Discovery to be set to Manual.

Value space: <S: 0, 255>

Format: Only the valid IP address format is accepted. An IP address that contains letters (192.a.2.0) or unvalid IP addresses (192.0.1234.0) will be rejected.

Example: `H323 Profile 1 Gatekeeper Address: "192.0.2.0"`

The H323 Profile settings, *cont...*

H323 Profile [1] Gatekeeper Discovery

Determines how the system shall register to a H.323 Gatekeeper.

Value space: <Manual/Auto>

Manual: The system will use a specific Gatekeeper identified by the Gatekeeper's IP-address.

Auto: The system will automatically try to register to any available Gatekeeper. If a Gatekeeper responds to the request sent from the codec within 30 seconds this specific Gatekeeper will be used. This requires that the Gatekeeper is in auto discovery mode as well. If no Gatekeeper responds, the system will not use a Gatekeeper for making H.323 calls and hence an IP-address must be specified manually.

Example: `H323 Profile 1 Gatekeeper Discovery: Manual`

H323 Profile [1] Authentication Mode

Set the authenticatin mode for the H.323 profile.

Value space: <On/Off>

On: If the H.323 Gatekeeper Authentication Mode is set to On and a H.323 Gatekeeper indicates that it requires authentication, the system will try to authenticate itself to the gatekeeper. NOTE! Requires the Authentication LoginName and Authentication Password to be defined on both the codec and the Gatekeeper.

Off: If the H.323 Gatekeeper Authentication Mode is set to Off the system will not try to authenticate itself to a H.323 Gatekeeper, but will still try a normal registration.

Example: `H323 Profile 1 Authentication Mode: Off`

H323 Profile [1] Authentication LoginName

The system sends the Authentication Login Name and the Authentication Password to a H.323 Gatekeeper for authentication. The authentication is a one way authentication from the codec to the H.323 Gatekeeper, i.e. the system is authenticated to the gatekeeper. If the H.323 Gatekeeper indicates that no authentication is required, the system will still try to register. NOTE! Requires the H.323 Gatekeeper Authentication Mode to be enabled.

Value space: <S: 0, 50>

Format: String with a maximum of 50 characters.

Example: `H323 Profile 1 Authentication LoginName: ""`

The H323 Profile settings, *cont...*

H323 Profile [1] Authentication Password

The system sends the Authentication Login Name and the Authentication Password to a H.323 Gatekeeper for authentication. The authentication is a one way authentication from the codec to the H.323 Gatekeeper, i.e. the system is authenticated to the gatekeeper. If the H.323 Gatekeeper indicates that no authentication is required, the system will still try to register. NOTE! Requires the H.323 Gatekeeper Authentication Mode to be enabled.

Value space: <S: 0, 50>

Format: String with a maximum of 50 characters.

Example: `H323 Profile 1 Authentication Password:`

The Network settings

Network [1] Speed

Set the Ethernet link speed.

Value space: <Auto/10half/10full/100half/100full/1000full>

Auto: Autonegotiate link speed.

10half: Force link to 10Mbps half-duplex.

10full: Force link to 10Mbps full-duplex.

100half: Force link to 100Mbps half-duplex.

100full: Force link to 100Mbps full-duplex.

1000full: Force link to 1Gbps full-duplex.

```
Example: Network 1 Speed: Auto
```

Network [1] Assignment

Define whether to use DHCP or Static IP assignment. NOTE! Changes to this setting requires a restart of the codec.

Value space: <Static/DHCP>

Static: When you set the network assignment to Static you must configure the static IP settings. Configure the settings: Network IPv4 Address, Network IPv4 SubnetMask and Network IPv4 Gateway.

DHCP: The system adresses are automatically assigend by the DHCP server.

```
Example: Network 1 Assignment: DHCP
```

Network [1] MTU

Set the Ethernet MTU (Maximum Transmission Unit).

Value space: <400..1500>

Range: Select a value from 400 to 1500bytes.

```
Example: Network 1 MTU: 1500
```

Network [1] VLAN Voice Mode

Set the VLAN voice mode.

Value space: <Tagged/Untagged>

Tagged: The voice packets in the VLAN network are tagged with Voice VlanId and Voice Priority.

Untagged: The voice packets in the VLAN network are untagged.

```
Example: Network 1 VLAN Voice Mode: Untagged
```

The Network settings, *cont...*

Network [1] VLAN Voice VlanId

Set the VLAN voice ID.

Value space: <0..4096>

Range: Select a value from 0 to 4096.

```
Example: Network 1 VLAN Voice VlanId: 0
```

Network [1] VLAN Voice Priority

Set the VLAN voice priority.

Value space: <0..7>

Range: Select a value from 0 to 7.

```
Example: Network 1 VLAN Voice Priority: 0
```

Network [1] VLAN Data Mode

Set the VLAN data mode.

Value space: <Tagged/Untagged>

Tagged: The data packets in the VLAN network are tagged with Data VlanId and Data Priority.

Untagged: The data packets in the VLAN network are untagged.

```
Example: Network 1 VLAN Data Mode: Untagged
```

Network [1] VLAN Data VlanId

Set the VLAN data ID.

Value space: <0..4096>

Range: Select a value from 0 to 4096.

```
Example: Network 1 VLAN Data VlanId: 0
```

Network [1] VLAN Data Priority

Set the VLAN data priority.

Value space: <0..7>

Range: Select a value from 0 to 7.

```
Example: Network 1 VLAN Data Priority: 0
```

The Network settings, *cont...*

Network [1] IPv4 Address

Define the Static IP network address for the system. Only applicable if the Network Assignment is set to Static.

Value space: <S: 0, 64>

Format: Only the valid IP address format is accepted. An IP address that contains letters (192.a.2.0) or unvalid IP addresses (192.0.1234.0) will be rejected.

Example: `Network 1 IPv4 Address: "192.0.2.0"`

Network [1] IPv4 SubnetMask

Define the IP network subnet mask. Only applicable if the Network Assignment is set to Static.

Value space: <S: 0, 64>

Format: Compact string with a maximum of 64 characters.

Example: `Network 1 IPv4 SubnetMask: "255.255.255.0"`

Network [1] IPv4 Gateway

Define the IP network gateway. Only applicable if the Network Assignment is set to Static.

Value space: <S: 0, 64>

Format: Compact string with a maximum of 64 characters.

Example: `Network 1 IPv4 Gateway: "192.0.2.0"`

Network [1] IPv4 QoS Mode

The QoS (Quality of Service) is a method which handles the priority of audio, video and data in the network. The QoS settings must be supported by the infrastructure. Diffserv (Differentiated Services) is a computer networking architecture that specifies a simple, scalable and coarse-grained mechanism for classifying, managing network traffic and providing QoS priorities on modern IP networks.

Value space: <Off/Diffserv>

Off: No QoS method is used.

Diffserv: When you set the QoS Mode to Diffserv you must configure the Diffserv sub menu settings (Audio, Data, Signalling and Video).

Example: `Network 1 IPv4 QoS Mode: diffserv`

The Network settings, *cont...*

Network [1] IPv4 QoS Diffserv Audio

The Diffserv Audio defines which priority Audio packets should have in an IP network. Enter a priority, which ranges from 0 to 63 for the packets. The higher the number, the higher the priority. These priorities might be overridden when packets are leaving the network controlled by the local network administrator. NOTE! Requires the Network IPv4 QoS Mode to be set to Diffserv.

Value space: <0..63>

Audio: A recommended value is Diffserv Code Point (DSCP) is AF41, which equals the value 34. If in doubt, contact your network administrator.

Range: 0-63

Example: `Network 1 IPv4 QoS Diffserv Audio: 0`

Network [1] IPv4 QoS Diffserv Data

The Diffserv Data defines which priority Data packets should have in an IP network. Enter a priority, which ranges from 0 to 63 for the packets. The higher the number, the higher the priority. These priorities might be overridden when packets are leaving the network controlled by the local network administrator. NOTE! Requires the Network IPv4 QoS Mode to be set to Diffserv.

Value space: <0..63>

Data: A recommended value is Diffserv Code Point (DSCP) AF23, which equals the value 22. If in doubt, contact your network administrator.

Range: 0-63

Example: `Network 1 IPv4 QoS Diffserv Data: 0`

Network [1] IPv4 QoS Diffserv Signalling

The Diffserv Signalling defines which priority Signalling packets should have in an IP network. Enter a priority, which ranges from 0 to 63 for the packets. The higher the number, the higher the priority. These priorities might be overridden when packets are leaving the network controlled by the local network administrator. NOTE! Requires the Network IPv4 QoS Mode to be set to Diffserv.

