TANDBERG Gatekeeper
User Manual

Software version N1
D13381.01

TANDBERG

Trademarks and copyright

Disclaimer

The information in this document is furnished for informational purposes only, is subject to change without prior notice, and should not be construed as a commitment by TANDBERG ASA.

The information in this document is believed to be accurate and reliable, however TANDBERG ASA assumes no responsibility or liability for any errors or inaccuracies that may appear in this document, nor for any infringements of patents or other rights of third parties resulting from its use. No license is granted under any patents or patent rights of TANDBERG ASA.

Environmental Issues

Thank you for buying a product which contributes to a reduction in pollution, and thereby helps save the environment. Our products reduce the need for travel and transport and thereby reduce pollution. Our products have either none or few consumable parts (chemicals, toner, gas, paper). Our products are low energy consuming products.

TANDBERG's Environmental Policy

- TANDBERG's Research and Development is continuously improving TANDBERG's products towards less use of environmentally hazardous components and substances as well as to make the products easier to recycle.
- TANDBERG's products are Communication Solutions. The idea of these solutions is to reduce the need for expensive, time demanding and polluting transport of people. Through people's use of TANDBERG's products, the environment will benefit from less use of polluting transport.
- TANDBERG's wide use of the concepts of outsourcing makes the company itself a company with a low rate of emissions and effects on the environment.
- TANDBERG's policy is to make sure our partners produce our products with minimal influence on the environment and to demand and audit their compatibility according to applicable agreements and laws (national and international).

Environmental Considerations

Like other electronic equipment, the TANDBERG Gatekeeper contains components that may have a detrimental effect on the environment. TANDBERG works continuously towards eliminating these substances in our products.

- Printed-wiring boards made of plastic, with flame-retardants like Chloride or Bromide.
- Component soldering that contains lead.
- Smaller components containing substances with possible environmental effect.

After the product's end of life cycle, it should be returned to authorized waste handling and should be treated according to National and International Regulations for waste of electronic equipment.

Operator Safety Summary

For your protection, please read these safety instructions completely before operating the equipment and keep this manual for future reference. The information in this summary is intended for operators. Carefully observe all warnings, precautions and instructions both on the apparatus and in the operating instructions.

Warnings

- Water and moisture - Do not operate the equipment under or near water - for example near a bathtub, kitchen sink, or laundry tub, in a wet basement, or near a swimming pool or in areas with high humidity.
- Cleaning - Unplug the apparatus from the wall outlet before cleaning or polishing. Do not use liquid cleaners or aerosol cleaners. Use a lint-free cloth lightly moistened with water for cleaning the exterior of the apparatus.
- Ventilation - Do not block any of the ventilation openings of the apparatus. Install in accordance with the installation instructions. Never cover the slots and openings with a cloth or other material. Never install the apparatus near heat sources such as radiators, heat registers, stoves, or other apparatus (including amplifiers) that produce heat.
- Grounding or Polarization - Do not defeat the safety purpose of the polarized or grounding-type plug. A polarized plug has two blades with one wider than the other. A grounding type plug has two blades and a third grounding prong. The wide blade or third prong is provided for your safety. If the provided plug does not fit into your outlet, consult an electrician.
- Power-Cord Protection - Route the power cord so as to avoid it being walked on or pinched by items placed upon or against it, paying particular attention to the plugs, receptacles, and the point where the cord exits from the apparatus.
- Attachments - Only use attachments as recommended by the manufacturer.
- Accessories - Use only with a cart, stand, tripod, bracket, or table specified by the manufacturer, or sold with the apparatus. When a cart is used, use caution when moving the cart/apparatus combination to avoid injury from tip-over.
- Lightning - Unplug this apparatus during lightning storms or when unused for long periods of time.
- Servicing - Do not attempt to service the apparatus yourself as opening or removing covers may expose you to dangerous voltages or other hazards, and will void the warranty. Refer all servicing to qualified service personnel.
- Damaged Equipment - Unplug the apparatus from the outlet and refer servicing to qualified personnel under the following conditions:
    - When the power cord or plug is damaged or frayed
    - If liquid has been spilled or objects have fallen into the apparatus
    - If the apparatus has been exposed to rain or moisture
    - If the apparatus has been subjected to excessive shock by being dropped, or the cabinet has been damaged
    - If the apparatus fails to operate in accordance with the operating instructions.

Table Of Contents

1 Introduction

This User Manual is provided to help you make the best use of your TANDBERG Gatekeeper.

A Gatekeeper is a central part of an H.323 infrastructure. It provides address translation and controls access to the network for H.323 terminals, Gateways and MCUs. The Gatekeeper also provides other services to the terminals, Gateways and MCUs such as bandwidth management and locating Gateways.

The main features of the TANDBERG Gatekeeper are:

- Automatic discovery and manual registrations of H.323 terminals, gateways and MCUs.
- Registration of H.323 ID, E.164 aliases and services.
- Supports up to 1000 registered devices and services.
- Supports up to 100 neighbouring zones.
- Direct call signaling intra- and inter-zone with up to 200 active calls.
- Flexible zone configuration with named zones and default zone.
- Can function as a leaf Gatekeeper or as a master Gatekeeper in a Gatekeeper hierarchy.
- Can be used to control the amount of bandwidth used both within a Gatekeeper zone and to neighbouring zones.
- Can limit total bandwidth usage and set maximum per call bandwidth usage with automatic down-speeding if call exceeds per-call maximum.
- Secure management with HTTPS, SSH, and SCP (secure file transfer).
- Can lock-down IP services.
- Can be managed with TANDBERG Management Suite 9.0 or newer, or as a standalone Gatekeeper with RS-232, Telnet, or SSH.
- Embedded setup wizard on serial port for initial configuration.

