Cisco TelePresence ISDN Gateway Version 2.1

Online help (printable format)

D14659.03

March 2011

Contents

Logging into the web interface

The Cisco TelePresence ISDN Gateway (ISDN Gateway) web interface is used for administering the Cisco TelePresence ISDN GW 3241 and 3200 Series units and the ISDN GW MSE 8321 and ISDN GW MSE 8310 blades, monitoring the progress of active and completed calls, managing dial plans and users, and for obtaining event logging information for reference or for troubleshooting complex issues.

When connecting to the ISDN Gateway web interface, you must log in so that the ISDN Gateway can associate the session with your configured user and a set of access privileges. The ISDN Gateway has a set of configured users, and each user has a username and password that are used for logging in.

1. Using a web browser, enter the host name or IP address of the ISDN Gateway.
2. To log in as the administrator, click **Log in** and enter your assigned **Username** and **Password**.
3. Click **OK**

The main menu appears, offering options based on your access privileges.

The **Login** page of the ISDN Gateway displays a welcome banner which administrators can configure to display text relevant to your organization. For more information, refer to Customizing the user interface.

Failing to log into the web interface

When connecting to the Cisco TelePresence ISDN Gateway web interface, you must log in so that the ISDN Gateway can associate the session with your configured user and a set of access privileges. The ISDN Gateway has a set of configured users, and each user has an ID and password that are used for logging in.

If you see the **Access denied** page, you have not been able to log in for one of the following reasons:

- **Invalid username/password**: you have typed the incorrect username and/or password.

  If Advanced account security mode is enabled and you incorrectly type the username and/or password three times and if this is an admin account, it is disabled for 30 minutes; for any other account, it is disabled indefinitely (or until you, the administrator, re-enable the account from the **User** page)
- **No free sessions**: the maximum number of sessions allowed simultaneously on the ISDN Gateway has been exceeded
- **Your IP address does not match that of the browser cookie you supplied**: try deleting your cookies and log in again
- **You do not have access rights to view this page**: you do not have the access rights necessary to view the page that you attempted to see
- **Page expired**: the **Change password** page can expire if the ISDN Gateway is not entirely happy that the user who requested to change password, is actually the user submitting the change password request. (This may happen if you use a new browser tab to submit the request.)

Invalid passwords

If Advanced account security mode has been enabled, the ISDN Gateway will disable a user's account if that user incorrectly enters a password three times consecutively. If this is an admin account, it is disabled for 30 minutes; for any other account, it is disabled indefinitely (or until you, the administrator, re-enable the account from the **Users** page).

Getting started with the Cisco TelePresence ISDN Gateway

Ensure you have correctly completed the physical setup of the Cisco TelePresence ISDN Gateway (ISDN Gateway) following the instructions in the Getting Started Guide that accompanied it. You must also ensure that your endpoints and MCU are correctly configured to operate with the ISDN Gateway.

Before you can make calls using the ISDN Gateway, you need to complete its setup using the web interface as follows:

1. **Log into the ISDN Gateway**: Use your browser to navigate to the IP address of the ISDN Gateway. Click **Change log in** and enter the user name 'admin' with no password. We recommend that you change the admin user account to use a password as soon as possible.
2. **Set up the ISDN interfaces**:
    a. Go to **Settings > ISDN**.
    b. Select the **ISDN interface type** to match that of your installation: *E1* is typically used in the UK and mainline Europe, and *T1* in North America. Use *T1* (Japan) in Japan.
    c. You may need to set other advanced ISDN settings. Only change these settings if you know of a specific requirement to do so.
    d. Click **Apply changes**.
    e. If you made any changes on this page, you must restart the ISDN Gateway before they will take effect. Go to **Settings > Shutdown** and click **Shut down ISDN GW**.
3. **Configure ISDN ports**: Go to Settings > ISDN ports:
    a. Set low and high channels:
        i. If you have a fully-populated PRI (this is the normal case) set **Low channel** to '1' for all network types and **High channel** to *Max*.
        ii. If you have a fractional PRI, where your provider offers a reduced number of B-channels, enter alternative values as appropriate.
    b. Set the **Channel search order**: When making calls, the ISDN Gateway examines which B-channels are free before placing a call. This search can be performed starting with the high channel and working down, or starting with the low channel and working up. Your ISDN provider will be able to advise which scheme to use, but the choice is not critical.
    c. Click **Apply changes** and then, if required, repeat the above steps to configure further ISDN ports. Select which port you want to configure using the numbered links at the top right of the page.
4. **Configure the dial plan**: The default behavior of the ISDN Gateway is to reject all calls. You must configure a dial plan to allow permitted calls to be placed. The simplest configuration is to create a dial plan that will connect any 'IP to ISDN' call that has been routed to the ISDN Gateway to the number that the caller has dialed (using any free enabled port) and that will connect any 'ISDN to IP' call to the auto attendant of your MCU:
    a. Go to **Dial plan > IP to ISDN** and click **Add rule**.
    b. For **Rule name**, type in a name for the new rule.
    c. For **Condition**, select *Match any called number*.
    d. For **Action**, select *Call with the original called number*.
    e. Leave the other values unchanged. Click **Add rule** to add the rule to the dial plan.

f. Now go to **Dial plan > ISDN to IP**, and click **Add rule**.
g. For **Rule name**, type in a name for the new rule.
h. For **Condition**, select *Match any called number*.
i. For **Action**, select *Call this number* and enter the IP address of your MCU.
j. Leave the other values unchanged. Click **Add rule** to add the rule to the dial plan.

For more information about dial plans, refer to Understanding the dial plan.

Making calls with the Cisco TelePresence ISDN Gateway

The Cisco TelePresence ISDN Gateway allows:

- users with ISDN endpoints to place calls to users with IP endpoints
- users with IP endpoints to place calls to users with ISDN endpoints

When configured correctly, the ISDN Gateway is transparent to users; they will require minimal assistance and training to place calls through the ISDN Gateway successfully.

One training consideration for users making ISDN calls which is not usually present for IP calls is that of cost; you may want to educate users that ISDN calls escalate in cost with increased bandwidth and duration. You may also want to configure the ISDN Gateway to limit these values if required (for more information, refer to Understanding the dial plan).

For information about setting up the ISDN Gateway, refer to:

- the Getting Started Guide.
- Getting started with the ISDN Gateway.

When you have the ISDN Gateway and associated devices (for example, the MCU) correctly configured, with an appropriate dial plan in place, calls can be placed through the ISDN Gateway.

ISDN to IP calls

If you have configured the dial plan as in Getting started with the ISDN Gateway, endpoints calling the phone number of the ISDN Gateway will, after the call is completely established, be forwarded to the auto attendant of the MCU. From here they may use the Far End Camera Controls (FECC) of their endpoint to navigate the menus and join conferences as normal.

IP to ISDN calls

An IP to ISDN caller needs to know the number of the ISDN user whom they are calling. However, if the call will be placed via an MCU, the ISDN user's number can be incorporated into the configured endpoint details stored on the MCU.

You can configure the ISDN Gateway to allow calls to a single ISDN number. In this case, a single rule in the dial plan will suffice, matching all numbers and calling out to a single phone number.

If you want users to be able to call any number, set the ISDN Gateway up as a 'H.323 gateway' on your MCU and direct calls to ISDN numbers via that. Alternatively, if you are using a gatekeeper on your IP network, you can register a prefix with which users may prefix the ISDN number they want to call (this is similar to dialing a '9' for an external line on many telephone systems).

Using the auto attendant

You can use the auto attendant on the Cisco TelePresence ISDN Gateway to enter the number you want to call directly from your endpoint. If you are calling from an IP endpoint, you should enter a phone number. If you are calling from an ISDN endpoint you should enter an IP address (optionally followed by an extension number or phone number).

If your administrator has set up calls to be directed to the auto attendant, then you will see the instruction: "Enter the number you wish to call", and hear an audio prompt. (Users of audio-only endpoints can use the auto attendant even though they can only hear the audio prompt.)

When you dial, you can use the following:

- Digits 0 to 9
- * (asterisk or star), which is interpreted as a dot for ISDN to IP calls
- ** interpreted as a : and used as an extension separator for ISDN to IP calls
- # (hash), to indicate that you have completed the number and to start dialing

To call a specific extension, separate the number/address from the extension by typing a colon (:). For example, to call the MCU with IP "10.2.1.33", and try to join a conference with numeric identifier "00000", you need to enter 10.2.1.33 : 00000 so you should type 10*2*1*33 ** 00000#

Note that if you do not include the #, the ISDN Gateway will dial after 20 seconds anyway. Equally, if you do not enter any numbers but leave the auto attendant idle, the ISDN Gateway will hang up the call after 60 seconds.

Using the Far End Camera Control

If FECC is enabled on your endpoint, use the Left arrow to delete the last character and the Right to start dialing

Using the Cisco TelePresence ISDN Gateway for voice-only calls

The Cisco TelePresence ISDN Gateway can be used to forward voice-only IP calls to the ISDN network (the PSTN); likewise, it can be used to forward voice-only ISDN calls from the PSTN to IP telephones on the IP network. If you want to use the ISDN Gateway to forward voice-only calls, there are two ways to configure this feature:

- **globally**: either
  - entirely as a voice-only gateway: where all IP calls and all ISDN calls are forwarded as voice-only calls, or
  - partly as a voice-only gateway: where incoming ISDN video-conferencing calls are allowed, but outgoing ISDN calls are voice only (or vice versa)
- **dial plan configuration**: where particular calls (ingoing and outgoing) are allowed to be video conferencing calls, and where particular calls are restricted to voice-only

IP to ISDN calls: IP endpoints often do not allow the caller to specify the type of call being made. For example, a caller may want to make a telephone call (that is, voice only), but are unable to specify that this is a telephone call. To overcome this problem, for IP data calls, if required, the ISDN Gateway can extract the voice part of the call and forward it to the ISDN network as a voice-only call. For IP to ISDN calls, if the ISDN Gateway receives a video conferencing call that has been restricted to being a voice-only call (due to the settings on the ISDN Gateway), the unit will forward it as a voice-only call (the call will not be dropped). If the IP endpoint does allow the call type to be specified, an IP telephone call will always be placed as such.

ISDN to IP calls: ISDN endpoints usually allow a caller to specify the type of call being made. This is important, because with ISDN calls the voice part of the call cannot be separated from the video part. Therefore, if the ISDN Gateway receives a video-conferencing call and the dial plan restricts the ISDN Gateway to voice-only calls, the unit will drop the call. Voice-only telephone calls will always be accepted by the ISDN Gateway.

Configuring the Cisco TelePresence ISDN Gateway as a voice-only gateway

1. Go to **Settings > ISDN.**
   a. To configure the ISDN Gateway to restrict incoming ISDN calls to voice-only calls, set the *Max incoming ISDN call rate* to *Telephone*.
   b. To configure the ISDN Gateway to restrict outgoing ISDN calls to voice-only calls, set the *Max outgoing ISDN call rate* to *Telephone*.
2. Complete the other ISDN settings as per your requirements. For more information about the ISDN settings page, refer to Configuring general ISDN Settings.

Note: You can set both the incoming and outgoing maximum call rates to *Telephone* to use the ISDN Gateway entirely as a voice-only gateway.

Dial plan configuration

You can configure the dial plan to restrict particular called numbers to voice-only calls. In this way, you can configure the ISDN Gateway to allow particular outgoing/incoming ISDN calls to be video-conferencing calls. Using the dial plan therefore allows you greater flexibility (if you need it) than using the global settings on the ISDN settings page.

You can use the dial plan to place a call where the ISDN Gateway will start sending DTMF tones after a telephone call has connected. This is useful if there is a call through the ISDN Gateway to a device which is perhaps behind another gateway which only supports DTMF to decide how to route the calls. The caller is not required to additionally enter the DTMF codes manually on the telephone keypad but instead can have the call re-routed automatically using the dial plan of the ISDN Gateway.

For more information about configuring the dial plan, refer to Understanding the dial plan, Adding and updating dial plan rules, and Example dial plan rules.

Calling a PSTN telephone from an MCU

If you want to call someone on a regular land-line telephone into a conference on the MCU, you must add the ISDN Gateway as a participant, using one of the following methods:

- specify it as a gateway with an extension.
- call a particular number registered to a common gatekeeper.
- call the ISDN Gateway by IP and let the ISDN Gateway itself work out which number to call based on dial plan rules.

Whichever method you use, you must have a dial plan configured such that a rule is invoked that has "Telephone" bandwidth specified for the call. Then the call will be established correctly.

Displaying ISDN port utilization

For each ISDN port, you can view details of any port activity for each ISDN channel. To display ISDN port utilization details, go to **ISDN > ISDN ports**.

A message shows the status of ISDN layers 1 (physical) and 2 (D-channel). The same information is shown in the ISDN Status page.

Note that if the ISDN Gateway is in leased line mode, there will be no status for layer 2.

The following information is displayed for each channel of every ISDN port:

Field	Field description
#	The ISDN channel number.
Activity	Whether or not this channel on this port is currently active. Activity is one of: ▶ *inactive*: not in use. ▶ *active (data):* in use. A voice and video call is taking place and is using this channel. ▶ *active (voice)*: in use. An audio-only call is taking place and is using this channel.
Direction	If the channel is active, the direction of the call is displayed. Either: ▶ *inbound*: for calls to the ISDN endpoint. ▶ *outbound*: for calls from the ISDN endpoint.
Calling party	The identity of the endpoint that initiated the call (depending on what that endpoint has provided): ▶ for IP-ISDN calls (that is, outbound calls), this is the name of the H.323 device, the telephone number, or "Cisco TelePresence ISDN Gateway". ▶ for ISDN-IP calls (that is, inbound calls), this is the telephone number of the endpoint that made the call.
Called party	The number that was dialed by the calling party. Note that if the ISDN Gateway is in leased line mode, there will be no called part number available.

For each port there is an **Activate D-channel now** button that is only active if layer 1 is up and layer 2 (D-channel) is not. If neither or both are up for a port, the button is disabled for that port. Click the button to bring up the D-channel.

Note: Typically, you need never do this because the ISDN Gateway automatically tries to bring up the D-channel periodically. Also clicking the button is not guaranteed to work.

Displaying the ISDN calls list

The ISDN Calls List displays both active calls and completed calls on the Cisco TelePresence ISDN Gateway together with their basic settings. The list enables you to disconnect active calls and to delete completed calls from the list. For active calls, you can display further details (see Displaying detailed call information).

Active calls are those calls that are taking place now. The active calls list shows *all* calls that are currently taking place. The maximum number of calls that can take place simultaneously is constrained by the ISDN bandwidth available to the ISDN Gateway. Completed calls are calls that have ended. The completed calls list shows only the most recent calls (up to 20 calls). Older calls are automatically deleted from the list.

To display the ISDN Calls List go to **ISDN > ISDN calls**.

Field	Field description
Type	The type of call, which will be *IP to ISDN* or *ISDN to IP*.
Participants	The participants in the call. An IP participant will be listed by IP address, E164 number or H.323 ID. An ISDN participant will be listed by Calling Party Number or "<none>" if this information is not supplied by your ISDN network.
Details	For example, the time that the call started, its duration and whether encryption is used.
Progress	Progress is indicated for active calls only.

Disconnecting and deleting calls

To disconnect active calls, go to **ISDN > ISDN Calls**:

- To disconnect particular calls, select the calls you want to disconnect and click **Disconnect selected**.
- To disconnect all active calls, click **Disconnect all.**

To delete calls from the list of completed calls, go to **ISDN > ISDN calls**:

- To delete particular calls from the list, select the calls you want to delete and click **Purge selected.**
- To delete all completed calls, click **Purge all**.

Diagnostic controls

By default diagnostic logging is disabled. This feature is for use by Cisco customer support and we suggest that you do not change the setting unless instructed to do so.

Displaying detailed call information

Active calls are listed along with some basic details in the ISDN Calls List (see Displaying the ISDN Calls List). To view additional details about an active call, go to **ISDN > ISDN Calls** and click **more** for the call about which you want more information.

On the Call details page, the call for which more details are provided is displayed with a number (example: "Call 15 details"). This number is generated by the Cisco TelePresence ISDN Gateway (numerically, starting from zero since the last reboot) for the purposes of internal identification.

Field	Field description
Started at	For IP to ISDN calls, this is the time at which the call was received by the ISDN Gateway. For ISDN to IP calls, this is the time at which all the channels comprising the call connected and bonded.
Call progress	The status of the call, which will be one of: ▶ *Initial*: an IP or ISDN call has just come in, and the ISDN Gateway is determining if it is allowed and where to direct it. ▶ *Calling out*: the ISDN Gateway is trying to make contact with the other side of the call. ▶ *Connected*: the call is in progress between and IP and ISDN endpoints. ▶ *Dying*: Displayed briefly while a call is terminated, either by one of the participants or via the web interface. Call progress also lists the caller's number, the number that was called and the destination, including the IP address for an IP destination.
Participant details	
Unique index	A unique numeric identifier given by the ISDN Gateway to this part of the call.
Name	The name the caller provided when the call was initiated.
E.164	The telephone number of the participant.
Call type	The participant's call type: either *H.320* (ISDN caller) or *H.323* (IP caller).
FECC	Whether Far-End Camera Control has been established or not.
Progress	The status of the participant's side of the call, which will be one of: ▶ *Initial*: the call is just starting. ▶ *Proceeding*: trying to make contact with the other side of the call. ▶ *Alerting*: the other side of the call is ringing (you might not see this state). ▶ *Connected*: the call is in progress. ▶ *Disconnecting*: the call is in the process of going down.

	► *Finished*: the call is disconnected (you might not see this state).
Encryption	This field tells you whether encryption is active and if so, whether all or only some of the media channels are encrypted.
Channel bonding map	Only for ISDN participants: The numbers of the ISDN channels that are in use for this call.
Channel rate	Only for ISDN participants: Whether or not restricted 56k mode is in use for the received (rx) and/or transmitted (tx) part of an ISDN call. For unrestricted calls (rx and/or tx), the channel rate will be 64kbps.

Understanding the dial plan

The Cisco TelePresence ISDN Gateway uses the dial plan to determine how to route calls between IP and ISDN networks. When the ISDN Gateway receives a request to initiate a new IP to ISDN or ISDN to IP call, it examines the called number (if available), and uses the dial plan to determine whether to reject the call, find out which number should be called to initiate the outgoing part of the call, and to check the allowed call bandwidth.

There are a number of different ways in which you can use the dial plan. For example, you can use the dial plan to enable callers to use a particular bandwidth for an IP to ISDN call. You can also use the dial plan to enable the ISDN Gateway to join incoming ISDN calls to the correct conference on an MCU. (For example dial plans, refer to Example dial plan rules.)

The dial plan is actually divided into two; an IP to ISDN dial plan and an ISDN to IP dial plan. If the incoming part of a connection is from an IP endpoint, the IP to ISDN dial plan is used; if it is from an ISDN endpoint, the ISDN to IP dial plan is used. The behavior of the two dial plans is nearly identical, and the sections below only make a distinction between the two where differences exist.

The maximum number of rules that can be added to each dial plan is 200.

Note that if you have configured the ISDN Gateway to use leased line mode, then the options available on the dial plan are different to those available in non-leased line mode. For information about configuring dial plans in leased line mode, refer to Adding and updating dial plan rules in leased line mode.

Refer to the sections below for more information about the use and administration of dial plans:

- Rules
- Using rules
- Rule ordering

Rules

Dial plans are administered using **rules**. Rules and their addition and control are nearly identical for the IP to ISDN and ISDN to IP dial plans.

Each rule has a name and comprises:

- a **Condition** that must be matched for the rule to be invoked
  The condition can be set to match any called number, to match a call that has no called number, or can specify the called number by specific number or pattern.
- an **Action** that is carried out if the rule is invoked
  The action can be to reject the call, enter the auto attendant, enter the auto attendant and use a TCS-4 extension (ISDN to IP only), to place the call using the original dialed number, or to specify the number/address to call.
- a set of **Additional parameters** that modify the action:
  - **Call type**: specifies whether the call is a normal video call, a telephone call, or a video call that supports legacy ISDN endpoints that use n x 64kbps or n x 56kbps

  - **Restrict (56k)**: whether a call will use 56kbps. Note that if 56k is specified for a rule, but the endpoint only supports 64kbps, then the call will be terminated rather than use 56kbps
  - **Maximum bandwidth:** used to limit the bandwidth available to for calls to particular numbers, or to allow users to select their own bandwidth (for more information, see Adding and updating dial plan rules)
  - **Encryption settings:** whether transparent encryption is to be used and if not, whether encryption is *Optional* or *Required* for the IP and ISDN parts of the call
  - **Place/Receive call on**: the port(s) to use if you need to bond channels to complete subsequent calls from the calling endpoint
- a choice of allowed codecs

Using rules

Each dial plan comprises a set of rules. When the ISDN Gateway receives a new incoming call, it selects the appropriate dial plan, then compares the called number (if available) to the condition of each rule in that dial plan until a match is found. When a match is found, no more rules are checked, and the action of the matching rule is used to determine what should be done next; typically the outgoing part of the connection will be initiated - calling a number specified by the action, the auto attendant is displayed or the connection will be rejected and the incoming part terminated.

If a dial plan contains no rules, or if no rule's condition matches the called number, calls are rejected by default.

For more information on adding and modifying dial plan rules, see Adding and updating dial plan rules.

Rule ordering

Rules are always checked in the same order for each incoming call. This means that a dial plan can be designed to handle specific calling cases first, then general calls if no specific cases match. For example, a dial plan might be set up to call a particular endpoint if an incoming call is received to a specific number, but all other incoming calls get connected to an operator. Such a dial plan might look like this:

1. *Condition*: **Called number is "6056"** / *Action*: **Call with the original called number**.
2. *Condition*: **Match any called number** / *Action*: **Call this number "1000"**

Clearly rule ordering is important to achieve this functionality. You can view and test the rule list comprising a dial plan, and modify the ordering of the rules by dragging and dropping as required. (You can also use the up and down links to reorder.) For more information, see Displaying and testing the dial plan.

Displaying and testing the dial plan

The dial plan is actually made up of two, separate dial plans: one for IP to ISDN calls and one for ISDN to IP calls. Refer to the sections below for more information.

To display or modify the IP to ISDN dial plan, go to **Dial plan > IP to ISDN**. To display or modify the ISDN to IP dial plan, go to **Dial plan > ISDN to IP**.

Note that if you have configured the Cisco TelePresence ISDN Gateway to use leased line mode, then the options available on the dial plan are different to those available in non-leased line mode. For information about configuring dial plans in leased line mode, refer to Adding and updating dial plan rules in leased line mode.

Displaying the rules list

As described above, the dial plan comprises a set of rules that are followed in response to the incoming part of a connection in order to determine how to proceed with the outgoing part of the connection.

You can view the set of rules comprising a dial plan as a list, with rules checked from top to bottom. Refer to the table below for details of the fields displayed.