Value space: <0..63>

Signalling: A recommended value is Diffserv Code Point (DSCP) AF31, which equals the value 26. If in doubt, contact your network administrator.

Range: 0-63

Example: `Network 1 IPv4 QoS Diffserv Signalling: 0`

The Network settings, *cont...*

Network [1] IPv4 QoS Diffserv Video

The Diffserv Video defines which priority Video packets should have in an IP network. Enter a priority, which ranges from 0 to 63 for the packets. The higher the number, the higher the priority. These priorities might be overridden when packets are leaving the network controlled by the local network administrator. NOTE! Requires the Network IPv4 QoS Mode to be set to Diffserv.

Value space: <0..63>

Video: A recommended value is Diffserv Code Point (DSCP) AF41, which equals the value 34. If in doubt, contact your network administrator.

Range: 0-63

Example: `Network 1 IPv4 QoS Diffserv Video: 0`

Network [1] DNS Server [1..5] Address

Define the network addresses for DNS servers. Up to 5 addresses may be specified. If the network addresses are unknown, contact your administrator or Internet Service Provider.

Value space: <S: 0, 64>

Format: String with a maximum of 64 characters.

Example: `Network 1 DNS Server 1 Address: ""`

Network [1] DNS Domain Name

DNS Domain Name is the default domain name suffix which is added to unqualified names.

Example: If the DNS Domain Name is "company.com" and the name to lookup is "MyVideoSystem", this will result in the DNS lookup "MyVideoSystem.company.com".

Value space: <S: 0, 64>

Format: String with a maximum of 64 characters.

Example: `Network 1 DNS Domain Name: ""`

Network [1] IEEE8021X Mode

The system can be connected to an IEEE 802.1X LAN network, with a port-based network access control that is used to provide authenticated network access for Ethernet networks.

Value space: <On/Off>

On: The 802.1X authentication is enabled.

Off: The 802.1X authentication is disabled (default).

Example: `Network 1 IEEE8021X Mode: Off`

The Network settings, *cont...*

Network [1] IEEE8021X AnonymousIdentity

The 802.1X Anonymous ID string is to be used as unencrypted identity with EAP (Extensible Authentication Protocol) types that support different tunneled identity, like EAP-PEAP and EAP-TTLS. If set, the anonymous ID will be used for the initial (unencrypted) EAP Identity Request.

Value space: <S: 0, 64>

Format: String with a maximum of 64 characters.

Example: `Network 1 IEEE8021X AnonymousIdentity: ""`

Network [1] IEEE8021X Identity

The 802.1X Identity is the user name needed for 802.1X authentication.

Value space: <S: 0, 64>

Format: String with a maximum of 64 characters.

Example: `Network 1 IEEE8021X Identity: ""`

Network [1] IEEE8021X Password

The 802.1X Password is the password needed for 802.1X authentication.

Value space: <S: 0, 32>

Format: String with a maximum of 32 characters.

Example: `Network 1 IEEE8021X Password: "***"`

Network [1] IEEE8021X Eap Md5

Set the Md5 (Message-Digest Algorithm 5) mode. This is a Challenge Handshake Authentication Protocol that relies on a shared secret. Md5 is a Weak security.

Value space: <On/Off>

On: The EAP-MD5 protocol is enabled (default).

Off: The EAP-MD5 protocol is disabled.

Example: `Network 1 IEEE8021X Eap Md5: On`

Network [1] IEEE8021X Eap TTLS

Set the TTLS (Tunneled Transport Layer Security) mode. Authenticates LAN clients without the need for client certificates. Developed by Funk Software and Certicom. Usually supported by Agere Systems, Proxim and Avaya.

Value space: <On/Off>

On: The EAP-TTLS protocol is enabled (default).

Off: The EAP-TTLS protocol is disabled.

Example: `Network 1 IEEE8021X Eap TTLS: On`

The Network settings, *cont...*

Network [1] IEEE8021X Eap Peap

Set the Peap (Protected Extensible Authentication Protocol) mode. Authenticates LAN clients without the need for client certificates. Developed by Microsoft, Cisco and RSA Security.

Value space: <On/Off>

On: The EAP-PEAP protocol is enabled (default).

Off: The EAP-PEAP protocol is disabled.

Example: `Network 1 IEEE8021X Eap Peap: On`

Network [1] TrafficControl Mode

Set the network traffic control mode to decide how to control the the video packets transmission speed.

Value space: <On/Off>

On: Transmit video packets at maximum 20Mbps. Can be used to smooth out bursts in the outgoing network traffic.

Off: Transmit video packets at link speed.

Example: `Network 1 TrafficControl: On`

The NetworkServices settings

NetworkServices Telnet Mode

Telnet is a network protocol used on the Internet or Local Area Network (LAN) connections.

Value space: <On/Off>

On: The Telnet protocol is enabled.

Off: The Telnet protocol is disabled. This is the factory setting.

Example: `NetworkServices Telnet Mode: Off`

NetworkServices HTTP Mode

Set the HTTP mode to enable/disable access to the system through a web browser. The web interface is used for system management, call management such as call transfer, diagnostics and software uploads.

Value space: <On/Off>

On: The HTTP protocol is enabled.

Off: The HTTP protocol is disabled.

Example: `NetworkServices HTTP Mode: On`

NetworkServices HTTPS Mode

Set the HTTP mode to enable/disable access to the system through a web browser. The web interface is used for system management, call management such as call transfer, diagnostics and software uploads.

Value space: <On/Off>

On: The HTTPS protocol is enabled.

Off: The HTTPS protocol is disabled.

Example: `NetworkServices HTTPS Mode: On`

NetworkServices HTTPS VerifyServerCertificate

When the system connects to an external HTTPS server (like a phonebook server or an external manager), this server will present a certificate to the system to identify itself. This setting tells the system if it should verify that the certificate is signed by a trusted Certificate Authority (CA). This requires that list of trusted CA's is uploaded to the system in advance.

Value space: <On/Off>

On: Verify server certificates.

Off: Do not verify server certificates.

Example: `NetworkServices HTTPS VerifyServerCertificate: Off`

The NetworkServices settings, *cont...*

NetworkServices SNMP Mode

SNMP (Simple Network Management Protocol) is used in network management systems to monitor network-attached devices (routers, servers, switches, projectors, etc) for conditions that warrant administrative attention. SNMP exposes management data in the form of variables on the managed systems, which describe the system configuration. These variables can then be queried (set to ReadOnly) and sometimes set (set to ReadWrite) by managing applications.

Value space: <Off/ReadOnly/ReadWrite>

Off: Disable the SNMP network service.

ReadOnly: Enable the SNMP network service for queries only.

ReadWrite: Enable the SNMP network service for both queries and commands.

Example: `NetworkServices SNMP Mode: ReadWrite`

NetworkServices SNMP CommunityName

Enter the name of the Network Services SNMP Community. The SNMP Community names are used to authenticate SNMP requests. The SNMP requests must have a 'password' (case sensitive) in order to receive a response from the SNMP Agent in the codec. The default password is "public". If you have the TANDBERG Management Suite (TMS) you must make sure the same SNMP Community is configured there too. NOTE! The SNMP Community password is case sensitive.

Value space: <S: 0, 50>

Format: String with a maximum of 50 characters.

Example: `NetworkServices SNMP CommunityName: "public"`

NetworkServices SNMP SystemContact

Enter the name of the Network Services SNMP System Contact.

Value space: <S: 0, 50>

Format: String with a maximum of 50 characters.

Example: `NetworkServices SNMP SystemContact: ""`

NetworkServices SNMP SystemLocation

Enter the name of the Network Services SNMP System Location.

Value space: <S: 0, 50>

Format: String with a maximum of 50 characters.

Example: `NetworkServices SNMP SystemLocation: ""`

The NetworkServices settings, *cont...*

NetworkServices SNMP Host [1..3] Address

Enter the address of up to three SNMP Managers. All traps will then be sent to the hosts listed.

The system's SNMP Agent (in the codec) responds to requests from SNMP Managers (a PC program etc.). SNMP Traps are generated by the SNMP Agent to inform the SNMP Manager about important events. Can be used to send event created messages to the SNMP agent about different events like: system reboot, system dialling, system disconnecting, MCU call, packet loss etc. Traps can be sent to multiple SNMP Trap Hosts.

Value space: <S: 0, 64>

Format: String with a maximum of 64 characters.

Example: `NetworkServices SNMP Host 1 Address: ""`

NetworkServices H323 Mode

Determines whether the system should be able to place and receive H.323 calls. NOTE! Requires a restart of the codec.