Note
Features may vary depending on software package.

1.1 TANDBERG Gatekeeper Overview

On the front of the Gatekeeper there are three LAN interfaces, a serial port (Data 1) and a Light Emitting Diode (Power). The LAN 1 interface is used for connecting the Gatekeeper to your local area network, LAN interface 2 and 3 are disabled. The serial port (Data 1) is for connection to a PC, and power on is indicated by the Light Emitting Diode (Power) being lit.

The back of the Gatekeeper has a power connector, a power switch, and a serial port (Data 2) for connecting to a PC.

2 Installation

Precautions:

- Never install communication equipment during a lightning storm.
- Never install jacks for communication cables in wet locations unless the jack is specifically designed for wet locations.
- Never touch uninstalled communication wires or terminals unless the communication line has been disconnected at the network interface.
- Use caution when installing or modifying communication lines.
- Avoid using communication equipment (other than a cordless type) during an electrical storm.
- There may be a remote risk of electrical shock from lightning.
- Do not use communication equipment to report a gas leak in the vicinity of the leak.
- The socket outlet shall be installed near to the equipment and shall be easily accessible.
- Never install cables without first switching the power OFF.
- This product complies with directives: LVD 73/23/EC and EMC 89/366/EEC.
- Power must be switched off before power supplies can be removed from- or installed into the unit.

2.1 Unpacking

The TANDBERG Gatekeeper is delivered in a special shipping box which should contain the following components**:**

- Gatekeeper unit
- Installation sheet
- User manual and other documentation on CD
- Rack-ears and screws
- Kit with 4 rubber feet.
- Cables:
    - Power cables
    - One Ethernet cable
    - One null-modem RS-232 cable

Installation site preparations

- Make sure that the Gatekeeper is accessible and that all cables can be easily connected.
- For ventilation: Leave a space of at least 10cm (4 inches) behind the Gatekeeper's rear and 5cm (2 inches) on the sides.
- The room in which you install the Gatekeeper should have an ambient temperature between 0°C and 35°C (32°F and 95°F) and between 10% and 90% non-condensing relative humidity.
- Do not place heavy objects directly on top of the Gatekeeper.
- Do not place hot objects directly on top, or directly beneath the Gatekeeper.
- Use a grounded AC power outlet for the Gatekeeper.

2.2 Mounting

The Gatekeeper comes with brackets for mounting in standard 19" racks.

Before starting the rack mounting, please make sure the TANDBERG Gatekeeper is placed securely on a hard, flat surface.

1. Disconnect the AC power cable.
2. Make sure that the mounting space is according to the `Installation site preparations' in section 0.
3. Attach the brackets to the chassis on both sides of the unit.
4. Insert the unit into a 19" rack, and secure it with screws.

2.3 Connecting Cables

Power cable
Connect the system power cable to an electrical distribution socket.

LAN cable
Connect a LAN cable from the LAN 1 connector on the front of the unit to your local area network.

Null-modem RS-232 cable
Connect the supplied null-modem RS-232 cable between the Gatekeeper's Data 1 connector and the COM-port on a PC.

2.4 Switching on the System

To start the TANDBERG Gatekeeper, make sure that the following has been done:

- The power cable is connected.
- The LAN cable is connected

Then switch the power switch button on the back of the unit to `1'.

On the front of the chassis you will see the Power LED being lit.

2.5 Gatekeeper Initial Configuration

The TANDBERG Gatekeeper requires some configuration settings before it can be used. This must be done using a PC connected to the serial port (Data 1).

The main thing that needs to be configured are the IP settings of the Gatekeeper. This includes the IP address, the IP subnet mask, and the IP gateway. The Gatekeeper has to be configured with a static IP address. Consult your network administrator for information on which addresses to use.

To set the initial configuration, do the following:

1. Connect the supplied null-modem RS-232 cable from Data 1 to a PC running a terminal program.
2. Start the terminal program and configure it with baud rate 115200, 8 data bits, no parity, 1 stop bit, no flow control.
3. Power on the unit if it is not already on.
4. You should see the unit display start up information.
5. After approximately 1 minute you will get a login prompt.
6. Enter username ‘admin’ and your password. The default password is TANDBERG.
7. You will be prompted if you want to run the install wizard. Type ‘Y’ and press Enter.

```
(none) login: admin
Password:
Run install wizard [n]: Y
```

8. Specify the following:
    a. The password you want to use for your Gatekeeper. This password is used to login to the Gatekeeper with the Admin user account.
    b. The IP address of the Gatekeeper.
    c. The IP subnet mask of the Gatekeeper.
    d. The IP default gateway of the Gatekeeper.
    e. The Ethernet speed.
    f. The local zone prefix you want to use for the zone controlled by this Gatekeeper.
    g. Whether you want to use SSH to configure the Gatekeeper.
    h. Whether you want to use Telnet to configure the Gatekeeper.
9. You will be prompted to login again. You should see the following welcome information.
10. Login with username ‘admin’ and your password.

```
Welcome to
TANDBERG Gatekeeper Release N1.0
SW Release Date: 2004-07-05
OK
```

11. Review other system settings. You may want to set the following:
    a. The name of the Gatekeeper. This is used to identify the Gatekeeper by the TANDBERG Management Suite. See the `xConfiguration SystemUnit` command in section 0 for more information on setting the name.
    b. Automatic discovery. If you have multiple Gatekeepers in the same network you may want to disable automatic discovery on some of the Gatekeepers. See the `xConfiguration Gatekeeper AutoDiscovery` command in section 0 for more information.
12. Reboot the Gatekeeper by typing the command `xCommand boot` to make your new settings take effect.
13. Disconnect the serial cable.

