



IP Gateway 3500 Series 1.1(1.1) Release Notes

Introduction

The Codian IP Gateway version 1.1(1.1) is a new feature release for the Codian IP Gateway 3500 Series. This document lists and describes the new features supported in this release.

If you experience any difficulties or unexpected results when using version 1.1 of the IP GW 3500 Series, consult the online help documentation for information on using the device and also the FAQs on the Codian web site before contacting Codian technical support.

Caution: If you have been using the built-in gatekeeper to bridge between two networks to allow direct dialing to E.164 numbers, when you upgrade to 1.1(1.1), you will need to configure the settings of the built-in gatekeeper to retain this functionality. For more information, read this document.

New features and functionality in 1.1(1.1)

- ▶ HD support
- ▶ Encryption
- ▶ Localization for web interface and voice prompts
- ▶ Multiple operators
- ▶ Caller on hold function for operators
- ▶ Multiple service prefixes
- ▶ Enable/disable direct calls between ports:
 - to IP addresses
 - to E.164 numbers
- ▶ Auto attendant for each port
- ▶ Enhanced auto attendant
- ▶ Configurable call groups
- ▶ Customizable banners for auto attendant and operator
- ▶ Configure up to two gatekeepers
- ▶ Enable/disable use of H.239
- ▶ Enhanced SIP support
- ▶ Configure up to five SIP registrars
- ▶ Convert out-of-band DTMF to in-band
- ▶ Dial plan applies to all calls dialed using the auto attendant
- ▶ Automatic detection of endpoints with Far End Camera Control disabled or not supported

HD support

Release 1.1 provides support for HD calls. HD calls are only possible if you have the High Definition (HD) video feature key installed.

HD calls through the IP gateway are non-transcoded calls between HD-capable H.323 endpoints.

To allow HD calls to take place go to **Settings > Calls** and enable **Allow non-transcoded calls**. Note that if you enable this setting, the IP gateway will attempt to use non-transcoded mode for any H.323 call where it can; that is, where there are common codecs and resolutions between the two endpoints in the call, the IP gateway can connect the call without transcoding. This is likely to be the case for most H.323 to H.323 calls.

Whether or not a call is transcoded is displayed in the **Status** column of the **Calls** page.

The HD video feature key enables the IP gateway to support calls of resolution greater than 4CIF.

Encryption

In Release 1.1, the IP gateway supports AES encryption of H.323 calls. If you have the encryption feature key installed, you can configure the IP gateway to encrypt calls and to accept encrypted calls.

Where encryption is used, the IP gateway encrypts and decrypts all the media to and from the H.323 endpoint.

Encryption is supported for both transcoded calls and for non-transcoded calls. (Non-transcoded calls will only take place on units with the HD video feature key, see above.)

Note that SIP calls cannot be encrypted. If you set **Encryption status** to *Required*, all SIP calls will fail. However, with **Encryption status** set to *Optional*, calls can take place between H.323 and SIP endpoints with encryption used for the H.323 part of the call.

The encryption control is on the **Settings > Calls** page. Choose from:

- **Optional**: Encryption will be used if one of the endpoints in the call requires it. Where both endpoints are set to encryption optional, whether or not encryption will be used is decided by the endpoints. In transcoded calls, it is possible that one part of the call will be encrypted and the other part will not be encrypted; in a non-transcoded call, encryption is either used for both parts of the call or not at all
- **Required**: Encryption must be used by both parts of the call (that is, by both endpoints in the calls). This setting precludes all SIP calls
- **Disabled**: Encryption will not be used by any call

The **Calls** page displays, for any caller capable of encryption, their encryption check code.

Localization for web interface and voice prompts

Release 1.1 allows your IP gateway to be localized. You can:

- upload tokens to provide a localized web interface
- upload voice prompts in a local language or with a more appropriate accent
- type Unicode characters in to any fields so that languages such as Japanese, Chinese and Russian are supported

Note: You may be unable to enter some user IDs or passwords in certain web browsers or FTP clients if they do not support Unicode.