Value space: <On/Off>

On: Enable the possibility to place and receive H.323 calls (default).

Off: Disable the possibility to place and receive H.323 calls.

Example: `NetworkServices H323 Mode: On`

NetworkServices SIP Mode

Determines whether the system should be able to place and receive SIP calls. NOTE! Requires a restart of the codec.

Value space: <On/Off>

On: Enable the possibility to place and receive SIP calls (default).

Off: Disable the possibility to place and receive SIP calls.

Example: `NetworkServices SIP Mode: On`

The NetworkServices settings, *cont...*

NetworkServices NTP Mode

The Network Time Protocol (NTP) is used to synchronize the time of the system to a reference time server. The time server will subsequently be queried every 24th hour for time updates. The time will be displayed on the top of the screen. The system will use the time to timestamp messages transmitted to Gatekeepers or Border Controllers requiring H.235 authentication. The system will use the time to timestamp messages transmitted to Gatekeepers or Border Controllers that requires H.235 authentication. It is also used for timestamping Placed Calls, Missed Calls and Received Calls.

Value space: <Auto/Manual>

Auto: The system will use the NTP server, by which address is supplied from the DHCP server in the network. If no DHCP server is used, or the DHCP server does not provide the system with a NTP server address, the system will use the static defined NTP server address specified by the user.

Manual: The system will always use the static defined NTP server address specified by the user.

Example: `NetworkServices NTP Mode: Manual`

NetworkServices NTP Address

Enter the NTP Address to define the network time protocol server address. This address will be used if NTP Mode is set to Manual, or if set to Auto and no address is supplied by a DHCP server.

Value space: <S: 0, 64>

Format: String with a maximum of 64 characters.

Example: `NetworkServices NTP Address: "1.tandberg.pool.ntp.org"`

The Phonebook settings

Phonebook Server [1] ID

Enter a name for the external phonebook.

Value space: <S: 0, 64>

Format: String with a maximum of 64 characters.

Example: `Phonebook Server 1 ID: “”`

Phonebook Server [1] Type

Select the phonebook server type.

Value space: <VCS/TMS/Callway>

VCS: Select VCS if the phonebook is located on the TANDBERG Video Communication Server.

TMS: Select TMS if the phonebook is located on the TANDBERG Management Suite server.

Callway: Select Callway if the phonebook is to be provided by the Callway subscription service. Contact your Callway provider for more information.

Example: `Phonebook Server 1 Type: TMS`

Phonebook Server [1] URL

Enter the address (URL) to the external phonebook server.

Value space: <S: 0, 255>

Format: String with a maximum of 255 characters.

Example: `Phonebook Server 1 URL: “http://tms.company.com/tmsapi-exampleublic/externalapi-examplehonebookapi-examplehonebook.asmx”`

The Provisioning settings

Provisioning Mode

Provides the possibility of managing the codec (endpoint) by using an external manager/management system.

Value space: <Off/TMS/Callway>

Off: The system will not try to register to any management system.

TMS: If set to TMS (TANDBERG Management System) the system will try to register with a TMS server. Contact your TANDBERG representative for more information.

Callway: If set to Callway the system will try to register with the Callway subscription provider. Contact your Callway provider for more information.

Example: `Provisioning Mode: TMS`

Provisioning LoginName

Enter the user id provided by the provisioning server. This is the user name part of the credentials used to authenticate towards the HTTP server when using HTTP provisioning.

Value space: <S: 0, 80>

Format: String with a maximum of 80 characters.

Example: `Provisioning LoginName: ""`

Provisioning Password

Enter the password provided by the provisioning server. This is the password part of the credentials used to authenticate towards the HTTP server when using HTTP provisioning.

Value space: <S: 0, 64>

Format: String with a maximum of 64 characters.

Example: `Provisioning Password: ""`

Provisioning HttpMethod

Select the HTTP method to be used for the provisioning.

Value space: <GET/POST>

GET: Select GET when the provisiong server supports GET.

POST: Select POST when the provisiong server supports POST.

Example: `Provisioning HttpMethod: POST`

The Provisioning settings, *cont...*

Provisioning ExternalManager Address

Enter the IP Address to the External Manager/Management system. If an External Manager address and a path is configured, the system will post an HTTP message to this address when starting up. When receiving this HTTP posting the External Manager (typically a management system) can return configurations/commands to the unit as a result. If the DHCP Option 242 is returned in the DHCP response from the DHCP server the system will interpret this as the External Manager address to use.

Value space: <S: 0, 64>

Format: Only the valid IP address format is accepted. An IP address that contains letters (192.a.2.0) or unvalid IP addresses (192.0.1234.0) will be rejected.

Example: `Provisioning ExternalManager Address: "192.0.2.0"`

Provisioning ExternalManager Protocol

Determines whether or not to use secure management.

Value space: <HTTP/HTTPS>

HTTP: Set to HTTP to disable secure management. Requires HTTP to be enabled in the NetworkServices HTTP Mode setting.

HTTPS: Set to HTTPS to enable secure management. Requires HTTPS to be enabled in the NetworkServices HTTPS Mode setting.

Example: `Provisioning ExternalManager Protocol: HTTP`

Provisioning ExternalManager Path

Set the path to the External Manager/Management system. If an External Manager address and a path is configured, the system will post an HTTP message to this address when starting up. When receiving this HTTP posting the External Manager (typically a management system) can return configurations/commands to the unit as a result. If the DHCP Option 242 is returned in the DHCP response from the DHCP server the system will interpret this as the External Manager address to use.

Value space: <S: 0, 255>

Format: String with a maximum of 255 characters.

Example: `Provisioning ExternalManager Path: "tmsapi-exampleublic/external/management/SystemManagementService.asmx"`

The SerialPort settings

SerialPort BaudRate

Specify the baud rate (data transmission rate, bits per second) for the COM 1 port on the codec. The default value is 38400.

Connection parameters for the COM port: Data bits: 8 Parity: None Stop bits: 1 Flow control: None.

Value space: <9600/19200/38400/57600/115200>

Range: Select a baud rate from the list of baud rates (bps).

Example: `SerialPort BaudRate: 38400`

SerialPort LoginRequired

The Serial Login setting determines whether or not there should be a login when connecting to the COM 1 port at the codec.

Value space: <On/Off>

On: Login is required when connecting to the codec through COM port.

Off: The user can access the codec through COM port without any login.

Example: `SerialPort LoginRequired: On`

The SIP Profile settings

SIP Profile [1] URI

The SIP URI or number is used to address the system. This is the URI that is registered and used by the SIP services to route inbound calls to the system. A Uniform Resource Identifier (URI) is a compact string of characters used to identify or name a resource.

Value space: <S: 0, 255>

Format: Compact string with a maximum of 255 characters.

Example: `SIP Profile 1 URI: "sip:firstname.lastname@company.com"`

SIP Profile [1] DefaultTransport

Select the transport protocol to be used over the LAN.

Value space: <UDP/TCP/TLS/Auto>

UDP: The system will always use UDP as the default transport method.

TCP: The system will always use TCP as the default transport method.

TLS: The system will always use TLS as the default transport method. For TLS connections a SIP CA-list can be uploaded using the web interface. If no such CA-list is available on the system then anonymous Diffie Hellman will be used.

Auto: The system will try to connect using transport protocols in the following order: TLS, TCP, UDP.

Example: `SIP Profile 1 DefaultTransport: Auto`

SIP Profile [1] Type

Enables SIP extensions and special behaviour for a vendor or provider.

Value space: <Standard/Alcatel/Avaya/Cisco/Microsoft/Nortel/Experimental/Siemens>

Standard: Should be used when registering to standard SIP proxy like OpenSer.

Alcatel: Must be used when registering to a Alcatel-Lucent OmniPCX Enterprise R7 or later.

Avaya: Must be used when registering to a Avaya Communication Manager.

Cisco: Must be used when registering to a Cisco CallManager version 5 or later.

Microsoft: Must be used when registering to a Microsoft LCS or OCS server.

Nortel: Must be used when registering to a Nortel MCS 5100 or MCS 5200 PBX.

Experimental: Can be used if auto is not working. NOTE! This mode is for testing purposes only.

Example: `SIP Profile 1 Type: Standard`

SIP Profile [1] Outbound

The client initiated connections mechanism for firewall traversal, connection reuse and redundancy. The current version supports http://tools.ietf.org/html/draft-ietf-sip-outbound-20.

Value space: <On/Off>

On: Set up multiple outbound connections to servers in the Proxy Address list.