Field	Field description	More information
Name	The unique number assigned to this rule and the rule's name.	Click on a number or name to view and modify rule details (see Adding and updating dial plan rules).
Condition	Which called numbers will cause this rule to be invoked.	Possible conditions include: ▶ **Called number is "1025"** meaning this rule is invoked if the called number is exactly as stated ▶ **No called number** meaning this rule is invoked if the incoming part of the call has no called number available ▶ **Match port <port number> leased line group <group number>**: meaning this rule is invoked if the incoming part of the call is using the port number and leased line group as stated in the rule ▶ **Match any called number** meaning this rule is always invoked if checked

Action	What will happen if this rule is invoked.	Possible actions include: ▸ *Reject the call*: if this rule is invoked the call will be terminated and the outgoing part of the call will not be established ▸ *Enter the auto attendant* : the call will be connected to the auto attendant ▸ *Enter the auto attendant + TCS-4*: the call will be connected to the auto attendant and an extension accepted ▸ *Call this number "xxx"*: where xxx represents what is displayed: o for IP to ISDN calls: a number or a pattern o for ISDN to IP calls: a pattern, a hostname, or an IP address meaning that "xxx" will be called if this rule is invoked. ▸ *Call with the original called number*: the original called number will be used to place the outgoing part of the call ▸ *Call these numbers*: meaning that this is a video call using N x 64kbps or N x 56kbps (for legacy ISDN endpoints only). The first two numbers to be called are listed here; click the dial plan number to view the complete list of numbers included in this rule ▸ *Call port <x> leased line group <x>*: if the ISDN Gateway is using leased line mode, this action indicates on which port the call will be made and using which leased line group
Bandwidth	The maximum ISDN bandwidth that will be used for the call if this rule is invoked.	The value will be one of: • **Telephone**: the call will be restricted to voice-only. • **<default>:** the default maximum bandwidth setting is used. To configure the default bandwidth go to Home > Settings > ISDN • **Number of kbps**: the maximum bandwidth allowed for calls matching this rule • **N x 64kbps:** the call is a video call using N x 64kbps (for legacy ISDN endpoints only)

		• **N x 56kbps**: the call is a video call using N x 56kbps (for legacy ISDN endpoints only)
Ports	The ISDN port(s) on which the call may be placed.	
Codecs	Shows the choice made when adding the dial plan rule.	One of Default, Custom or Safe. (See Adding and updating dial plan rules for more details.)
UID	The unique identifier for the dial plan rule.	Each rule in the dial plan is assigned a unique ID number generated by the ISDN Gateway. This UID uniquely identifies the dial plan rule when it is referenced in the audit log.
*** (asterisk)**	Identifies the rule you have just moved.	If you have just moved a rule in the list, it will be marked with an asterisk (*). This is to help you see the changes you have made.

Modifying the rules list

To change the order of rules, drag and drop the rule that you want to move or use the up and down links.

To add a rule, click **Add rule** (see Adding and updating dial plan rules).

To remove a rule, select one (or more) and click **Delete selected rules**.

Testing the dial plan

It may take some experimentation to create the dial plan that you require. The ISDN Gateway provides a facility to test the dial plan to see how your set of rules acts on a particular number.

To test the dial plan:

1. Go to **Dial plan**.
2. If you want to test how the dial plan acts
    - o on a particular number or address for an ISDN to IP connection, ensure you are on the **ISDN to IP dial plan** tab
    - o on a particular number for an IP to ISDN connection, ensure you are on the **IP to ISDN dial plan** tab
3. In the **Test dial plan** section, enter the number to test and click **Test number**.

The ISDN Gateway displays the number that you have tested, the rule that the condition matched, the outcome (that is, whether the call was rejected or the number that has been dialed in response) and the bandwidth.

Adding dial plan rules

The options that are available to you when you are configuring dial plan rules depend on whether or not the Cisco TelePresence ISDN Gateway is in *leased line mode*. (Leased line mode is configured on the **Settings > ISDN** page.)

Select the help topic that you need:

- Adding and updating dial plan rules (non-leased line mode)
- Adding dial plan rules in leased line mode

Adding and updating dial plan rules

This page describes how to add rules to the dial plan. It also tells you how to update rules.

Note that you may also find it helpful to refer to Example dial plan rules.

Adding dial plan rules

To add a dial plan rule:

1. Go to **Dial Plan**. If you want to add an
    - IP to ISDN rule, use the **IP to ISDN** page.
    - ISDN to IP rule, use the **ISDN to IP** page.
2. Click **Add rule**.
3. Type a name for the rule.
4. For *Condition* choose one of:
    - *Match any called number*: this condition matches any called number and also includes calls where the called number is not known or unavailable. Generally, this kind of rule should be used towards the bottom of the dial plan list to match numbers not recognized by more specific rules higher up.
    - *No called number*: this condition matches when the called number is not known or unavailable for ISDN calls. For IP calls, this condition matches when the caller uses the IP address or hostname of the Cisco TelePresence ISDN Gateway.
    - Called number matches***:***
        - To match a specific number, enter that specific number.

          Example: to match calls to "001234", type **001234**. The condition will match that and only that number.

          Use S to match * (asterisk) and use P to match # (pound/hash). Examples: to match calls to "*234", type **S234**; to match calls to "#0987", type **P0987**
        - To match a more general number, use the wildcard character, **D**. This matches any digit as well as # and *.

          Example: to match any number that starts with "55" followed by exactly two more digits, type **55DD**. This condition will match "5500", "5523", "5555", "5599", etc. but not "55" or "55233".
        - For more general matching, you may use one of the three repeat characters. These modify the character immediately before, whether it is a specific digit or the wildcard character. The repeat characters are:
          ? match once or zero times.
          + match once or more.
          ***** match zero or more times.
          For example, "5+" means " match at least one 5, but possibly more".
          "D*" means "match any digit, any number of times". D matches any digit as well as # and *.

          Example: to match any number that starts with "01", has any amount of digits in the middle, and ends with "5", type **01 D* 5**.

- To include any of the incoming called digits in the outgoing called number, enclose each substitution group in a set of parentheses. Note that if you want to include the complete number, you do not need to enclose the whole expression in parentheses.

  Example: to match any number starting with "678", then followed by three or four digits, and you want the final digits to form part of the called number, type the expression: **678 (DDDD?)**. This will match "6780000", "678123", "6789999" etc. but not "67822" or "775000".

5. For *Action* (that is, what happens to the outgoing part of the call if this rule is invoked) choose one of:
   - *Reject the call*: the call will be terminated and the outgoing part of the call will not be established.
   - *Enter the auto attendant*: the call will be connected to the auto attendant.
   - *Enter the auto attendant + TCS-4*: the call enters the auto attendant and sends a TCS-4 request; when the auto attendant receives the reply, it dials out the TCS-4 extension. Usually the TCS-4 reply is fast enough that the auto-attendant is not displayed; however, you may see it briefly with the TCS-4 extension shown. (For more information about using TCS-4 see Example dial plan rules)
   - *Call with the original called number*: (not valid if you are going to select *Video using H.221 aggregation (legacy)* as the Call type in the **Additional parameters** section) the outgoing part of the call will be placed to the number that was the original called number. For example, an incoming ISDN call to "54321" will result in an outgoing call placed over IP to "54321".
   - *Call this number*: (not valid if you are going to select *Video using H.221 aggregation (legacy)* as the Call type in the **Additional parameters** section) the outgoing call will be placed to the number that is entered here. Type a number, or for ISDN to IP rules you can also type an IP address or hostname.
     - To call a specific number (or for ISDN to IP calls, you can also specify an IP address, hostname, or H.323 URI), type that number (or IP address, hostname, or H.323 URI). IPv6 addresses must be enclosed in brackets [ ].

       Example: to specify that when this rule is invoked, the MCU with hostname my_mcu is called, type **my_mcu**.

       Example: suppose the domain "cisco.com" has a H.323 service (SRV) record set up. To call a H.323 video endpoint residing in that domain, e.g. with URI example.person@cisco.com, set an action to call **example.person@cisco.com**. For information about domain (DNS) SRV records, see RFC 2782.

     - To call a specific extension, separate the number/address from the extension by typing an exclamation mark (!).

       Example: to call the MCU with IP address "10.2.1.33", and try to join a conference with numeric identifier "00000", type **10.2.1.33 ! 00000**

     - To include any of the digits from the incoming called number in the outgoing number, specify a substitution, by typing the dollar sign ($) followed by a index. Valid indices are:
       A: substitute the entire incoming called number.
       1..9: substitute the digits enclosed in the relevant set of parentheses of the condition.

Example: for all calls matching the condition of "55 (DDDD)", set an action to call the MCU with name "my_mcu" and join the call to the conference with identifier that matches "(DDDD)". For this example, type the action of **my_mcu ! 00 $1**. In this case, an incoming call to "551234" will attempt to join conference with numeric identifier "001234" on the MCU with the name "my_mcu".

Example: in an IP to ISDN dial plan rule, for calls matching a condition (D*)P(D*), setting an action to call $1!$2 will match any numbers which have a '#' in, using the number before the '#' for the phone number and the number after the '#' as the TCS-4 extension. (For more information about using TCS-4 see Example dial plan rules)

- *Call these numbers*: this option only becomes available if you select *Video using H.221 aggregation* (legacy) as the call type (for IP to ISDN calls) in the **Additional parameters** section. Only use *Video using H.221 aggregation* (legacy) if you are supporting legacy ISDN endpoints that need this feature. You must ensure you enter the correct number of telephone numbers. For example, if you select 3 x 64kbps as the call bandwidth, you must enter three telephone numbers here. Note that you can use the same scheme of substitutions as described for *Call this number*.

6. Complete the **Additional parameters**, if required:
   - *Call type*: Specify the type of outgoing call:
     - *Telephone*: if the call is a voice-only telephone call.
     - *Video using BONDING (default)*: a "typical" video call.
     - *Video using H.221 aggregation (legacy)*: only select this if you need to support legacy ISDN endpoints that require n x 64kbps or n x 56kbps channels. This option is only available for IP to ISDN calls
   - *Restrict (56k)*:***(this is only for IP to ISDN dial plan rules)*** when selected, for calls matching this dial plan rule the ISDN Gateway will make the outgoing ISDN call in restricted 56k mode. Do not select this option unless your network requires it. Note that for a call matching a rule that uses 56k mode, if the endpoint only supports 64k, the ISDN Gateway will drop the call rather than use 64k.
   - *Maximum call bandwidth*: optionally, select a maximum bandwidth for the ISDN part of the call, which will otherwise be set to the default value. To view or edit the default value, go to **Settings > ISDN**. The maximum bandwidth settings on the **Settings > ISDN** page are global settings. Therefore, if you choose a greater setting in the dial plan than you have as a global setting, the global setting will be used as the maximum value. For example, if in the dial plan you choose to set *320kbps (5 x B channels)* as the maximum bandwidth and the global setting for maximum bandwidth for outgoing ISDN calls is *256kbps (4 x B channels)*, the maximum bandwidth available to the call will never be more than 256kbps.

     Note that if you have selected *Telephone* as the call type, this option is unavailable and the bandwidth set automatically.

     Note that if you have selected *Video using H.221 aggregation (legacy)* as the call type, you must ensure you select a bandwidth that matches the number of telephone numbers that you have entered.
   - *Encryption settings*:
     - *Use transparent encryption*: when selected, the ISDN Gateway will simulate point-to-point encryption. That is, it will set the encryption state (enabled/disabled) used on the received call as that to be used on the outgoing call. That is, the ISDN Gateway will attempt to match the encryption state for the

outgoing call to that of the incoming call. This means that if the encryption state changes on either the incoming or outgoing call, the ISDN Gateway will attempt to change the encryption state on the other side of the call. This can be helpful if a call starts as an encrypted call both sides of the ISDN Gateway and then the incoming call stops being encrypted for some reason; the outgoing part of the call will also drop the encryption and both callers will know that the call is no longer encrypted.

- Select *Required* in the appropriate checkbox(es) if you always want the IP and/or ISDN part of a call to be encrypted or *Optional* if encryption is only to be used to endpoints that support it. Note that:
  - Encryption must also be enabled globally in the **Settings > Encryption** page.
  - If *Required* is selected and the endpoint does not support encryption, the call will be disconnected. If the endpoint does support encryption, no media is passed until encryption can be ensured. However if you select *Optional* and the endpoint supports encryption, then a call to may start even before encryption can be guaranteed but will use encryption as soon as possible
  - If the *Call type* is *Telephone*, then ISDN encryption is *Disabled*
  - These settings for IP and ISDN encryption are not available if you have selected to use *transparent encryption* for this dial plan rule

- *Place call on*: (IP to ISDN only) optionally, select the ISDN port(s) on which the call may be placed. The selected ports will be used in ascending or descending order as specified in the Port search order field in the **Settings > ISDN** page.
- *Receive call on*: (ISDN to IP only) select the port(s) to advertise to the calling endpoint. These ports may be used to complete subsequent calls from the calling end. The selected ports will be used in ascending or descending order as specified in the Port search order field in the **Settings > ISDN** page.

7. For *Codecs allowed* select an option from the drop-down list: <use default choices>, Custom codec choices or Safe codec choices. The last two options are provided for older endpoints that you cannot connect to when some codecs are enabled (even if the endpoint supports those codecs). We recommend that you only use these options when you experience a problem.
   - When you select Custom codec choices, the screen refreshes and you can select the audio, video and H.239 video codecs that are allowed with this dial plan
   - Safe codec choices only allows G711 and H261
8. Click **Add rule**.

Updating dial plan rules

To update an existing dial plan rule:

1. Go to **Dial plan** and find the rule you want to modify.
2. Click on the number or name of the rule to view its details.
3. Modify the rule details using the information listed above in Adding dial plan rules to help you.
4. Click **Update rule**.

You may wish to create a new rule very similar to an existing rule. To do this, find the existing rule and click on its name or number to view its details. Press **Copy rule** to create a new rule, initialized with the existing parameters, then proceed as normal, pressing **Add rule** when you have finished

Adding and updating dial plan rules in leased line mode

This page describes how to add rules to the dial plan when the Cisco TelePresence ISDN Gateway is in leased line mode. It also tells you how to update rules.

When you use the ISDN Gateway in leased line mode, the options on the dial plan are different to those in 'non leased line mode'. This is because as there is no D-channel, no number is sent over the leased line call; this necessarily affects the options available for the configuration of the dial plan.

Note that you may also find it helpful to refer to Example dial plan rules.

Adding dial plan rules

To add a dial plan rule:

1. Go to **Dial Plan**. If you want to add an
   - IP to ISDN rule, use the **IP to ISDN** page.
   - ISDN to IP rule, use the **ISDN to IP** page.
2. Click **Add rule**.
3. Type a name for the rule.
4. For *Condition* choose one of:
   - *Match any incoming call* : this condition matches any incoming call and also includes calls where the called number is not known or unavailable. Generally, this kind of rule should be used towards the bottom of the dial plan list to match numbers not recognized by more specific rules higher up.
   - *No called number*: *(**this is only for IP to ISDN dial plan rules**)* this condition matches when the caller uses the IP address or hostname of the ISDN Gateway
   - *Called number matches: (**this is only for IP to ISDN dial plan rules**)*
     - To match a specific number, enter that specific number.

       Example: to match calls to "001234", type **001234**. The condition will match that and only that number.

       Use S to match * (asterisk) and use P to match # (pound/hash). Examples: to match calls to "*234", type **S234**; to match calls to "#0987", type **P0987**
     - To match a more general number, use the wildcard character, **D**. This matches any digit as well as * and #.

       Example: to match any number that starts with "55" followed by exactly two more digits, type **55DD**. This condition will match "5500", "5523", "5555", "5599", etc. but not "55" or "55233".
     - For more general matching, you may use one of the three repeat characters. These modify the character immediately before, whether it is a specific digit or the wildcard character. The repeat characters are:
       ? match once or zero times.
       + match once or more.

***** match zero or more times.
For example, "5+" means " match at least one 5, but possibly more".
"D*" means "match any digit, any number of times". D matches any digit as well as * and #

Example: to match any number that starts with "01", has any amount of digits in the middle, and ends with "5", type **01 D* 5**.

- To include any of the incoming called digits as the port number, leased line group, and optionally the TCS-4 extension for the outgoing call, enclose each substitution group in a set of parentheses.

  Example: For an incoming number that starts with "678", and is followed by two digits, and where you want the penultimate digit to be used as the outgoing port number and the final digit to be used as the outgoing leased line group, type the expression: **678 (D)(D)**. This will match the incoming called digits: "67812". (For more information about using substitution groups in leased line mode see Example dial plan rules)

  Example: For an incoming number that starts with 987 and that is followed by the port number, the leased line group number, and a TCS-4 extension of four or more digits, type the expression **987(D)(D)(DDDD+)**. This will match the incoming digits: "987235678" and "98733456789. (For more information about using substitution groups in leased line mode see Example dial plan rules).

- *Match calls incoming on port leased line group*: ***(this is only for ISDN to IP dial plan rules)*** this condition matches calls using the specified port number and leased line group number. Note that you can specify *Any* for either/or both the port and the leased line group.

5. For *Action* (that is, what happens to the outgoing part of the call if this rule is invoked) choose one of:

   - *Reject the call*: the call will be terminated and the outgoing part of the call will not be established.
   - *Call port <X> leased line group <x>*: ***(this is only for IP to ISDN dial plan rules)***You can select the port number and leased line group number for the outgoing ISDN call. You can either specify these as digits or use substitution groups from the *Called number matches* field in the condition of this dial plan rule (refer to the information above for more details about using substitution groups in the *Called number matches* field).
   - *Enter the auto attendant*: ***(this is only for ISDN to IP dial plan rules)*** the call will be connected to the auto attendant. Note that the ISDN Gateway applies the dial plan to numbers dialed in the auto attendant.
   - *Enter the auto attendant + TCS-4*: ***(this is only for ISDN to IP dial plan rules)*** the call enters the auto attendant and sends a TCS-4 request; when the auto attendant receives the reply, it dials out the TCS-4 extension. Usually the TCS-4 reply is fast enough that the auto-attendant is not displayed; however, you may see it briefly with the TCS-4 extension shown. (For more information about using TCS-4 see Example dial plan rules).
   - *Call this number*: ***(this is only for ISDN to IP dial plan rules)*** the outgoing call will be placed to the number that is entered here. Type a number, or you can also type an IP address or hostname.

     - To call a specific number, IP address or hostname, type that number, IP address, or hostname. IPv6 addresses must be enclosed in brackets [ ].

       Example: to specify that when this rule is invoked, the Cisco TelePresence MCU with hostname my_mcu is called, type **my_mcu**.

- To call a specific extension, separate the number/address from the extension by typing an exclamation mark (!).

  Example: to call the Cisco TelePresence MCU with IP address "10.2.1.33", and try to join a conference with numeric identifier "00000", type **10.2.1.33 ! 00000**

6. Complete the **Additional parameters**, if required:

   - *TCS-4 extension digits (optional)*:(***this is only for IP to ISDN dial plan rules***) specify the TCS-4 extension to be used for calls matching this rule. Note that you can either type the TCS-4 extension to be used, or you can specify a substitution group such that digits from the original called number will be used as the TCS-4 extension.
     Example: if you specify **99(D+)** for the **Called number matches** field, and **$1** for the TCS-4 extension, then a call to 991234 will use "1234" as the TCS-4 extension.
   - *Restrict (56k)*:(***this is only for IP to ISDN dial plan rules***) when selected, for calls matching this dial plan rule the ISDN Gateway will make the outgoing ISDN call in restricted 56k mode. Do not select this option unless your network requires it. Note that for a call matching a rule that uses 56k mode, if the endpoint only supports 64k, the ISDN Gateway will drop the call rather than use 64k.
   - *Maximum call bandwidth*:(***this is only for ISDN to IP dial plan rules***) optionally, select a maximum bandwidth for the ISDN part of the call, which will otherwise be set to the default value. To view or edit the default value, go to **Settings > ISDN**. The maximum bandwidth settings on the **Settings > ISDN** page are global settings. Therefore, if you choose a greater setting in the dial plan than you have as a global setting, the global setting will be used as the maximum value. For example, if in the dial plan you choose to set *320kbps (5 x B channels)* as the maximum bandwidth and the global setting for maximum bandwidth for outgoing ISDN calls is *256kbps (4 x B channels)*, the maximum bandwidth available to the call will never be more than 256kbps.
   - *Encryption settings*:
     - *Use transparent encryption*: when selected, the ISDN Gateway will simulate point-to-point encryption. That is, it will set the encryption state (enabled/disabled) used on the received call as that to be used on the outgoing call. That is, the ISDN Gateway will attempt to match the encryption state for the outgoing call to that of the incoming call. This means that if the encryption state changes on the incoming call, the ISDN Gateway will attempt to change the encryption state on the outgoing call. This can be helpful if a call starts as an encrypted call both sides of the ISDN Gateway and then the incoming call stops being encrypted for some reason; the outgoing part of the call will also drop the encryption and both callers will know that the call is no longer encrypted.
     - Select *Required* in the appropriate checkbox(es) if you always want the IP and/or ISDN part of a call to be encrypted or *Optional* if encryption is only to be used to endpoints that support it. Note that:
       - Encryption must also be enabled globally in the **Settings > Encryption** page.
       - If *Required* is selected and the endpoint does not support encryption, the call will be disconnected. If the endpoint does support encryption, no media is passed until encryption can be ensured. However if you select *Optional* and the endpoint supports encryption, then a call to may start even before encryption can be guaranteed but will use encryption as soon as possible
       - These settings for IP and ISDN encryption are not available if you have selected to use *transparent encryption* for this dial plan rule

7. For *Codecs allowed* select an option from the drop-down list: <*use default choices*>, *Custom codec choices* or *Safe codec choices*. The last two options are provided for older endpoints that you cannot connect to when some codecs are enabled (even if the endpoint supports those codecs). We recommend that you only use these options when you experience a problem.
    - When you select *Custom codec choices*, the screen refreshes and you can select the audio, video and H.239 video codecs that are allowed with this dial plan
    - *Safe codec choices* only allows G.711 and H.261
8. Click **Add rule**.

Updating dial plan rules

To update an existing dial plan rule:

1. Go to **Dial plan** and find the rule you want to modify.
2. Click on the number or name of the rule to view its details.
3. Modify the rule details using the information listed above in Adding dial plan rules to help you.
4. Click **Update rule**.

You may wish to create a new rule very similar to an existing rule. To do this, find the existing rule and click on its name or number to view its details. Press **Copy rule** to create a new rule, initialized with the existing parameters, then proceed as normal, pressing **Add rule** when you have finished.

Example dial plan rules

Use the examples on this page to help you configure your own dial plan rules:

- Allocating bandwidth using rules for IP to ISDN calls
- Allocating bandwidth using rules for ISDN to IP calls
- Forwarding ISDN calls to an operator or a conference
- Specifying voice-only IP to ISDN telephone calls
- Setting up dial plans rules when using TCS-4

Note these examples do not apply if the Cisco TelePresence ISDN Gateway is in leased line mode. Refer to the following example dial plan rules for leased line mode:

- Dial plan examples in leased line mode

Allocating bandwidth using rules for IP to ISDN calls

Using rules, it is possible to limit the bandwidth available for calls to particular numbers, or to allocate more bandwidth to priority calls. For example, you may want to allocate maximum bandwidth to calls to the chief executive of your company. In this case, set a *Condition* that matches calls to that specific number, set the *Action* to call with the original called number, and set the *Maximum call bandwidth* to use 768kbps.