NOTE
To secure the Gatekeeper you should disable SSH and Telnet. SSH is a more secure way of communicating with the Gatekeeper than Telnet so if you need IP connectivity you should use SSH.

NOTE
If you don't have an IP gateway, configure it with a non used IP address that is valid in your subnet as your IP gateway.

3 Using the Gatekeeper

The gatekeeper is used by H.323 terminals, Gateways and MCUs. These devices register with the gatekeeper and the gatekeeper then provides address translation and controls access to the network.

3.1 Registration

Before an endpoint can use the Gatekeeper it must register with the Gatekeeper. There are two ways an endpoint can register:

- Automatically.
- Manually by specifying the IP address of the Gatekeeper.

You can disable automatic registration on the Gatekeeper. See auto discovery in section 0 for more information.

When registering, the endpoint registers with one or more of the following:

- A H.323 ID
- One or more E.164 aliases.
- One or more services.

Users on other registered endpoints can then call the endpoint by using either the H.323 ID, an E.164 alias, or one of the services.

Consult the endpoint documentation for information on how to configure it with a Gatekeeper.

NOTE
Automatically discovery is a function that allows the Gatekeeper to reply to Gatekeeper discovery messages from the endpoint.

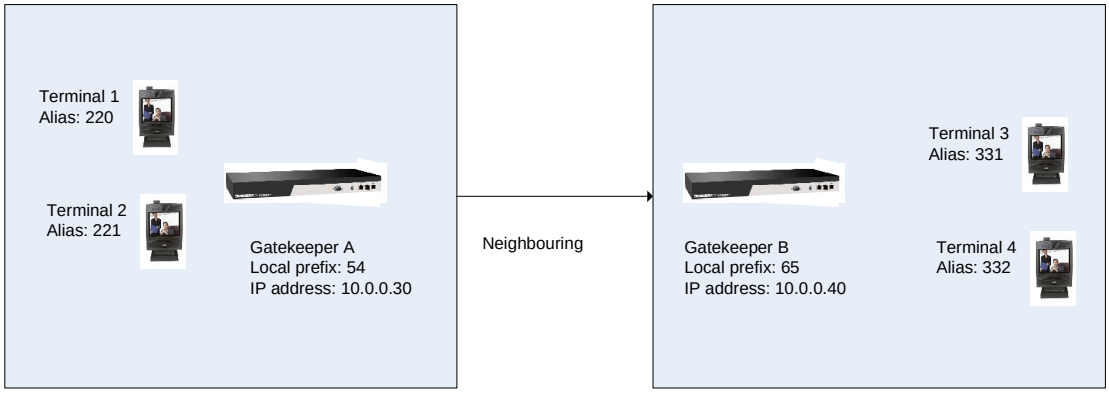
NOTE
If you have problems registering the endpoint, try turning on automatic discovery. Some endpoints require automatic registration to be enabled on the gatekeeper.

3.2 Zones

A zone is the collection of all terminals, Gateways, and Multipoint Control Units managed by a single Gatekeeper. A zone has one and only one Gatekeeper. A zone may be independent of network topology and may be comprised of multiple network segments.

Each zone has a local prefix which is used to reach the zone from other zones. A zone may be connected to other zones by configuring neighbouring.

The figure below shows an example with two zones, zone A with local prefix 54 and zone B with local prefix 65. A also has B configured as its neighbour.



This means that a system in zone A can call a system in zone B. If terminal 1 wants to dial terminal 3 it can do so by prefixing the number of terminal 3 with the zone prefix of zone B; the number to dial will then be 65331.

The TANDBERG Gatekeeper also supports a default or parent gatekeeper. A gatekeeper can have only one parent gatekeeper. The parent gatekeeper is contacted if the number called does not match a registered system, a service or a configured zone.