Off: Connect to the single proxy configured first in Proxy Address list.

Example: `SIP Profile 1 Outbound: Off`

The SIP Profile settings, *cont...*

SIP Profile [1] Proxy [1..4] Discovery

Select if the SIP Proxy address is to be obtained manually or by using Dynamic Host Configuration Protocol (DHCP).

Value space: <Auto/Manual>

Manual: When Manual is selected, the manually configured SIP Proxy address will be used.

Auto: When Auto is selected, the SIP Proxy address is obtained using Dynamic Host Configuration Protocol (DHCP).

Example: `SIP Profile 1 Proxy 1 Discovery: Manual`

SIP Profile [1] Proxy [1..4] Address

The Proxy Address is the manually configured address for the outbound proxy. It is possible to use a fully qualified domain name, or an IP address. The default port is 5060 for TCP and UDP but another one can be provided. If Outbound is enabled, multiple proxies can be addressed.

Value space: <S: 0, 255>

Format: Compact string with a maximum of 255 characters. An IP address that contains letters (192.a.2.0) or unvalid IP addresses (192.0.1234.0) will be rejected.

Example: `SIP Profile 1 Proxy 1 Address: ""`

SIP Profile [1] Authentication [1] LoginName

This is the user name part of the credentials used to authenticate towards the SIP proxy.

Value space: <S: 0, 50>

Format: String with a maximum of 50 characters.

Example: `SIP Profile 1 Authentication 1 LoginName: ""`

SIP Profile [1] Authentication [1] Password

This is the password part of the credentials used to authenticate towards the SIP proxy.

Value space: <S: 0, 50>

Format: String with a maximum of 50 characters.

Example: `SIP Profile 1 Authentication 1 Password:`

The Standby settings

Standby Control

Determine whether the system should go into standby mode or not.

Value space: <On/Off>

On: Enter standby mode when the Standby Delay has timed out. NOTE! Requires the Standby Delay to be set to an appropriate value.

Off: The system will not enter standby mode.

Example: `Standby Control: On`

Standby Delay

Define how long (in minutes) the system shall be in idle mode before it goes into standby mode. NOTE! Requires the Standby Control to be enabled.

Value space: <1..480>

Range: Select a value from 1 to 480 minutes.

Example: `Standby Delay: 10`

Standby WakeupAction

Define the camera position when leaving standby mode.

Value space: <None/Preset1/Preset2/Preset3/Preset4/Preset5/Preset6/Preset7/Preset8/Preset9/Preset10/Preset11/Preset12/Preset13/Preset14/Preset15/RestoreCameraPosition/DefaultCameraPosition>

None: No action.

Preset1 to Preset15: When waking up from standby the camera position will be set to the position defined by the selected preset.

RestoreCameraPosition: When waking up from standby the camera position will be set to the position it had before entering standby.

DefaultCameraPosition: When waking up from standby the camera position will be set to the factory default position.

Example: `Standby WakeupAction: RestoreCameraPosition`

The Standby settings, *cont...*

Standby BootAction

Define the camera position after a restart of the codec.

Value space: <None/Preset1/Preset2/Preset3/Preset4/Preset5/Preset6/Preset7/Preset8/Preset9/Preset10/Preset11/Preset12/Preset13/Preset14/Preset15/RestoreCameraPosition/DefaultCameraPosition>

None: No action.

Preset1 to Preset15: After a reboot the camera position will be set to the position defined by the selected preset.

RestoreCameraPosition: After a reboot the camera position will be set to the position it had before the last boot.

DefaultCameraPosition: After a reboot the camera position will be set to the factory default position.

Example: `Standby BootAction: DefaultCameraPosition`

Standby StandbyAction

Define the camera position when going into standby mode.

Value space: <Noneapi-examplerivacyPosition>

None: No action.

PrivacyPosition: Turns the camera to a sideways position for privacy.

Example: `Standby StandbyAction: PrivacyPosition`

The SystemUnit settings

SystemUnit MenuType

Normally you would use the inTouch unit to control the system, but in some cases you may want to control the EX90 from the menu on screen, using the TANDBERG Remote Control.

Value space: <Indicators/Full>

Indicators: When set to Indicators the system is controlled from the inTouch unit. There will be no menus on the monitor screen.

Full: When set to Full the system can be controlled both from the inTouch unit, and from the menus on the monitor screen using the TANDBERG Remote Control. NOTE! Requires the SystemUnit IrSensor Mode to be enabled.

Example: `SystemUnit MenuTypee: Indicators`

SystemUnit Name

Enter a System Name to define a name of the system unit. If the H.323 Alias ID is configured on the system then this ID will be used instead of the system name. The system name will be displayed:

1) When the codec is acting as an SNMP Agent.

2) Towards a DHCP server.

Value space: <S: 0, 50>

Format: String with a maximum of 50 characters.

Example: `SystemUnit Name: "Meeting Room Name"`

SystemUnit MenuLanguage

The setting is used to select the language for the GUI (Graphical User Interface).

Value space: <English/Norwegian/Swedish/German/French/Italian/Japanese/Russian/Spanish/Korean/Finnish/ChineseSimplified/ChineseTraditional/PortugueseBrazilian/Turkish/Polish/Danish/Dutch

Example: `SystemUnit MenuLanguage: English`

SystemUnit IrSensor Mode

The System Unit IR Sensor setting determines whether the infrared receiver on the codec should be enabled or not. The IR sensor LED is located in the front of the codec and flickers when an IR signal is received from the remote control.

Value space: <On/Off/Auto>

On: Enable the IR sensor on the codec.

Off: Disable the IR sensor on the codec.

Auto: Both the TANDBERG codec and camera has an IR sensor. The system will automatically disable the IR sensor on the codec if the IR sensor at camera is enabled. Otherwise the IR sensor on the codec will be enabled.

Example: `SystemUnit IrSensor Mode: On`

The SystemUnit settings, *cont...*

SystemUnit CallLogging Mode

Set the call logging mode for calls that are received or placed by the system. The call logs may then be viewed via the GUI or using the xHistory command.

Value space: <On/Off>

On: Enable logging.

Off: Disable logging.

Example: `SystemUnit CallLogging Mode: On`

The Time settings

Time Zone

Set the time zone where the system is located, using Windows time zone description format.

Value space: <GMT-12:00 (International Date Line West)/GMT-11:00 (Midway Island, Samoa)/GMT-10:00 (Hawaii)/GMT-09:00 (Alaska)/GMT-08:00 (Pacific Time (US & Canada) Tijuana)/GMT-07:00 (Arizona)/GMT-07:00 (Mountain Time (US & Canada))/GMT-07:00 (Chihuahua, La Paz, Mazatlan)/GMT-06:00 (Central America)/GMT-06:00 (Saskatchewan)/GMT-06:00 (Guadalajara, Mexico City, Monterrey)/GMT-06:00 (Central Time (US & Canada))/GMT-05:00 (Indiana (East))/GMT-05:00 (Bogota, Lima, Quito)/GMT-05:00 (Eastern Time (US & Canada))/GMT-04:30 (Caracas)/GMT-04:00 (La Paz)/GMT-04:00 (Santiago)/GMT-04:00 (Atlantic Time (Canada))/GMT-03:30 (Newfoundland)/GMT-03:00 (Buenos Aires, Georgetown)/GMT-03:00 (Greenland)/GMT-03:00 (Brasilia)/GMT-02:00 (Mid-Atlantic)/GMT-01:00 (Cape Verde Is.)/GMT-01:00 (Azores)/GMT (Casablanca, Monrovia)/GMT (Coordinated Universal Time)/GMT (Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London)/GMT+01:00 (West Central Africa)/GMT+01:00 (Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna)/GMT+01:00 (Brussels, Copenhagen, Madrid, Paris)/GMT+01:00 (Sarajevo, Skopje, Warsaw, Zagreb)/GMT+01:00 (Belgrade, Bratislava, Budapest, Ljubljana, Prague)/GMT+02:00 (Harare, Pretoria)/GMT+02:00 (Jerusalem)/GMT+02:00 (Athens, Istanbul, Minsk)/GMT+02:00 (Helsinki, Kyiv, Riga, Sofia, Tallinn, Vilnius)/GMT+02:00 (Cairo)/GMT+02:00 (Bucharest)/GMT+03:00 (Nairobi)/GMT+03:00 (Kuwait, Riyadh)/GMT+03:00 (Moscow, St. Petersburg, Volgograd)/GMT+03:00 (Baghdad)/GMT+03:30 (Tehran)/GMT+04:00 (Abu Dhabi, Muscat)/GMT+04:00 (Baku, Tbilisi, Yerevan)/GMT+04:30 (Kabul)/GMT+05:00 (Islamabad, Karachi, Tashkent)/GMT+05:00 (Ekaterinburg)/GMT+05:30 (Chennai, Kolkata, Mumbai, New Delhi)/GMT+05:45 (Kathmandu)/GMT+06:00 (Sri Jayawardenepura)/GMT+06:00 (Astana, Dhaka)/GMT+06:00 (Almaty, Novosibirsk)/GMT+06:30 (Rangoon)/GMT+07:00 (Bangkok, Hanoi, Jakarta)/GMT+07:00 (Krasnoyarsk)/GMT+08:00 (Perth)/GMT+08:00 (Taipei)/GMT+08:00 (Kuala Lumpur, Singapore)/GMT+08:00 (Beijing, Chongqing, Hong Kong, Urumqi)/GMT+08:00 (Irkutsk, Ulaan Bataar)/GMT+09:00 (Osaka, Sapporo, Tokyo)/GMT+09:00 (Seoul)/GMT+09:00 (Yakutsk)/GMT+09:30 (Darwin)/GMT+09:30 (Adelaide)/GMT+10:00 (Guam, Port Moresby)/GMT+10:00 (Brisbane)/GMT+10:00 (Vladivostok)/GMT+10:00 (Hobart)/GMT+10:00 (Canberra, Melbourne, Sydney)/GMT+11:00 (Magadan, Solomon Is., New Caledonia)/GMT+12:00 (Fiji, Kamchatka, Marshall Is.)/GMT+12:00 (Auckland, Wellington)/GMT+13:00 (Nuku alofa)>