As cost is an issue with calls to the ISDN network, you may want to provide users with a list of prefixes that they can use to control the bandwidth for the calls they make. In this way, rules enable you to allow users to select their own appropriate bandwidth for a call. The table below shows some rules that you could configure to set up different prefixes to represent the number of channels that will be available to the call. It also shows how the IP to ISDN dial plan will remove those prefixes and dial the required number.

#	Condition	Action	Call type	Bandwidth	Description
0	Called number matches "552 (D*)"	Call this number "$1"	Video with BONDING	128Kbps	This rule allocates 128kbps (that is, two channels) to any call with prefix 552. The specified action means that the dial plan removes the prefix and dials the following group of characters in the condition. For example, an incoming call to "55264321" will cause an outgoing call allocated with two channels to be placed to "64321".

1	Called number matches "553 (DDDD)"	Call this number "$1"	Video with BONDING	192Kbps	This rule allocates 192kbps (that is, three channels) to any call with prefix 553. The specified action means that the dial plan removes the prefix and dials the group of four characters (containing 0 through 9 and # and *) that match the four characters represented by "(DDDD)" in the condition. For example, an incoming call to "5539876" will cause an outgoing call allocated with three channels to be placed to "9876".
2	Called number matches "558 (DDDD)"	Call this number "$1"	Video with BONDING	512Kbps	This rule allocates 512kbps (that is, eight channels) to any call with prefix 558. The specified action means that the dial plan removes the prefix and dials the group of four characters (containing 0 through 9 and # and *) that match the four characters represented by "(DDDD)" in the condition. For example, an incoming call to "5585678" will cause an outgoing call allocated with eight channels to be placed to "5678".

In the above example, in the absence of any further rules, any calls that do not match the listed conditions will be rejected because that is the default behavior of the dial plan.

Allocating bandwidth using rules for ISDN to IP calls

Using rules, it is possible to limit the bandwidth available for incoming ISDN calls. This is useful where you want to limit the network resources available to individual calls. In this way, you can prevent any one call using the resources to the extent that other incoming calls are prevented.

#	Condition	Action	Call type	Bandwidth	Description
0	Match any called number	Call with the original called number	Video with BONDING	384Kbps	This rule forwards all calls to the dialed number with a bandwidth of 384Kbps

Forwarding ISDN calls to an operator or a conference

The dial plan below forwards any calls from the ISDN network ending in 0000 to an operator and forwards any other dialed number of four digits or more to the MCU to join a conference where the conference identifier is the last four numbers of the original dialed number.

The dial plan shown below is an ISDN to IP dial plan:

#	Condition	Action	Call type	Bandwidth	Description
0	Called number matches "D+ 0000"	Call this number "10.2.1.10"	Video with BONDING	384Kbps	This rule catches any number ending in 0000 and forwards it to, for example an operator, at 10.2.1.10
1	Called number matches "D+(DDDD)"	Call this number "10.2.1.20 ! $1"	Video with BONDING	384Kbps	This rule catches any set of four characters or more and tries to join a conference on the MCU at 10.2.1.20 with the numeric identifier that matches the last four digits. Note that although D matches ~ and * as well as 0 through 9, the numeric identifier of a conference can only be a number.

Specifying voice-only IP to ISDN telephone calls

Use the following dial plan to specify how IP telephone calls (that is voice-only calls) will be forwarded to the ISDN network.

IP endpoints sometimes do not allow users to specify the type of call being made. The following dial plan shows that users can be told the prefix to dial, should their call be a telephone call rather than a video and voice call.

This dial plan also includes an example of how you can use the dial plan to specify DTMF tones to be dialed after the call has been answered.

The dial plan shown below is an IP to ISDN dial plan:

#	Condition	Action	Call type	Bandwidth	Description
0	Called number matches "550 (D+)"	Call this number "$1"	Telephone	None	This rule specifies a voice-only call to any call with prefix 550. The specified action means that the dial plan removes the prefix and dials the group of numbers that match the characters represented by "(D+)" in the condition. For example, an incoming call to "5504321" will cause an outgoing voice-only call to be placed to "4321".

1	Called number matches "99555"	Call this number "01753 548333!555P,,888P "	Telephone	None	This rule allows a caller to connect to a PIN protected audio conference on an audio bridge. In this example, the audio bridge will answer the call. After a two second pause the ISDN Gateway sends the DTMF tones for the conference ID (555); these are the digits after the exclamation mark (!) which indicates where the number to dial ends and the DTMF tones begin. There is a four second pause (represented by two commas) and then the ISDN Gateway sends the PIN (888). The audio bridge requires a caller to press pound/hash after the ID and the PIN; these are represented with 'P'.
2	Match any called number	Call with original called number	Video with BONDING	128Kbps	This rule catches any other called number and will place it as a video-conferencing call (that is video and voice) using the lowest bandwidth.

Setting up dial plan rules when using TCS-4

TCS-4 is a protocol that only applies to H.320 video calls and is a method of signaling an extension number after an H.320 call has been established. By using a TCS-4 extension to pass the extra digits to the ISDN Gateway, customers can dial from a predefined endpoint phone list, rather than entering the extension using DTMF in the auto attendant.

ISDN to IP calls

There is a new **Action** in the ISDN to IP dial plan: *Enter the auto attendant + TCS-4*. When used, the call enters the auto attendant and sends a TCS-4 request; when the auto attendant receives the reply, it dials out the TCS-4 extension. Usually the TCS-4 reply is fast enough that the ISDN Gateway auto-attendant is not displayed; however, you may see it briefly with the TCS-4 extension shown.

To send a TCS-4 extension:

- from an ISDN-capable Cisco TelePresence endpoint, dial the ISDN number followed by a * and then enter the TCS-4 extension. For example, if the ISDN Gateway TCS-4 dial plan incoming number match is 1234 and the required TCS-4 extension is 5678, dial 1234*5678 from your endpoint. The ISDN Gateway will then connect to the TCS-4 dial plan and dial out 5678 from the ISDN Gateway auto attendant without you having to enter the extension via DTMF

- from a Polycom endpoint, replace the * with ##
- from LifeSize and Sony endpoints, replace the * with #. For other endpoints, please refer to the user manual.

It is possible to send an alphanumeric H.323 ID as a TCS-4 extension from most endpoints. For example, you can dial 1234*MCU, where MCU is the registered H.323 ID with the gatekeeper (usually case sensitive).

It is also possible to send an IP address as a TCS-4 extension from ISDN-capable Cisco TelePresence endpoints.

IP > ISDN > ISDN > IP calls

When using TCS-4 in an "ISDN bridge between IP islands" (in which two IP endpoints/MCUs communicate traversing an ISDN link), two ISDN Gateways are required. The first ISDN Gateway (for the IP to ISDN conversion) cannot do TCS-4 because TCS-4 functionality only works in ISDN to IP direction. However, the second ISDN Gateway will be able to process a TCS-4 request and therefore needs to be set up with the TCS-4 dial plan as discussed above.

The first ISDN Gateway needs to forward a number to the second ISDN Gateway in the same format as a TCS-4 request received from any other ISDN endpoint. That is why, even though the first ISDN Gateway does not perform TCS-4 extension dialing, it should be set up so that it can call out with a number that is same as sending a TCS-4 request to the second ISDN Gateway. This new functionality has been implemented for the IP to ISDN dial plan on the ISDN Gateway, as described below.

When you dial from the calling IP endpoint, you need to send both the dial plan call-in match parameters of the two ISDN Gateways as well as the required TCS-4 extension. Assume that:

- the first ISDN Gateway dial plan call-in number match is 123
- the second ISDN Gateway TCS-4 dial plan call-in number match is 456
- the TCS-4 extension required to dial the called IP endpoint is 789

Dial the full number 123456#789 from the calling IP endpoint separating the 789 portion with the appropriate * or # mark to indicate that this is the TCS-4 extension. The first ISDN Gateway strips the 123 portion from this number and sends the rest of the number 456789 to the second ISDN Gateway in such a format that the second ISDN Gateway understands that the 456 portion is the dial plan match number and the 789 is the TCS-4 extension. The second ISDN Gateway then dials the TCS-4 extension using its TCS-4 dial plan.

- To set up the first ISDN Gateway to send a number string that matches a TCS-4 request, a new delimiter ! has been introduced. This delimiter is used to split the **Call this number** field, where the part before the ! is the ISDN number to call, and the rest (after !) is the extension address to respond to a TCS-4 request. Therefore, in the **Call this number** field, enter <ISDN number of second GW>!<the TCS-4 extension used by the second ISDN Gateway>

To dial 123456#789 from an IP endpoint, set up the first ISDN Gateway with an IP to ISDN dial plan:

  - **Called number match** : 123(D*)P(D*)
  - **Action**: *Call out number*: $1 ! $2

The first (D*) group matches the numbers before the Pound (hash) sign and the second (D*) group matches the number after the Pound sign. Therefore in the **Call out number** field, $1 will replace the first (D*) group, $2 will replace the second (D*) group after the # sign (the TCS-4 extension) and the ! sign will indicate to the second ISDN Gateway that the first part is an ISDN number and the second portion is the TCS-4 extension. In this example, the first ISDN Gateway will call out 456!789 to the second ISDN Gateway which will receive it as a TCS-4 request (see below)

- Set up the second ISDN Gateway with an ISDN to IP dial plan:
  - **Called number match**: 456
  - **Action: Enter the auto attendant + TCS-4**

The second ISDN Gateway treats 456!789 as a TCS-4 request and any digits after "!" as the TCS-4 extension. It matches 456 to this dial plan and calls the TCS-4 extension 789 to connect to the IP endpoint

For the ISDN to IP TCS-4 dialing rule, you have to use *, # or ## to separate the ISDN number and the TCS-4 extension depending on the ISDN endpoint manufacturer. However, in this case, when you are dialing from the IP endpoint to the first ISDN Gateway, you can either use * or # irrespective of the endpoint you're using. For example, when you dial 123456#789 from the IP endpoint, you could also dial 123456*789. In the latter case, simply change the **Called number match** of the first ISDN Gateway from 123(D*)P(D*) to 123(D*)S(D*) (S denotes *).

Notes:

- It is not possible to send alphanumeric characters as a TCS-4 extension from the IP side. That is, you cannot dial 123456*MCU or 123456#MCU from an IP endpoint because the extension number (after the * or #) is parsed by the dial plan and there is no way to match letters in the **Called number matches** field. Therefore the $1 and $2 groups on the dial plan of the first ISDN Gateway would only match numbers and not characters.
- It is not possible to send an IP address as a TCS-4 extension from the IP endpoint to the first ISDN Gateway.

Dial plan examples in leased line mode

ISDN to IP dial plan (leased line mode)

The dial plan rule below forwards any some calls from the ISDN network to an auto attendant on the Cisco TelePresence MCU. It allows for some calls to arrive with a TCS-4 extension. It has a catch all rule that forwards other calls to an operator.

The dial plan shown below is the ISDN to IP dial plan:

#	Condition	Action	Maximum call bandwidth	Description
0	Match calls incoming on port "1" leased line group "2"	Call this number "10.2.1.12 ! 555"	<use default value>	This rule matches any call arriving from the ISDN network using leased line group 2 on ISDN port 1 and forwards it to the auto attendant on the MCU at 10.2.1.12. (The MCU's auto attendant is configured with *Numeric ID* 555.)
1	Match calls incoming on port "2" leased line group "1"	Enter the auto attendant + TCS-4	<use default value>	This rule matches any call arriving from the ISDN network using leased line group 1 on ISDN port 2 and forwards it to the auto attendant which dials out using the TCS-4 extension.
2	Match calls incoming on port "Any" leased line group "Any"	Call this number "10.2.1.10"	<use default value>	This rule matches any call arriving from the ISDN network (that has not matched either of the above two rules) and forwards it to, for example an operator, at 10.2.1.10

IP to ISDN dial plan (leased line mode)

The dial plan shown below is the IP to ISDN dial plan:

#	Condition	Action	TCS-4 extension	Description
0	Called number matches "98(D)(D)(D+)"	Call port $1 leased line group $2	$3	This rule matches any call to a four-digit number beginning 98. The dialed digits also provide the ISDN port number, the leased line group, and the TCS-4 extension. For example, if the called number is 9812777, the call will be made on ISDN port 1 using leased line group 2, with TCS-4 extension 777.
1	Match any incoming call	Call port "2" leased line group"3"		This rule matches any call that does not match the first rule in the dial plan. In this example, calls to port 2 leased line group 3 will be answered by an operator.

Dial plan syntax

This page describes the syntax that you can use when adding dial plans.

Note: All IPv6 address fields in the ISDN Gateway require the IPv6 address to be enclosed in square brackets [ ].

Syntax for conditions (*Called number matches*)

When you configure the *Condition* for a dial plan rule, you may want to specify a pattern for the called number rather than specifying any of: match any called number, no called number or the exact called number.

The table below describes the syntax you can use to express a pattern for the *Called number matches* field in the condition of a rule:

Syntax	Description	Example
Numbers 0 to 9	To match a specific number, enter that number.	Example: to match calls to "001234", type 001234. The condition will match that and only that number.
S	To match an * (known as an asterisk or star), enter an S.	Example: to match calls to "**1234", type SS1234. The condition will match that and only that number.
P	To match a # (known as a pound or hash), enter a P.	Example: to match calls to "#1234", type P1234. The condition will match that and only that number.
D	To match any digit, # (known as a pound or hash), and/or * (known as an asterisk or star) use the wildcard character **D**	Example: to match any number that starts with "623" followed by exactly two more digits, type 623DD. This condition will match "62300", "62323", "62355", "62399" "623*#", etc. but not "623" or "623233".
?	To match once or zero times, use **?**	Example: "6?" means match one 6 or no 6s, and is useful when used with the wildcard "**D**" where you do not know how long a number will be. The expression: "67800D?" will match "67800" and "678004" but not "67800666".
+	To match once or more, use +	Example: "5+" means "match at least one 5, but possibly more".
*	To match zero or more times, use *. This is useful when used with the wildcard: "D*" means "match any digit, any number of times".	Example: to match any number that starts with "01", has any amount of digits in the middle, and ends with "5", type **01 D* 5.**
()	Parentheses indicate substitution groups. To include any of the incoming called digits in the	Example: to match any number starting with "678", then followed by a number of

	outgoing called number, enclose them in parentheses. Note that if you wish to include the complete number, you do not need to enclose the whole expression in parentheses.	other digits, and you want the final digits to form part of the called number, type the expression: 678 (D*). This will match "6780000", "678123", "6789999" etc. but not "775000".

Syntax for actions (*Call this number*)

When you configure the **Action** for a dial plan rule, you may want to specify a pattern for the number to call, rather than specifying any of: call original called number, reject the call, or the exact number to call.

The table below describes the syntax you can use to express a pattern for the *Call this number* field in the action of a rule:

Syntax	Field description	Example
Letters and numbers for address	To call a specific number (or for ISDN to IP calls, you can also specify an IP address, hostname, or H.323 URI), type that number (or IP address, hostname, or H.323 URI). IPv6 addresses must be enclosed in brackets [ ].	Example: to specify that when this rule is invoked, the MCU with hostname my_mcu is called, type **my_mcu**. Example: Suppose the domain " cisco.com" has a H.323 service (SRV) record set up. To call a H.323 video endpoint residing in that domain, e.g. with URI example.person@cisco.com, set an action to call **example.person@cisco.com**. For information about domain (DNS) SRV records, see RFC 2782.
:	To call a specific extension, separate the number/address from the extension by typing a colon (**:**).	Example: to call the Cisco TelePresence MCU with IP "10.2.1.33", and try to join a conference with numeric identifier "00000", type **10.2.1.33 : 00000.**
!	To call a specific extension, separate the number/address from the extension by typing an exclamation mark **(!)**.	Example: to call the MCU with IP "10.2.1.33", and try to join a conference with numeric identifier "00000", type **10.2.1.33 ! 00000**.
$	To include any of the digits from the incoming called number in the outgoing number, specify a substitution, by typing the dollar sign ($), followed by a index. Valid indices are: **A**: substitute the entire incoming called number. **1 to 9** : substitute the digits enclosed in the nth set of parentheses of the condition.	Example: for all calls matching the condition of "55 (DDDD)", set an action to call the MCU with name "my_mcu" and join the call to the conference with identifier that matches "(DDDD)". For this example, type the action of **my_mcu ! 00 $1**. In this case, an incoming call to "551234" will attempt to join conference with numeric identifier "001234" on the MCU with the name "my_mcu". Note that if the substitution creates an

		empty number, the call will be rejected; in the above example, an incoming call to 55 would result in an empty substitution.
!	This delimiter is only for use in an "ISDN bridge between IP islands" when you want to use TCS-4 extensions. In this case use the ! before TCS-4 extension in the dial plan for the first ISDN Gateway so that it is passed to the second ISDN Gateway in a format recognized as a TCS-4 extension..	A detailed example and further explanation of TCS-4 is provided in Example dial plan rules.
!	This is a delimiter that can be used for telephone calls where there is a number to dial which must be followed by DTMF tones.	This feature is for IP to ISDN telephone calls. It allows you to configure the dial plan to start sending DTMF tones after a telephone call has connected. This is useful if there is a call through the ISDN Gateway to a device which is perhaps behind another gateway which only supports DTMF to decide how to route the calls. The caller is not required to additionally enter the DTMF codes manually on the telephone keypad but instead can have the call re-routed automatically using the dial plan of the ISDN GW. To do this, when completing the *Call this number* field, first type the number to call then type an exclamation mark (!) and type the DTMF extension after it.
,	When sending DTMF tones in a telephone call, a comma indicates a two second pause. Two commas (,,) indicate a four second pause. You can insert as many two second pauses as you want.	Pauses are useful where there are more than one set of DTMF tones to enter. For example, if the call is answered by an automated operator system which requires that the caller chooses an option from a menu and is then transferred to an audio conferencing system (for example) and then is asked to enter the conference ID. Refer to the section "Specifying voice-only IP to ISDN telephone calls" in Example dial plan rules.

Displaying the built-in gatekeeper registration list

The Cisco TelePresence ISDN Gateway contains a built-in gatekeeper with which devices can register multiple IDs. IDs can be numbers, H.323 IDs (e.g. Fredsendpoint) or prefixes.

Up to 25 devices can be registered without a feature key. Feature keys can be purchased to increase this number.

Note: The ISDN Gateway can register with its own built-in gatekeeper. The ISDN Gateway then counts as one registered device. See Configuring H.323 gatekeeper settings.

Configuring the built-in gatekeeper

To start the gatekeeper:

1. Go to **Network > Services** and select **H.323 gatekeeper** to open a port for the gatekeeper. (On the ISDN Gateway, ports are not open by default for security reasons.)
2. Go to **Gatekeeper**, select *Enabled* in the **Status** field and click **Apply changes**. If you attempt to enable the built-in gatekeeper without opening the port, an error message is displayed.

Configuring neighboring gatekeepers

You can optionally configure the built-in gatekeeper with up to two neighboring gatekeepers. This means that if the built-in gatekeeper receives a request (known as an Admission Request or ARQ) to resolve an ID to an IP address and that ID is not currently registered with it then it will forward that request to its neighbor gatekeeper(s), as a Location Request (LRQ). The built-in gatekeeper will then use the information received from the neighbor(s) to reply to the original request.

You can also configure the behavior of the built-in gatekeeper on receipt of LRQs from another gatekeeper. It can:

- send LRQs regarding unknown IDs to its neighbor(s)
- reply to LRQs from other gatekeepers
- accept LCFs (Locations Confirms) from non-neighboring gatekeepers

Refer to this table for assistance when configuring the built-in gatekeeper:

Field	Field description	Usage tips
Status	Enables or disables the built-in gatekeeper.	To use the built-in gatekeeper, you must enable it here.
Neighbor gatekeeper 1 and 2	Enter the IP address(es), or hostname(s) (or <host>:<port number> to specify a port other than the default of 1719 on the neighboring gatekeeper), of the neighboring gatekeeper(s).	These are the gatekeepers to which the built-in gatekeeper will send an LRQ if it has received an ARQ to resolve an ID which it does not

		currently have registered. The built-in gatekeeper will then use the information received from the neighbor(s) to reply to the original request.
Accept LRQs	Configures the built-in gatekeeper to reply to LRQs from other gatekeepers.	These requests can come from any gatekeeper which has the ISDN Gateway's built-in gatekeeper configured as one of its neighbors.
Forward LRQs for unknown IDs	Configures the built-in gatekeeper to send (or not to send) LRQs regarding unknown IDs to its neighbor(s). Choose from the options: ▶ *Disabled*: The ISDN Gateway will only respond to LRQs about IDs registered with itself. It will not forward LRQs about IDs that are not registered with itself to neighboring gatekeepers. ▶ *Enabled, using local return address*: The ISDN Gateway will put, in the LRQ, its own address as the return address for the LCF. ▶ *Enabled, using received return address*: The ISDN Gateway will put, in the LRQ, the address of the gatekeeper that originated the request as the return address for the LCF. Use this option only if you are configuring the ISDN Gateway to operate in an environment with a multiple-level gatekeeper hierarchy. For example, the 'received address' is required by the national gatekeepers connected to the Global Dialing Scheme (GDS).	Unless you have selected to *Accept LRQs*, you cannot configure the ISDN Gateway to forward any LRQs. Enabling *using received return address* can be a significant security risk. Only use this setting with proper cause.
Accept LCFs from non-neighbors	This setting enables the built-in gatekeeper to accept LCF message responses from any IP address.	This setting is for use in environments with a multiple-level gatekeeper hierarchy. For example, this feature is required by the national gatekeepers connected to the Global Dialing Scheme (GDS). Enabling this setting can be a significant security risk. Only use this setting with proper cause.

Gatekeeper status

The number of registered devices is shown in the format X / Y where Y is the number of registered devices that your built-in gatekeeper is licensed for. Equally, the total number of registered IDs is shown as Z / 1000, where 1000 is the maximum number of registrations allowed over all registered devices.

Below these summary figures is a table showing individual registrations. Registrations can be viewed by registered ID (the "ID view") or by device (the "Registration view"), giving complete and easily searchable lists. Switch between the views by clicking on the appropriate button.

The Registration view shows the summary per device (also known as the registrant), while the ID view shows individual registrations. This means that registrations from the same device are not necessarily listed together in the ID view but the view can be sorted by Registrant or Index to help you identify IDs belonging to the same registrant.

ID view

Field	Field description	Usage tips
ID	The ID which the registrant has registered with the gatekeeper.	IDs can be numbers, H.323 IDs or prefixes.
Type	The type of registration.	One of: E.164 (digits), H.323 ID or Prefix.
Index	This registrations index within the total number of registrations that this registrant has made with the gatekeeper.	In the format X / Y where Y is the number of registrations that this registrant has made with the built-in gatekeeper, and X is this particular registration's position within the total. Therefore, if a device registered 3 IDs with the gatekeeper and this was the second registration to be made, the Index would be 2 / 3.
Registrant	The IP address of the device that this registration was made from.	If the remote device has indicated via the RAI (Resource Availability Indication) mechanism that it is close to its resource limit, the Registrant will be labeled as "almost out of resources".