Note: There will be limitations in using MS-DOS FTP commands with these localized units, because MS-DOS is unable to support any Unicode characters and cannot display any other languages apart from English. Therefore FTP commands (e.g. "ls", "dir" etc.) in MS-DOS will not be able to list names in Chinese, Russian etc. Units in English will be able to use MS-DOS FTP commands as before. Other FTP clients, such as SmartFTP (download free from www.smartftp.com), that support Unicode can be used instead of MS-DOS.

For more information, refer to the topic: *Customizing the user interface* in the online help.

Multiple operators

Release 1.1 allows you to configure multiple operators. Previously, there was only support for one operator. Where you have more than one operator, you can use one of three schemes to determine how an operator is selected to receive an incoming call:

- **Priority:** The IP gateway will put the call through to the first operator in the list of operators on the **Settings > Operator** page. If this operator does not answer the call, the IP gateway will try the next operator in the list. This process will continue until an operator answers the call
- **Round robin:** The IP gateway will put calls through to the operators in turn. That is, each call will be put through to the operator who has least recently answered a call
- **Try all:** All operators receive the call simultaneously; the first operator to answer takes the call

To configure the scheme, go to **Settings > Operator**.

Caller on hold function for operators

In Release 1.1, when an operator answers a call, he can choose to put the caller on hold and speak to the proposed receiver of the call before connecting the call. This functionality is provided by a **Speak to receiver** button on the Operator's home page. When speaking to the receiver, to connect the call the operator must hang up. Note that if the receiver hangs up, the caller will be reconnected to the operator. If the caller hangs up while the operator is talking to the destination, a message will appear on the screen: "Caller disconnected".

Multiple service prefixes

Release 1.1 provides support for multiple service prefixes (known on the IP gateway as *Dial plan prefixes*). Multiple service prefixes provide greater dial plan flexibility.

For each gatekeeper with which the IP gateway is registered, up to ten such prefixes can be registered. To register prefixes, go to **Settings > H.323** and select the gatekeeper with which you want to register prefixes. Refer to the online help for more information.

Enable/disable direct calls between ports

To IP addresses

Release 1.1 supports calls from endpoints on one port to IP addresses on the other port with the following provisos:

- the calling endpoint must be registered with the internal gatekeeper
- routing must be correctly configured so that the IP gateway knows on which port to find an IP address

In the same way, calls to hostnames are also supported provided that in addition to the above provisos, the calling endpoint can perform a DNS lookup which returns an IP on the other side of the IP gateway.

Direct calling to IP addresses between ports can be enabled/disabled on a per-port basis; you can choose to allow callers on Port A, Port B, or both ports to have this functionality. To enable direct calling to IP addresses between ports, go to **Gatekeeper** and set the **Full Proxy** option to *Between ports (any destination)* for the port(s) on which you require this functionality. Note that with this option enabled, direct calling to E.164 numbers as described below is also allowed.

To E.164 numbers

Release 1.1 supports calls from endpoints on one port to E.164 numbers on the other port. Both the calling endpoint and the receiving endpoint must be registered with the internal gatekeeper.

Direct calling to E.164 numbers between ports can be enabled/disabled on a per-port basis; you can choose to allow callers on Port A, Port B, or both ports to have this functionality. To enable direct calling to E.164 numbers between ports, go to **Gatekeeper** and set the **Full Proxy** option to *Between ports (to registered aliases)* for the port(s) on which you require this functionality. Note that with this option enabled, direct calling to IP addresses between ports (as described above) is not allowed. You must also correctly configure the dial plan. For more information, refer to the topic: “Displaying the built-in gatekeeper registration list” in the online help.

Upgrading to Release 1.1

Note that if you have been using the built-in gatekeeper to bridge between two networks, when you upgrade to Release 1.1 to retain that functionality you must reconfigure the built-in gatekeeper. This is because by default any sort of direct calling between ports is disabled. You must set **Full proxy** to *Between ports (to registered aliases)* to retain your original functionality or to *Between ports (any destination)* if you want to allow direct dialing to IP addresses too. Note that you must set this option per port as required.

Auto attendant for each port

In Release 1.1, there is an individually-configurable auto attendant for each port. That is, there are two auto attendants: one for calls arriving on Port A and one for calls arriving on Port B. The default behavior of the two auto attendants is identical. However, you configure them individually so that you can have calls treated differently on each port. For configured endpoints and call groups, you can choose whether to have them displayed as options in each auto attendant.