Select a time zone from the list time zones. If using a command line interface watch up for typos.Set the time zone.

Example: `Time Zone: "GMT (Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London)"`

The Time settings, *cont...*

Time TimeFormat

Set the time format.

Value space: <24H/12H>

24H: Set the time format to 24 hours.

12H: Set the time format to 12 hours.

Example: `Time TimeFormat: 24H`

Time DateFormat

Set the date format.

Value space: <DD_MM_YY/MM_DD_YY/YY_MM_DD>

DD_MM_YY: The date January 30th 2010 will be displayed: 30.01.10

MM_DD_YY: The date January 30th 2010 will be displayed: 01.30.10

YY_MM_DD: The date January 30th 2010 will be displayed: 10.01.30

Example: `Time DateFormat: DD _ MM _ YY`

The Video settings

Video Selfview

The Video Selfview setting determines whether or not the main video source (selfview) should be displayed on screen.

Value space: <On/Off>

On: Show self view on screen.

Off: Hide self view on screen.

Example: `Video Selfview: On`

Video WallPaper

The Video Wallpaper setting determines whether or not a background picture should be displayed on screen when idle, and on the inTouch unit.

Value space: <None/Growing/Summersky/Custom/Wallpaper01/Wallpaper02/Wallpaper03/Wallpaper04/Wallpaper05/Wallpaper06/Wallpaper07/Wallpaper08/Wallpaper09/Wallpaper10/Wallpaper11/Wallpaper12>

None: No wallpaper will be displayed on screen. The background on the inTouch unit will not change.

Summersky, Growing: When you select Summersky or Growing the picture will display on screen. The background on the inTouch unit will not change.

Custom: The custom wallpaper must be uploaded to the codec from the web interface.

1) On the video system: Find the IP address of the codec. Open the menu and go to Settings > System information to find the IP Address.

2) On your computer: Open a web browser and enter the IP address of the codec. Select "Wallpaper" from the menu, browse for the file, and press the "Upload" button.

3) On the video system: Open the menu and go to Settings > Wallpaper > Custom. Give it a few seconds to display the new picture. If the picture does not show, toggle once between "None" and "Custom" wallpaper to make the change take effect.

Wallpaper01 to Wallpaper12: When you select Wallpaper01 to Wallpaper12 the same picture will display on screen and on the inTouch unit.

Example: `Video WallPaper: Summersky`

Video MainVideoSource

Define which video input source shall be used as the main video source.

Value space: <1..3>

Range: Select the source to be used as the main video source.

Example: `Video MainVideoSource: 1`

The Video settings, *cont...*

Video DefaultPresentationSource

Define which video input source shall be used as the default presentation source (e.g. when you press the Presentation key on the remote control). The input source is configured to a video input connector.

Value space: <1..3>

Range: Select the video source to be used as the presentation source.

Example: `Video DefaultPresentationSource: 2`

Video Input Source [1..3] Name

Enter a name for the video input source 1 to 3.

Value space: <S: 0, 50>

Format: String with a maximum of 50 characters.

Example: `Video Input Source 1 Name: ""`

Video Input Source 1 Connector

Select which video input connector to be active on video input source 1.

Value space: <HDMI>

HDMI: Select HDMI when you want to use the HDMI as input source 1.

Example: `Video Input Source 1 Connector: HDMI`

Video Input Source 2 Connector

Select which video input connector to be active on video input source 2.

Value space: <DVI>

DVI: Select DVI when you want to use the DVI-I as input source 2.

Example: `Video Input Source 2 Connector: DVI`

Video Input Source 3 Connector

Select which video input connector to be active on video input source 3.

Value space: <CAMERA>

CAMERA: Select CAMERA when you want to use the camera as input source 3.

Example: `Video Input Source 3 Connector: CAMERA`

The Video settings, *cont...*

Video Input Source [1..3] Quality

When encoding and transmitting video there will be a tradeoff between high resolution and high framerate. For some video sources it is more important to transmit high framerate than high resolution and vice versa. The Quality setting specifies whether to give priority to high frame rate or to high resolution for a given source.

Value space: <Motion/Sharpness>

Motion: Gives the highest possible framerate. Used when there is a need for higher frame rates, typically when a large number of participants are present or when there is a lot of motion in the picture.

Sharpness: Gives the highest possible resolution. Used when you want the highest quality of detailed images and graphics.

Example: `Video Input Source 1 Quality: Motion`

Video Input Source [1..3] CameraControl Mode

Set the camera control mode for the camera associated with the video source 1 to 3.

Value space: <On/Off>

On: Enable camera control.

Off: Disable camera control.

Example: `Video Input Source 1 CameraControl Mode: On`

Video Input Source [1..3] CameraControl CameraId

Select the ID of the camera. NOTE! Requires the Video Input Source CameraControl Mode to be enabled.

Value space: <1..5>

Range: Select the ID of the camera.

Example: `Video Input Source 1 CameraControl CameraId: 1`

The Video settings, *cont...*

Video Input Source [1..3] OptimalDefinition Profile

Adjust how rapidly the system will increase the transmitted resolution when increasing the bandwidth. NOTE! Requires that the Video Input Source Quality is set to Motion.

Normal: Use this setting for normal to poorly lit environment. If the source is a camera with 1920x1080p60, the system will transmit 1920x720p60 at about 2.2Mb/sec and above with this setting set to normal.

Medium: Requires better than normal and consistent lighting and good quality video inputs. If the source is a camera with 1920x1080p60, the system will transmit 1920x720p60 at about 1.4Mb/sec and above with this setting set to medium.

High: Requires good lighting conditions for a good overall experience and good quality video inputs. If the source is a camera with 1920x1080p60, the system will transmit 1920x720p60 at about 1.1Mb/sec and above with this setting set to high.

Value space: <Normal/Medium/High>

See Table 1: Optimal definition for systems supporting 1080p and Table 2: Optimal definition for systems supporting 720p60.

Example: `Video Input Source 1 OptimalDefinition Profile: Normal`

Table 1: Optimal definition, for systems supporting 1080p

	w288p30	*w448p30*	*w576p30*	*720p30*	*1080p30*
Normal	256kbit/s	512 kbit/s	768 kbit/s	1152 kbit/s	2560 kbit/s
Medium	128kbit/s	384 kbit/s	512 kbit/s	1152 kbit/s	1920 kbit/s
High	128kbit/s	256 kbit/s	512 kbit/s	768 kbit/s	1472 kbit/s

Table 2: Optimal definition, for systems supporting 720p60

	w144p60	*w288p60*	*w448p60*	*w576p60*	*720p60*
Normal	128kbit/s	512 kbit/s	1152 kbit/s	1472 kbit/s	2240 kbit/s
Medium	128kbit/s	384 kbit/s	768 kbit/s	1152 kbit/s	1920 kbit/s
High	128kbit/s	256 kbit/s	512 kbit/s	768 kbit/s	1152 kbit/s

The Video settings, *cont...*

Video Input Source [1..3] OptimalDefinition Threshold60fps

For each video input, this setting tells the system the lowest resolution where it should transmit 60fps. So for all resolutions lower than this, the maximum transmitted framerate would be 30fps, while above this resolution 60fps would also be possible, if the available bandwidth is adequate.