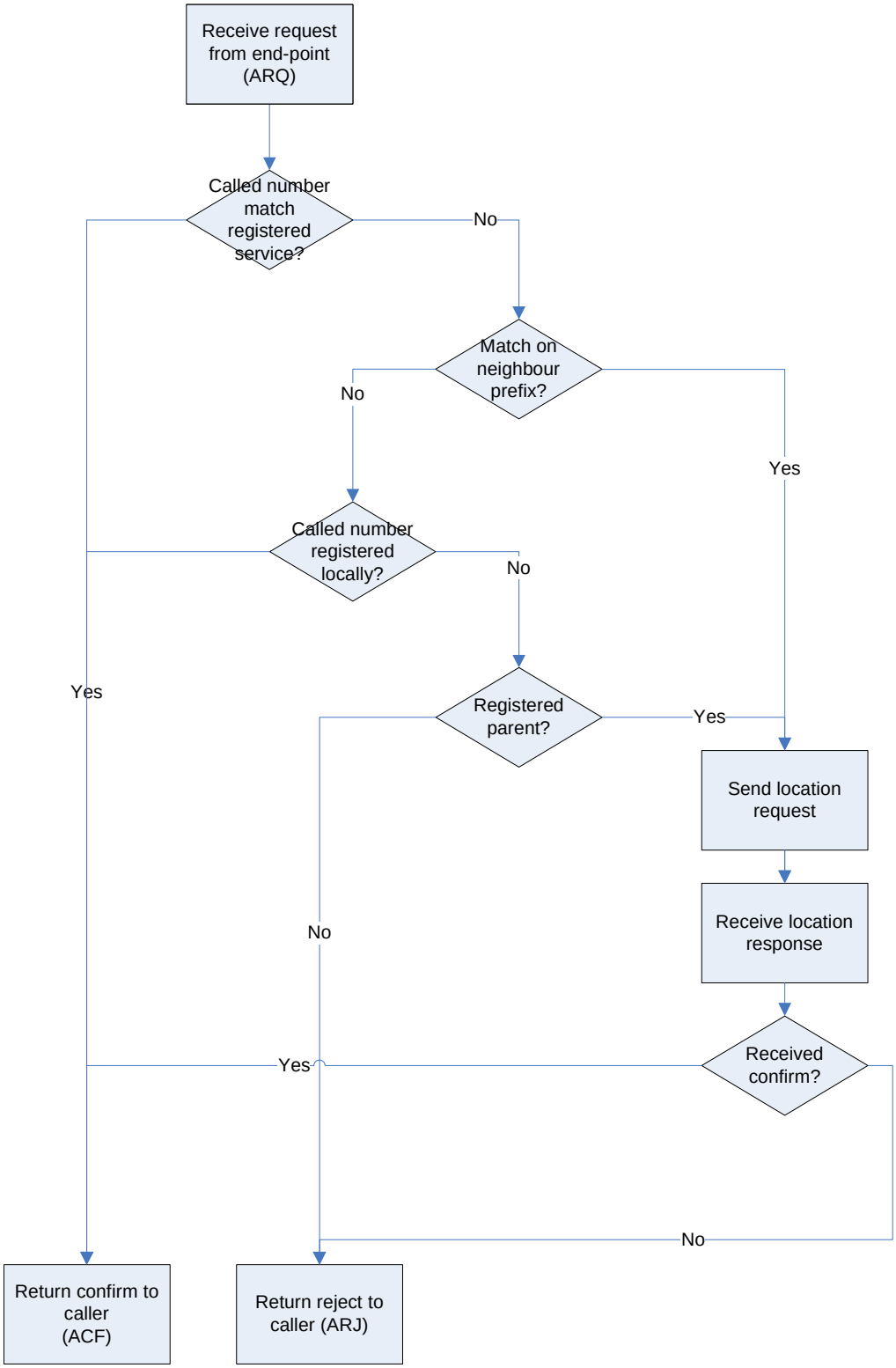
In the example above, if Gatekeeper A had configured Gatekeeper B as its parent. Terminal 1 could call Terminal 3 by dialing 331. Gatekeeper A will not recognize 331 as a registered alias and because of this “forward” the request to the parent gatekeeper in zone B.

3.3 Call Control

When an end-point wants to call another endpoint it presents the number it wants to call to the gatekeeper using a protocol knows as RAS. The Gatekeeper tries to resolve the number and supplies the calling endpoint with information about the called endpoint.

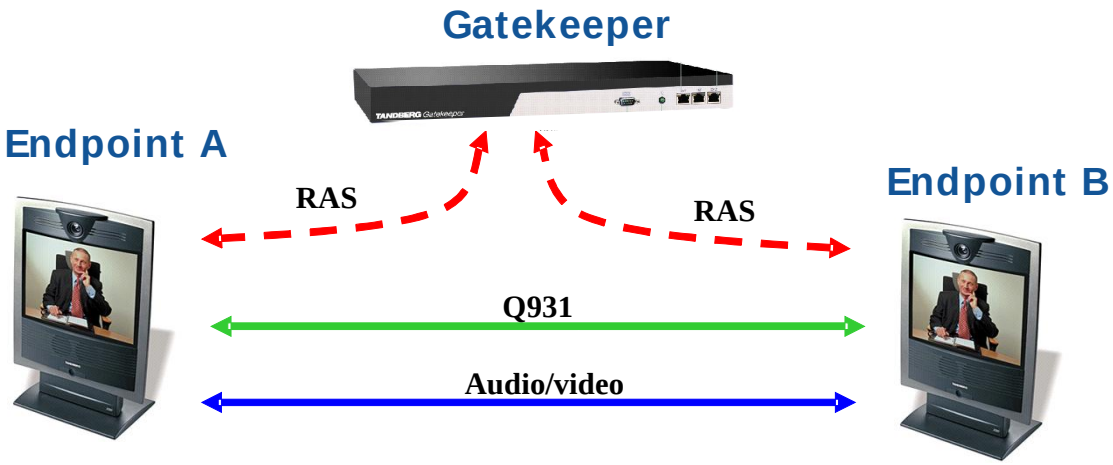
NOTE
RAS, Registration, Admission and Status Protocol. Used by endpoints and gatekeepers to communicate.

The diagram below illustrates the process the gatekeeper performs when receiving the request:



When a confirm message is sent back to the caller, the confirm message includes information about the called system, including the IP address.

The calling endpoint then sets up the call to the other endpoint directly using a protocol know as Q931. Audio and video is also transmitted directly between the endpoints. The figure below illustrates this:



NOTE
Q931 is used for call setup to establish and disconnect H.323 calls.

3.4 Bandwidth Control

The TANDBERG Gatekeeper can be used to control the amount of bandwidth used by H.323 systems in a gatekeeper zone or between gatekeeper zones.