To configure the auto attendants go to **Dial plan > Auto attendant**. To toggle between the Port A and Port B auto attendants, use the [Port](#) link on the right of the display.

Enhanced auto attendant

In Release 1.1, the auto attendant has been enhanced to display on a range of different resolutions. Callers in the auto attendant can now use Far End Camera Control (FECC) zoom to change the display font size. The dial option in the auto attendant now features a graphic of a small telephone.

Configurable call groups

In Release 1.1, you can group configured endpoints into call groups. When a call group receives a call, all endpoints in the call group will ring and the first to be answered will take the call. Call groups can be useful in organizations that have, for example, sales or support teams where anyone from the team can take a call. Call groups will appear on the list of configured endpoints from which the operator can select to forward a call; call groups can also be configured to appear on either port's auto attendant thereby enabling a caller to select to be connected to that call group, rather than having to know and enter the address of an endpoint.

Customizable banners for auto attendant and operator

Release 1.1 allows you to upload your own corporate (or other) banner for the auto attendant and operator screens. The image file must be GIF or Windows BMP format with a maximum size of 352 x 64 pixels.

To upload banners for the auto attendant, go to **Dial plan > Auto attendant**.

Configure up to two gatekeepers

Release 1.1 allows you to configure up to two H.323 gatekeepers on the IP gateway. Where there are two gatekeepers, they must both be physically on different networks; that is, attached to different ports. You can only associate a maximum of one gatekeeper with each port.

To configure gatekeepers, go to **Settings > H.323**.

The gatekeeper to be used for any individual call can be determined by one of the following:

- You can specify the gatekeeper to be queried for a call in individual dial plan rules
- You can also specify the gatekeeper to be queried in an endpoint's configuration on the IP gateway
- An operator can be allowed to specify the gatekeeper to be used for a call

The associated gatekeeper for a port is the gatekeeper to which the IP gateway sends a query for all incoming connections on that port, and for all outgoing connections on that port that are dialed by address rather than by E.164 phone number (unless the dial plan or the configuration of an endpoint specifies otherwise). By querying the gatekeeper, the IP gateway ascertains whether or not the gatekeeper permits the call.

If no gatekeeper is associated with a port, either on the **Settings > H.323** page or explicitly in a dial plan rule, the IP gateway will always make (for outgoing calls) or accept (for incoming calls) the call. That is, the IP gateway will not require validation from a gatekeeper before handling a call on that port.

One gatekeeper can be associated with both ports; one port can have a maximum of one associated gatekeeper.

Enable/disable use of H.239

In Release 1.1, you can choose to enable or disable H.239 content channel video. The **H.239 content channel video** option is on the **Settings > Calls** page.

With this option unselected, H.239 content will not be available to any endpoint. If you check this option, H.239 content can be used in both transcoded and where the unit supports HD calls, non-transcoded calls.

Enhanced SIP support

In Release 1.1, the IP gateway performs automatic codec selection for SIP calls and allows use of all video and audio codecs. That is for codec selection, SIP now works the same way as H.323.

Configure up to five SIP registrars

In Release 1.1, the IP gateway can be registered with up to five SIP registrars.

The SIP registrar to be used for any individual call can be determined by one of the following:

- You can specify the SIP registrar to be queried for a call in individual dial plan rules
- You can also specify the SIP registrar to be queried in an endpoint's configuration on the IP gateway
- An operator can be allowed to specify the SIP registrar to be used for a call

Convert out-of-band DTMF to in-band

Release 1.1 enables the IP gateway to convert out-of-band DTMF tones to in-band DTMF if so required.

The **Convert out-of-band to in-band DTMF** option is on the **Settings > Calls** page.

Both H.323 and SIP can send DTMF tones in-band (within the audio stream) and out-of-band. Out-of-band DTMF has the advantage that the tones do not sound over any voice, but will not be compatible with analogue telephones. For example, if you are calling out from an IP phone system through an IP gateway to a traditional call center with an automated audio menu, you will need to be using in-band DTMF tones to select an option, so this option may be required.