Value space: <512_288/768_448/1024_576/1280_720/Never>

512_288: Set the threshold to 512x288.

768_448: Set the threshold to 768x448.

1024_576: Set the threshold to 1024x576.

1280_720: Set the threshold to 1280x720.

Never: Do not set a threshold for transmitting 60fps.

Example: `Video Input Source 1 OptimalDefinition Threshold60fps: 1280 _ 720`

Video Input DVI [2] Type

The official DVI standard supports both digital and analog signals. In most cases the default AutoDetect setting can detect whether the signal is analog RGB or digital. However, in some rare cases when DVI-I cables are used (these cables can carry both the analog and digital signals) the auto detection fails. This setting makes it possible to override the AutoDetect and select the correct DVI video input.

Value space: <AutoDetect/Digital/AnalogRGB/AnalogYPbPr>

AutoDetect: Set to AutoDetect to automatically detect if the signal is analog RGB or digital.

Digital: Set to Digital to force the DVI video input to Digital when using DVI-I cables with both analog and digital pins and AutoDetect fails.

AnalogRGB: Set to AnalogRGB to force the DVI video input to AnalogRGB when using DVI-I cables with both analog and digital pins and AutoDetect fails.

AnalogYPbPr: Set to AnalogYPbPr to force the DVI video input to AnalogYPbPr, as the component (YPbPr) signal cannot be auto detected.

Example: `Video Input DVI 2 Type: AutoDetect`

Video Output HDMI [1] Resolution

Select the preferred resolution for the monitor connected to the video output HDMI connector. This will force the resolution on the monitor.

Value space: <Auto/640_480_60/800_600_60/1024_768_60/1280_1024_60/1280_720_60/1920_1080_60/1280_768_60/1360_768_60/1366_768_60/1600_1200_60/1920_1200_60>

Auto: The system will automatically try to set the optimal resolution based on negotiation with the connected monitor.

Range: 640x480@60p, 800x600@60p, 1024x768@60p, 1280x1024@60p, 1280x720@60p, 1920x1080@60p, 1280x768@60p, 1360x768@60p, 1366x768@60p, 1600x1200@60p, 1920x1200@60p

Example: `Video Output HDMI 1 Resolution: 1920 _ 1080 _ 60`

The Video settings, *cont...*

Video Output HDMI [1] OverscanLevel

Some TV's or other monitors may not display the whole image sent out on the systems video output, but cuts the outer parts of the image. In this case this setting can be used to let the system not use the outer parts of video resolution. Both the video and the OSD menu will be scaled in this case.

Value space: <Medium/High/None>

Medium: The system will not use the outer 3% of the output resolution.

High: The system will not use the outer 6% of the output resolution

None: The system will use all of the output resolution.

Example: `Video Output HDMI 1 OverscanLevel: None`

Video Output LCD [2] Resolution

Set the screen resolution.

Value space: <1920_1200_60>

Range: The screen resolution is 1920 x 1200 60Hz.

Example: `Video Output LCD 2 Resolution: 1920 _ 1200 _ 60`

Video Output LCD [2] Brightness

Set the brightness level for the monitor.

Value space: <S: 0, 100>

Range: Select a value from 0 to 100.

Example: `Video Output LCD 2 Brightness: 50`

Video Output LCD [2] Red

Set the Red color level for the monitor.

Value space: <S: 0, 100>

Range: Select a value from 0 to 100.

Example: `Video Output LCD 2 Red: 50`

Video Output LCD [2] Green

Set the Green color level for the monitor.

Value space: <S: 0, 100>

Range: Select a value from 0 to 100.

Example: `Video Output LCD 2 Green: 50`

The Video settings, *cont...*

Video Output LCD [2] Blue

Set the Blue color level for the monitor.

Value space: <S: 0, 100>

Range: Select a value from 0 to 100.

Example: `Video Output LCD 2 Blue: 50`

Video ControlPanel Brightness

Set the brightness level for the inTouch unit.

Value space: <S: 0, 100>

Range: Select a value from 0 to 100.

Example: `Video ControlPanel Brightness: 100`

Video OSD Mode

The Video OSD (On Screen Display) Mode lets you define if information and icons should be displayed on screen.

Value space: <On/Off>

On: Display the on screen menus, icons and indicators.

Off: Hide the on screen menus, icons and indicators.

Example: `Video OSD Mode: On`

Video OSD Output

The Video OSD (On Screen Display) Output lets you define which monitor should display the on screen menus, information and icons. By default the OSD is sent to the monitor connected to the Video OSD Output 1. If you cannot see the OSD on screen, then you must re-configure the OSD Output. You can do this by entering a key sequence on the remote control, from the web interface, or by a command line interface.

Using the TANDBERG Remote Control TRC5: Press the Disconnect key followed by: * # * # 0 x # (where x is output 1 to 2).

Using the web interface: Open a web browser and enter the IP address of the codec. Open the Advanced menu and navigate to Video OSD Output and select the video output.

Using a command line interface: Open a command line interface and connect to the codec (if in doubt of how to do this, see the API Guide for the codec). Enter the command: xConfiguration Video OSD Output [1..2] (select the OSD Output).

Value space: <1..2>

Range: Select 1 for HDMI 1 output, or select 2 for HDMI 2 output.

Example: `Video OSD Output: 1`

The Video settings, *cont...*

Video Layout Scaling

Define how the system shall adjust the aspect ratio for images or frames when there is a difference between the image and the frame it is to be placed in.

Value space: <On/Off>

On: Let the system automatically adjust aspect ratio.

Off: No adjustment of the aspect ratio.

Example: `Video Layout Scaling: On`

Video Layout ScaleToFrame

Define what to do if the aspect ratio of a video input source doesn't match the aspect ratio of the corresponding image frame in a composition. For example if you have a 4:3 input source (like XGA) to be displayed on a 16:9 output (like HD720).

Value space: <Manual/MaintainAspectRatio/StretchToFit>

Manual: If the difference in aspect ratio between the video input source and the target image frame is less than the ScaleToFrameThreshold configuration (in percent), the image is stretched to fit. If not, the system will maintain the original aspect ratio.

MaintainAspectRatio: Will maintain the aspect ratio of the input source, and fill in black in the rest of the frame (letter boxing or pillar boxing).

StretchToFit: Will stretch (horizontally or vertically) the input source to fit into the image frame.

Example: `Video Layout ScaleToFrame: MaintainAspectRatio`

Video Layout ScaleToFrameThreshold

Only applicable if the ScaleToFrame configuration is set to manual. If the difference in aspect ratio between the video input source and the target image frame is less than the ScaleToFrameThreshold configuration (in percent), the image is stretched to fit. If not, the system will maintain the original aspect ratio.

Value space: <0..100>

Range: Select a value from 0 to 100 percent.

Example: `Video Layout ScaleToFrameThreshold: 5`

The Experimental menu

The Advanced configurations menu has an option called Experimental. The settings within this menu are beta preview features and can be used 'as is' and will not be fully documented.

NOTE! The Experimental menu WILL change, without further notice.

Experimental CapsetFilter

Value space: <S: 0, 100>

Example: `Experimental CapsetFilter: ""`

Experimental Video OSD AlertOnIncomingCall

Value space: <On/Off>

Example: `Experimental Video OSD AlertOnIncomingCall: On`

Experimental Conference [1] PacketLossResilience

Value space: <On/Off>

Example: `Experimental Conference 1 PacketLossResilience: Off`

Experimental SoftwareUpgrade Mode

Value space: <Auto/Manual>

Example: `Experimental SoftwareUpgrade Mode: Auto`

Experimental SoftwareUpgrade ServerAddress

Value space: <S: 0, 255>

Example: `Experimental SoftwareUpgrade ServerAddress: "http://csupdate.tandberg.com/getswlist.py"`

The appendices section provides you with additional information that you may find useful as an system administrator for the EX90.

CHAPTER 4

APPENDICES

Password protection

The system can be password protected:

- The Codec can be password protected with an administrator password.
- The Web interface is password protected with the same administrator password as for the codec, but to make this happen, the codec must be restarted after having set or changed the password

Password settings

Setting the codec administrator password

NOTE! It is recommended to keep a copy of the password in a safe place. Contact your TANDBERG representative if you have forgotten the password.