You can specify four different settings:

- Maximum bandwidth for a call to an endpoint in the zone (intra zone).
- Maximum bandwidth for a call to an endpoint outside the zone (inter zone).
- Maximum total bandwidth used for all calls in the zone (intra zone).
- Maximum total bandwidth used for all calls to and from endpoints outside the zone (inter zone).

If an endpoint tries to set up a call with a bandwidth higher than the per call limit, the gatekeeper will down-speed the call to the maximum bandwidth.

If a call would make the maximum total bandwidth limitation be exceeded, the call will be rejected.

4 Software Upgrade

Software upgrade can be done in one of two ways:

- Using a web browser (HTTP/HTTPS).
- Using secure copy (SCP).

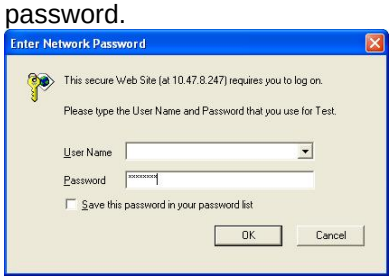
NOTE
To upgrade the Gatekeeper, a valid Release Key and software file is required. Contact your TANDBERG representative for more info.

NOTE
Configuration is restored after performing an upgrade but we recommend that you make a backup of the existing configuration using the TANDBERG Management Suite before performing the upgrade.

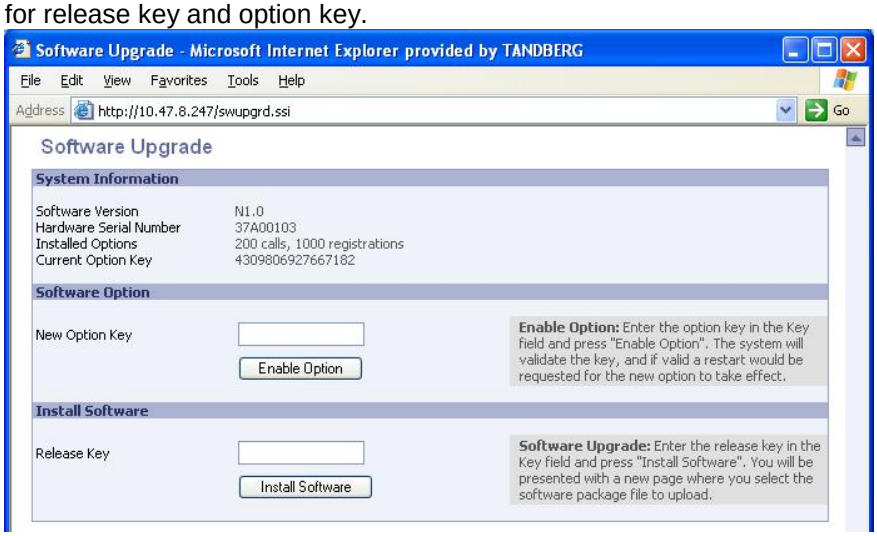
4.1 Upgrading Using HTTP(S)

To upgrade using HTTP(S), do the following:

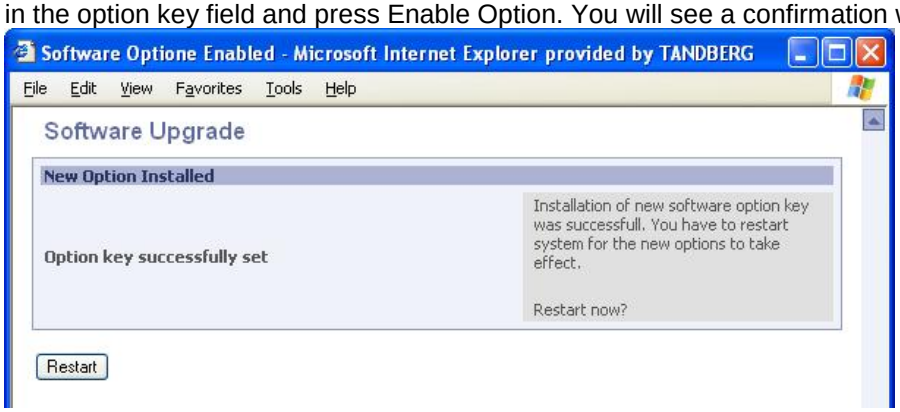
1. Point your browser at the IP address of the Gatekeeper. You will be prompted for password.



2. Leave the user name blank, enter the password and press OK. You will be prompted for release key and option key.

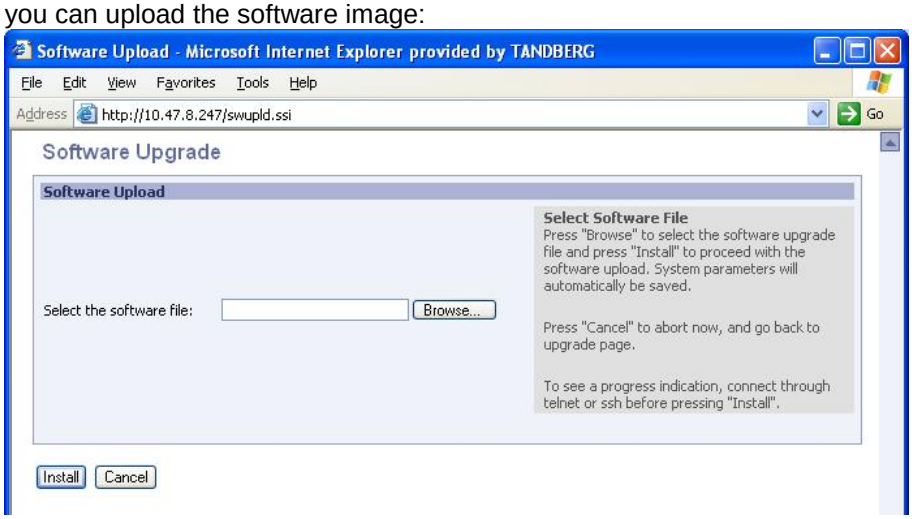


3. If you have no new options, you can skip to step 5. If you do have new options you should install the new option key before installing the software. Enter the option key in the option key field and press Enable Option. You will see a confirmation window:

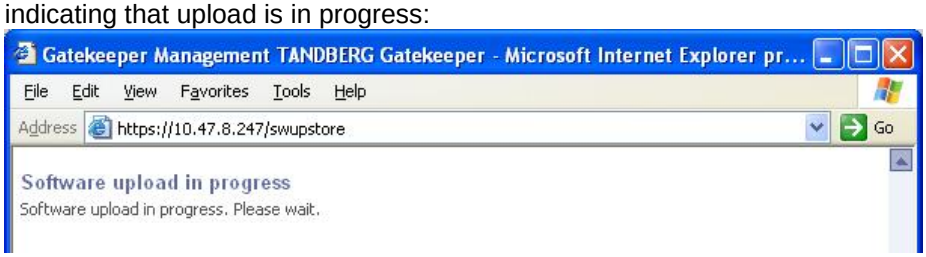


4. You should install the new software before restarting, select Back in your browser to go back to the install software page.

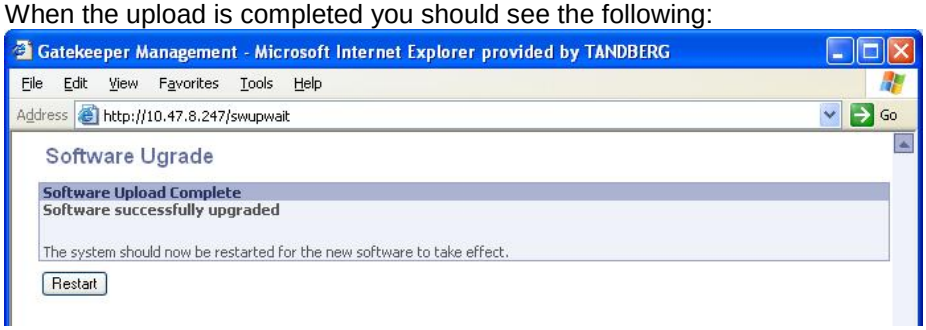
5. Enter the release key and press Install Software. You will get a new screen where you can upload the software image:



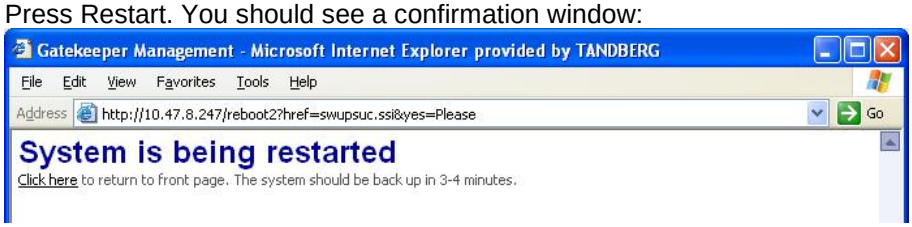
6. Browse to the file containing the software and press Install. You should see a page indicating that upload is in progress:



7. When the upload is completed you should see the following:



8. Press Restart. You should see a confirmation window:



9. The software is installed. The system will then perform another reboot to restore system parameters. After 3-4 minutes, the gatekeeper is ready for use.

4.2 Upgrading Using SCP

To upload using SCP you need an SCP program.

Using SCP you need to transfer two files to the Gatekeeper

- A text file containing the release key.
- A file containing the software image.

NOTE
Make sure you transfer the release key file before transferring the software image. Also make sure you name the files exactly as described below.

NOTE
The release key file should contain the 16 character release key, noting else. Make sure it does not contain line feeds.

To upgrade using SCP, do the following:

1. Connect the supplied null-modem RS-232 cable from Data 2 to a PC running a terminal program to monitor the transfer. You can also use SSH to monitor the transfer.
2. Start the terminal program and configure it with baud rate 115200, 8 data bits, no parity, 1 stop bit and no flow control.
3. Make sure the gatekeeper is turned on and available on IP.
4. Upload the release key file using scp to the /tmp folder on the Gatekeeper, e.g. `pscp release-key root@10.47.8.247:/tmp/release-key`
5. Enter password when prompted.
6. Copy the software image using SCP. The target name must be /tmp/tandberg-image.tar.gz, e.g.

```
pscp s42000n10.tar.gz root@10.47.8.247:/tmp/tandberg-
image.tar.gz
```

7. Enter password when prompted.
8. Wait until the software has installed completely. This should not take more than 2 minutes.
9. Reboot the gatekeeper.
10. After one minute the gatekeeper is ready to use.

5 Configuring the Gatekeeper

To configure and monitor the gatekeeper you can to use the command line interface which is available over SSH and Telnet, or through the serial port. The interface is the same using serial port, Telnet, and SSH.

To enter commands you should start a Telnet or an SSH session and login with username 'admin' and your password.

The interface groups information in different commands

- *Status root command:*
  - `xstatus`
- *Configuration root command:*
  - `xconfiguration`
- *Command root command:*
  - `xcommand`

To list all root commands, type '?'.