Registration view

This view shows a one-line summary for each device registered with the built-in gatekeeper.

To deregister one or more devices (and all registrations for these devices), select the check boxes for the appropriate entries and then click **Deregister selected**.

Field	Field description	Usage tips
Registrant	The IP address of the device.	If the remote device has indicated via the RAI (Resource Availability Indication) mechanism that it is close to its resource limit, the Registrant will be labeled as "almost out of resources".
H.323 ID	The registered H.323 ID of the device.	To help identify registering devices, if the registrant has registered a H.323 ID (which will typically be its device name) that H.323 ID is shown here. If the device has registered multiple H.323 IDs, only the first is displayed.
Registered IDs	The number of registrations that this device has made with the built-in gatekeeper.	Click **(view)** to display individual registrations for the selected device. (The format is the same as the ID view, but the table only includes entries for one device.)
Registration time	The time today or date and time of the last registration.	

Displaying the user list

The User list gives you a quick overview of all configured users on the Cisco TelePresence ISDN Gateway and provides a summary of some of their settings. To view the **User list** page, go to **Users**. Refer to the table below for assistance.

Field	Field description
User ID	The user name that the user needs to access the web interface of the ISDN Gateway. Although you can enter text in whichever character set you require, note that some browsers and FTP clients do not support Unicode characters. Click on a name for further details (see Updating a user).
Name	The full name of the user.
Privilege	Access privileges associated with this user. An *administrator* can change any ISDN Gateway configuration, and view all status information. A user with the *list only* privilege can only view basic details about active calls.

Deleting users

To delete a user, select the user you want to delete and click **Delete selected users**. You cannot delete the admin and guest users.

Adding and updating users

You can add users to and update users on the Cisco TelePresence ISDN Gateway. Although most information is identical for both tasks, some fields differ.

Adding a user

To add a user:

1. Go to the **Users** page**.**
2. Click **Add user**.
3. Complete the fields referring to the table below to determine the most appropriate settings for the user.
4. After entering the settings, click **Add user**.

Updating a user

To update an existing user:

1. Go to **Users**.
2. Click a user name.
3. Edit the fields as required referring to the table below to determine the most appropriate settings for the user.
4. After entering the settings, click **Update user settings**.

Field	Field description	Usage tips
User ID	Identifies the log-in name that the user will use to access the ISDN Gateway web browser.	Although you can enter text in whichever character set you require, note that some browsers and FTP clients do not support Unicode characters. The following user ids are reserved and cannot be added: ▸ admin ▸ guest ▸ invalid ▸ system ▸ unknown
Password	The required password, if any.	Although you can enter text in whichever character set you require, note that some browsers and FTP clients do not support Unicode characters.

		In advanced security mode (configured on the **Settings > Security** page), passwords must have: ▶ at least fifteen characters ▶ at least two uppercase alphabetic characters ▶ at least two lowercase alphabetic characters ▶ at least two numeric characters ▶ at least two non-alphanumeric (special) characters ▶ not more than two consecutive repeating characters. That is, two repeating characters are allowed, three are not In advanced security mode, a password must be different from the previous ten used with that account. Also, a password will expire if it is not changed within 60 days. If the ISDN Gateway is not using advanced security mode, any password can be used. Note that passwords are stored in the configuration.xml file as plain text unless the ISDN Gateway is configured (or has ever been configured) to use advanced security mode. For more information, refer to Configuring security settings. Note that this field is only active when adding a new user. If you are updating an existing user and want to change that user's password, click **Change password** control instead.
Re-enter password	Verifies the required password.	
Disable user account	Select to disable this account.	This can be useful if you want to keep an account's details, but do not want anyone to be able to use it at the moment. You cannot disable the system-created admin account. The system-created guest account is disabled by default. If you enable it, the ISDN Gateway will create a security warning. In advanced account security mode, a non-admin account will expire after 30 days of inactivity; that is, the ISDN Gateway will disable it. To re-enable a disabled account, clear this

		option. For more information about advanced security mode, refer to Configuring security settings.
Lock password	Prevents user from changing password.	This is useful where you want multiple users to be able to use the same user ID. The system-created guest account has *Lock password* enabled by default.
Force user to change password on next login	Select this option to force a user to change their password. Next time this user attempts to log in to the ISDN Gateway, a change password prompt will appear.	This option is enabled by default for a newly created account. It is a good idea for new users to set their own secure passwords. This option is not available for accounts where *Lock password* is selected. When the user changes his password, the ISDN Gateway clears this check box automatically.
Privilege level	The access privileges to be granted to this user.	An administrator can change any ISDN Gateway configuration, and view all status information; a user with the list only privilege can only view basic details about active calls. The system-created guest account is fixed with privilege level of *list only*. All users can view the online help documentation.

Updating your user profile

You can make some changes to your user profile. To do this, go to **User profile**. Refer to the table below for tips.

Field	Field description	More information
Current password	Type your current password.	
Password	Type your new password.	In advanced security mode, passwords must have: ▶ at least fifteen characters ▶ at least two uppercase alphabetic characters ▶ at least two lowercase alphabetic characters ▶ at least two numeric characters ▶ at least two non-alphanumeric (special) characters ▶ not more than two consecutive repeating characters. That is, two repeating characters are allowed, three are not In advanced security mode, a new password must be different to the previous 10 passwords that have been used with an account.
Re-enter password	Verify your new password.	

Changing your password

In advanced security mode, passwords must have:

- at least fifteen characters
- at least two uppercase alphabetic characters
- at least two lowercase alphabetic characters
- at least two numeric characters
- at least two non-alphanumeric (special) characters
- not more than two consecutive repeating characters. That is, two repeating characters are allowed, three are not

In advanced account security mode, a new password must be different to the previous 10 passwords that have been used with an account.

In advanced account security mode, if a user logs in with a correct but expired password the Cisco TelePresence ISDN Gateway asks that user to change the password. If the user chooses not to change it, that user is allowed two more login attempts to change the password before the account gets disabled.

In advanced account security mode, users other than administrator users are not allowed to change their password more than once in a 24 hour period.

If the ISDN Gateway is not in advanced account security mode, there are no criteria for password selection.

If the ISDN Gateway is in advanced account security mode, the above criteria for passwords are displayed on the **Change password** page.

Configuring network settings

To configure the network settings on the Cisco TelePresence ISDN Gateway and check the network status, go to **Network > Port A** or **Network > Port B**.

The ISDN Gateway has two Ethernet interfaces, *Port A* and *Port B*. The configuration pages for the two interfaces look and behave similarly, and so are described together. Differences will be noted as appropriate.

Port A and Port B can be configured to be allocated their IP address by DHCP (IPv4) or SLAAC/DHCPv6 (IPv6). Connect Port A to your local network and connect Port B to a second subnet or the internet depending on your application of the ISDN Gateway.

In this section:

IP configuration settings

These settings determine the IP configuration for the appropriate Ethernet port of the ISDN Gateway. When you have finished, click **Update IP configuration** and then reboot the ISDN Gateway.

Field	Field description	Usage tips
IPv4 configuration		
IP configuration	Specifies whether the port should be configured manually or automatically. If set to *Automatic via DHCP* the ISDN Gateway obtains its own IP address for this port automatically via DHCP (Dynamic Host Configuration Protocol). If set to *Manual* the ISDN Gateway will use the values that you specify in the Manual configuration fields below.	
Manual configuration		
IP address	The dot-separated IPv4 address for this port, for example 192.168.4.45.	You only need to specify this option if you have chosen *Manual* IP configuration, as described above. If **IP configuration** is set to *Automatic by DHCP* this setting will be ignored.
Subnet mask	The subnet mask required for the IP address you wish to use, for example	

	255.255.255.0	
Default gateway	The IP address of the default gateway on this subnet, for example 192.168.4.1	
IPv6 configuration		
IP configuration	Specifies whether the port should be configured manually or automatically. If set to *Automatic via SLAAC/DHCPv6* the ISDN Gateway obtains an IP address for the port automatically. The protocol used will be SLAAC, Stateful DHCPv6, or Stateless DHCPv6 as indicated by the ICMPv6 Router Advertisement (RA) messages (for details see Automatic IPv6 address preferences below). If set to *Manual* the ISDN Gateway will use the values that you specify in the Manual configuration fields below.	
Manual configuration		
IPv6 address	The hexadecimal colon-separated global IPv6 address for this port. For example [2001:DB8::1]	Only specify this option if IP configuration is set to *Manual*. If **IP configuration** is set to *Automatic via SLAAC/DHCPv6* this setting is ignored. When you enter an IPv6 address anywhere in the user interface, the address must be enclosed in square brackets [ ].
Prefix length	The decimal prefix length value for the global IPv6 address for this port.	
Default gateway	Optionally, specifies the IPv6 address of the default gateway on this subnet.	The address can be global or link-local.

IP status

Use the IP Status fields to verify the current IP settings for the appropriate Ethernet port of the ISDN Gateway, which were obtained using DHCP or configured manually (see IP configuration settings) including:

- DHCP
- IP address
- Subnet mask (IPv4)
- Default gateway
- Link-local address (IPv6)

Ethernet configuration

These settings determine the Ethernet settings for the appropriate port of the ISDN Gateway. Refer to the table for assistance with these settings. When you have finished, click **Update Ethernet configuration**.

Field	Field description	Usage tips
Ethernet settings	Specify whether you want this Ethernet port to automatically negotiate its Ethernet settings with the device it is connected to, or if it should use the values that you specify in the Manual configuration fields below.	It is important that your Ethernet settings match those of the device to which this port is connected. For example, both devices must be configured to use automatic negotiation, or both configured with fixed and matching speed and duplex settings (see below).
Manual configuration		
Speed	Identifies the connection speed: *10 Mbit/s* or *100 Mbit/s*. Use automatic negotiation if a connection speed of *1000 Mbit/s* is required.	The connection speed must match that of the device to which this port is connected. You only need to select this option if you have chosen *manual* Ethernet settings, as described above.
Duplex	Identifies the connection duplex mode: ▶ **Full duplex** Both devices can send data to each other at the same time ▶ **Half duplex** Only one device can send to the other at a time	The duplex setting must match that of the device to which this port is connected. You only need to select this option if you have chosen *manual* Ethernet settings, as described above.

Ethernet status

Field	Field description	Usage tips
Link status	Indicates whether this Ethernet port is connected to or disconnected from the network.	
Speed	The speed (*10*/*100*/*1000 Mbit/s*) of the network connection to the ISDN Gateway on this port.	This value is negotiated with the device to which this port is connected or based on your Manual configuration selected above.
Duplex	The duplex mode (*full duplex* or *half duplex*) of the network connection to this port.	This value is negotiated with the device to which this port is connected or based on your Manual

		configuration selected above.
MAC address	The fixed hardware MAC (Media Access Control) address of this port.	This value cannot be changed and is for information only.
Packets sent	Displays a count of the total number of packets sent from this port by the ISDN Gateway. This includes all TCP and UDP traffic.	When troubleshooting connectivity issues, this information can help you confirm that the ISDN Gateway is transmitting packets into the network.
Packets received	Displays a count of the total number of packets received by this port of the ISDN Gateway. This includes all TCP and UDP traffic.	When troubleshooting connectivity issues, this information can help you confirm that the ISDN Gateway is receiving packets from the network.
Statistics	The fields display further statistics for this port. ▶ Multicast packets sent ▶ Multicast packets received ▶ Total bytes sent ▶ Total bytes received ▶ Receive queue drops ▶ Collisions ▶ Transmit errors ▶ Receive errors	Use these fields for advanced network diagnostics, such as resolution of problems with Ethernet link speed and duplex negotiation.

Automatic IPv6 address preferences

This table details the address assignment preferences that are applied for IPv6 addressing when port configuration is set to *Automatic*.

*RA flags			Preferred address
a	o	m	
0	0	0	NA
1	0	0	SLAAC
0	1	0	NA
1	1	0	Stateless DHCPv6
0	0	1	Stateful DHCPv6
1	0	1	Stateful DHCPv6
0	1	1	Stateful DHCPv6
1	1	1	Stateful DHCPv6

*a: ICMPv6 prefix information, auto flag
*o: ICMPv6, other flag
*m, ICMPv6, managed flag

DNS settings

This section describes how to configure and view DNS settings for the Cisco TelePresence ISDN Gateway.

Configuring DNS settings

To configure DNS settings on the ISDN Gateway, go to **Network > DNS**. These settings determine the DNS configuration for the ISDN Gateway.

Click **Update DNS configuration** after making any changes.

Field	Field description	Usage tips
DNS configuration		
Name server (DNS) preference	Select a DNS server preference from the list or select *Manual* to specify DNS settings manually.	The DNS settings of the preferred DNS information source will only be applied if the corresponding interface address configuration method is used. For example, to apply IPv6 DNS information for Port A requires the IPv6 address configuration for Port A to be set to *Automatic*.
Host name	Specifies a name for the ISDN Gateway.	Depending on your network configuration, you may be able to use this host name to communicate with the ISDN Gateway, without needing to know its IP address.
Name server	The IP address of the name server.	
Secondary name server	Identifies an optional second name server.	The secondary DNS server is only used if the first is unavailable. If the first server returns that it does not know an address, the secondary DNS server will not be queried.
Domain name (DNS suffix)	Specifies an optional suffix to add when performing DNS lookups.	This option can allow you to use non-fully qualified host names when referring to a device by host name instead of IP address. For example, if the domain name is set to *cisco.com*, then a request to the name server to look up the IP address of host *endpoint* will actually lookup *endpoint.cisco.com*.

Viewing DNS status

Use the DNS status fields to verify the current DNS settings for the ISDN Gateway, including:

- Host name
- Name server
- Secondary name server
- Domain name (DNS suffix)

Configuring IP routes settings

You need to set up one or more routing settings to control how IP traffic flows in and out of the Cisco TelePresence ISDN Gateway. It is important that these settings are configured correctly, or you may be unable to make calls or access the web interface.

To configure the route settings, go to **Network > Routes**.

In this section:

Port preferences

If both Ethernet ports are enabled, it is necessary to specify which port is used in certain special circumstances. Make the appropriate selections described below. Click **Apply changes**.

Field	Field description	Usage tips
IPv4 gateway preference	The IPv4 address to which the ISDN Gateway will send packets in the absence of more specific routing (see IP routes configuration). Therefore, it only makes sense to have precisely one default gateway, even though *different* default gateways may have been configured for Ports A and B. Use this option to decide which port's default gateway configuration to use as the ISDN Gateway's default gateway.	If Ethernet Port B is disabled, you cannot specify that port as the default gateway preference. Selecting Port B as default gateway preference then disabling Port B will cause the preference to revert to Port A.
IPv6 gateway preference	The IPv6 address to which the ISDN Gateway will send packets in the absence of more specific routing (see IP routes configuration). As in the IPv4 case, it only makes sense to have precisely one default gateway, even though *different* default gateways may have been configured for Ports A and B. Use this option to decide which port's default gateway configuration to use as the ISDN Gateway's default gateway.	If Ethernet Port B is disabled, you cannot specify that port as the default gateway preference. Selecting Port B as default gateway preference then disabling Port B will cause the preference to revert to Port A.

IP routes configuration

In this section you can control how IP packets should be directed out of the ISDN Gateway. You should only change this configuration if you have a good understanding of the topology of the network(s) to which the ISDN Gateway is connected.

Configuration of routes is divided into two sections: addition of new routes, and the display and removal of existing routes.

Adding a new IP route

To add a new route, enter the details using the table below for reference. Click **Add IP route** to make the addition. If the route already exists, or aliases (overlaps) an existing route, you will be prompted to correct the problem and try again.

Field	Field description	Usage tips
IP address / mask length	Use these fields to define the type of IP addresses to which this route applies. For IPv4 addressing, the IP address pattern must be in the dot-separated IPv4 format, while the mask length is chosen in the **IP address / mask length** field. The mask field specifies how many bits of the address are fixed; unfixed bits must be set to zero in the address specified. For IPv6 addressing, the IP address pattern must be in standard CIDR notation (address/prefix length). IPv6 addresses must be enclosed in square brackets [ ].	To route all IPv4 addresses in the range 192.168.4.128 to 192.168.4.255 for example, specify the IP address as 192.168.4.128 and the mask length as 25, to indicate that all but the last seven bits address are fixed.
Route	Use this field to control how packets destined for addresses matching the specified pattern are routed.	You may select *Port A*, *Port B* or *Gateway*. If *Gateway* is selected, specify the IP address of the gateway to which you want packets to be directed. Selecting *Port A* results in matching packets being routed to Port A's default gateway (see Configuring network settings). Selecting *Port B* will cause matching packets to be routed to Port B's default gateway. If Ethernet Port B is disabled, the option to route packets to Port B will be disabled.

Viewing and deleting existing IP routes

Configured routes are listed below the Add IP route controls. For each route, the following details are shown:

- The IP address pattern and mask
- Where matching packets will be routed, with the possibilities being:
  - Port A - meaning the default gateway configured for Port A
  - Port B - meaning the default gateway configured for Port B
  - **<**IP address**>** - a specific address has been chosen
- Whether the route has been configured automatically as a consequence of other settings, or added by the user as described above.

The *default* route is configured automatically in correspondence with the *Default gateway preference* field (see Port preferences) and cannot be deleted. Any packets not covered by manually configured routes will be routed according to this route.

Manually configured routes may be deleted by selecting the appropriate checkbox and clicking **Delete selected**.

Routes behavior with disabled ports

If the default gateway preference is set to Port B and that port is disabled, the default route will be updated automatically to route packets not covered by any manually configured route via Port A.

If a manually configured route specifies Port B and that port is disabled, packets matching that route **will not** be automatically routed via Port A, but discarded. You should take care to avoid this situation.

Current IP status

This table shows the current default gateway and name server(s) for Ethernet Ports A and B. No fields can be changed, and are provided for reference when configuring the other parameters described in the sections above.

Configuring IP services

To configure IP services, go to **Network > Services**.

Use this page to control the type of services that may be accessed via Ethernet Ports A and B. You might want to configure the services that are available on each port if you want to use one port for management and the other for calls, for example, by only allowing web access on Port B. The Cisco TelePresence ISDN Gateway does not allow IP to IP calls (calls between Ethernet ports). Refer to the table below for more details.

To prevent accidental lock-outs the system does not allow you to disable the service that is currently being used to administer the ISDN Gateway. For example, if you are configuring the gateway over http and coming in on Port A, then the option to change the http service for Port A will be unavailable in the interface.

In addition to controlling the Ethernet interfaces over which a service operates, this page also allows an administrator to specify the port number on which that service is provided. If the port number for a service is changed, it is necessary to ensure that the new value chosen does not clash with the port number used by any of the other services; it is not, however, normally necessary to use anything other than the pre-configured default values.

The settings on this page apply to both IPv4 and IPv6 addressing. The page displays the IPv4 and/or IPv6 values per port, depending on whether IPv4 and/or IPv6 are enabled for the port. When specifying settings use the appropriate column for the required addressing scheme.

Note that by default SNMP Traps are sent to port UDP port 162 (on the destination network management station); this is configurable. For more information, refer to Configuring SNMP settings.

To reset all values back to their factory default settings, click **Reset to default** and then click **Apply changes**.

Field	Field description	Usage tips
TCP service		
Web	Enable/disable web access on the appropriate port.	Web access is required to view and change the ISDN Gateway web pages and read online help files. If you disable web access on Port A you will need to use the serial console interface to re-enable it. If you require advanced security for the ISDN Gateway, disable web access. If a port is disabled, this option will be unavailable.
Secure web	Enable/disable secure (HTTPS) web access on the appropriate port.	This field is only visible if the ISDN Gateway has the *Secure management (HTTPS)* feature key or an *Encryption* feature key installed. For more information about installing feature keys, refer to Upgrading the firmware. By default, the ISDN Gateway has its own SSL

		certificate and private key. However, you can upload a new private key and certificates if required. For more information about SSL certificates, refer to Configuring SSL certificates. If a port is disabled, this option will be unavailable.
Incoming H.323	Enable/disable the ability to receive incoming calls to the ISDN Gateway using H.323 or change the port that is used for this service.	Disabling this option will not prevent outgoing calls to H.323 devices being made by the ISDN Gateway. If a port is disabled, this option will be unavailable.
FTP	Enable/disable FTP access on the specified interface or change the port that is used for this service.	FTP can be used to upload and download ISDN Gateway configuration. You should consider disabling FTP access on any port that is outside your organization's firewall. If you require advanced security for the ISDN Gateway, disable FTP access. If a port is disabled, this option will be unavailable.
UDP service		
SNMP	Enable/disable the receiving of the SNMP protocol on this port or change the port that is used for this service.	If a port is disabled, this option will be unavailable. You must use the same port number for both Port A and Port B. The number is automatically refreshed for Port B. Note that by default SNMP Traps are sent to port UDP port 162 (on the destination network management station); this is configurable. For more information, refer to Configuring SNMP settings. If you require advanced security for the ISDN Gateway, disable the SNMP service.
H.323 gatekeeper	Enable/disable access to the built-in H.323 gatekeeper or change the port that is used for the built-in H.323 gatekeeper.	If a port is disabled, this option will be unavailable. You must use the same port number for both Port A and Port B. The number is automatically refreshed for Port B.

Configuring SNMP settings

To configure monitoring using SNMP, go to **Network > SNMP**.

The Cisco TelePresence ISDN Gateway sends out an SNMP trap when the device is shut down or started up. The SMNP page allows you to set various parameters; when you are satisfied with the settings, click **Update SNMP settings**.

Note that:

- The 'system up time' that appears in the trap is the time since SNMP was initialized on the ISDN Gateway (and therefore will differ from the *Up time* reported by the ISDN Gateway on the **Status** > **General** page).
- The SNMP MIBs are read-only.

System information

Field	Field description	Usage tips
Name	Identifies the ISDN Gateway in the SNMP system MIB.	Usually you would give every device a unique name. The default setting is: Cisco ISDN GW
Location	The location that appears in the system MIB.	An optional field. It is useful where you have more than one ISDN Gateway to identify where the unit is located. The default setting is: *Unknown*
Contact	The contact details that appear in the system MIB.	An optional field. The default setting is: *Unknown* Add the administrator's email address or name to identify who to contact when there is a problem with the device. If SNMP is enabled for a port on the public network, take care with the details you provide here.
Description	A description that appears in the system MIB.	An optional field, by default this will indicate the model number of the unit. Can be used to provide more information on the ISDN Gateway.

Configured trap receivers

Field	Field description	Usage tips
Enable traps	Select this check box to enable the ISDN Gateway to send traps.	If you do not check this box, no traps will be sent.
Enable authentication failure trap	Select this check box to enable authentication failure traps.	You cannot select this check box unless you have selected to *Enable traps* above. Authentication failure traps are generated and sent to the trap receivers when someone tries to read or write a MIB value with an incorrect community string.
Trap receiver addresses 1 to 4	Enter the IP address or hostname for up to four devices that will receive both the general and the authentication failure traps.	The traps that are sent by the ISDN Gateway are all SNMP v1 traps. You can configure trap receivers or you can view the MIB using a MIB browser. You can set the UDP port number for the trap in the format <IP address>: <port number>. By default the UDP port number is 162.