Note that IP phones can interpret in-band DTMF and will continue to work as expected with this option enabled.

Dial plan applies to all calls dialed using the auto attendant

In Release 1.1, the dial plan is applied to all calls dialed using the auto attendant. This differs from Release 1.0 where it was optional whether the dial plan would be applied or not.

Automatic detection of endpoints with Far End Camera Control disabled or not supported

In Release 1.1, the IP gateway will automatically detect if it receives a call from an endpoint that has FECC disabled or that does not support FECC communication with the IP gateway for any other reason; in this case, the auto attendant will ask the caller to do one of the following:

- press * (star/asterisk) to connect to the operator
- press # (pound/hash) twice to use DTMF tones to navigate the auto attendant

Limitations and bugs

FTP upgrades not supported

The IP gateway cannot be upgraded via FTP. Upgrade the unit using the web interface as described below.

FECC disabled for TANDBERG endpoints when IP GW is in non-transcoding mode

When the IP gateway has encryption enabled and is using non-transcoding mode, Far End Camera Control (FECC) does not work in the auto attendant; the IP gateway detects that FECC is not supported and the user can navigate the menu using DTMF keys by pressing ##. For unencrypted calls and for transcoded calls, FECC operates as expected.

Non-transcoding mode disabled on Cisco Call Manager and Polycom HDX and ViewStations endpoints

Non-transcoding mode is disabled entirely for Cisco Call Manager and Polycom HDX endpoints.

Encryption disabled to Lifesize endpoints in non-transcoding mode

When the IP gateway is in non-transcoding mode, encryption to Lifesize endpoints is disabled.

Using Mirial Softphone with the IP GW

If you are using a Mirial Softphone to call via the IP GW, ensure you are using Mirial build 5.3.5. This fixes an issue with the G.722.1c audio codec.

Upgrading Software

Using a web browser

1. Unzip the image file.
2. Browse to the current IP address of the IP gateway using an IE-compatible Web browser. Click **Click here to log in** and then **Change log in**.
3. When prompted, type **admin** for the user name and its associated password (this is blank in a new unit).
4. Go to the **Settings > Upgrade** page.
5. In the Main software image section, type in, or browse to the location of the software image file.
6. Click the **Upgrade software image** button.

The Web browser uploads the file to the IP gateway. This takes some time – dependent on your network connection. Do not move your Web browser away from the Upgrade Software page or refresh this page during the upload process; otherwise, it may abort.

After a number of minutes, the Web browser refreshes automatically and displays “Main image upload completed”. Close this window.
7. Click the **Shutdown button** on the main upgrade page. This option will now change to **Confirm IP GW shutdown**. Click to confirm.
8. Click the **Restart IP GW and Upgrade** button. This button only appears in the Upgrade page during this process.

The unit will reboot and upgrade itself – this also takes a number of minutes.

Note: If you have been logged out due to inactivity, log in again as admin and click **Restart IP GW and upgrade** at the bottom of the Upgrade software page to complete the upgrade.

Notes

- ▶ The progress of the upgrade can be monitored through the serial port
- ▶ Before upgrading, make sure that the IP gateway is not in use. Anyone using the IP gateway at the time of the upgrade may experience poor performance and loss of connectivity
- ▶ The time required to download and upgrade depends on the speed of your network connection. With a fast connection the total time to download, upgrade and restart the IP gateway is several minutes

Checking for updates and getting help

It is a good idea to regularly check for updates of the software image on the Codian web site.

If the documentation does not answer your question or you have a problem with one of our products:

1. Refer to the Technical FAQ section of the Codian web site which is kept up to date with the latest information from our technical support team regarding the resolution of customer issues.
2. Contact your reseller. Our resellers have a wealth of experience with our products and this is often a quick way of solving a problem.
3. If your query remains unsolved, there is a web form in the Support area of the Codian web site that you can complete. Ensure that you provide all the details requested by the form to assist the technical support team in resolving your problem:
 - a. The serial number and product model number (for example: IP GW 3510) of the unit.
 - b. The software build number. (To find this, in the web interface, go to **Status > General**).
 - c. Where you purchased the unit.
 - d. Your contact email address or telephone number.

Note that you can also send an email to our technical support team at support@codian.com