This chapter lists the basic usage of each command. The commands also support more advanced usage, which is outside the scope of this document.

5.1 Status

The status root command, xstatus, returns status information from the gatekeeper.

To list all xstatus commands type

```
xstatus ?
```

To list all status information, type

```
xstatus
```

Command	*Usage*	*Description*

Call	`xstatus Calls`
	
	`xstatus Calls Call <n>`
		Returns a list of active calls on the gatekeeper
		
		or
		
		information about a specific call

Ethernet	`xstatus Ethernet MacAddress`	Returns the MAC address of the LAN 1 interface
	`xstatus Ethernet Speed`	Returns the speed of the Ethernet link. Reports Down if the link is down or not connected.
IP	`xstatus IP`	Returns the active IP configuration of the Gatekeeper with IP address, subnet mask and gateway. Note that if you have changed the IP configuration without rebooting, xstatus IP will return the original settings currently in effect.

Command	*Usage*	*Description*

Registrations	`xstatus Registrations`
	
	`xstatus Registrations Registration <n>`
		Returns a list of registered endpoints on the gatekeeper
		
		or information about a specific registration

ResourceUsage	`xstatus ResourceUsage`	Reports usage of system resources. `Registrations`: Number of currently registered endpoints. `MaxRegistrations`: Maximum number of registered endpoints since system start. `PortRegistrations`: Total number of currently registered endpoints and services. `MaxPortRegistratoins`. Maximum number of registered endpoints and services since system start. `Calls/PortCalls`: Number of currently active calls. `MaxCalls/MaxPortCalls`: Maximum number of calls since system start. `IntraZoneBandwidth`: Total bandwidth used intra zone. `InterZoneBandwidth`. Total bandwidth used to all neigbouring zones.
SystemUnit	`xstatus SystemUnit`	Reports information about the system • Product name • Uptime • Software version • Software name • Release date • Number of calls supported • Number of registered endpoints and services supported • Hardware serial number

Zones	`xstatus Zones`
	
	`xstatus Zones Zone <n>`
		List all configured neigbouring zones or information about a specific zone.

5.2 Configuration

The configuration root command, xconfiguration, is used to set configuration settings.

To list all xconfiguration commands type

```
xconfiguration ?
```

To list all configuration data, type

```
xconfiguration
```

To show a specific configuration value, type

```
xconfiguration <name>
```

To show usage information for a specific configuration value, type

```
xconfiguration <name> ?
```

To set a configuration element type

```
xconfiguration <name> <param1>: value1 <param2>: value2
```

There is also a shorthand for configuration element with several parameters:

```
xconfiguration <name> value1 value2
```

NOTE
Remember to use the colon after naming the parameters.

Command	*Usage*	*Description*
Ethernet	`xconfiguration Ethernet Speed: <Auto/10half/10full/100half/100full/>`	Sets the speed of the Ethernet link. Use auto to automatically configure the speed. To get the current speed, use the `xstatus Ethernet Speed` command. You must restart the gatekeeper for changes to take effect.
LocalPrefix	`xConfiguration Gatekeeper LocalPrefix: <prefix>`	Set the local zone prefix of the gatekeeper.
IntraZone Bandwidth	`xConfiguration Gatekeeper IntraZoneBandwidth Total: <bandwidth>`	Set the maximum total bandwidth allowed within the gatekeeper zone. Specify the value in kbps, e.g. to specify a maximum of 10000 kbps (10Mb) `xConfiguration Gatekeeper IntraZoneBandwidth Total: 10000` To have no limit, specify 0. See also section 0.
	`xConfiguration Gatekeeper IntraZoneBandwidth PerCall: <bandwidth>`	Set the maximum bandwidth allowed for a call within the gatekeeper zone. Specify the value in kbps, e.g. to specify a maximum of 768 kbps: `xConfiguration Gatekeeper PerCall: 768` To have no limit, specify 0. See also section 0.
InterZone Bandwidth	`xConfiguration Gatekeeper InterZoneBandwidth Total: <bandwidth>`	Set the maximum total bandwidth allowed to and from end points outside the gatekeeper zone. Specify the value in kbps, e.g. to specify a maximum of 5000 kbps: `xConfiguration Gatekeeper InterZoneBandwidth Total: 5000` To have no limit, specify 0. See also section 0.
	`xConfiguration Gatekeeper InterZoneBandwidth PerCall: <bandwidth>`	Set the maximum bandwidth allowed for a call to or from endpoints outside the gatekeeper zone. Specify the value in kbps, e.g. to specify a maximum of 384 kbps: `xConfiguration Gatekeeper PerCall: 384` To have no limit, specify 0. See also section 0.