Access control

Field	Field description	Usage tips
RO community	Community string/password that gives read-only access to all trap information.	Note that SNMP community strings are not secure. They are sent in plain text across the network. It is advisable to change the community strings before enabling SNMP as the defaults are well known.
RW community	Community string/password that gives read/write access to all trap information.	
Trap community	Community string/password that is sent with all traps.	Some trap receivers can filter on trap community.

Configuring QoS settings

To configure Quality of Service (QoS) on the ISDN Gateway for audio and video, go to **Network > QoS**.

QoS is a term that refers to a network's ability to customize the treatment of specific classes of data. For example, QoS can be used to prioritize audio transmissions and video transmissions over HTTP traffic. These settings affect all audio and video packets to H.323 endpoints. All other packets are sent with a QoS of 0.

The ISDN Gateway allows you to set a six-bit value for Type of Service (IPv4) or Traffic Class (IPv6), which can be interpreted by networks as either Type of Service (ToS) or Differentiated Services (DiffServ).

Note: Do not alter the QoS settings unless you need to do so.

Further information about QoS, including values for ToS and DiffServ, can be found in the following RFCs, available on the Internet Engineering Task Force web site www.ietf.org:

- RFC 791
- RFC 2474
- RFC 2597
- RFC 3246

In this section:

About QoS configuration settings

The table below describes the settings on the **Network > QoS** page.

Field	Field description	Usage tips
IPv4 configuration		
Audio	Six bit binary field for prioritizing audio data packets on the network.	Do not alter these settings unless you need to.
Video	Six bit binary field for prioritizing video data packets on the network.	
IPv6 configuration		

Audio	Six bit binary field for prioritizing audio data packets on the network.	Do not alter these settings unless you need to.
Video	Six bit binary field for prioritizing video data packets on the network.	

ToS configuration

ToS configuration represents a tradeoff between the abstract parameters of precedence, delay, throughput, and reliability.

ToS uses six out of a possible eight bits. The ISDN Gateway allows you to set bits 0 to 5, and will place zeros for bits 6 and 7.

- Bits 0-2 set IP precedence (the priority of the packet).
- Bit 3 sets delay: 0 = normal delay, 1 = low delay.
- Bit 4 sets throughput: 0 = normal throughput, 1 = high throughput.
- Bit 5 sets reliability: 0 = normal reliability, 1 = high reliability.
- Bits 6-7 are reserved for future use and cannot be set using the ISDN Gateway interface.

You need to create a balance by assigning priority to audio and video packets whilst not causing undue delay to other packets on the network. For example, do not set every value to 1.

DiffServ configuration

DiffServ uses six out of a possible eight bits to set a codepoint. (There are 64 possible codepoints.) The ISDN Gateway allows you to set bits 0 to 5, and will place zeros for bits 6 and 7. The codepoint is interpreted by DiffServ nodes to determine how the packet is treated.

Default settings

The default settings for QoS are:

- *Audio 101110:*
  - For ToS, this means IP precedence is set to 5 giving relatively high priority. Delay is set to low, throughput is set to high, and reliability is set to normal.
  - For Diff Serv, this means expedited forwarding.
- *Video 100010:*
  - For ToS, this means IP precedence is set to 4 giving quite high priority (but not quite as high as the audio precedence). Delay is set to normal, throughput is set to high, and reliability is set to normal.
  - For DiffServ, this means assured forwarding (codepoint 41).

To return the settings to the default settings, click **Reset to default**.

Network connectivity testing

The Network connectivity page can be used for troubleshooting issues that arise because of problems in the network between the Cisco TelePresence ISDN Gateway and a remote video conferencing device being called (or a device from which a user is attempting to call the ISDN Gateway).

The Network connectivity page enables you to attempt to 'ping' another device from the ISDN Gateway's web interface and perform a 'traceroute' of the network path to that device. The results show whether or not you have network connectivity between the ISDN Gateway and another device. You can see from which port the ISDN Gateway will route to that address. For a hostname, the IP address to which it has been resolved will be displayed.

To test connectivity with a remote device, go to **Network > Connectivity**. In the text box, enter the IP address or hostname of the device to which you want to test connectivity and click **Test connectivity**.

For each successful 'ping', the time taken for the ICMP echo packet to reach the host and for the reply packet to return to the ISDN Gateway is displayed in milliseconds (the round trip time). The TTL (Time To Live) value on the echo reply is also displayed.

For each intermediate host (typically routers) on the route between the ISDN Gateway and the remote device, the host's IP address and the time taken to receive a response from that host is shown. Not all devices will respond to the messages sent by the ISDN Gateway to analyse the route; routing entries for non-responding devices is shown as <unknown>. Some devices are known to send invalid ICMP response packets (e.g. with invalid ICMP checksums); these responses are not recognized by the ISDN Gateway and therefore these hosts' entries are also shown as <unknown>.

Notes:

The ping message is sent from the ISDN Gateway to the IP address of the endpoint that you enter. Therefore, if the ISDN Gateway has an IP route to the given IP address, regardless of whether that route lies out of port A or port B, the ping will be successful. This feature allows the ISDN Gateway's IP routing configuration to be tested, and it has no security implications.

If you are unable to ping the device then check your network configuration especially any firewalls using NAT.

Configuring general ISDN settings

These settings are global settings, which affect the configuration of the Cisco TelePresence ISDN Gateway with regard to ISDN network type and options, and allowed call features. To access these settings, go to **Settings > ISDN**.

Note that some ISDN configuration must be done on a port-by-port basis; see Configuring ISDN ports settings.

Refer to the sections below for assistance configuring the general ISDN settings. After making any changes, click **Apply changes**.

Basic settings

Field	Field description	Usage tips
ISDN interface type	The ISDN network type to which the ISDN Gateway is connected. Choose from *E1*, *T1 (USA and Canada)*, and *T1 (Japan)* as appropriate.	E1 is usually used in the UK and mainland Europe. T1 is usually used in the US and Canada. T1 (Japan) is usually used in Japan. Refer to your ISDN network provider if you are unsure of which interface type to select. The ISDN Gateway may have to be restarted for changes of this setting to take effect (see Shutting down the ISDN Gateway).
ISDN switch type	If the ISDN interface type is T1 or J1, select the *ISDN switch type.* Choose from: ▶ *National ISDN:* default switch type for use with the ISDN Gateway ▶ *4ESS*: a custom switching protocol designed by AT&T ▶ *DMS-100*: a custom protocol used with Nortel network infrastructure with T1 networks	This field only applies to ISDN Gateway models that end with a 1, for example the 3201 or 8321. This setting has no effect when the ISDN Gateway is in leased line mode. Select the **ISDN switch type** appropriate for the ISDN switch to which the ISDN Gateway is connected.
Leased line mode	Select this option to configure the ISDN Gateway to use leased line mode. Only use this mode if your ISDN Gateway is connected to a permanent leased line connection.	When this setting is enabled, **all** PRIs will be set to use leased line. If you select or deselect *Leased line mode*, you must restart the ISDN Gateway (see Shutting down the ISDN Gateway).
Compatibility	Select the appropriate settings.	▶ *Send "sending complete":* If enabled (the default), the ISDN Gateway will send a message to the network when it has finished sending the dial string. Some networks require this but others do not. Leave this enabled, but if you

		find that outbound calls fail (and inbound calls succeed), then try disabling this setting ▶ Select the *Legacy capabilities* option if you experience difficulties connecting your older endpoints to the ISDN GW. When enabled, the ISDN Gateway will detect when one of those endpoints is being called and send a reduced capability set
Send calling number to ISDN network	Select the appropriate setting. Some networks do not allow you to set this and the call will fail if you; in others, the call will only work if the caller's number is forwarded and the DN is set exactly right; and in most networks, the setting is completely ignored. Experiment and see which setting works best.	▶ Select *Always* if you want all IP to ISDN calls to forward the caller's number where available ▶ Select *Only if numeric* to forward only numeric caller numbers ▶ Select *Never* if IP to ISDN calls should never forward the caller's number
Max incoming ISDN call rate	Select the maximum bandwidth at which the ISDN side of ISDN to IP calls can be established. The options offered show the bandwidth in terms of Kbps, and the corresponding number of ISDN B-channels required. This setting also enables you to use the ISDN Gateway as a PSTN to voice-over-IP gateway (that is, as a voice-only gateway, rather than a video-conferencing gateway); in this case, set the call rate to *Telephone*. Voice calls from the PSTN can then be placed to IP telephones.	The value entered is the maximum bandwidth for an incoming ISDN call. The dial plan cannot override this value with a higher maximum bandwidth. However, by using the dial plan you can impose a lower bandwidth for particular calls. Also, note that the calling ISDN endpoint may elect to establish a call at a lower bandwidth. If you have selected *Telephone*, then the ISDN Gateway will forward ISDN calls as audio-only IP calls (see Using the ISDN Gateway for voice-only calls).
Max outgoing ISDN call rate	Select the maximum bandwidth at which the ISDN side of IP to ISDN calls can be established. The options offered show the bandwidth in terms of Kbps, and the corresponding number of ISDN B-channels required. This setting also enables you to use the ISDN Gateway as a voice-over-IP to PSTN gateway (that is, as a voice-only gateway, rather than a video-conferencing gateway); in this case, set the call rate to *Telephone*. Voice calls from IP telephones can then be placed to regular PSTN telephones.	The value you enter here is the maximum bandwidth for an outgoing ISDN call. The dial plan cannot override this value with a higher maximum bandwidth. However, by using the dial plan you can impose a lower bandwidth for particular calls. Also, note that the calling ISDN endpoint may elect to establish a call at a lower bandwidth. If you have selected *Telephone*, then the ISDN Gateway will forward IP calls as audio-only ISDN calls (see Using the ISDN Gateway for voice-only calls).
Maximum call duration	Limits the length of all calls unless you select *no time limit*.	You may wish to impose a maximum call duration to limit ISDN calling costs.

Allow parallel dialing	Parallel dialing allows all ISDN calls to be bonded to be dialed simultaneously.	Enable parallel dialing if your ISDN endpoints support it. Since parallel dialing is not supported by all equipment, disabling parallel dialing may improve interoperability with legacy endpoints; however, call setup times for outgoing ISDN calls may increase slightly. This option does not affect incoming ISDN calls.
Port search order	Whether free B-channels will be selected starting with the low-numbered port and working towards the high-numbered port, or the other way around. When making outgoing ISDN calls, this setting is used to select which port to place the call on; when receiving incoming ISDN calls, it is used to select which port number to advertise to the ISDN endpoint.	This order is applied to the ports selected in the dial plan.
Load balancing	Use this option to forward calls to another gateway if all of this ISDN Gateway's channels are full or unavailable. Your ISDN network must support this functionality. Select *Active* on its own or in combination with *Use higher numbered channels only*.	When *Active* is selected, the ISDN Gateway rejects incoming ISDN calls if not enough channels are available, and sends a 'Redirection to new destination' message to the ISDN network. It is up to your ISDN network provider to redirect the call to another gateway. To work out the number of free B-channels, if *Use higher numbered channels only* is selected, the gateway considers only higher-numbered channels than the channel used by the initial call. If you are unsure whether you need to enable this option, refer to your ISDN network provider.
Outgoing ISDN calls	Select from the drop down list.	When *Establish layer 2* is selected, only layer 1 needs to be up before placing a call. The ISDN Gateway will attempt to bring up layer 2. If *Require layer 2* is selected, then layer 2 must be up before calls are allowed. (This was the default behavior in older software versions.)

ISDN advanced settings

Field	Field description	Usage tips
Specify national/international type of number	Some ISDN configurations, including certain 4ESS switches, need the ISDN Type of Number (TON) to be explicitly set to National	If this option is selected, then an outgoing ISDN call has a National TON or International TON depending on whether the beginning of the dialed number matches the value

	or International. In such cases select this option to set the TON for outgoing ISDN calls to National or International as required. For International you must also specify the **International prefix setting**.	specified in the **International prefix** field. If there is a match the call is International; otherwise the call is National. For example, assume that **Specify national/international type of number** is selected and **International prefix** is set to 011. If a user then calls 01144555333 the number will have an International TON and is sent as 44555333 (the international prefix is stripped from the outgoing call). If the user had instead called 11144555333 then the number would have a National TON and be sent as 11144555333. If no value is specified in the **International prefix** field, then no called number will match the international prefix and all calls will have a National TON.
International prefix	This field only applies if you selected **Specify national/international type of number**. Use this field to specify the dialing code prefix for international numbers dialed from your network (for example, 00 from networks in Portugal or 011 from the United States).	For aggregation calls, if one sub-call has the International prefix present then all sub-calls must have the prefix.
E1 CRC-4 enabled	With an ISDN interface type of E1 selected in the Basic settings, this option selects whether ISDN signalling should make use of the CRC-4 mechanism.	Most E1 ISDN networks require CRC-4 to be enabled, although some (in particular, some French networks) require it to be disabled. Refer to your ISDN network provider if you are unsure whether to enable or disable CRC-4. The ISDN Gateway may have to be restarted for changes of this setting to take effect (see Shutting down the ISDN Gateway).
T1 ESF enabled	With an ISDN interface type of T1 selected, this option selects whether ISDN signalling should make use of the Extended Superframe Framing technique.	Most T1 ISDN networks require ESF to be enabled. Refer to your ISDN network provider if you are unsure whether to enable or disable ESF. The ISDN Gateway may have to be restarted for changes to this setting to take effect.
Send channel ID in Q.931	Do not change these settings unless advised to do so by Cisco	Not all settings apply to all networks. For example, the National bits are

Line length **Line impedance** **Line coding** **Transmit pulse shape** **National bits (Sa4..Sa8)**	customer support, or if you are an experienced ISDN administrator.	relevant only for E1 networks.
Video NSF **Telephone NSF**	These fields allow you to choose a value between 1 and 31, or to leave the Network Specific Facility disabled (which is the default behavior and the implied setting in previous releases of the ISDN Gateway). Do not change these settings unless advised to do so by Cisco customer support, or if you are an experienced ISDN administrator.	Setting a value adds a field to ISDN call setup messages which is required by some ISDN networks. The two fields allow for networks in which a different value is required for video and telephone calls.

ISDN codec settings

Field	Field description	Usage tips
Audio codecs allowed	Restricts the choice of audio codecs that endpoints calling through the ISDN Gateway may select. (You cannot disable the G.711 codec.)	IP and ISDN endpoints negotiate between themselves which audio codecs to use during a call. Use these options if you wish to restrict the choices available. Prohibiting audio codecs may prevent endpoints negotiating a compatible codec; use these options only if you experience a particular problem when using a certain codec with the ISDN Gateway. If the IP endpoint is a Cisco TelePresence MCU or IP VCR, consider disabling the codec on that device instead.
Video codecs allowed	Restricts the choice of video codecs that endpoints calling through the ISDN Gateway may select. (You cannot disable the H.261 codec.)	IP and ISDN endpoints negotiate between themselves which video codecs to use during a call. Use these options if you wish to restrict the choices available. Prohibiting video codecs may prevent endpoints negotiating a compatible codec; use these options only if you experience a particular problem when using a certain codec with the ISDN Gateway. If the IP endpoint is a Cisco TelePresence MCU or IP VCR, consider disabling the codec on that device instead. Note that *H.263* also encompasses *H.263+*.
Content video	Restricts the choice of content	IP and ISDN endpoints between

codecs allowed	codecs that endpoints calling through the ISDN Gateway may select. Content allows a separate presentation stream alongside the video stream.	themselves negotiate which content codecs to use during a call. Use these options if you wish to restrict the choices available. **Note:** The ISDN Gateway does not advertise content at bandwidths of 128kbps or lower. Cisco recommends a total call bandwidth of at least 384kbps for a video call with content. Prohibiting content codecs may prevent endpoints negotiating a compatible codec; use these options only if you experience a particular problem when using a certain codec with the ISDN Gateway. If the IP endpoint is a Cisco TelePresence MCU or IP VCR, consider disabling the codec on that device instead.

ISDN multipoint settings

Field	Field description	Usage tips
H.243 floor and chair control allowed	Enables or disables the passing through of chair and/or floor control requests.	The ISDN Gateway passes any floor/chair control requests received. It does not process them in any way.

Configuring ISDN ports settings

The options that are available to you when you are configuring ISDN ports depend on whether or not the Cisco TelePresence ISDN Gateway is in *leased line mode*. (Leased line mode is configured on the **Settings > ISDN** page.)

Select the help topic that you need:

- Configuring ISDN ports settings
- Configuring ISDN ports settings in leased line mode

Configuring ISDN ports settings (non-leased line mode)

These settings affect the per-port ISDN configuration of the ISDN Gateway. Use these settings to configure ISDN ports to the requirements of your ISDN network. To access these settings, go to **Settings > ISDN ports**.

Note that some ISDN configuration must be done on a blade-wide basis; see Configuring general ISDN settings.

You can configure multiple ports at once. After making changes, click **Apply changes to update the settings for the port(s)**.

Refer to the table below for assistance with configuring the ISDN ports settings.

Port settings

Field	Field description	Usage tips
Enabled	Whether this port may be used to make and receive ISDN calls.	
Overlap receiving number length	Specify the number of digits that a caller will dial before the ISDN Gateway will apply the dial plan and make the IP part of the call. When the ISDN Gateway has received that number of dialed digits, it will connect the call immediately. If you do not want to use overlap receiving, enter 0 to disable this feature.	Overlap receiving ensures that the ISDN Gateway waits for all dialed digits before connecting the call. To use overlap receiving, it must be supported by your ISDN infrastructure. When overlap receiving is enabled, the ISDN Gateway can collect a series of dialed digits sent from an endpoint before it starts the IP leg of the call. Overlap receiving is configured on an individual PRI port basis. Note that this setting is not available when the ISDN Gateway is operating in leased line mode.
Directory Number (DN)	The directory number of this ISDN port.	Enter the phone number of this port, as assigned by your ISDN network provider. In many applications, all ISDN ports will share a common directory number; this is referred to as the ports being part of a *hunt group*. Incoming

		calls may arrive at any one of the ports with a shared directory number. Note that when receiving an incoming ISDN call, the gateway advertises the directory numbers of the ports selected in the dial plan. If no directory number is specified, it assumes the directory number of the nearest lower-numbered port. If no ports have a specified directory number, the calling endpoint will be instructed to use the same number to place subsequent calls as it used to make the first call.
Prefix for national calling party numbers	The national prefix that the ISDN Gateway adds.	This setting adds a prefix to the calling party number information which the ISDN Gateway gets from an incoming ISDN call and then sends out over the IP part of the call. This calling party number can then be used by an IP participant to return a call to the ISDN participant. This feature should be used in conjunction with the overall dial plan mechanism.
Prefix for international calling party numbers	The international prefix that the ISDN Gateway adds.	This setting adds a prefix to the calling party number information which the ISDN Gateway gets from an incoming ISDN call and then sends out over the IP part of the call. This calling party number can then be used by an IP participant to return a call to the ISDN participant. This feature should be used in conjunction with the overall dial plan mechanism.
Low channel	The lowest numbered B-channel available.	An ISDN PRI comprises a number of B-channels. A complete PRI has 30 available B-channels when using E1, and 23 when using T1 or J1. Your ISDN network provider may offer a complete or *fractional* PRI (where a reduced number of B-channels are available). In either case, the low channel number is generally 1. Refer to your ISDN network provider if you are unsure of which value to use here.
High channel	The highest numbered B-channel available or *Max*.	An ISDN PRI comprises a number of B-channels. A complete PRI has 30 available B-channels when using E1, and 23 when using T1 or J1. Your ISDN network provider may offer a complete or *fractional* PRI (where a reduced number of B-channels are available).

		Use *Max* if you are unsure of which value to use here or refer to your ISDN network provider. Also use *Max* if you may switch between E1 and T1/J1 modes.
Channel search order	Select whether free B-channels should be selected starting with the low-numbered channel and working towards the high-numbered channel, or the other way around.	When making outgoing ISDN calls, the ISDN Gateway requests that the ISDN network makes the call using a particular set of B-channels; when receiving incoming ISDN calls, the ISDN network informs the ISDN Gateway which B-channels are in use. To minimize the risk of a new incoming call using the same B-channels as a new outgoing call starting at the same time, you should generally set the ISDN Gateway to search free channels in the reverse order to the ISDN network. Refer to your ISDN network provider if you are unsure of which value to use here.
Allow NFAS	Select to enable Non-Facility Associated Signaling (NFAS).	This field only applies to ISDN Gateway models ending with a 1, for example the 3201 or 8321. This setting is only visible when the ISDN Gateway is configured to use T1 as the **ISDN interface type** in **Settings > ISDN**. NFAS allows multiple PRIs (in T1 mode) to use a single D-channel. The NFAS settings on the ISDN Gateway must match the settings on the ISDN switch to which the ISDN Gateway is connected.
NFAS group ID	Select an ID for the NFAS group.	Allocate the same NFAS group ID to each port that will use the same D-channel. Ports with the same NFAS group ID are in the same NFAS group.
NFAS interface ID	Select an ID for the NFAS interface.	This field only applies to ISDN Gateway models ending with a 1, for example the 3201 or 8321. Within the NFAS group, each NFAS interface ID must be unique, must be between 0 and 31, and must be the same as that set on the switch to which the ISDN GW is connected.
D-channel type	Select the D-channel type.	Within the NFAS group, one port must have the D-channel type set to Primary (active) and the other ports must have D-channel type set to None. This must

		match the settings on the switch.

Configuring ISDN ports settings in leased line mode

These settings affect the per-port ISDN configuration of the Cisco TelePresence ISDN Gateway when it is leased line mode. Use these settings to enable the ports and to configure leased line groups. To access these settings, go to **Settings > ISDN ports**.

In leased line mode, there is no way to dynamically decide how many B-channels to use in a call (because that requires the D-channel); instead, both devices must be set up with the same "leased line groups". In this way, a number of B-channels are grouped together and are used simultaneously as a pipe for audio and video data.

Refer to the table below for information about the settings. After making changes, click **Apply changes** and then restart the ISDN Gateway for the changes to leased line groups to take effect.

Port settings

Field	Field description	Usage tips
Enabled	Whether this port may be used to make and receive ISDN calls.	
Leased line group	Indicates the number of the leased line group.	You can configure a maximum of five numbered leased line groups. Each group is a collection of contiguous B-channels for that port.
Start channel	Select the lowest numbered B-channel that will be in this leased line group.	The B-channels that you select must be in contiguous blocks and not span PRIs. The B-channels that you configure for this group on the ISDN Gateway must match exactly the groups configured on the leased line to which it is connected. For each PRI you can use B-channels 1-31 in E1 mode and 1-24 in T1 mode. However, on the MSE 8310 and 3200 series ISDN gateways this is further limited to channels 1-15 and 17-31 in E1 mode and channels 1-23 in T1 mode.
Number of channels	Select the number of B-channels that will be in this leased line group.	Setting this to 0 means that this leased line group is not used.