Define the administrator password on the codec:

1. Connect to the codec through the network or the serial data port, using a command line interface (ssh, telnet or scp).
2. Log in to the codec with user name (admin) and no password (password is blank).
3. Run the following API command and enter a password:
   `xCommand SystemUnit AdminPassword Set Password: "****"`
4. The password format is a string with 0–255 characters.
5. **Reboot** the codec.

Login to the codec

- When logging on to the codec, using a command line interface (ssh, telnet or scp), you are prompted for both the user name and password.
- The user name is admin, and cannot be changed.

How to deactivate the administrator password

1. Connect to the codec through the network, using a command line interface (ssh, telnet or scp).
2. Login to the codec with the required user name (admin) and password.
3. Run the following API command with a blank password:
   `xCommand SystemUnit AdminPassword Set Password: ""`
4. **Reboot** the codec.

Password protection of the web interface

NOTE! If the password protection on the web interface does not work, be aware that after having defined or changed the administrator password, a reboot of the codec is required. Without a reboot the administrator password will only apply when logging in to the codec.

The web interface is password protected with the same administrator password as for the codec.

Login to the web interface

- When logging on to the codec, using a web browser, you are prompted for both the user name and password.
- The user name is admin, and cannot be changed.
- The password cannot be set or changed from the web interface.

Optimal Definition Profiles

Under ideal lighting conditions the bandwidth requirements can be substantial reduced with the optimal definitions profiles.

Generally, we recommend the Optimal Definition set at Normal.

If lighting condition is conducive TANDBERG recommends that you test the endpoint on the various Optimal Definition setting prior to implementation.

To set the optimal definition profile, open a web browser and enter the IP address of the EX90.

- Navigate to Advanced configurations > Video > Input > Source [1..3] > OptimalDefinition > Profile and set the Profile parameters.
- Navigate to Advanced configurations > Video > Input > Source [1..n] > OptimalDefinition > Threshold60fps and set the Threshold60fps parameters.

The video input quality settings must be set to Motion to ensure the Optimal Definition to work. With the video input quality set to Sharpness, the endpoint will transmit the highest resolution possible, regardless of frames per second.

Set the video input quality:

- Navigate to Advanced configurations > Video > Input > Source [1..5] > Quality and set the video quality parameters.

Optimal definition profile

High (720p60)

Typically used in dedicated video conferencing rooms. Requires good lighting conditions for a good overall experience.

Under ideal conditions the bandwidth requirements can be reduced by up to 50%.

Medium (w576p60)

Typically used in rooms with better than normal, and consistent lighting.

The bandwidth requirements can be reduced by up to 25%.

Normal (w448p60)

This setting is typically used in office environments where the environment is normal to poorly lit.

Generally, we recommend the Optimal Definition set at Normal.

Table 1: Optimal definition, for systems supporting 1080p

	w288p30	w448p30	w576p30	720p30	1080p30
Normal	256kbit/s	512 kbit/s	768 kbit/s	1152 kbit/s	2560 kbit/s
Medium	128kbit/s	384 kbit/s	512 kbit/s	1152 kbit/s	1920 kbit/s
High	128kbit/s	256 kbit/s	512 kbit/s	768 kbit/s	1472 kbit/s

Table 2: Optimal definition, for systems supporting 720p60

	w144p60	w288p60	w448p60	w576p60	720p60
Normal	128kbit/s	512 kbit/s	1152 kbit/s	1472 kbit/s	2240 kbit/s
Medium	128kbit/s	384 kbit/s	768 kbit/s	1152 kbit/s	1920 kbit/s
High	128kbit/s	256 kbit/s	512 kbit/s	768 kbit/s	1152 kbit/s

CE Declaration for TANDBERG EX90

For an official, signed version of this document, or details regarding documentation from the technical construction file, please contact TANDBERG.

CE Declaration

EC Declaration of conformity	
MANUFACTURER:	TANDBERG Telecom AS
PRODUCT NAME:	TANDBERG EX90
TYPE NUMBER:	TTC7-19
DESCRIPTION:	Video Conferencing Equipment
DIRECTIVES: This equipment complies with.	LVD 2006/95/EC EMC 2004/108/EC
HARMONIZED STANDARDS: Applied in order to verify compliance with directives.	EN 60950-1:2006 EN 55022 (2006) Class A EN 55024 (1998) + A1 (2001) + A2 (2003) EN 61000-3-2 (2006) EN 61000-3-3 (2008)
TEST REPORTS and CERTIFICATES ISSUED BY:	Reports/Certificates No.: LVD (Nemko AS) 138050 EMC (Nemko AS) E09773.00
TECHNICAL CONSTRUCTION FILE NO.:	X14639
YEAR WHICH THE CE-MARK WAS AFFIXED:	2010

China RoHS table

This products described in this guide complies with the Chineese RoHS.

China RoHS table

产品中有毒有害物质表

部件名称	有毒有害物质或元素					
	铅	汞	镉	六价铬	多溴联苯	多溴二苯醚
金属部件	X	O	O	O	O	O
印刷电路板及组件	X	O	O	O	O	O
线缆和线缆组装	X	O	O	O	O	O
显示器（包括照明灯）	X	X	O	O	O	O

说明:

O：表示该有毒有害物质在此部件所有均质材料中的含量均在中国标准《电子信息产品中有毒有害物质的限量要求》(SJ/T 11363-2006) 所规定的限量要求以下。

X：表示该有毒有害物质至少在该部件的某一均质材料中的含量超出中国标准《电子信息产品中有毒有害物质的限量要求》(SJ/T 11363-2006) 所规定的限量要求。

注意：在所售产品中未必包含所有上述所列部件。

除非在产品上有另外特别的标注，以下标志为针对所涉及产品的环保使用期限标志。环保使用期限只适用于产品在产品手册中所规定的使用条件。

Supported RFCs in SIP

The RFC (Request for Comments) series contains technical and organizational documents about the Internet, including the technical specifications and policy documents produced by the Internet Engineering Task Force (IETF).

RFCs in SIP

Current RFCs and drafts supported in SIP

- RFC 1889 RTP: A Transport Protocol for Real-time Applications
- RFC 2190 RTP Payload Format for H.263 Video Streams
- RFC 2327 SDP: Session Description Protocol
- RFC 2396 Uniform Resource Identifiers (URI): Generic Syntax
- RFC 2429 RTP Payload Format for the 1998 Version of ITU-T Rec. H.263 Video (H.263+)
- RFC 2617 Digest Authentication
- RFC 2782 DNS RR for specifying the location of services (DNS SRV)
- RFC 2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals
- RFC 2976 The SIP INFO Method
- RFC 3016 RTP Payload Format for MPEG-4 Audio/Visual Streams
- RFC 3047 RTP Payload Format for ITU-T Recommendation G.722.1
- RFC 3261 SIP: Session Initiation Protocol
- RFC 3262 Reliability of Provisional Responses in SIP
- RFC 3263 Locating SIP Servers
- RFC 3264 An Offer/Answer Model with SDP
- RFC 3311 UPDATE method
- RFC 3361 DHCP Option for SIP Servers
- RFC 3420 Internet Media Type message/sipfrag
- RFC 3515 Refer method
- RFC 3550 RTP: A Transport Protocol for Real-Time Applications
- RFC 3581 Symmetric Response Routing
- RFC 3605 RTCP attribute in SDP
- RFC 3711 The Secure Real-time Transport Protocol (SRTP)
- RFC 3840 Indicating User Agent Capabilities in SIP
- RFC 3890 A Transport Independent Bandwidth Modifier for SDP
- RFC 3891 The SIP "Replaces" Header
- RFC 3892 Referred-By Mechanism
- RFC 3960 Early Media
- RFC 3984 RTP Payload Format for H.264 Video
- RFC 4028 Session Timers in SIP
- RFC 4145 TCP-Based Media Transport in the SDP
- RFC 4568 SDP:Security Descriptions for Media Streams
- RFC 4574 The Session Description Protocol (SDP) Label Attribute
- RFC 4582 The Binary Floor Control Protocol
- RFC 4585 Extended RTP Profile for RTCP-Based Feedback
- RFC 4587 RTP Payload Format for H.261 Video Streams
- RFC 4629 RTP Payload Format for ITU-T Rec. H.263 Video
- RFC 5168 XML Schema for Media Control
- RFC 4796 The SDP Content Attribute
- RFC 4583 SDP Format for BFCP Streams
- RFC 5589: SIP Call Control Transfer
- draft-ietf-avt-rtp-h264-rcdo-02
- draft-ietf-avt-rtp-rfc3984bis-06
- draft-ietf-sip-outbound-20: Managing Client Initiated Connections

Media capabilities supported in SIP

The audio and video media capabilities supported in SIP are the same as for H.323.