Command	*Usage*	*Description*
AutoDiscovery	`xConfiguration Gatekeeper AutoDiscovery: <On/Off>`	Specifies if the gatekeeper supports automatic registration of endpoints. The default is On
Parent Gatekeeper	`xConfiguration Gatekeeper ParentGatekeeper: <IPAddr>`	Specifies the IP address of a parent gatekeeper. See section 0 for more information. To disable the parent gatekeeper, specify 0.0.0.0 as the IP address.
HTTP	`xConfiguration HTTP Mode: <On/Off>`	Enables/disables HTTP support. You must restart the gatekeeper for changes to take effect.
HTTPS	`xConfiguration HTTPS Mode: <On/Off>`	Enables/disables HTTPS support. Note that HTTP must also be enabled. You must restart the gatekeeper for changes to take effect.
IP	`xConfiguration IP Address: <IPAddr>`	Specify the IP address of the gatekeeper. You must restart the gatekeeper for changes to take effect.
	`xConfiguration IP SubnetMask: <IPAddr>`	Specify the IP subnet mask of the gatekeeper. You must restart the gatekeeper for changes to take effect.
	`xConfiguration IP Gateway: <IPAddr>`	Specify the IP gateway of the gatekeeper. You must restart the gatekeeper for changes to take effect.
OptionKey	`xConfiguration OptionKey Calls: <optionkey>`	Specify the option key of your software options. The command xstatus system software configuration can be used to query the existing options enabled. You must restart the gatekeeper for changes to take effect.
SNMP	`xConfiguration SNMP Mode: <On/Off>`	Turn on/off SNMP support. You must restart the gatekeeper for changes to take effect
	`xConfiguration SNMP CommunityName: <name>`	SNMP Community names are used to authenticate SNMP requests. SNMP requests must have this `password' in order to receive a response from the SNMP agent in the Gatekeeper. You must restart the gatekeeper for changes to take effect.
	`xConfiguration SNMP SystemContact: <name>`	Used to identify the system contact via SNMP tools such as TANDBERG Management Suite or HPOpenView. You must restart the gatekeeper for changes to take effect.
	`xConfiguration SNMP SystemLocation: <name>`	Used to identify the system location via SNMP tools such as TANDBERG Management Suite or HPOpenView. You must restart the gatekeeper for changes to take effect.
SSH	`xConfiguration SSH Mode: <On/Off>`	Enables/disables SSH and SCP support. You must restart the gatekeeper for changes to take effect.
SystemUnit Name	`xConfiguration SystemUnit Name: <name>`	The name of the unit. Choose a name that uniquely identifies the gatekeeper.
SystemUnit Password	`xConfiguration SystemUnit Password: <password>`	Specify the password of the unit. The password is used to login with Telnet, HTTP(S), SSH, SCP, and on the serial port. To set an empty password type `xConfiguration SystemUnit Password: ""`

Command	*Usage*	*Description*
Telnet	`xConfiguration Telnet Mode: <On/Off>`	Enables/disables Telnet support. You must restart the gatekeeper for changes to take effect.

5.3 Command

The command root command, xcommand, is used to execute commands on the gatekeeper.

To list all xconfiguration commands type

```
xcommand ?
```

To get usage information for a specific command, type

```
xcommand <commandname> ?
```

Command	*Usage*	*Description*
Boot	`xCommand Boot`	Restarts (boots) the gatekeeper. This takes approximately 1 minute to complete.
DisconnectCall	`xCommand DisconnectCall Call: <callid>`	Disconnects the specified call
ZoneAdd	`xCommand ZoneAdd <name> <prefix> <address>`	Adds a new zone with the specified name, zone prefix and IP address. E.g. `xCommand ZoneAdd B 65 10.0.0.30`
ZoneDel	`xCommand ZoneDel <name>`	Deletes the zone with the specified name. E.g. `xCommand ZoneDel B`

5.4 Other commands

Command	*Usage*	*Description*
eventlog	`eventlog [n/all]`	Lists the eventlog with trace information. n is the number of lines from end of event log to dump all – dumps the whole event log If no parameters are provided, the whole event log will be dumped.
syslog	`syslog <level> [ipaddr] [ipaddr] ...`	Enables tracing. <level> - is the log level, 0-3, 3 gives most logging. ipaddr – specify up to 10 IP addresses to log information for, all if none specified. Type syslog 0 to turn off logging.

Command	*Usage*	*Description*
About	`about`	Shows information about the system.

Approvals

The product has been approved by various international approval agencies, among others: UL and Nemko. According to their Follow-Up Inspection Scheme, these agencies also perform production inspections at a regular basis, for all production of TANDBERG's equipment.

The test reports and certificates issued for the product show that the TANDBERG Gatekeeper, Type number TTC2-02, complies with the following standards.

EMC Emission - Radiated Electromagnetic Interference

- EN55022:1994 + A1:1995 + A2:1997 Class A.
- FCC Rules and Regulations 47CFR, Part 2, Part 15.
- CISPR PUB.22 Class A

EMC Immunity

- EN 55024:1998 + A1:2001
- EN 61000-3-2:2000
- EN 61000-3-3:1995 + A1:2001

Electrical Safety

- IEC 60950 3rd edition 1999
- EN 60950 3rd edition 2000
- UL 60950 3. Edition
- CSA C22.2 No. 950-M95

Technical Specifications

Systems Capacity
100-1000 registered endpoints
25-200 concurrent calls
(The systems capacity depends on the systems option)

Ethernet Interfaces
3 x LAN/Ethernet (RJ-45) 10/100 Base-TX

System consol port
2 x COM ports (front and rear), RS-323 DB-9 connector
2 x USB (disabled)

ITU standard
ITU-T H.323 version 4
ITU-T H.224 version 4

Security Features
IP Administration passwords
Management via SSH
Software upgrade via HTTPS and SCP

System Management
Configuration via serial connection, Telnet and SSH
Software upgraded via HTTP, HTTPS and SCP

Environmental Data
Operation temperature: 0°C to 35°C (32°F to 95°F)
Relative humidity: 10% to 90% non-condensing

Physical Dimensions
Height: 4.35 cm (1.72 inches)
Width: 42.6 cm (16.8 inches)
Depth: 22.86 cm (9 inches)
1U rack mounted chassis

Power supply
90 ~ 264V full range @47 ~ 63 Hz

Certification
LVD 73/23/EC
EMC 89/366/ECC