Configuring H.323 gatekeeper settings

You can configure the Cisco TelePresence ISDN Gateway to use a gatekeeper, which can make it easier for end-users to make calls using directory numbers rather than requiring them to know the IP address or host name of the ISDN Gateway. You can register the ISDN Gateway with an external gatekeeper or you can enable its own built-in gatekeeper.

To configure gatekeeper settings, go to **Settings > H.323**.

Gatekeeper settings

Refer to this table for assistance configuring the gatekeeper settings. After making any configuration changes, click **Apply Changes**.

Field	Field description	Usage tips
H.323 gatekeeper usage	Enables the ISDN Gateway to use an H.323 gatekeeper for registration of numeric identifiers for its conferences.	Choose from: ▶ *Disabled*: the gatekeeper is not consulted when determining where to direct a call. No gatekeeper registrations will be attempted (and existing registrations will be torn down), regardless of other gatekeeper settings. ▶ *Enabled*: the gatekeeper is consulted to see if it knows where to direct a call. The ISDN Gateway will attempt to make registrations with the gatekeeper, and the gatekeeper will be contacted for incoming and outgoing calls. If the gatekeeper does not respond, calls are still connected if possible. ▶ *Required*: the gatekeeper is consulted to determine where to direct a call. If that fails, the call will not be allowed.

H.323 gatekeeper address	The network address of the gatekeeper to which ISDN Gateway registrations should be made.	This can be specified either as a host name or as an IP address. This field will have no effect if *H.323 Gatekeeper usage* (see above) is set to *Disabled*. The gatekeeper can be either the built-in gatekeeper enabled on the **Gatekeeper** page (see Displaying the built-in gatekeeper registration list) or an external gatekeeper. To use the built-in gatekeeper enter the IP address of this ISDN Gateway, "localhost" or "127.0.0.1". For an external gatekeeper, enter its host name or IP address.
Gatekeeper registration type	Set to *Gateway* unless you are using a Cisco gatekeeper.	Either *Gateway* or *Gateway (Cisco GK compatible)*.
Ethernet port association	To use the gatekeeper you must select Port A. Then the gatekeeper will validate the connection of all incoming calls, and outgoing calls dialed by address rather than by E.164 phone number.	
H.323 ID	An identifier that the ISDN Gateway uses to register itself with the gatekeeper. You can specify a name or number.	If you are using a gatekeeper, you must enter a registration ID. Before the ISDN gateway can register any conferences with the H.323 gatekeeper, it must make a unit wide registration.
Use password	If the configured gatekeeper required password authentication from registrants, check the *Use password* box and type the password.	Note that where password authentication is used, the *(Mandatory) H.323 ID to register* will be used as the username.
Dial plan prefixes (space-separated)	Up to ten groups of up to ten digits (separated by a space) any of which will identify calls to be routed to the ISDN Gateway.	This field is optional. If set, users dialing a number beginning with any of the prefixes will have their call directed to the ISDN Gateway. Registering several prefixes allows you to create IP to ISDN rules that use different prefixes for calls at different kbps for example. This field will have no effect if *H.323 gatekeeper usage* is disabled.

Send resource availability indications	Select this option if you want the ISDN Gateway to inform the gatekeeper about its availability or non-availability. This information will be used by the gatekeeper when it is selecting where to place calls. There are two scenarios where you can use this feature: ▶ where multiple ISDN Gateways are registered with the same dial plan prefix on the same gatekeeper. When resource availability indications (RAI) are configured, the ISDN Gateway will inform the gatekeeper when it is unavailable; gatekeepers that support this functionality (the Cisco gatekeeper for example) will favor ISDN Gateways in the available state when choosing where to place new calls ▶ where there is only one ISDN Gateway, and you want to limit the use of the gateway by IP calls. In this way, you can ensure that there will always be some capacity for calls from the ISDN network When selected, the ISDN Gateway will inform the gatekeeper when it is unavailable (that is, all its ports are already in use).	The ability of the ISDN Gateway to send resource availability messages is useful in a network where there are multiple ISDN Gateways or where there are several ISDN Gateway blades in an MSE. In an environment with multiple ISDN Gateways registered with the same gatekeeper, that gatekeeper should favor devices in the available state when choosing where to place new calls. For example, when one ISDN Gateway sends the gatekeeper a message indicating that it is not available, the gatekeeper will then attempt to use a different ISDN Gateway for new calls. Enter the *Threshold* above which messages will be sent to the gatekeeper. The threshold is the percentage of available B-channels in use; where an "available" port is a port which has at least layer 1 up and the channel is not in use as a D-channel/reserved channel. For example, if you set the threshold to 80%, the ISDN Gateway will send a message to the gatekeeper to say that is busy when 80% of its available B-channels are in use.
Deregister from gatekeeper if no ISDN link	Selecting this checkbox ensures that the gatekeeper will not forward any call to the ISDN Gateway if the gateway is not in a state to receive calls. This can be used to allow redundancy: if an ISDN switch is down, the ISDN Gateway will deregister and the gatekeeper may use an alternative ISDN Gateway.	Note that all the PRIs have to be down for deregistration. Deregistration will not occur when the ISDN Gateway is fully loaded with active calls.

Gatekeeper status

The ISDN Gateway also displays brief status information about any registered gatekeepers.

Field	Field description	Usage tips
H.323 gatekeeper status	The status of the gatekeeper currently being used by the ISDN Gateway.	One of: ▶ *name resolved to <IP address>:* the ISDN Gateway has successfully validated the IP address of the gatekeeper. ▶ *not in use*: there is no gatekeeper in use ▶ *name resolution in progress*: the ISDN Gateway is trying to validate an IP address or find the IP address that corresponds to the specified host name for the gatekeeper. ▶ *retrying name resolution*: the ISDN Gateway is trying to validate an IP address again or find the IP address that corresponds to the specified host name for the gatekeeper. ▶ *failed to resolve gatekeeper name*: the ISDN Gateway could not find the IP address of the gatekeeper.
Registered address	Displays the local IP address and port number that the ISDN Gateway has registered with the gatekeeper.	This information might be useful if the ISDN Gateway has more than one IP address, for instance if both Ethernet interfaces are in use.
Alternate gatekeepers available	Displays the number of 'alternate' gatekeepers configured on the H.323 gatekeeper. This figure comes from the gatekeeper itself; if there are any 'alternate' gatekeepers configured, the gatekeeper tells the ISDN Gateway their IP addresses.	Where the configured gatekeeper has told the ISDN Gateway about any configured 'alternate' gatekeepers and if the ISDN Gateway loses contact with the configured gatekeeper, the ISDN Gateway will attempt to register with each of the 'alternates' in turn. If none of the 'alternate' gatekeepers responds, the ISDN Gateway will report that the registration has failed. If the ISDN Gateway successfully registers with an 'alternate' gatekeeper: ▶ the *H.323 gatekeeper status* will indicate that registration is with an 'alternate' ▶ the list of 'alternates' received from the new gatekeeper will replace the previous list ▶ the ISDN Gateway will only revert back to the original gatekeeper if the 'alternate' fails and only if the original gatekeeper is configured as an 'alternate' on the current gatekeeper's

		list of 'alternates' Note that if the ISDN Gateway registers with an 'alternate' that does not itself supply a list of 'alternates', the ISDN Gateway will retain the original list and if it loses contact with the current gatekeeper, each one will be attempted from the top again as before.
Number of active registrations	This number refers to the H.323 ID and the dial plan prefix. It also shows whether these registrations are pending (in progress, but not fully registered) or active (fully registered).	The number of registrations can therefore be: 0,1, or 2.
H.323 ID registration	Displays the identifier that the ISDN Gateway has used to register itself with the H.323 gatekeeper.	For more information about the H.323 ID, refer to the table above.
Resource availability status	Displays whether the gatekeeper is configured to send resource availability indications and if it is, it displays the current state of the resource availability status of the ISDN Gateway.	The possible statuses are: ▶ **resources available** ▶ **resources unavailable** ▶ **<indications not configured>**
Dial plan prefixes	Displays the dial plan prefixes that the ISDN Gateway has registered with the gatekeeper.	For more information about these prefixes, refer to the table above.

Configuring encryption settings

You can configure the Cisco TelePresence ISDN Gateway to encrypt the IP "leg", the ISDN leg or both legs of a call. The encryption technology that the ISDN Gateway uses is Advanced Encryption Standard (AES).

To use encryption, you must have the Encryption feature key present on the ISDN Gateway. For information about installing feature keys, refer to Upgrading the firmware.

When encryption is in use, the ISDN Gateway will encrypt audio, video, and content media (rather than control encryption or authentication encryption).

To access encryption settings, choose **Settings > Encryption**. After making any configuration changes, click **Apply changes**.

You can:

- configure the ISDN Gateway to advertise its ability to encrypt connections, such that it will use encryption on the IP leg if an H.323 endpoint can use AES encryption
- configure the ISDN Gateway to advertise its ability to encrypt connections, such that it will use encryption on the ISDN leg if an ISDN endpoint can use AES encryption
- configure each dial plan rule to require encryption or to use it optionally if an H.323 or ISDN endpoint can use AES encryption. Note that if encryption is required on either leg of the call but the appropriate endpoint cannot use it, the call will be disconnected
- configure each dial plan rule to use transparent encryption. When transparent encryption is used, the ISDN Gateway will simulate point-to-point encryption. That is, it will set the encryption state (enabled/disabled) used on the received call as that to be used on the outgoing call. That is, the ISDN Gateway will attempt to match the encryption state for the outgoing call to that of the incoming call. For more information, see Adding and updating dial plan rules.

Field	Field description	Usage tips
IP encryption status	Whether the ISDN Gateway is able to use encryption on the IP leg of a call or not.	When *Enabled*, the ISDN Gateway advertises itself as being able to use encryption for IP. With IP encryption enabled, for each dial plan you must select whether encryption is required or optional when using that dial plan. See Adding and updating dial plan rules. Note that if you disable encryption here but leave it as *Required* in a dial plan rule, then all calls using that rule will be rejected.
ISDN encryption status	Whether the ISDN Gateway is able to use encryption on the ISDN leg of a call or not.	When *Enabled*, the ISDN Gateway advertises itself as being able to use encryption for ISDN. With encryption enabled, for each dial plan you must select whether encryption is required or optional when using that dial plan. See Adding and updating dial plan rules. Note that if you disable encryption here but leave it as *Required* in a dial plan rule, then all calls using that rule will be rejected.

Displaying and resetting system time

The system date and time for the Cisco TelePresence ISDN Gateway can be set manually or using the Network Time Protocol (NTP).

To configure Time settings, go to **Settings > Time**.

System time

The current system date and time is displayed.

If you do not have NTP enabled and need to update the system date and/or time manually, type the new values and click **Change system time**.

NTP

The ISDN Gateway supports the NTP protocol. Configure the settings using the table below for help, and then click **Update NTP settings**.

The ISDN Gateway re-synchronizes with the NTP server via NTP every hour.

If there is a firewall between the ISDN Gateway and the NTP server, configure the firewall to allow NTP traffic to UDP port 123.

If the NTP server is local to Port A or Port B then the ISDN Gateway will automatically use the appropriate port to communicate with the NTP server. If the NTP server is not local, the ISDN Gateway will use the port that is configured as the default gateway to communicate with the NTP server, unless a specific IP route to the NTP server's network/IP address is specified. To configure the default gateway or an IP route, go to **Network > Routes**.

Field	Field description	Usage tips
Enable NTP	If selected, use of the NTP protocol is Enabled on the ISDN Gateway.	
UTC offset	The offset of the time zone that you are in from Greenwich Mean Time.	You must update the offset manually when the clocks go backwards or forwards: the ISDN gateway does not adjust for daylight saving automatically.
NTP host	The IP address or hostname of the server that is acting as the time keeper for the network.	

Using NTP over NAT (Network Address Translation)

If NAT is used between the ISDN Gateway and the NTP server, with the ISDN Gateway on the NAT's local network (and not the NTP server), no extra configuration is required.

If NAT is used between the ISDN Gateway and the NTP server, with the NTP server on the NAT's local network, then configure the NAT forwarding table to forward all data to UDP port 123 to the NTP server.

Configuring security settings

To configure security settings, go to **Settings > Security**.

Field	Field description
User authentication settings	
Enable advanced security mode	Advanced security mode causes the Cisco TelePresence ISDN Gateway to hash passwords before storing them in the configuration.xml file (see below). Note that hashing user passwords is an irreversible process. If you enable advanced security mode, we recommend that you back up your configuration. The ISDN Gateway gives you the option to do that after you have enabled Advanced account security mode. If you enable advanced security mode, all current passwords (created when the ISDN gateway was not in advanced security mode) will expire and users must change them. Advanced security mode is described in greater detail below.
Redirect HTTP requests to HTTPS	Enable this option to have HTTP requests to the ISDN Gateway automatically redirected to HTTPS. This option is unavailable if either HTTP (*Web*) or HTTPS (*Secure web*) access is disabled on the **Network > Services** page.
Idle web session timeout	The timeout setting for idle web sessions. The user must log in again if the web sessions expires. The timeout value must be between 1 and 60 minutes. Note that status web pages that auto-refresh will keep a web session active indefinitely. You can configure the ISDN Gateway not to auto-refresh those pages; to do so, go to **Settings > User interface**.
Serial console settings	
Hide log messages on console	The serial console interface displays log messages. If that is considered to be a security weakness in your environment, select this option to hide those messages.
Disable serial input during startup	Select this option for enhanced serial port security.
Require administrator login	Select this option to require an administrator login by anyone attempting to connect to the ISDN Gateway via the console port. If this is not enabled, anyone with physical access to the MCU (or with access to your terminal server) can potentially enter commands on the serial console.
Idle console session timout	If you have enabled **Require administrator login**, you can configure a session timeout period. The timeout setting for idle console sessions. The admin must log in again if the console sessions expires. The timeout value must be between 1 and 60 minutes.

Advanced security mode

You can configure the ISDN Gateway to use advanced security mode. Advanced security mode has the following features:

- The ISDN Gateway will hash passwords before storing them in the configuration.xml file (see Hashing passwords below)
- The ISDN Gateway will demand that passwords fulfill certain criteria, using a mixture of alphanumeric and non-alphanumeric (special) characters (see Password format below)
- Passwords will expire after 60 days
- A new password for an account must be different from the last ten passwords used with that account
- The ISDN Gateway will disable a user's account if that user incorrectly enters a password three times consecutively. If this is an admin account, it is disabled for 30 minutes; for any other account, it is disabled indefinitely (or until you, the administrator, re-enable the account from the **User** page)
- Non-administrator account holders are not allowed to change their password more than once in any 24 hour period
- Administrators can change any user account's password and force any account to change its password by selecting **Force user to change password on next login** on the **User** page. Administrators can prevent any non-administrator account from changing its password by selecting **Lock password** on the **User** page.
- The ISDN Gateway will disable any non-administrator account after a 30 day period of account inactivity. To re-enable the account, you must edit that account's settings on the **User** page

If you enable advanced security, all current passwords (created when the ISDN Gateway was not in advanced security mode) will expire and users must change them.

When using Advanced account security mode, we recommend that you rename the default administrator account. This is especially true where the ISDN Gateway is connected to the public internet because security attacks will often use "admin" when attempting to access a device with a public IP address. Even on a secure network, if the default administrator account is "admin", it is not inconceivable that innocent attempts to log into the ISDN Gateway will cause you to be locked out for 30 minutes.

We recommend that you create several accounts with administrator privileges. This will mean that you will have an account through which you can access the ISDN Gateway even if one administrator account has been locked out.

If there are API applications accessing the ISDN Gateway, we recommend that you create dedicated administrator accounts for each application.

In advanced security mode, if a user logs in with a correct but expired password the ISDN Gateway asks that user to change the password. If the user chooses not to change it, that user is allowed two more login attempts to change the password before the account gets disabled.

Hashing passwords

In advanced security mode, the ISDN Gateway will hash passwords before storing them in the configuration.xml file. The configuration.xml file is used for backing up and restoring the configuration of the ISDN Gateway (see Upgrading and backing up the ISDN Gateway). If you do not select to use advanced password security, all user passwords are stored in plain text in the configuration.xml; this might be a security issue. If you select to use advanced password security, they will not be stored anywhere on the ISDN Gateway in plain text; instead the passwords will be stored as hash sums. Note that hashing user passwords is an irreversible process.

Password format

In advanced security mode, passwords must have:

- at least fifteen characters
- at least two uppercase alphabetic characters
- at least two lowercase alphabetic characters
- at least two numeric characters
- at least two non-alphanumeric (special) characters
- not more than two consecutive repeating characters. That is, two repeating characters are allowed, three are not

In advanced security mode, a new password must be different to the previous 10 passwords that have been used with an account.

Expiring passwords

In advanced security mode, if a user logs in with a correct but expired password the ISDN Gateway asks that user to change the password. If the user chooses not to change it, that user is allowed two more login attempts to change the password before the account gets disabled.

Upgrading and backing up the Cisco TelePresence ISDN Gateway

In this section:

Upgrading the main ISDN Gateway software image

The main Cisco TelePresence ISDN Gateway software image is the only firmware component that you will need to upgrade.

To upgrade the main ISDN Gateway software image:

1. Go to **Settings > Upgrade**.
2. Check the *Current version* field to verify the currently installed version.
3. Log onto the support pages to identify whether a more recent image is available.
4. Download the latest available image and save it to a local hard drive.
5. Unzip the image file.
6. Log on to the ISDN Gateway web browser interface.
7. Go to **Settings > Upgrade**.
8. Click **Browse** to locate the unzipped file on your hard drive.
9. Click **Upload software image**. The browser begins uploading the file to the ISDN Gateway, and a new browser window opens to indicate the progress of the upload. When finished, the browser window refreshes and indicates that the "Main image upgrade completed."
10. The upgrade status displays in the ISDN Gateway *software upgrade status* field.
11. Shutdown and restart the ISDN Gateway.

Upgrading the loader software image

Upgrades for the Loader software image are not typically available as often as upgrades to the main software image.

To upgrade the loader software image:

1. Go to **Settings > Upgrade**.
2. Check the *Current version* field to verify the currently installed version.
3. Go to the software download pages of the web site to identify whether a more recent image is available.
4. Download the latest available image and save it to a local hard drive.
5. Unzip the image file.
6. Click **Browse** to locate the unzipped file on your hard drive.

7. Click **Upload software image**. The browser begins uploading the file to the ISDN Gateway, and a new browser window opens to indicate the progress of the upload. When finished, the browser window refreshes and indicates that the "Loader image upgrade completed."
8. The upgrade status displays in the *Loader upgrade status* field.
9. Shutdown and restart the ISDN Gateway.

Backing up and restoring the configuration

The Back up and restore section of the **Upgrade** (**Settings > Upgrade**) page allows you to back up and restore the configuration of the ISDN Gateway using the web interface. This enables you to either go back to a previous configuration after making changes or to effectively "clone" one unit as another by copying its configuration.

To back up the configuration, click **Save backup file** and save the resulting "configuration.xml" file to a secure location.

To restore configuration at a later date, locate a previously-saved "configuration.xml" file and click **Restore backup file**. When restoring a new configuration file to an ISDN Gateway you can control which parts of the configuration are overwritten:

- If you select **Network settings**, the network configuration will be overwritten with the network settings in the supplied file. Typically, you would only select this check box if you were restoring from a file backed up from the same ISDN Gateway or if you were intending to replace an out of service ISDN Gateway. If you copy the network settings from a different, active, ISDN Gateway and there is a clash (for instance, both are now configured to use the same fixed IP address) one or both boxes may become unreachable via IP. If you do not select **Network settings**, the restore operation will not overwrite the existing network settings, with the one exception of the QoS settings. QoS settings are overwritten regardless of the **Network settings** check box.
- If you select the **User settings** check box, the current user accounts and passwords will be overwritten with those in the supplied file. If you overwrite the user settings and there is no user account in the restored file corresponding to your current login, you will need to log in again after the file has been uploaded.

By default, the overwrite controls are not selected, and therefore the existing network settings and user accounts will be preserved. Note that you can also back up and restore the configuration of the ISDN Gateway using FTP. For more information, refer to Backing up and restoring the configuration using FTP.

Enabling ISDN Gateway features

The Cisco TelePresence ISDN Gateway requires activation before most of its features can be used. (If the ISDN Gateway has not been activated, the banner at the top of the web interface will show a prominent warning; in every other respect the web interface will look and behave normally.)

If this is a new ISDN Gateway you should receive the ISDN Gateway already activated; if it is not, you have upgraded to a newer firmware version, or you are enabling a new feature, you may need to contact your supplier to obtain an appropriate activation code. Activation codes are unique to a particular ISDN Gateway so ensure you know the ISDN Gateway's serial number such that you may receive a code appropriate to your ISDN Gateway. Regardless of whether you are activating the ISDN Gateway or enabling an advanced feature, the process is the same.

To activate the ISDN Gateway or enable an advanced feature:

1. Check the *Activated features* (ISDN Gateway activation is shown in this same list) to confirm that the feature you require is not already activated.
2. Enter the new feature code into the *Activation code* field exactly as you received it, including any dashes.
3. Click **Update features**. The browser window should refresh and list the newly activated feature, showing the activation code beside it. Activation codes may be time-limited. If this is the case, an expiry date will be displayed, or a warning that the feature has already expired. Expired activation codes remain listed, but the corresponding feature will not be activated. If the activation code is not valid, you will be prompted to re-enter it.
4. Cisco recommends that you record the activation code in case you need to re-enter it in the future.

Successful ISDN Gateway or feature activation has immediate effect and will persist even if the ISDN Gateway is restarted.

Note that you can remove ISDN Gateway feature keys by clicking the **Remove** link next to the feature key in this page.

Shutting down and restarting the Cisco TelePresence ISDN Gateway

It is sometimes necessary to shut down the Cisco TelePresence ISDN Gateway, generally to restart as part of an upgrade (see Upgrading and backing up the ISDN Gateway). You should also shut down the ISDN Gateway before intentionally removing power from it.

Shutting down the ISDN Gateway will disconnect all active calls.

To shut down the ISDN Gateway:

1. Go to **Settings > Shutdown**.
2. Click **Shut down ISDN Gateway**.
3. Confirmation of shutdown is required; the button changes to **Confirm ISDN gateway shutdown**.
4. Click again to confirm.
5. The ISDN Gateway will begin to shut down. The banner at the top of the page will change to indicate this.
   When the shutdown is complete, the button changes to **Restart ISDN gateway**.
6. Click this button a final time to restart the ISDN Gateway.

Displaying general status

The General Status displays an overview of the Cisco TelePresence ISDN Gateway status. To access this information, go to **Status > General.**

Refer to the table below for details of the information displayed

Field	Field description
System status	
Model	The specific Cisco TelePresence ISDN Gateway model.
Serial number	The unique serial number of the ISDN Gateway.
Software version	The installed software version. You will need to provide this information when speaking to Customer support.
Build	The build version of installed software. You will need to provide this information when speaking to Customer support.
Up time	The time since the last restart of the ISDN Gateway.
Host name	The host name assigned to the ISDN Gateway.
IP address	The IP address assigned to the ISDN Gateway.
CPU load	The current processor utilization of the ISDN Gateway.
System time	
Current time	The system time on the ISDN Gateway. Click **New time** to modify this value. The **Time Settings** page opens in which you can update the system date and time manually or refresh the time from an NTP server. For more information about the **Time Settings** page, refer to Displaying and resetting system time.
System log	
▶ **User requested shutdown** ▶ **User requested upgrade** ▶ **Unknown**	The system log displays the last eight shutdown and upgrade events in date order with the most recent system log event at the top of the list. The log will also display "unknown" if there has been an unexpected reboot or power failure, which you should report to Customer support if it happens repeatedly.
Diagnostic information	
Download diagnostic information	If required to do so by Customer support, click **Download diagnostic information** to save a set of diagnostic files.