Technical specifications

The unit is delivered with a fully integrated codec, display, camera, microphone and loudspeakers, and the TANDBERG InTouch controller, including detachable wideband handset.

Technical specifications for EX90

UNIT DELIVERED COMPLETE WITH:

Fully integrated codec, display, camera, microphone and loudspeakers

TANDBERG InTouch controller including detachable wideband handset

DVI-I-cable, DVI-I to VGA adapter, 3,5 mm jack audio cable, LAN cable, power adapter and power cable

DISPLAY

24" LCD monitor

Resolution: 1920 x 1200 (WUXGA)

Contrast ratio: 1000:1

Viewing angle: 160/160°

Response time: 5ms

Brightness: 300cd/m2

5°-15° tilt

PC AND SECOND SOURCE VIDEO INPUTS

DVI-I

HDMI

SUPPORTED PC INPUT RESOLUTIONS

SVGA (800x600) to WUXGA (1920X1200)

DUAL DISPLAY OUTPUT*

HDMI

CAMERA

TANDBERG PrecisionHD™ design

Document camera mode

1/3" CMOS sensor

2.7 megapixels

Aperture F1.7

1920x1080@60 fps

Optical, motorized zoom

45°-65° horizontal field of view

40°-27° vertical field of view

Auto focus

Mechanical auto iris

Focus distance 0.3m–infinity

Automatic and manual exposure and white balance

Ambient light frequency detection (50/60 Hz)

Integrated privacy shutter

AUDIO SYSTEM

2 stereo front speakers

Integrated subwoofer

Integrated full range microphone

Support for TANDBERG Performance Mic 20 external microphone

1x3.5 mm line in jack for PC or other audio source

2x3.5 mm jack for headset

HDMI audio input/output

Wideband handset

Bluetooth ready

USER INTERFACE

TANDBERG inTouch

8" projected capacitive touch screen

480x800 resolution

BANDWIDTH

H.323/SIP up to 6 Mbps point-to-point

FIREWALL TRAVERSAL

TANDBERG Expressway™ Technology

H.460.18, H.460.19 Firewall Traversal

VIDEO STANDARDS

H.261, H.263, H.263+, H.264

VIDEO FEATURES

16:9 Widescreen

Advanced Screen Layouts

Intelligent Video Management

Local Auto Layout

LIVE VIDEO RESOLUTIONS (ENCODE/DECODE)

176 x 144@30 fps (QCIF)

352 x 288@30 fps (CIF)

512 x 288@30 fps (w288p)

576 x 448@30 fps (448p)

768 x 448@30 fps (w448p)

704 x 576@30 fps (4CIF)

1024 x 576@30 fps (w576p)

640 x 480@30 fps (VGA)

800 x 600@30 fps (SVGA)

1024 x 768@30 fps (XGA)

1280 x 1024@30 fps (SXGA)

1280 x 720@30 fps (720p30)

1280 x 768@30 fps (WXGA)

1920 x 1080@30 fps (1080p30)*

1440 x 900@30 fps (WXGA+)*

1680 x 1050@30 fps (WSXGA+)*

1600 x 1200@30 fps (UXGA)*

1920 x 1200@15 fps (WUXGA)*

512 x 288@60 fps (w288p60)*

768 x 448@60 fps (w448p60)*

1024 x 576@60 fps (w576p60)*

1280 x 720@60 fps (720p60)*

AUDIO STANDARDS

G.711, G.722, G.722.1, 64/128kbps MPEG4 AAC-LD, AAC-LD Stereo

AUDIO FEATURES

CD-quality 20kHz stereo

Acoustic echo cancelling

Automatic gain control

Automatic noise reduction

Active lip synchronization

Technical specifications for EX90, *continued...*

DUAL STREAM

H.239 (H.323) dual stream

BFCP (SIP) dual stream

Support for resolutions up to 1080p30 in both main stream and dual stream simultaneously

MULTISITE FEATURES*

4-way 720p30 Continuous Presence (CP) MultiSite**

Full individual audio and video transcoding

Individual layouts for all participants (CP layout without self view)

H.323/SIP/VoIP in the same conference

Best Impression (Automatic CP Layouts)

H.264, encryption and dual stream from any site

IP downspeeding

Dial in/Dial out

Conference rates up to 10 Mbps

PROTOCOLS

H.323

SIP

EMBEDDED ENCRYPTION

H.323/SIP point-to-point

Standards-based: H.235 v2 & v3 and AES

Automatic key generation and exchange

Supported in dual stream

IP NETWORK FEATURES

DNS lookup for service configuration

Differentiated Services (QoS)

IP adaptive bandwidth management (including flow control)

Auto gatekeeper discovery

Dynamic playout and lip-sync buffering

H.245 DTMF tones in H.323

Date and time support via NTP

Packet loss based downspeeding

URI dialing

TCP/IP

DHCP

802.1x network authentication

802.1q VLAN

SECURITY FEATURES

Management via HTTPS and SSH

IP administration password

Menu administration password

Disable IP services

Network settings protection

NETWORK INTERFACES

Internal 2 port Ethernet switch

1 x LAN/Ethernet (RJ-45) 10/100/1000 Mbit for PC

1 x LAN/Ethernet (RJ-45) 10/100/1000 Mbit for LAN

OTHER INTERFACES

1x USB device for future applications

2x USB host for future applications

Bluetooth for future applications

SYSTEM MANAGEMENT

Support for the TANDBERG Management Suite

Total management via embedded SNMP, Telnet, SSH, XML, SOAP

Remote software upload: via web server, SCP, HTTP, HTTPS

InTouch interface menu system

DIRECTORY SERVICES

Support for local directories (My Contacts)

Corporate directory

Unlimited entries using server directory supporting

LDAP and H.350

Unlimited number for corporate directory (through TMS)

200 number local directory

Received calls

Placed calls

Missed calls with date and time

POWER

Auto-sensing power supply

100–240 VAC, 50/60 Hz

150 watts max

OPERATING TEMPERATURE AND HUMIDITY

0° C to 35° C (32° F to 95° F) ambient temperature

10% to 90% Relative Humidity (RH)

STORAGE AND TRANSPORT TEMPERATURE

-20° C to 60° C (-4° F to 140° F) at RH 10–90% (non-condensing)

APPROVALS

Directive 2006/95/EC (Low-Voltage Directive) — Standard EN 60950-1

Directive 2004/108/EC (EMC Directive) — Standard EN 55022, Class A — Standard EN 55024 — Standard EN 61000-3-2/-3-3

Approved according to UL 60950-1 and CSA 60950-1-07

Complies with FCC15B Class A

TANDBERG EX90 MAIN UNIT DIMENSIONS

Length: 56.7 cm (22.3")

Height: 54.5 cm (21.4")

Depth: 17.3 cm (6.8")

Weight: 11.0 kg (24.2 lbs)

TANDBERG INTOUCH CONTROLLER DIMENSIONS

Length: 22.8 cm (9.0"). 29.0 cm (11.4") with handset

Height: 4.4cm (1.7") cm. 7.7 cm (3.0") with handset

Depth: 14.5 cm (5.7"). 18.7 cm (7.4") with handset

Weight: 0.64 kg (1.4 lbs). 0.94 kg (2.1 lbs) with handset

Cable length: 120 cm (47")

* Requires option

** 3 way MultiSite in first release

All specifications subject to change without notice, system specifics may vary.

All images in these materials are for representational purposes only, actual products may differ.

MTBF PRODUCT RELIABILITY/MTBF

The predicted reliability is expressed in the expected random Mean Time Between Failures (MTBF) for the electronic components based on the Power On Hours: Power On Hours (POH) > 69 000 hoursUseful Life Cycle > 6 yearsISO 9001 certificate is available upon request

June 2010

TANDBERG

TANDBERG is now a part of Cisco

U.S. HEADQUARTERS
TANDBERG
1212 Avenue of the Americas
24th Floor
New York, NY 10036
Telephone: +1 212 692 6500
Fax: +1 212 692 6501
Video: +1 212 692 6535
E-mail: tandberg@tandberg.com

EUROPEAN HEADQUARTERS
TANDBERG
Philip Pedersens vei 20
1366 Lysaker
Norway
Telephone: +47 67 125 125
Fax: +47 67 125 234
Video: +47 67 126 126
E-mail: tandberg@tandberg.com