Displaying ISDN status

The ISDN status page displays an overview of the current state and configuration of the ISDN ports.

To display ISDN status, go to **Status > ISDN**.

Information is shown in a table, with one row per physical port of the ISDN Gateway. Refer to the table below for details of the information displayed in each row.

Field	Field description	Usage tips
Port	The number of the port to which this information relates.	
State	Whether or not this port is enabled.	A port may be disabled because it is not supported by the particular model of ISDN Gateway, because the port is not applicable or not licensed or because it has been explicitly disabled by the user (see Configuring ISDN ports settings). Note that for ISDN GW blades the number of licensed ports depends on the number of PRI port licenses allocated to the blade.
Layer 1	Shows *up* when the physical layer is connected. Shows *down* otherwise.	
Layer 2	Shows *up* when the D-channel is connected to, and has established communication with, the ISDN network. Shows *down* otherwise.	If the ISDN Gateway is in leased line mode, there will be no layer 2 status.
Type	The interface type configured for this port.	To change the interface type, see Configuring general ISDN settings.

Displaying hardware health status

The Health Status displays information about the hardware components of the Cisco TelePresence ISDN Gateway.

Note: The *Worst status seen* conditions are those since the last time the unit was restarted.

To reset these values, click **Clear**. Refer to the table below for assistance in interpreting the information displayed.

Field	Field description	Usage tips
Fans (3201 series only) **Voltages** **RTC battery**	Displays two possible states: ▶ OK ▶ Out of spec States indicate both **Current status** and **Worst status seen** conditions.	▶ **OK** – component is functioning properly ▶ **Out of spec** – Check with your support provider; component might require service If the **Worst status seen** column displays "Out of spec", but **Current status** is "OK", monitor the status regularly to verify that it was only a temporary condition.
Temperature	Displays three possible states: ▶ OK ▶ Out of spec ▶ Critical States indicate both **Current status** and **Worst status seen** conditions.	▶ **OK** – temperature of the ISDN Gateway is within the appropriate range ▶ **Out of spec** – Check the ambient temperature (should be less than 34 degrees Celsius) and verify that the air vents are not blocked ▶ **Critical** – temperature of ISDN Gateway is too high. An error also appears in the event log indicating that the system will shutdown in 60 seconds if the condition persists If the **Worst status seen** column displays "Out of spec", but **Current status** is "OK", monitor the status regularly to verify that it was only a temporary condition.

Displaying security status

The Security status page displays a list of active security warnings for the Cisco TelePresence ISDN Gateway. To access this information, go to **Status > Security.**

Security warnings identify potential weaknesses in the security of the ISDN Gateway's configuration. Note that some security warnings might not be relevant for your organization. For example if the ISDN Gateway is inside a secure network, enabling HTTP may not be a security issue. For information about all possible security warnings, refer to Understanding security warnings.

To acknowledge a security warning, select that warning and click **Acknowledge selected**. Acknowledged warnings will not appear on the ISDN Gateway's Home page. If the ISDN Gateway reboots, the warnings are reset and previously acknowledged warnings will need re-acknowledging.

To fix a security issue, click on the **Action** link for the warning message relating to the issue. When you fix a security issue, the security warning disappears from this list (on the **Status > Security** page), but it will be logged in the Audit log. For more information about the audit log, refer to Working with the audit logs.

Refer to the table below for details of the information displayed.

Field	Field description
Warning	The text of the security warning.
State	For every security warning, the state will one of: ▶ **New**: A new security warning is one that has been raised by the ISDN Gateway, but you have not acknowledged it. New warnings also appear on the ISDN Gateway Home page. ▶ **Acknowledged**: An acknowledged security warning is one that you have acknowledged, but have not fixed. When you fix a security issue, the security warning disappears from this list, but it will be logged in the Audit log. For more information about the audit log, refer to Working with the audit logs.
Action	For every security warning, there is a corresponding action that explains how to fix the security issue. Usually this is a link that takes you to the page where you can make the configuration change that will fix the security issue.

Working with the event logs

If you are experiencing complex issues that require advanced troubleshooting, you may need to collect information from the Cisco TelePresence ISDN Gateway logs. Typically, you will be working with Customer support who can help you obtain these logs.

Event log

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

You can:

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

Event capture filter

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

Note: You should not modify these settings unless instructed to do so by Customer support**.** Modifying these settings can impair the performance of your ISDN Gateway.

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

Event display filter

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

Syslog

You can configure the ISDN Gateway to send event messages to up to four syslog servers. To add or remove a syslog server, go to **Logs > Syslog** and make the changes you require. See Logging using syslog.

H.323

The H.323 log page records every H.323 message received or transmitted from the ISDN Gateway. The log can be exported in an .xml file. By default the H.323 log is disabled because it affects performance, but Technical support may ask you to enable it if there is a problem with an ISDN Gateway in your network.

Audit log

The audit log records any user action on the ISDN Gateway which might compromise the security of the unit, of its functions, or of the network. For more information, refer to Working with the audit logs.

Call Detail Records

In addition to the logs described above, the ISDN Gateway can also store Call Detail Records (CDR) which may be used for auditing and billing purposes. Events in the log are displayed in the CDR log page. See Working with Call Detail Records for more details.

Working with the audit logs

The audit log records any user action on the Cisco TelePresence ISDN Gateway which might compromise the security of the unit, of its functions, or of the network.

By enabling auditing, all network settings, security settings, creation/deletion of dial plans and any changes to the audit log itself are logged on the ISDN Gateway.

All relevant actions on the ISDN Gateway are logged, including those made through the serial console, a supervisor blade (for MSE blades), the API, FTP, and the web interface. The module that has caused a log is listed within the details of that log and will be one of:

- **Web**: For configuration changes made through the web interface.
- **Serial**: For configuration changes made through the serial interface.
- **API**: For configuration changes made through the API.
- **Supervisor**: For configuration changes made through the Supervisor Blade (only applies to MSE blades).
- **System**: For audit messages from the ISDN Gateway.
- **FTP**: For audit messages recording requests made to the ISDN Gateway over FTP.

Each log also has a severity associated with it (Error, Severe Warning, Warning, Info, or Status Warning).

You must enable the audit log for it to record these actions.

To enable and view the audit log, go to **Logs** and select the **Audit log** tab.

Audit log

The last 2000 audit messages generated by the ISDN Gateway are displayed in the **Audit log** page.

The last 100,000 audit messages are stored on the compact flash if there is one; otherwise, the last 100,000 audit messages are stored internally. You can only view the last 2000 through the web interface, but you can download all stored audit messages (up to the 100,000) as XML.

You can delete audit messages, but you cannot delete the most recent 400 audit messages. If you delete any audit messages, that will be audited in a new audit message.

You cannot send the audit log to a syslog server.

Understanding security warnings

The **Security status** page displays a list of active security warnings for the Cisco TelePresence ISDN Gateway. To access this information, go to **Status > Security**. Security warnings identify potential weaknesses in the security of the ISDN Gateway's configuration. For more information on configuring security settings, refer to Configuring security settings. For more detailed information on the security status, refer to Displaying security status.

The table below details the warnings that appear, and the relevant actions needed to rectify them.

Warning	Action	Explanation
Advanced password security is disabled	Enable advanced security mode in user authentication settings	If Advanced security mode is not enabled, passwords will be stored in plain text or MD5, and therefore be unsecure. To enable Advanced security mode, go to **Settings > Security** and select *Enable Advanced security mode*.
Hide log messages on console is disabled	Enable hide log messages on console in serial console settings	To hide log messages on the console, go to **Settings > Security** and select *Hide log messages on console*. This will stop event messages appearing on the console.
Require administrator login to console is disabled	Enable require administrator login in serial console settings	Having to log in as administrator on the serial console increases security. To do this, go to **Settings > Security** and select *Require administrator login*.
Guest account is enabled	Disable the guest account	By default the guest user account is assigned the privilege of 'conference list only', meaning that users who log in as guest can view the list of active conferences and change their own profile. Disabling the guest account makes the ISDN Gateway more secure. To disable the guest account, go to **Users > User list** and select *Guest*. Select *Disable user account*.
Admin account has default username	Change the admin account username	The ISDN Gateway must have at least one configured user with administrator privileges. By default, the User ID is "admin" and no password is required. To change the admin account username, go to **Users > User list** and select *admin*. Enter a new username in the *User ID* field and click **Update user settings**.

Unsecured FTP service is enabled	Disable FTP in network TCP services	Information sent using FTP is unencrypted and sent in plain text; therefore, it is possible for people to discover usernames and passwords easily. To disable FTP, go to **Network > Services** and deselect the *FTP* check box.
Unsecured HTTP service is enabled	Disable HTTP in network TCP services	Information sent using HTTP (Web) is unsecured and not encrypted. To disable HTTP, go to **Network > Services** and deselect the *Web* check box. We recommend that you enable *Secure web*.
Unsecured SNMP service is enabled	Disable SNMP in network UDP services	Information sent using SNMP is unencrypted and sent in plain text; therefore, it is possible for people to discover usernames and passwords easily. To disable SNMP, go to **Network > Services** and deselect the *SNMP* check box.
Auto-refresh of web pages is enabled	Change auto-refresh interval to "No auto-refresh"	If your ISDN Gateway is set to auto-refresh it could mean that an unattended ISDN Gateway will never have a session timeout. To turn off auto-refresh, go to **Settings > User interface** and change *Status page auto-refresh interval* to *No auto-refresh*.
Audit logging of configuration changes is disabled	Enable the audit log	If the audit log is disabled, the ISDN Gateway will not create an audit log. To enable audit logs, go to **Logs > Audit log** and select **Enable auditing**. For more information on the audit log, refer to Working with the audit logs.
Audit logs dropped due to lack of compact flash, audit system integrity compromised	Check the system configuration for possible security changes	If no compact flash card is installed in the ISDN Gateway, logs are only stored up to a maximum of 200 events. The 200 events do not 'wrap', and therefore when the maximum is reached the log is deleted and started over again. To rectify this problem, insert a compact flash card. For more information on the audit log, refer to Working with the audit logs.

Audit logs hash check failed, audit system integrity compromised	Check system configuration for possible security changes	If audit logs checks fail, it is possible that your ISDN Gateway has been compromised. For example, someone may have taken the compact flash card out and deleted some audit logs. For more information on the audit log, refer to Working with the audit logs.
Compact flash card not present, audit and CDR logs will not be saved	Insert a compact flash card or check whether the existing compact flash card is functional	If no compact flash card is installed in the ISDN Gateway, logs are only stored up to a maximum of 200 events. The 200 events do not 'wrap', and therefore when the maximum is reached the log is deleted and started over again. The ISDN Gateway will give you this warning when you are nearing the 200 maximum. To rectify this problem, insert a compact flash card.
Call encryption is disabled	Enable call encryption	When encryption status is *Disabled*, no calls on the ISDN Gateway will be able to use encryption. To enable encryption, go to **Settings > Encryption**. For *Encryption status*, select *Enabled*.
Audit log above 75% capacity	Download and delete audit logs.	The audit log has a maximum capacity of 100,000 audit events, or the size limit of the compact flash card. When you are nearing either of these limits, the ISDN Gateway will give you this warning. If you reach full capacity of the compact flash card, the ISDN Gateway will 'wrap' meaning that older logs will be deleted. To rectify this problem download and clear the audit log. To do this, go to **Logs > Audit log** and select **Download as XML**. Once this has completed, click **Delete all records**.
Audit log above 90% capacity	Download and delete audit logs.	The audit log has a maximum capacity of 100,000 audit events, or the size limit of the compact flash card. When you are nearing either of these limits, the ISDN Gateway will give you this warning. If you reach full capacity of the compact flash card, the ISDN Gateway will 'wrap' meaning that older logs will be deleted. To rectify this problem download and clear the audit log. To do this, go to **Logs > Audit log** and select **Download as XML**. Once this has completed, click **Delete all records**.

Encryption not available on this device	Add feature key for encryption.	To use encryption on your ISDN Gateway you must have the Encryption feature key installed. To purchase this feature key, contact your reseller.
Shell not secured for startup	Disable the serial input during startup.	If *Disable serial input during startup* isn't selected, the serial console is not protected during application startup. This means users will have access to debug services in the operating system. To disable this, go to **Settings > Security**, and select the *Disable serial input during startup* tick box.

Logging using syslog

You can send the Event log to one or more syslog servers on the network for storage or analysis.

To configure the syslog facility, go to **Logs > Syslog**

In this section:

Syslog settings

Refer to this table for assistance when configuring Syslog settings:

Field	Field description	Usage tips
Host address 1 to 4	Enter the IP addresses of up to four Syslog receiver hosts.	The number of packets sent to each configured host will be displayed next to its IP address.
Facility value	A configurable value for the purposes of identifying events from the Cisco TelePresence ISDN Gateway on the Syslog host. Choose from the following options: ▸ *0 - kernel messages* ▸ *1 - user-level messages* ▸ *2 - mail system* ▸ *3 - system daemons* ▸ *4 - security/authorization messages (see Note 1)* ▸ *5 - messages generated internally by syslogd* ▸ *6 - line printer subsystem* ▸ *7 - network news subsystem* ▸ *8 - UUCP subsystem* ▸ *9 - clock daemon (see Note 2)* ▸ *10 - security/authorization messages (see Note 1)* ▸ *11 - FTP daemon* ▸ *12 - NTP subsystem* ▸ *13 - log audit (see Note 1)* ▸ *14 - log alert (see Note 1)* ▸ *15 - clock daemon (see Note 2)* ▸ *16 - local use 0 (local0)*	Choose a value that you will remember as being the ISDN Gateway. Note: Various operating system daemons and processes have been found to utilize Facilities 4, 10, 13 and 14 for security/authorization, audit, and alert messages which seem to be similar. Various operating systems have been found to utilize both Facilities 9 and 15 for clock (cron/at) messages. Processes and daemons that have not been explicitly assigned a Facility value may use any of the "local use" facilities (16 to 21) or they may use the "user-level" facility (1) - and these are the values that we recommend you select.

	▸ *17 - local use 1 (local1)* ▸ *18 - local use 2 (local2)* ▸ *19 - local use 3 (local3)* ▸ *20 - local use 4 (local4)* ▸ *21 - local use 5 (local5)* ▸ *22 - local use 6 (local6)* ▸ *23 - local use 7 (local7)*	

Using syslog

The events that are forwarded to the syslog receiver hosts are controlled by the event log capture filter.

To define a syslog server, simply enter its IP address and then click **Update syslog settings**. The number of packets sent to each configured host is displayed next to its IP address.

Note: Each event will have a severity indicator as follows:

- 0 - Emergency: system is unusable (unused by the ISDN Gateway)
- 1 - Alert: action must be taken immediately (unused by the ISDN Gateway)
- 2 - Critical: critical conditions (unused by the ISDN Gateway)
- 3 - Error: error conditions (used by ISDN Gateway *error* events)
- 4 - Warning: warning conditions (used by ISDN Gateway *warning* events)
- 5 - Notice: normal but significant condition (used by ISDN Gateway *info* events)
- 6 - Informational: informational messages (used by ISDN Gateway *trace* events)
- 7 - Debug: debug-level messages (used by ISDN Gateway *detailed trace* events)

Working with Call Detail Records

The Cisco TelePresence ISDN Gateway can display up to 20 pages of Call Detail Records. However, the ISDN Gateway is not intended to provide long-term storage of Call Detail Records. You must download the Call Detail Records and store them elsewhere.

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

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

Call Detail Record log controls

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

Field	Field description	Usage tips
Current status	This field indicates whether CDR logging is enabled or disabled. Use the two buttons (**Enable logging** and **Disable logging**) to change status. When you enable logging, the ISDN Gateway writes the CDRs to the compact flash card.	Enabling or disabling CDR logging has immediate effect. There is no need to press **Update display** after clicking one of these buttons. Ensure there is a compact flash card available - either in the slot on the front of the ISDN Gateway or internally.
Messages logged	The current number of CDRs in the log.	
Filter string	Use this field to limit the scope of the displayed Call Detail Records. The filter string is not case-sensitive.	The filter string applies to the *Message* field in the log display. If a particular record has expanded details, the filter string will apply to these as well.
Expand details	By default, the CDR log shows only brief details of each event. When available, select from the options listed to display more details.	Selecting **All** will show the greatest amount of detail for all messages, regardless of which other options are checked.

Call Detail Record log

This table shows the logged Call Detail Records, subject to any filtering applied (see Call Detail Record log controls, above). The fields displayed and the list's associated controls are described below:

- CDR log display

Downloading and clearing the log

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

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

Note: Only download CDRs when the unit is not under heavy load, otherwise performance of the unit may be impaired.

The range of logs that you can download to the web interface works in groups. Therefore you may see **Download X to Y as XML** and Y will not increase even though the log is filling up. When a threshold is reached, then Y increases. However, you always have the option to download the full log with **Download as XML**.

In addition the web interface displays a maximum of 20 pages. If the log includes more events than can be displayed on those pages, the more recent events are displayed. Therefore you may see **Download X to Y as XML** where X keeps increasing when the page is refreshed. Again you can download the full log with **Download as XML**.

To clear the CDR log, click **Delete X to Y**. This will permanently remove Call Detail Records X to Y. Due to the way the CDR log works, it may not be possible to delete all records; the button name indicates which records can be deleted. For example, if you delete the 0-399 entries, then the 400th entry appears as the first entry in this page, even if you download the full log. The download button would then show that you can download for example 400-674 (if 674 is the maximum number of entries in the log) and the delete button will be greyed out again (because it is only available when a certain number of entries are in the log).

To avoid duplicate entries when you download repeatedly, each time delete the entries that you have just downloaded.

CDR log display

The CDR log list shows some or all of the stored records, depending on the filtering and display settings (see Call Detail Record log controls). Click on a column heading to sort by that field. Refer to the table below to understand the fields displayed in the CDR log list:

Field	Field description	Usage tips
# (record number)	The unique index number for this Call Detail Record.	
Time	The time at which the Call Detail Record was created.	Records are created as different connection events occur. The time the record was created is the time that the event occurred.
Connections	The number of the connection to which this record applies	Each new connection is created with a unique numeric index. All records pertaining to a particular connection display the same connection number. This can make auditing connection events much simpler.
Message	The type of the Call Detail Record, and brief details, if available.	The display settings allow you to display more extensive details for different record types. The *filter string* allows you to select for display only records where a particular word or string occurs.

Further information about CDR time field

The CDR log time stamp is stored in UTC time and not local time like the Event log, but converted to local time when displayed in the CDR log.

Changing the time and NTP's UTC Offset (on the **Settings** > **Time** page) will affect the CDR log time in the following ways:

- Changing the time, either changing the system time or via an NTP update will cause new CDR logs to show the new time but no change will be made to existing logged CDR events
- With NTP enabled, setting a UTC offset will change the displayed time for all the CDR events; the stored time will remain the same because it is stored in UTC and the offset is applied for display purposes
- Enabling or disabling NTP when an offset is configured will cause the display time to change for all existing events and the UTC time will change for logging future CDR events. This is because, when NTP is disabled, the current time is treated as UTC with an offset of 0

Customizing the user interface

In this section:

Note: the user interface (that is the text you see on the web interface of the Cisco TelePresence ISDN Gateway) can be localized by Cisco or by your reseller. This type of customization is the localization of the text on the web interface and these online help pages. That is, the text has been translated into your local language. In the case where you have a localized ISDN Gateway, the *Use localization package* check box will be checked. For more information refer to Customization: more information.

Some localization packages are available on the company FTP site.

The ISDN Gateway allows you to type using any character set when entering text into the web interface. For example, when naming endpoints or users, you can use any character set you require.

Configuring user interface settings

Controlling the auto-refreshing of status pages on the ISDN Gateway

Some pages on the ISDN Gateway auto-refresh to ensure that the information displayed is current. Auto-refreshing pages keep web sessions alive indefinitely meaning that an administrator login will never timeout. This may be considered to be a security weakness, and if necessary you can disable all auto-refreshing.

To control the auto-refreshing of status pages on the ISDN Gateway:

1. Go to **Settings > User interface**.
2. Choose the time interval for page auto-refreshes or, to stop pages from auto-refreshing, choose *No auto-refresh*.

   The status pages affected by this control are as follows:

   - **Status > General**
   - **Status > ISDN**
   - **Status > Health**
   - **ISDN > ISDN calls**
   - **ISDN > ISDN ports**
   - **ISDN > ISDN calls > Call details**
3. Click **Apply changes**.

Configuring welcome messages for the Login and Home pages

You can configure a message banner to appear on the Login page of the ISDN Gateway. For example, some organizations might require some legal text on the login page of the ISDN Gateway. You can also configure a message banner to appear on the Home page. You can configure a separate title (maximum: 100 characters) and text (maximum: 1500 characters) for each banner. To configure the message banners:

1. Go to **Settings > User interface**.
2. In the **Welcome messages** section, enter the text you require for the titles and the text of the messages.

Customizing voice prompts on the ISDN Gateway

By default the ISDN Gateway includes English voice prompts spoken by an American woman. These prompts are used by the ISDN Gateway to provide callers with information, for example: "Thank you. I'll connect you now".

You may want to replace these prompts with your own in order to change the wording, language or accent used. Alternative prompts may be uploaded individually using the web interface. Alternatively, a collection of voice prompts may be uploaded in one go by means of a *resource package* (see Uploading a customization package.)

Some customization packages are available on the company FTP site.

The customization of voice prompts is controlled via the web interface. Go to **Settings > User interface**. Refer to the sections below for details of the options available and for a description of the information displayed:

- Using default English voice prompts
- Uploading a customization package
- Viewing the available voice prompts
- Uploading and downloading customized voice prompts
- Voice prompt specification
- Making the best possible recordings

Using default English voice prompts

The default set of voice prompts is provided in US English and is the standard set of voice prompts supplied with the ISDN Gateway. These are spoken by a female voice in Americanized English.

If your ISDN Gateway is using customized voice prompts and you want to return to using the default set of voice prompts:

1. Go to **Settings > User interface**.
2. In the **Select customization section**, clear **Use customized voice prompts**.
3. If your ISDN Gateway was provided to you as a localized unit, clear **Use localization package**.
4. Click **Apply changes**.

The default voice prompts will be applied immediately, although it may take a few seconds before everyone connected to the ISDN Gateway is able to hear the new prompts.

Uploading a customization package

It is possible to upload a collection of alternative voice prompts to the ISDN Gateway with a single upload operation, using a *customization package*. Such a package may have been supplied to you by Cisco or one of its representatives, or you may have created the package yourself (see Downloading a customization package).

To upload a package:

1. Go to **Settings > User interface**.
2. In the **Upload customization package** section, click **Browse** and locate the *.package* file on your computer.
3. Click **Upload package**.

The upload may take several seconds, depending on the size of the package file and the speed of your network connection. When the upload is complete, a status screen will be shown, displaying some or all of the individual voice prompt customizations included in the package if the upload was a success, or an error message if the upload failed for some reason.

To apply the uploaded customization package:

- In the **Select customization** section, select Use customized voice prompts.

Note: If you were already using uploaded alternative voice prompts on the ISDN Gateway, then these will be immediately replaced by those in the customization package. If a particular customized file is not included in the package, then any existing customization is unchanged. This allows customization sets to be built up using several different packages if required.

Viewing the available voice prompts

You can review the voice prompt customizations available in the table headed **Voice prompts**. The **Voice prompts** list displays all voice prompt customizations, providing details for those which have alternatives uploaded. Because these lists can be quite long, by default they are hidden. Instead, the number of customizations (files) available is shown. If any have been modified (meaning an alternative customization has been uploaded, either individually, or as part of a package), then this is indicated by an asterisk after the table name.

To expand any list to show all customizations, click **show file details**; to hide it again, click **hide file details**.

In the expanded state, the table shows, for each customization, a description of the file, the standard ISDN Gateway filename for the customization, and the length and date modified (uploaded) of alternative customizations present. Extra information is provided by the following symbols:

- Customizations where an alternative is available that can be individually uploaded or downloaded are indicated by two asterisks (**) after their name
- Customizations where an alternative is available that cannot be uploaded or downloaded individually are indicated by one asterisk (*) (these are files that have been provided by Customer support)

Customizations that are part of a localization package from Cisco or your reseller are indicated by a plus sign (+)

Uploading and downloading customized voice prompts

Refer to the sections below for details of further functionality provided by the **Installed voice prompts** list:

- Uploading individual voice prompts
- Downloading individual voice prompts
- Downloading a customization package
- Deleting customized voice prompts

Uploading individual voice prompts

You may upload individual voice prompts. To do this:

1. Go to **Settings > User interface**.
2. In the **Installed voice prompts** section, click **show files details** and locate the voice prompt file you require.
3. For that voice prompt, click **upload**. You may do this regardless of whether an alternative customization has already been uploaded.
4. You will be presented with a new screen, allowing you to locate and upload the customization of your choice. Click **Browse** to locate the voice prompt file on your computer. Voice prompt files must be in the following format:
    - Microsoft WAVE (.WAV) format
    - 16kHz (16000Hz) sample rate
    - Mono
    - Uncompressed
    - Maximum 10 seconds long

    If you upload a file that is not in this format, the upload may fail or the voice prompt may sound distorted when heard by users. Use an audio editing package of your choice to make any conversions required. See Making the best possible recordings for how to obtain the best possible voice prompts for your ISDN Gateway customization.

    Note that in addition to the 10 second length limit per prompt, there is a total length limit of four minutes for the full set of prompts. That is, if all samples were played back-to-back, it should take no more than 240 seconds.
5. When you have located the file you want to upload, click **Upload customization**. If the upload is successful, a page displaying the size of the file uploaded will be displayed; otherwise an error will be shown. If the upload fails, check your audio file matches the specification above before contacting your support representative.
6. To activate the new voice prompt, select Use customized voice prompts.

Downloading individual voice prompts

You may wish to review a customization that has been previously uploaded to the ISDN Gateway. To do this,

1. Go to **Settings > User interface**.
2. In the **Installed voice prompts** section, locate the voice prompt file you require.
3. For that voice prompt, right-click **download** and choose **Save Target As** (or your web browser's equivalent operation). The file will be downloaded to your computer for reference.

Only alternative customizations can be downloaded in this way; the default voice prompts may not be downloaded. In addition, only customizations uploaded as individual files may be downloaded; those uploaded as part of a package may not be downloaded.

Downloading a customization package

Once you are satisfied with your customizations, you may wish to apply the entire set to another ISDN Gateway. Rather than individually uploading the alternative voice prompts to each one, you may create a *customization package*.

To create a customization package containing all of the alternative voice prompts previously uploaded:

1. Go to **Settings > User interface**.
2. Click **Download package** at the bottom of the **Installed voice prompts** list. The customization package will be downloaded to your computer.

A package may only contain resources uploaded as separate files; those uploaded as part of another package may not be included. The package download option may be unavailable if no voice prompts qualify for inclusion.

Deleting customized voice prompts

If you are dissatisfied with a voice prompt that you have uploaded to the ISDN Gateway, you may delete it in the following manner:

1. Locate the voice prompt of interest in the list.
2. Click the check box to the left of the voice prompt.
3. Click **Delete selected** to remove the voice prompt.

Only alternative voice prompts may be deleted in this way; the default voice prompts cannot be deleted. If you delete an alternative customization, it will immediately revert to the default prompt, even if you have selected *Use customized voice prompts* at the top of the page.

You may want to delete all customizations. To do this, click **Delete all**. Remember that you may revert to the default set of voice prompts without needing to delete any alternative customizations (see Using default English voice prompts).

Voice prompt specification

Below is a complete list of the voice prompts that may be customized. The default wording is shown for each prompt. You do not have to use exactly the same wordings if they are not appropriate for your needs, and are provided only as a guide.

Filename	Default wording
voice_prompt_connecting	Thank you. I'll connect you now
voice_prompt_enter_number	Please enter the number you wish to dial followed by the hash key
voice_prompt_welcome_isdn_gw	Hello

Making the best possible recordings

There are many factors to consider when recording alternative voice prompts in order to get the best results. Below is a summary of the points to bear in mind.

Recording format

It is best to make each recording with the ideal settings and hence avoid any sample-rate or resolution changes. As discussed, the ideal format is Microsoft Wave (.WAV) format, uncompressed, mono, at 16 kHz and 16-bit resolution.

If you are unable to make mono recordings, the ISDN Gateway can convert stereo recordings.

Background noise

It is important to minimize background noise (hiss) as much as possible. This includes ambient noises such as road noise and slamming doors etc. but also try to keep fan noise and similar to a minimum.

When played back by the ISDN Gateway, samples with background noise are very apparent.

Consistency

If possible, record all voice prompts in one session. This will ensure that all voice and background conditions remain constant and the recorded voice will sound similar from prompt to prompt.

Volume

Record prompts using a relatively constant loudness of voice. Although it may take some trial and error, the best recordings will result from speaking loud enough that the voice is recorded loudly compared to any residual background noise, but not so loudly that it sounds distorted when played back.

Customization: More information

There are three customization levels on the Cisco TelePresence ISDN Gateway (for voice-prompts, web interface, help pages, and text messages):

- the factory default files that are provided in UK English
- localization files that are sometimes installed by a reseller
- customized voice prompts files that can be uploaded and downloaded by you

Precedence

For every customizable file:

1. If there is a customization file present, that file will be used.
2. Otherwise, if **Use localization package** is checked, the ISDN Gateway will use the localized file.
3. If 1 and 2 are not true, then the ISDN Gateway will use the default UK English file.

The factory default file set

The files that compose the default file set for the web interface, the voice prompts, the text prompts, the help pages, and text messages cannot be deleted. If you are using your own customization files or a localized ISDN Gateway, you can return the ISDN Gateway to using the default file set:

To return to the defaults:

1. Go to **Settings > User interface**.
2. Ensure **Use localization package** is unchecked.
3. Delete any customized voice prompts.
4. If there is a customized text prompt file, delete it.

Localization files

In some parts of the world, ISDN Gateways are available where the help pages, the voice prompts, the text messages, and some of the web interface are in the local language. In this case, Cisco or the reseller has uploaded a package that provides localized files to replace files in the default file set. If you have a localized ISDN Gateway, you are able to select to return to the default US English file set (see above). Localization is a global change and affects all customizable files. If you have a localized ISDN Gateway, you cannot upload and download localized files on a file by file basis.

Some customization packages are available on the company FTP site.

Customization files

Customization files for voice prompts can be recorded and uploaded by any admin user of the ISDN Gateway. These files can be uploaded one by one or as a package. You can create your own package by uploading all the files you require to an ISDN Gateway and then downloading them as a package. For more information, refer to Customizing the user interface. A customization package does not have to include a complete set of files. Where a file name duplicates an existing uploaded voice prompt file, that file will be overwritten.

Backing up and restoring the configuration using FTP

You can back up and restore the configuration of the Cisco TelePresence ISDN Gateway through its web interface. To do so, go to **Settings > Upgrade**. For more information, refer to Upgrading and backing up the ISDN Gateway.

You can also save the configuration of the ISDN Gateway using FTP.

To back up the configuration via FTP:

1. Ensure that FTP is enabled on the **Network > Services** page.
2. Connect to the ISDN Gateway using an FTP client. When asked for a user name and password, enter the same ones that you use to log in to the ISDN Gateway's web interface as an administrator.
3. You will see a file called configuration.xml. This contains the complete configuration of your ISDN Gateway.
4. Copy this file and store it somewhere safe.

The backup process is now complete.

To restore the configuration using FTP:

1. Locate the copy of the configuration.xml file that you want to restore.
2. Ensure that FTP is enabled on the **Network > Services** page.
3. Connect to the ISDN Gateway using an FTP client. When asked for a user name and password, use the same ones that use to log in to the ISDN Gateway's web interface as an administrator.
4. Upload your configuration.xml file to the unit, overwriting the existing file on the unit.
5. If the restored configuration file contained changes to the ISDN port settings, you need to restart the ISDN Gateway. Go to **Settings > Shutdown**.

The restore process is now complete.

Note: that the same process can be used to transfer a configuration from one ISDN Gateway to another of the same model number. However, before doing this, be sure to keep a copy of the original feature keys from the ISDN Gateway whose configuration is being replaced.

If you are using the configuration file to configure a duplicate ISDN Gateway, for example in a network where you have more than one, be aware that if the original ISDN Gateway was configured with a static address, you will need to reconfigure the IP address on any others on which you have used the configuration file.

Configuring SSL certificates

If the Cisco TelePresence ISDN Gateway has the *Secure management (HTTPS)* or *Encryption* feature key installed, and you enable *Secure web* on the **Network > Services** page, you will be able to access the web interface of the ISDN Gateway using HTTPS. The ISDN Gateway has a local certificate and private key pre-installed and this will be used by default when you access the unit using HTTPS. However, we recommend that you upload your own certificate and private key to ensure security as all ISDN Gateways have identical default certificates and keys.

To upload your own certificate and key, go to **Network > SSL certificates**. Complete the fields using the table below for help and click **Upload certificate and key**. Note that you must upload a certificate and key simultaneously. After uploading a new certificate and key, you must restart the ISDN Gateway.

If you have uploaded your own certificate and key, you can remove it later if necessary; to do this, click **Delete custom certificate and key**.

The table below details the fields you see on the **Network > SSL certificates** page.

Field	Field description	Usage tips
Local certificate		
Subject	The details of the business to which the certificate has been issued: ▶ **C**: the country where the business is registered ▶ **ST**: the state or province where the business is located ▶ **L**: the locality or city where the business is located ▶ **O**: the legal name of the business ▶ **OU**: the organizational unit or department ▶ **CN**: the common name for the certificate, or the domain name	
Issuer	The details of the issuer of the certificate.	Where the certificate has been self-issued, these details will be the same as for the *Subject*.
Issued	The date on which the certificate was issued.	
Expires	The date on which the certificate will expire.	
Private key	Whether the private key matches the certificate.	Your web browser uses the SSL certificate's public key to encrypt the data that it sends back to the ISDN Gateway. The private key is used by the ISDN Gateway to decrypt that data. If the *Private key*

		field shows 'Key matches certificate' then the data is securely encrypted in both directions.
Local certificate configuration		
Certificate	If your organization has bought a certificate, or you have your own way of generating certificates, you can upload it. Browse to find the certificate file.	
Private key	Browse to find the private key file that accompanies your certificate.	
Private key encryption password	If your private key is stored in an encrypted format, you must enter the password here so that you can upload the key to the ISDN Gateway.	
Trust store	You can upload a 'trust store' of certificates that the ISDN Gateway will use to verify the identity of the other end of a TLS connection. If you have a trust store certificate on the ISDN Gateway, you can delete it; to do so, click **Delete trust store**. The trust store must be in '.pem' format.	Note that uploading a new trust store replaces the existing store.
Certificate verification settings	Choose to what extent the ISDN Gateway will verify the identity of the far end for a connection: ▸ *No verification*: all outgoing connections are permitted to proceed, even if the far end does not present a valid and trusted certificate. ▸ *Outgoing connections only*: outgoing connections are only permitted if the far end has a certificate which is trusted. ▸ *Outgoing connections and incoming calls*: outgoing connections and incoming connections for SIP calls using TLS must have a certificate which is trusted otherwise the ISDN Gateway will not allow the connection to proceed.	The trust store contains 'master' certificates that can be used to verify the identity of a certificate presented by the far end. Outgoing connections are connections such as SIP calls which use TLS.

Contact details and license information

Refer to the following sections for notices and software license information:

TANDBERG

TANDBERG is now part of Cisco. TANDBERG Products UK Limited is a wholly owned subsidiary of Cisco Systems, Inc.

Software licenses

The Cisco TelePresence ISDN Gateway includes software developed by the NetBSD Foundation, Inc. and its contributors (specifically the NetBSD operating system), hardware and software developed by N.A.T. GmbH, software developed by Spirit Corporation (specifically G.728 audio codec implementation), software developed by Tecgraf, PUC-Rio (specifically Lua), and software developed by the Internet Systems Consortium, Inc (specifically DHCP). The following copyright notices are reproduced here in order to comply with the terms of the respective licenses.

This product can use HMAC-SHA1 to authenticate packets and AES to encrypt them.

The following copyright notices are reproduced here in order to comply with the terms of the respective licenses.

AVC VIDEO

THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD (“AVC VIDEO”) AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Accordingly, please be advised that service providers, content providers, and broadcasters are required to obtain a separate use license from MPEG LA prior to any use of AVC/H.264 encoders and/or decoders.

RSA Data Security Inc.

License to copy and use this software is granted provided that it is identified as the "RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing this software or this function.

License is also granted to make and use derivative works provided that such works are identified as "derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing the derived work.

RSA Data Security, Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided "as is" without express or implied warranty of any kind.

These notices must be retained in any copies of any part of this documentation and/or software.

The Internet Society

Uses material from IETF RFC 2617.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

NetBSD

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement: *This product includes software developed by the NetBSD Foundation, Inc. and its contributors.*
4. Neither the name of The NetBSD Foundation nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE NETBSD FOUNDATION, INC. AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE FOUNDATION OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The Cisco TelePresence ISDN Gateway includes software developed by the authors listed below. These notices are required to satisfy the license terms of the software mentioned in this document. All product names mentioned herein are trademarks of their respective owners.

- The University of California, Berkeley and its contributors.
- The University of California, Lawrence Berkeley Laboratory and its contributors.
- The NetBSD Foundation, Inc. and its contributors.
- Jonathan R. Stone, Manuel Bouyer, Charles M. Hannum, Christopher G. Demetriou, TooLs GmbH, Terrence R. Lambert, Theo de Raadt, Christos Zoulas, Paul Kranenburg, Adam Glass, Winning Strategies, Inc, Frank van der Linden, Jason R. Thorpe, Chris Provenzano.

Info-ZIP

Copyright © 1990-2007 Info-ZIP. All rights reserved.

For the purposes of this copyright and license, "Info-ZIP" is defined as the following set of individuals:

Mark Adler, John Bush, Karl Davis, Harald Denker, Jean-Michel Dubois, Jean-loup Gailly, Hunter Goatley, Ed Gordon, Ian Gorman, Chris Herborth, Dirk Haase, Greg Hartwig, Robert Heath, Jonathan Hudson, Paul Kienitz, David Kirschbaum, Johnny Lee, Onno van der Linden, Igor Mandrichenko, Steve P. Miller, Sergio Monesi, Keith Owens, George Petrov, Greg Roelofs, Kai Uwe Rommel, Steve Salisbury, Dave Smith, Steven M. Schweda, Christian Spieler, Cosmin Truta, Antoine Verheijen, Paul von Behren, Rich Wales, Mike White.

This software is provided "as is," without warranty of any kind, express or implied. In no event shall Info-ZIP or its contributors be held liable for any direct, indirect, incidental, special or consequential damages arising out of the use of or inability to use this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the above disclaimer and the following restrictions:

1. Redistributions of source code (in whole or in part) must retain the above copyright notice, definition, disclaimer, and this list of conditions.
2. Redistributions in binary form (compiled executables and libraries) must reproduce the above copyright notice, definition, disclaimer, and this list of conditions in documentation and/or other materials provided with the distribution. The sole exception to this condition is redistribution of a standard UnZipSFX binary (including SFXWiz) as part of a self-extracting archive; that is permitted without inclusion of this license, as long as the normal SFX banner has not been removed from the binary or disabled.
3. Altered versions--including, but not limited to, ports to new operating systems, existing ports with new graphical interfaces, versions with modified or added functionality, and dynamic, shared, or static library versions not from Info-ZIP--must be plainly marked as such and must not be misrepresented as being the original source or, if binaries, compiled from the original source. Such altered versions also must not be misrepresented as being Info-ZIP releases--including, but not limited to, labeling of the altered versions with the names "Info-ZIP" (or any variation thereof, including, but not limited to, different capitalizations), "Pocket UnZip," "WiZ" or "MacZip" without the explicit permission of Info-ZIP. Such altered versions are further prohibited from misrepresentative use of the Zip-Bugs or Info-ZIP e-mail addresses or the Info-ZIP URL(s), such as to imply Info-ZIP will provide support for the altered versions.
4. Info-ZIP retains the right to use the names "Info-ZIP," "Zip," "UnZip," "UnZipSFX," "WiZ," "Pocket UnZip," "Pocket Zip," and "MacZip" for its own source and binary releases.

Independent JPEG Group's JPEG software

Software is based in part on the work of the Independent JPEG Group

The authors make NO WARRANTY or representation, either express or implied, with respect to this software, its quality, accuracy, merchantability, or fitness for a particular purpose. This software is provided "AS IS", and you, its user, assume the entire risk as to its quality and accuracy.

This software is copyright © 1991-1998, Thomas G. Lane. All Rights Reserved except as specified below.

Permission is hereby granted to use, copy, modify, and distribute this software (or portions thereof) for any purpose, without fee, subject to these conditions:

1. If any part of the source code for this software is distributed, then this README file must be included, with this copyright and no-warranty notice unaltered; and any additions, deletions, or changes to the original files must be clearly indicated in accompanying documentation.
2. If only executable code is distributed, then the accompanying documentation must state that "this software is based in part on the work of the Independent JPEG Group".
3. Permission for use of this software is granted only if the user accepts full responsibility for any undesirable consequences; the authors accept NO LIABILITY for damages of any kind.

These conditions apply to any software derived from or based on the IJG code, not just to the unmodified library. If you use our work, you ought to acknowledge us.

Permission is NOT granted for the use of any IJG author's name or company name in advertising or publicity relating to this software or products derived from it. This software may be referred to only as "the Independent JPEG Group's software".

We specifically permit and encourage the use of this software as the basis of commercial products, provided that all warranty or liability claims are assumed by the product vendor.

The OpenSSL Project

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

==========

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com) All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscape's SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)" The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related :-).
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

N.A.T. GmbH

Copyright © 1990-2005 by N.A.T. GmbH

All rights reserved. Copying, compilation, modification, distribution or any other use whatsoever of this material is strictly prohibited except in accordance with a Software License Agreement with N.A.T. GmbH.

The Cisco TelePresence ISDN Gateway includes hardware and software developed by and used under license from N.A.T. GmbH.

Spirit Corporation

Copyright © 1995-2003, SPIRIT

The Cisco TelePresence ISDN Gateway includes a G.728 audio codec used under license from Spirit Corporation.

AES License

Copyright (c) 2001, Dr Brian Gladman, Worcester, UK.

All rights reserved.

LICENSE TERMS

The free distribution and use of this software in both source and binary form is allowed (with or without changes) provided that:

1. distributions of this source code include the above copyright notice, this list of conditions and the following disclaimer;
2. distributions in binary form include the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other associated materials;
3. the copyright holder's name is not used to endorse products built using this software without specific written permission.

DISCLAIMER

This software is provided 'as is' with no explicit or implied warranties in respect of its properties, including, but not limited to, correctness and fitness for purpose.

Issue Date: 29/07/2002

HMAC License

Copyright (c) 2002, Dr Brian Gladman, Worcester, UK. All rights reserved.

LICENSE TERMS

The free distribution and use of this software in both source and binary form is allowed (with or without changes) provided that:

1. distributions of this source code include the above copyright notice, this list of conditions and the following disclaimer;
2. distributions in binary form include the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other associated materials;
3. the copyright holder's name is not used to endorse products built using this software without specific written permission.

ALTERNATIVELY, provided that this notice is retained in full, this product may be distributed under the terms of the GNU General Public License (GPL), in which case the provisions of the GPL apply INSTEAD OF those given above.

DISCLAIMER

This software is provided 'as is' with no explicit or implied warranties in respect of its properties, including, but not limited to, correctness and/or fitness for purpose.

Issue Date: 26/08/2003

SHA1 License

Copyright (c) 2002, Dr Brian Gladman, Worcester, UK. All rights reserved.

LICENSE TERMS

The free distribution and use of this software in both source and binary form is allowed (with or without changes) provided that:

1. distributions of this source code include the above copyright notice, this list of conditions and the following disclaimer;
2. distributions in binary form include the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other associated materials;
3. the copyright holder's name is not used to endorse products built using this software without specific written permission.

ALTERNATIVELY, provided that this notice is retained in full, this product may be distributed under the terms of the GNU General Public License (GPL), in which case the provisions of the GPL apply INSTEAD OF those given above.

DISCLAIMER

This software is provided 'as is' with no explicit or implied warranties in respect of its properties, including, but not limited to, correctness and/or fitness for purpose.

Issue Date: 01/08/2005

Lua

Lua 5.0 license

Copyright © 2003-2004 Tecgraf, PUC-Rio.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

1. The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Telenetworks

Regents of the University of California

Redistribution and use in source and binary forms are permitted provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that the software was developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission. THIS SOFTWARE IS PROVIDED ``AS IS'' AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTIBILITY AND FITNESS FOR A PARTICULAR PURPOSE.

DHCP

Permission to use, copy, modify, and/or distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ISC DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Net-SNMP

Various copyrights apply to this package, listed in various separate parts below. Please make sure that you read all the parts.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* The name of Cambridge Broadband Ltd. may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 4: Sun Microsystems, Inc. copyright notice (BSD) -----

Copyright © 2003 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A. All rights reserved.

Use is subject to license terms below.

This distribution may include materials developed by third parties.

Sun, Sun Microsystems, the Sun logo and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of the Sun Microsystems, Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 5: Sparta, Inc copyright notice (BSD) -----

Copyright (c) 2003-2009, Sparta, Inc
All rights reserved.

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

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

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

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

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

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

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